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

AS-AATIC-135-2022
11 de julio de 2022

Doctor
Roberto Cervantes Barrantes, gerente
GERENCIA GENERAL-1100

Doctor
Randall Álvarez Juárez, gerente
GERENCIA MÉDICA-2901

Licenciado
Gustavo Picado Chacón, gerente
GERENCIA FINANCIERA-1103

Licenciado
Luis Fernando Campos, gerente
GERENCIA ADMINISTRATIVA-1104

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

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

Licenciado
Jaime Barrantes Espinoza, gerente
GERENCIA DE PENSIONES-9108

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

Estimados(a) señores(a):

ASUNTO:	**Oficio de Asesoría sobre el impacto en la prestación de servicios y medidas de contingencia, producto del ataque cibernético en la plataforma tecnológica institucional.**

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 los resultados de visita efectuada a 58 unidades institucionales (áreas de salud, hospitales y sucursales), sobre el impacto en la prestación de servicios y medidas de contingencia, 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. Lo anterior, con el propósito de efectuar un diagnóstico situacional y posibles medidas que se podrían adoptar en esta temática.

Al respecto, los resultados obtenidos son los siguientes:

I. ANTECEDENTES

En declaraciones efectuadas el 17 de mayo de 2022, a medios de comunicación nacional e internacional, el presidente de Costa Rica, Rodrigo Alberto Chaves Robles, afirmó que el país se encontraba en "guerra" contra los "terroristas cibernéticos" del grupo Conti, que el pasado 17 de abril comenzaron una serie de ataques de los que el país aún sufre las consecuencias, *"Estamos en guerra y esa no es una exageración. Costa Rica está sufriendo un ataque terrorista cibernético y por eso hemos decretado estado de emergencia nacional para enfrentar esa amenaza"*, declaró Chaves al anunciar una serie de acciones.

Las entidades públicas - Ministerio de Hacienda, Ministerio de Ciencia Tecnología y Telecomunicaciones (MICITT) y la Caja Costarricense de Seguro Social- han sido blanco de múltiples ataques tipo ransomware, que impide a los usuarios e instituciones acceder a sus sistemas o archivos y que exige el pago de un rescate para poder disponer nuevamente de ellos, situación que llevó al país a publicar una declaratoria de emergencia nacional en todo el sector público (mediante Decreto No. 43542-MP-MICITT) e institucional (mediante oficio GA-CAED-0260-2022 del 02 de junio de 2022).

En este contexto, 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

En relación con lo anterior, esta auditoria les consultó a 58 unidades institucionales (áreas de salud, hospitales y sucursales), sobre el impacto en la prestación de servicios a causa del ataque cibernético en la plataforma tecnológica institucional, así como, las medidas de contingencia aplicadas para atender la emergencia suscitada, a partir del 31 de mayo del 2022.

Las unidades visitadas y consultadas fueron, las siguientes:

1. Área de Salud Goicoechea 1 y 2.
2. Hospital de Upala.
3. Área de Salud Heredia Cubujuquí.
4. Hospital Calderón Guardia.
5. Área de Salud Santa Bárbara.
6. Hospital de Guápiles.
7. Área de Salud Turrialba.
8. Hospital de la Anexión.
9. Área Salud Acosta.
10. Hospital de los Chiles.
11. Área Salud Alajuela Norte.
12. HOMACE.
13. Área Salud Alajuelita.
14. Hospital Escalante Pradilla.
15. Área Salud Coronado.
16. Hospital Max Peralta.
17. Área Salud de Aserrí.
18. Hospital México.
19. Área Salud El Guarco.
20. Hospital Monseñor Sanabria.
21. Área Salud Guápiles.
22. Hospital San Juan de Dios.
23. Área Salud Liberia.
24. Hospital San Rafael de Alajuela.
25. Área Salud Limón.
26. Hospital San Vicente de Paúl.
27. Área Salud Moravia.
28. Hospital Tony Facio.
29. Área Salud Nicoya.
30. Hospital William Allen.
31. Área Salud Oreamuno.
32. Sucursal de Alajuela.
33. Área Salud Paraíso.
34. Sucursal de Cartago.
35. Área Salud Pérez Zeledón.
36. Sucursal de Desamparados.
37. Área Salud Río Frío.
38. Sucursal de Esparza.
39. Área Salud Santo Domingo.
40. Sucursal de Guadalupe.
41. Área Salud Siquirres.
42. Sucursal de Guápiles.

43. Área Salud Tres Ríos.
45. Clínica Carlos Durán.
47. Clínica Central.
49. Clínica Clorito Picado.
51. Clínica Moreno Cañas.
53. Clínica San Rafael de Puntarenas.
55. Clínica Solón Núñez.
57. COOPESAIN.
44. Sucursal de Heredia.
46. Sucursal de Limón.
48. Sucursal de los Chiles.
50. Sucursal de Nicoya.
52. Sucursal de Pérez Zeledón.
54. Sucursal de Puntarenas.
56. Sucursal de Turrialba.
58. Sucursal de Upala.

A continuación, se mencionan algunos de los resultados de mayor relevancia para la atención de los usuarios y la continuidad de los servicios en la institución:

a) Respecto a la comunicación oficial (por parte de las autoridades institucionales del nivel central, regional y local) de las causas e impacto del evento provocado por el ataque cibernético a la plataforma tecnológica institucional, se estableció que, 48 (83 %) de las unidades indicaron "Sí" haber recibido información y 10 (17 %) de ellas respondieron que "No"; además, como medios de comunicación se indicaron los grupos o chats por WhatsApp y Telegram, charlas por Facebook Live y Microsoft Teams, noticieros (por radio y televisión) y correos electrónicos.

Por otra parte, según lo indicado por las unidades, al utilizarse distintas fuentes y medios para difundir la información, se emitían diversas opiniones de los funcionarios incluidos en los chats, generando desorden y confusión, al no tener certeza (en algunos de los casos) si la información provenía de fuentes oficiales o autoridades institucionales correspondientes.

b) Sobre la definición de protocolos institucionales de contingencia ante la ausencia de sistemas de información, 40 (69 %) de las unidades indicaron "Sí" tener conocimiento sobre la existencia de éstos y 18 (31 %) mencionaron que "No". Asimismo, los funcionarios consultados mencionan que, los protocolos o planes de contingencia que se tenían no contemplaban situaciones como la acontecida con el ciberataque.

En el cuadro 1, se mencionan algunas de las respuestas efectuadas por las unidades:

Cuadro 1
Definición de protocolos institucionales de contingencia
ante la ausencia de sistemas de información
periodo de consulta del 6 al 15 de junio de 2022

Nombre de la unidad consultada	¿Tiene conocimiento sobre definición de protocolos institucionales de contingencia ante la ausencia de sistemas de información?
Área de salud de Guápiles	Sí. Antes estaba el plan de contingencia cuando fallaba el EDUS, pero por caída general de los sistemas no conocía la existencia de protocolos.
Área de Salud Alajuela Norte	Si. Si, el plan de contingencia de la Dirección de Tecnologías de Información, pero este plan no contiene nada al respecto de una situación como el hackeo que nos está afectando.
Área de Salud Dr. Solón Núñez Frutos	No. nosotros tenemos planes de contingencia a nivel local que está en constante revisión año a año.
Sucursal Los Chiles	No. Se ha mantenido talonario y/o formularios físicos de pensiones, trabajadores independientes, voluntarios; se resguarda la información para cuando haya sistema incluirlos. Respecto a las incapacidades, por la afectación al sistema no se han podido cancelar.
Área de Salud Zapote - Catedral	Si. De contingencia se indicó es el uso de papel. Instrucción de uso alterno del plan de continuidad.
Sucursal de Puntarenas	Sí. Conforme se presenta la situación del ataque, la institución nos va dando a conocer los protocolos a seguir, para la continuidad de los servicios.

Área de Salud de Liberia	No. Ni en salud en la parte de EDUS, ni en la parte Administrativa.
Hospital San Rafael de Alajuela	Si. El único que se conoce es el que hizo con respecto al EDAC (Expediente Digital en Ambiente Contingencia) que es el que debería funcionar al traerse los equipos, desconocemos porque no ha funcionado, no ha sido lo suficientemente robusto. El EDAC no sincroniza en tiempo real sino cada 3 horas, no es inmediato, no resuelve necesidades de Laboratorios, Farmacia, biopsias. El EDAC no levanta consulta externa.
Hospital de Guápiles	No conozco un protocolo institucional con la ausencia de todos los sistemas de información. Pero sí ya estábamos acostumbrados a trabajar de forma manual, previo al EDUS.
Área de Salud Acosta	No se tiene conocimiento de protocolos, únicamente las circulares que se han emitido para esta situación del ciberataque en concreto, y la atención de las diferentes inquietudes que se han ido evacuando.
Hospital México	Si. se han remitido protocolos, por parte del nivel superior. Sin embargo, el hospital ya contaba con planes de contingencia, el cual fueron implementados para garantizar la prestación de los servicios de salud. Además, se solicitó a los diferentes servicios del hospital un plan alterno de trabajo.
Sucursal Cartago	No contamos con un protocolo de contingencia a nivel local, no está definido Institucionalmente para cuando falla absolutamente todo, como por ejemplo un ciber ataque.

Fuente: Elaboración propia de auditoría, información suministrada por unidades institucionales en consulta efectuada del 6 al 15 de junio de 2022.

c) La totalidad de las unidades consultadas indicaron haber sido instruidos respecto al apagado y desconexión los equipos de cómputo, lo anterior, mediante grupos o chats de WhatsApp, aproximadamente entre las 03:00 a.m. y 07:00 a.m. del 31 de mayo de 2022.

d) Referente a la definición de protocolos de comunicación a los usuarios sobre el impacto y medidas de contingencia establecidas en torno al ciberataque, indicaron lo siguiente:

- Se habilitó una línea telefónica donde el usuario puede llamar a solicitar información.
- Se efectuaron comunicados por redes sociales Facebook e Instagram.
- Traslado de información a grupos comunitarios, Asociaciones de Desarrollo y miembros de Juntas de Salud.
- Comunicados por noticieros (radio y televisión).
- Líneas de atención por WhatsApp.
- Funcionarios brindando información en la entrada de las unidades.
- Comunicados y colaboración de la municipalidad y cooperativas.
- Afiches de información.

Además, indicaron que, al no disponer de un protocolo previamente establecido (a nivel local, regional o central), los centros de salud y sucursales implementaron algunas medidas según sus posibilidades y utilizando los medios disponibles en ese momento.

En relación con lo anterior, uno de los funcionarios consultados, indicó:

> *"Considero es necesario se les diga a las personas desde el ámbito central como se debe afrontar la atención de los usuarios, la comunicación no ha sido la más certera por parte del Nivel central.*
>
> *Sin embargo, directamente al usuario no se le ha comunicado una realidad por parte, de las autoridades del nivel central.*
>
> *Sentimos una restricción de comunicación, ya que, debemos pasar todo por medio de comunicación institucional, previo a la socialización".*

e) Sobre los planes de continuidad de negocio, establecidos a nivel central o regional que permitan la integración de esfuerzos ante eventos de interrupción de servicios; 30 (52 %) de las unidades indicaron "No" tener conocimiento sobre la existencia de éstos y 28 (48 %) mencionaron que "Sí".

Al respecto, es importante señalar que, de las unidades que respondieron de manera afirmativa "Sí", algunas de ellas hacen mención del **Plan de Continuidad de la Gestión TIC** o **medidas de contingencia** comunicadas después del ciberataque, lo cual, denota un posible desconocimiento o confusión respecto al concepto o estructura de un **Plan de Continuidad de Negocio**, según se muestra, a continuación:

> *"Sí. La (…) tiene Planes de Continuidad, pero ninguna Área de Salud dispone de funcionarios de CGI. La Dirección dispone de 3 funcionarios en el CGI, por lo que hay muy poco personal para brindar servicio a todas las unidades adscritas".*
>
> *"(…) Hemos tenido el apoyo del nivel regional y central, la continuidad del negocio se da por defecto en atención de la emergencia, pero establecido formalmente por la Institución no lo conocemos".*
>
> *"Sí, de previo a que se presentase el evento no se tenía conocimiento de estos planes, sino conforme se está en la situación.*
>
> *Hay que aclarar que cada unidad tiene su plan de continuidad, el conocimiento de los planes de otra unidad se da asertivamente en el momento en que sucede el evento".*
>
> *"Si. Si se tiene conocimiento de planes de continuidad y contingencia a nivel central (los cuales se facilitarán). Sobre el particular, es importante aclarar que una situación como la actual no se dimensionaba en esos documentos".*

En aras de una mayor claridad, un **Plan de Contingencia de las TIC** (Tecnologías de la Información y las Comunicaciones) consiste en una estrategia planificada en fases, constituida por un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos de actuación, encaminados a conseguir una restauración ordenada, progresiva y ágil de los **sistemas que soportan la información y los procesos de negocio considerados críticos**.

Por su parte, el **Plan de Continuidad de Negocio** puede ser definido como un conjunto formado por planes de actuación, planes de emergencia, planes financieros, planes de comunicación y planes de contingencias destinados a mitigar el impacto provocado por la concreción de determinados riesgos sobre la información y los procesos de negocio de la organización.

f) La totalidad de las unidades indicaron haber efectuado la instalación del software MicroClaudia en las computadoras de la unidad; sin embargo, dicha instalación se efectuó de forma posterior al ciberataque del 31 de mayo de 2022, según orden emitida por la Dirección de Tecnología de Información y Comunicaciones.

Asimismo, 26 (45 %) de los funcionarios indicaron "No" haber recibido capacitación sobre el uso de este software, 30 (52 %) mencionaron que "Sí" y 2 (3 %) indicaron que dicha pregunta no aplicaba para su unidad "N/a".

g) Sobre la implementación de un procedimiento interno para la actualización de sistemas operativos y antivirus en los equipos TIC (previo al ciberataque suscitado el 31 de mayo del 2022), 48 (83 %) de las unidades respondieron que "Sí" efectuaban la actualización, 6 (10 %) que "No" y 4 (7 %) que no aplicaba dicha pregunta "N/a".

A continuación, se transcribe algunas de las respuestas emitidas:

Cuadro 3
Implementación de procedimiento interno para la actualización de sistemas operativos y antivirus, en unidades institucionales periodo de consulta del 6 al 15 de junio de 2022

Nombre de la unidad consultada	¿De previo a este evento, tenía establecido un procedimiento interno para la actualización de sistemas operativos y antivirus en las computadoras de esta unidad?
Hospital Monseñor Sanabria Martínez	Sí. Aproximadamente de forma bimensual se están revisando las actualizaciones de sistemas operativos y antivirus. Además, a nivel institucional se dispone de una herramienta SCCM, la cual se supone fuerza las actualizaciones en los equipos.
Sucursal de Esparza	Sí. De hecho, estaban actualizados, únicamente la de consulta a usuarios externos estaba desactualizada, ya que se utiliza poco y no la tiene en uso ningún funcionario en específico
Área de salud de Guápiles	No. Dependemos de las actualizaciones automáticas porque no tenemos CGI.
Área de Salud Alajuela Norte	Sí. Con las actualizaciones del nivel central, esto no se hace localmente.
Área de Salud Los Chiles	Sí. Desde el nivel central se envían las actualizaciones.
Sucursal de Upala	N/A. El CGI de la Dirección tiene estos controles.
Área de salud Goicoechea 2	Sí. estábamos en proceso de actualización de Windows server y SQL
Sucursal CCSS Turrialba	Si. Había un cronograma de actualizaciones administrado por nivel central, el cual realizaban remotamente."
Área de Salud Aserrí	Sí. Los únicos equipos que no estaban actualizados del todo son los del Laboratorio por la particularidad de los mismo.
Sucursal de San Ignacio de Acosta	A nivel del CGI de la Gerencia Financiera al final de mes se distribuyen los paquetes más importantes para actualizar los equipos incluido el Windows Defender. El lunes 30 de mayo 2022 ya algunos equipos tenían la vacuna de Micro Claudia.
Hospital San Juan de Dios	Políticas DTIC. SCCM se hace de manera escalonada y en las tardes.
Área de Salud Dr. Ricardo Moreno Cañas	Nosotros tenemos un WSUS que fue brindado por la Institución, el mismo es un servidor de actualizaciones, pero es administrado por la CCSS.
Área de Salud Paraíso-Cervantes	No. Las actualizaciones por política se realizan a nivel central.
Área de Salud Oreamuno-Pacayas-Tierra Blanca	No. Por política se realiza en el nivel central, si no hay directriz no se puede realizar.
Sucursal Cartago	Sí. mensualmente se realizar actualizaciones a nivel general, que comunica previamente el CGI de la Gerencia Financiera.
Hospital Dr. Rafael A. Calderón Guardia	No. porque todo es política de la CAJA, ellos nos informan cuando se dispone de actualizaciones

Fuente: Elaboración propia de auditoría, información suministrada por unidades institucionales en consulta efectuada del 6 al 15 de junio de 2022.

Del cuadro anterior, se establece que, según lo indicado por las unidades consultadas, las actualizaciones de software y antivirus son comunicadas, enviadas o distribuidas por los CGI Gerenciales o autoridades institucionales en TIC (nivel central), algunas de éstas se ejecutan de manera automática mediante herramientas como el SCCM y otras se aplican de forma manual en el nivel local, cuya periodicidad es variable.

h) Respecto a la existencia de un Plan de Continuidad de TIC (aprobado y actualizado), 50 (86 %) de las unidades respondieron que “Sí” disponían de este instrumento de contingencia y 8 (14%) indicaron “No” tenerlo.

Por otra parte, al consultarles sobre la utilidad del plan, para atender la emergencia tecnológica suscitada a nivel institucional, 36 (62 %) de las unidades indicaron su imposibilidad de aplicarlo o utilizarlo en la presente situación, señalando algunas de ellas, lo siguiente:

Cuadro 4
Utilidad del Plan de Continuidad de TIC, para atender la emergencia tecnológica suscitada a nivel institucional periodo de consulta del 6 al 15 de junio de 2022

Nombre de la unidad consultada	¿Le resultó útil el Plan de Continuidad de TIC para atender la emergencia suscitada a partir del 31 de mayo del 2022?
Hospital Monseñor Sanabria Martínez	En parte, justamente porque el documento se elabora en base a las acciones que se debe realizar a lo interno en el hospital, sin embargo, a lo externo se sale de nuestro alcance. Además, que el plan de contingencia que se tenía con EDUS no funcionó.
Área de salud de Guápiles	No abarca situaciones como la ocurrida.
Área de Salud Alajuela Norte	El plan de contingencia no es aplicable para un evento de este tipo.
Área de Salud Los Chiles	No fue funcional, el impacto fue muy grande, por lo general se respalda la información en el servidor, pero estos se vieron afectados.
Área de Salud Dr. Solón Núñez Frutos	No, esto debido al alcance de la emergencia que es a nivel global, nuestro plan es para atender emergencias locales.
Hospital de Los Chiles	Se encuentra desactualizado y no incluyó el tema de continuidad de servicios ante hackeos.
Sucursal Los Chiles	El plan diseñado es para periodos cortos, y el tema del hackeo al afectar los sistemas ha excedido la capacidad de respuesta.
Área de Salud Alajuelita	El plan estaba enfocado principalmente a fallas de conexión, sin embargo, esta emergencia ha tenido incluso la imposibilidad de utilizar los equipos.
Área de Salud Horquetas Río Frío	El plan a lo largo del tiempo funcionó para realizar el reemplazo de los equipos, pero para esta situación no, fue una situación reactiva porque esos planes no están diseñados para prevenir esta emergencia.
Sucursal CCSS Turrialba	En estas situaciones los planes no fueron efectivos pues un evento de esta magnitud no estaba contemplado en los planes locales.
Área de Salud de Turrialba	No por la magnitud de la emergencia si están deshabilitados todos los servidores centrales y no funcionan las aplicaciones.
Área de Salud Aserrí	Estaba en el servidor y el mismo está afectado, no se pudo disponer de él.
Sucursal de Desamparados	El Jefe de Sucursal indica que no fue útil, ya que considera que no es útil para atender esta macro emergencia, solo valioso para extraer datos a nivel local.
Área de Salud Pérez Zeledón	No se tenía contemplada una situación como la actual.
Área de Salud Heredia Cubujuqui	No fue útil ya que todos los respaldos en servidores fueron infectados.
Área de Salud Tibás Uruca Merced	No, los procedimientos alternos de trabajo en caso de falla de los sistemas de información críticos, contiene el uso de equipo de cómputo y por ejemplo en el caso del EDUS, el uso del EDAC, por lo que los mismos no pudieron implementarse, ya que la afectación se dio directamente en el equipo informático.
Área de Salud Oreamuno-Pacayas-Tierra Blanca	No, porque la instrucción fue no encender equipos, motivo por el cual no se pudo activar ese plan de contingencia.
Sucursal Cartago	No, nuestro plan de continuidad aprobado no es para este tipo de eventos.

Fuente: Elaboración propia de auditoría, información suministrada por unidades institucionales en consulta efectuada del 6 al 15 de junio de 2022.

i) Referente a la consulta sobre las áreas o procesos con afectaciones más críticas en la unidad, en el cuadro 5 se indican las respuestas efectuadas por algunas de las unidades consultadas:

Cuadro 5
Áreas o procesos con afectación más crítica
en unidades institucionales
periodo de consulta del 6 al 15 de junio de 2022

Nombre de la unidad consultada	Describa cuales han sido las áreas / procesos con afectaciones más críticas en esta unidad:
Sucursal de Nicoya	Incapacidades por su complejidad siendo la más grave, no reciben salarios, depende muchos de otros sistemas, SICERE, RCPI, SICO, SIGE. Plataforma de servicios. Cajas en la recepción de pagos y por los servicios de pagos de pasajes y otros subsidios. Fondo rotatorio que es el pago de proveedores facturas importantes facturas eléctricas. Pensiones (no se generaron pagos del cual no podemos dar información con certera al respecto). Inspección (la inscripción de trabajadores).
Hospital Monseñor Sanabria Martínez	Laboratorio en primer lugar, al ser táctico para la toma de decisiones, y al habernos quedado sin el LABCORE fue caótico. Visualizador de placas en segundo lugar, no obstante, el impacto no es tan fuerte, porque los funcionarios se trasladaban a la consola de rayos equis a ver las placas, donde se demostró la vocación del personal. Esto obviamente afectó los tiempos de respuesta, pero como medida de contingencia, se debió realizar. Por lo anterior, rayos X impactó en consulta externa principalmente. El tercer servicio que se afectó fuertemente fue Redes, al no poder saber qué va a llegar el día siguiente, complicó la gestión. Y el otro es sala de operaciones, donde debieron suspenderse los casos que tenían valoración preoperatoria, sin embargo, los demás no se suspendieron, sin embargo, se dificultó la gestión, al no tener expedientes para identificar posibles complicaciones de los usuarios. Pese a eso, se ha seguido trabajando con valentía sin exponer la vida de estos. En virtud de lo anterior, se debió reprogramar las salas de cirugía, ya que algunas afecciones como cáncer no se podían operar, pero se operó lo que tiene menos riesgo, sin embargo, eso no soluciona el problema crítico. La primera semana, se logró recuperar la base de datos de ARCA, donde está la lista de pacientes programados para cirugía, de un respaldo que se tenía actualizado al 30 de mayo 2022, aspecto vital, ante las ordenanzas de la sala constitucional, vía recursos de amparo, y que nos facilitó la gestión correspondiente.
Área de Salud San Rafael de Puntarenas	Farmacia: la base de datos del sistema de farmacia está encriptada, esto implica que se detenga el proceso ordinario de digitación y solicitud de medicamentos, y por ende todo el sistema de copias de recetas subsecuentes, por lo que la afectación es muy importante. Laboratorio: está afectada la computadora principal, no obstante, el servidor aguantó el ataque. Además, al estar ligada al EDUS, el LABCORE no está funcionando, por lo que se ha tenido que recurrir a procesos manuales. Redes: al no tener EDUS no se tiene acceso a las agendas respectivas, afectando así la logística de atención. Radiología tampoco tiene conectividad. Por lo anterior, se está manejando con discos compactos y con láminas de acetato. Administración: sin accesos a la red, en este caso no se pueden hacer consultas ni a presupuesto, ni a recursos humanos, entre otros. Además, en tema de validación de derechos es crítico, ya que no podemos ver si los usuarios tienen o no seguro, en caso de accidentes de tránsito se escanea la boleta que traen. Se cobraron algunos dineros a usuarios que manifiestan no tener seguro, y se hace el cobro. En caso de incapacidades no se han podido refrendar, pero se están entregando de forma manual, además, se está registrando en la hoja de evolución del expediente físico.
Sucursal de Esparza	Definitivamente pensiones e incapacidades, aclarar que todas las áreas han sido afectadas, pero estas son las más críticas. Se espera que a partir del lunes 13 de junio se pueda realizar el cobro de facturas por cuotas obrero-patronales, de trabajador independientes y de seguro voluntario, para lo cual se tomará como punto de partida la planilla del mes de abril que se cobró en mayo, a fin de replicar los montos. En caso de solicitudes posteriores de revisión, se valorará la estrategia que a nivel de Gerencia Financiera se defina. Con respecto a incapacidades, todavía no se tiene un horizonte claro de acción. En cuanto al tema de pensiones, a partir del lunes se estará habilitando el SIP a nivel central únicamente, a fin de que todas las solicitudes sean trasladadas ahí. Esto es una situación preocupante, debido al volumen de trabajo que esto significa. Sin duda los procesos de otorgamiento de pensión se atrasarán. Con respecto al pago de pensión, para este corte no hubo problema en la región, sin embargo, se desconoce la operativa para próximos pagos.

Área de Salud Los Chiles	Prestación de servicios médicos por el EDUS, SIFA. Certificados de vacunación. Trámite de Recursos Humanos, no se dispone de SOGERH. No se tenían computadoras habilitadas solamente una computadora. Para digitar se tuvo que acudir a expedientes para verificar la información, para permisos inicialmente se solicitaban por correo personal. No se han recibido instrucciones de cómo se procederá. Hay atrasos en el trámite de nombramientos de compañeros que laboran en otras unidades. El impacto en la gestión de Recursos Humanos fue muy significativo. Contenido presupuestario, se está trabajando manual, con el reporte del Mayor Auxiliar del mes de mayo, no se puede verificar. Para la contratación de tercerizados se está teniendo problemas. Verificación de cuotas obrero-patronales al día. GETI no funciona, viáticos se elaboran con formularios viejos, y se cancelan por Caja Chica. Las liquidaciones de Caja Chica se trabaja en coordinación con la Sucursal. En Farmacia se tiene un equipo menos, y se están tomando medidas para hacer solicitudes al almacén, se lleva contabilización física de medicamentos. No se tiene control de los medicamentos que se entregan, no tenemos como verificar la entrega de documentos. Tenemos un brote de malaria, y al no tener sistemas no podemos verificar la aplicación de tratamientos. Las recetas se emiten manualmente. Se ha tenido que devolver a pacientes porque no trae información de los medicamentos que le corresponde, consideran que esta Área de Salud queda lejana para muchos usuarios, lo que implica que ellos tengan gastos por transporte, aunado a que son zonas donde existe mucha pobreza. No se ha podido realizar entregas de medicamentos a las regiones más lejanas como Veracruz, por lo que se solicitó que se apersonaran a los EBAIS de adscripción para poder emitir la receta, ya que al no tener accesibilidad al sistema no se puede verificar tratamientos. Afectación en el pago a proveedores. No se pueden pagar subsidios por incapacidades. Se requiere de CGI en el área de Salud que brinde soporte a los equipos. Esto generará reprocesos una vez que se habiliten sistemas, y no se cuenta con personal para incluir los registros físicos emitidos. No se pueden emitir certificaciones de vacunación, laboral, núcleo familiar, ya que los sistemas se encuentran inhabilitados. Se han utilizados varios profesionales de medicina contratados bajo la modalidad de sustitución por excepción que ante la emergencia están brindando apoyo en los EBAIS para la atención de los usuarios y la emisión de las recetas, porque no se cuentan con los sistemas de información que se utilizan para dar seguimiento a los casos de malaria, COVID-19 entre otros.
Coopesain- Tibás	Farmacia: específicamente con las recetas médicas se ha tenido afectación, ya que no se tiene el nombre del medicamento, se ha solicitado a los usuarios las etiquetas de los medicamentos. Las recetas copias se deben pasar a recetas manuales. Odontología: el seguimiento a los pacientes se ha visto afectado. Consulta externa: el no poder acceder a resultados, o cualquier otro estudio realizado tanto dentro como fuera del área, ya que no se tiene acceso al historial, limita la atención que se le brinda al paciente. Laboratorio: los equipos se alimentaban de forma automática, ahora tienen que digitar de forma manual. La Administración no ha tenido problemas, porque su funcionalidad es distinta al ser un servicio tercerizado. La afectación mayor la tiene los servicios que tienen relación con la atención de pacientes y con cualquier aplicativo o plataforma CCSS.
Hospital México	Hospitalización; se tuvo que recurrir a hacer todo manual con papelería. Consulta Externa: por cuanto, es difícil dar el seguimiento a los usuarios. Financiero: debido a aspectos de pago a proveedores, ya que no se tiene la estrategia a seguir. Recurso humano: se debe realizar toda la papelería en físico o a puño y letra. Abastecimiento; Se debe dar continuidad a los procesos de compra con los pocos equipos disponibles de cómputo. Imágenes médicas: no se pueden compartir los estudios, no se pueden ver, los médicos deben dirigirse a rayos X, para tomar decisiones. Farmacia: se ha generado retraso en la oportunidad de atención de pacientes. Los usuarios deben presentar las etiquetas de sus medicamentos para que se les pueden entregar las recetas médicas. Laboratorio: Se debe hacer la búsqueda manual de los resultados impresos.

Fuente: Elaboración propia de auditoría, información suministrada por unidades institucionales en consulta efectuada del 6 al 15 de junio de 2022.

De la información anteriormente citada, se establece que, la emergencia tecnológica suscitada en la Caja Costarricense de Seguro Social provocó una suspensión total del funcionamiento de los diferentes sistemas de información institucionales, utilizados en los servicios médicos, administrativos y financieros; lo anterior, generando afectación de la atención brindada a los usuarios internos y externos.

A continuación, se indican algunos de los servicios y procesos afectados, según la información suministrada:

- Atención médica (mediante el Expediente Digital Único en Salud).
- Farmacia.
- Laboratorio.
- Rayos X.
- Listas de Espera.
- Cirugías.
- Incapacidades.
- Banco de Sangre.
- COVID19.
- Recursos Humanos.
- Aprovisionamiento Bienes y Servicios.
- Presupuesto.
- Gestión de Activos.
- Mantenimiento.
- Producción Industrial.
- Validación de Derechos.
- Recaudación.
- Pensiones.
- Inspección y Cobros.
- Facturación de Servicios.
- Plan de Continuidad TI.
- Afectación Equipos Cómputo, entre otros.

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 institución debe asegurar que las acciones hayan sido comunicadas y entendidas por las partes interesadas, además de realizar pruebas periódicas para validar la vigencia y aplicabilidad.*
>
> *La Unidad de TI debe definir acciones formales que permitan brindar una garantía razonable sobre la continuidad de los servicios tecnológicos internos y los administrados por terceros, procesos ante situaciones de contingencia y restablecimiento de los recursos tecnológicos, ante una interrupción; manteniendo adicionalmente acuerdos de servicio con los proveedores de bienes y servicios que le permitan solventar situaciones de interrupción".*

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

En conferencia de prensa virtual, del 30 de abril de 2022, sobre los ataques informáticos del grupo cibercriminal Conti, que reciben las instituciones estatales del país desde el mes de abril 2022, el director de Gobernanza Digital, Jorge Mora Flores informó que el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) detectó **más de cuatro millones de ciberataques** contra entidades públicas de Costa Rica en 24 horas; estos intentos de ciberataques están divididos en 2,7 millones de Malware, 800 mil de Phishing, 84 mil de Cryptomining y 1,2 millones de Actividades de comando y control (tipo Conti).

Con el paso del tiempo, los ciberdelincuentes se vuelven más sofisticados, organizados, persistentes y económicamente motivados, por lo que, para protegerse y recuperarse de un ciberataque, la organización debe implementar un plan eficaz de respuesta, una plataforma que reúna defensas inteligentes, robustas, resilientes y organizadas, así como, la definición de roles específicos, responsabilidades claras y medios de comunicación previamente definidos (para evitar ambigüedad y confusión en la información).

La comunicación con los funcionarios y usuarios de los servicios (médico, administrativos y financieros) debe ser constante tras un ciberataque, ya que se debe conocer el alcance del incidente y las medidas de respuesta y contingencia establecidas por las autoridades institucionales; asimismo, es importante abordar una estrategia de monitorización de redes sociales para analizar cómo está afectando el ciberataque a los usuarios y a la imagen institucional, y así poder dar una respuesta oportuna y transparente, para generar confianza.

En este contexto, este órgano de fiscalización considera importante mencionar lo indicado por Ahmed Saleh, Líder de inteligencia y respuesta a incidentes IBM X-FORCE, en publicación del 30 de agosto 2017:

> *"(…) Es indispensable hacer de la comunicación un componente central, el silencio solo genera incertidumbre y desconfianza (…)*
>
> *Tratar con un ciberataque puede ser agotador. Desafortunadamente, no hay un buen momento para descansar, ni siquiera cuando un ataque y su impacto están contenidos. Ese es el momento de mirar atrás y determinar lo que salió bien y lo que salió mal, y luego incorporar lo que se ha aprendido en la planificación para el próximo ataque. Documentar los hallazgos y vacíos, controlar las deficiencias y priorizarlas hasta el final. Esto debe ocurrir no sólo dentro del entorno, sino también dentro del propio programa de respuesta a incidentes (…)".*

En relación con lo anterior, esta Auditoría considera necesario establecer una estrategia integral en conjunto con todos los niveles organizacionales, con el fin de efectuar una revisión y análisis de las actuaciones previas y posteriores al ataque cibernético en la plataforma tecnológica institucional a partir del 31 de mayo del 2022, así como sus efectos en la continuidad del negocio, con el propósito de documentar lecciones aprendidas (en los niveles centrales, regionales y locales), en torno a evitar una situación similar en el futuro y/o mejorar la capacidad reacción institucional ante eventos de este tipo o cualquiera que atente contra la prestación de servicios.

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 y la gestión de Tecnologías de Información y Comunicaciones.

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 que aún afecta a la CCSS.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.07.15 16:08:48 -06'00'

Lic. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/AEBB/lbc

C Auditoría.