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

AD-ATIC-038-2022
21 de abril de 2022

Doctor
Roberto Cervantes Barrantes, Gerente a.i
GERENCIA GENERAL, 1100

Ing. Roberto Blanco Topping, subgerente
DIRECCION DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES - 1150

Estimado señor:

Asunto:	**Oficio de advertencia sobre la continuidad de servicios bajo el contexto del evento de interrupción de los servicios tecnológicos a nivel Institucional presentado el 7 de marzo de 2022.**

En cumplimiento de las labores de asesoría y advertencia constituidas en la Ley General de Control Interno, esta Auditoría Interna ha revisado aspectos referentes a la continuidad de servicios bajo el contexto del incidente de interrupción de los servicios tecnológicos a nivel Institucional presentado el 7 de marzo del 2022.

Este Órgano de Fiscalización y Control mediante oficio AI-417-2022 y AI-518-2022 solicitó información sobre evento presentado en la plataforma tecnológica el 7 de marzo del 2022. Al respecto, se recibió nota GG-DTIC-1368-2022 del 11 de marzo de 2022 y GG-DTIC-1739-2022 del 29 de marzo de 2022, en los cuales se atienden consultas efectuadas y se remiten informes y oficios generados a lo interno de esa dirección.

Al respecto, se señalan a continuación aspectos generales y observaciones identificadas por esta Auditoría

1. **Sobre el incidente ocurrido el 7 de marzo del 2022**

De acuerdo con el informe denominado: “Informe técnico incidencia presentada en equipos de seguridad por tráfico anómalo “de fecha 9 de marzo del 2022, remitido en oficio GG-DTIC-1368-2022 por el Ing. Roberto Blanco Topping, Subgerente de Tecnologías de Información y Comunicaciones, la incidencia se presentó a las 8:06 am del 7 de marzo del 2022, al respecto, se indicó lo siguiente:

> “(…) *Esta incidencia se presentó a las 08:06 am, a las 9:25am se aplicó una primera acción correctiva, que permitió habilitar los servicios, y las acciones finales correctivas se dieron a las 8:00pm. Esto por cuanto a pesar de que se dio la atención técnica en los dispositivos de seguridad, el alto tráfico generado provocó lentitud por un tiempo mientras se estabilizaba la infraestructura, en el momento que el tráfico bajó toda la infraestructura volvió a su estabilidad, así como todos los servicios alojados en la misma.*
>
> *Los sistemas impactados fueron: EDUS y SICERE, y la autenticación de las Redes Virtuales Privadas (VPN, sus siglas en inglés) ya que todos estos servicios se encuentran en el Datacenter Institucional, y el equipo de seguridad que presentó la afectación se encuentra instalado en la entrada principal de dicho sitio. Cabe indicar que el Office 365 no se vio afectado.*

Según lo indica la Dirección de Tecnologías de Información y Comunicaciones (DTIC) se trató de una incidencia presentada en equipos de seguridad por tráfico anómalo.

A nivel general, se entiende por tráfico anómalo, como aquel considerado por la institución fuera de lo normal y que pudiera alterar el funcionamiento de las redes de datos o causar interrupciones en el servicio.

2. Sobre los equipos involucrados en el incidente

Mediante oficio GG-DTIC-1725-2022 del 28 de marzo 2022 suscrito por la Máster Mayra Ulate Rodríguez, jefe Área de Seguridad y Calidad Informática, Máster Jorge Sibaja Alpízar, jefe Área Soporte Técnico y Jessica Cordero Ríos, Jefe Área Comunicaciones y Redes Informáticas remitieron al Máster Roberto Blanco Topping, Subgerente a.i. DTIC, información adicional solicitada por esta Auditoría, indicando sobre los equipos involucrados en el incidente, lo siguiente:

Dos equipos de Intrusión Prevention System [1](IPS), marca McAfee, modelo NS9100, los cuales se encuentran ubicados en el Centro de Datos[2] ubicado en Llorente de Tibás (CODISA)

El proceso de adquisición de estos IPS´s se realizó en el año 2015, mediante proceso de contratación 2015CD-000183-5101, y se renovó su licenciamiento y soporte técnico en el año 2019, a través del proceso de contratación 2019CD-000021-1150, “Licenciamiento y Soporte Técnico para la solución de prevención contra intrusos y concentrador de VPN”.

Adicionalmente, otros equipos involucrados en el evento fueron los siguientes:

Equipos virtuales de Firewalls[3]: Dos equipos con licenciamiento para Cisco, modelo FTD 2140, lo cuales cuentan con soporte 24x7 con la empresa Fusionet S.A. Estos están virtualizados en el VMWare[4] de Oficinas Centrales.

Respecto al proceso de adquisición de estos firewalls, se realizó en el 2021, mediante proceso de contratación LA-000008-0001101150, cuyo objeto de contratación fue: “Licencias de software para Muros de Fuego de nueva generación.

3. Sobre el Monitoreo de Seguridad de la Institución

En materia de seguridad, es innegable, la necesidad de vigilar los activos tecnológicos de la institución, equipo, red, software e información, entre otros, por lo que disponer de una primera línea de defensa dedicada 24/7contra cualquier incidente o intruso, siendo una de sus funciones buscar, detectar y evitar ataques de forma proactiva, a partir de información otorgada por herramientas de inteligencia de amenazas y tendencias de explosión de vulnerabilidades.

De acuerdo con información suministrada por la DTIC, el monitoreo de los equipos de seguridad IPS y firewall lo realizan funcionarios del Subárea de Seguridad en Tecnologías de Información. Asimismo, indicaron que se encuentra en ejecución el contrato de Servicios Tercerizados de Seguridad 24x7 con la empresa Deloitte & Touche S. A., bajo la contratación 2018LN-000002-1150 “Servicios Profesionales de Seguridad en TI”.

En ese sentido, se hace necesario que la CCSS revise los procedimientos de monitoreo establecidos, su documentación, las herramientas utilizadas, integración con procesos interinstitucionales, recursos asignados,

[1] Sistema de prevención de intrusiones (Instrusion Prevention System) el cual ayuda a las organizaciones a identificar tráfico malicioso.
[2] centro de procesamiento de datos, lugar donde se concentran recursos necesarios para la gestión de la información de una organización. (Data Center)
[3] dispositivo de seguridad de la red que monitorea el tráfico entrante y saliente y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.
Los firewalls han constituido una primera línea de defensa e
[4] Sistema de virtualización por software que simula computadores físicos

indicadores, jerarquía de comunicación, gestión de alertas, reglas definidas, entre otros, a fin de garantizar la detección de situaciones que pudieran comprometer la continuidad del servicio que presta la institución.

4. Sobre eventos similares y lecciones aprendidas.

De acuerdo con información provista por la Direccion en torno a eventos similares al presentado el 7 de marzo del 2022, sólo se había presentado el siguiente:

> "*29 de junio 2020. Caso Problema: 113399. Problemas de denegación de servicios a nivel de DNS interno - Externo. Situación: Se presenta una caída de servicios a nivel de DNS Interno y Externo. Resolución: Se realiza el cambio del CCSS-IPS1 por un dispositivo nuevo, ya que el mismo se dañó por la cantidad de tráfico, y casa matriz asume la garantía por parte del fabricante. Se gestiona con Cisco, el cambio dentro de la infraestructura de los IPS, de modo que se pudiera manejar la cantidad de tráfico que estaba llegando, el cual estaba sobrepasando los 10gigas, que es la capacidad máxima de los dispositivos. Cabe indicar que en Oficinas Centrales los IPS se encontraban en modo activo-pasivo. Se adjunta Anexo del caso Problema "Formulario Gestión de Conocimiento - Problema 113399".*

Adicionalmente, de acuerdo con oficio AD-ATIC-706-2020 de esta Auditoría, el 22 de octubre del 2019, se presentó una interrupción de servicios tecnológicos relacionada con los equipos IPS, al respecto, se indicó:

> *"(…) este Ente de Fiscalización conoció mediante la Resolución No. DTIC-6614-2019, suscrita por el Ing. Christian Chacón Rodríguez, que la interrupción sufrida por un periodo aproximado de 3 horas fue causada por un evento presentado en los equipos denominados "IPS" (traducción al español Sistema de Protección de Intrusos) de la plataforma tecnológica institucional. No obstante, una solución temporal fue aislarlos y/o apagarlos, tanto los ubicados en Oficinas Centrales como los instalados en el Data Center de CODISA…"*
> (Destacado no corresponde al original)

En virtud de lo anterior, es necesario hacer una revisión y análisis de las actuaciones previas y posteriores a los incidentes presentados, especialmente el último evento, con el propósito de generar lecciones aprendidas en torno a la gestión y tratamiento de este tipo de situaciones.

De la información revisada por la Auditoría Interna, se han presentado tres incidencias en donde estuvieron involucrados equipos de seguridad, por lo que es preciso el análisis y la documentación de las oportunidades de mejora, así como la evaluación de procesos asociados, considerando entre otros la capacidad de reacción y de prevención, así como el nivel de madurez en esta materia.

Si bien es cierto el incidente presentado se asoció a seguridad, este Órgano de Fiscalización y Control estima fundamental considerar también el crecimiento de la plataforma tecnológica institucional, a fin de que ambas plataformas estén articuladas y planificadas, conforme la evolución y requerimientos de la demanda del negocio.

5. Fortalecimiento de la Plataforma tecnológica institucional y sitio alterno

La DTIC dispone del Programa de Fortalecimiento de la Arquitectura de la Plataforma Tecnológica Institucional (Centro de Datos Principal y Centro de Datos Alterno), proyecto que tiene como objetivo asegurar la continuidad de los servicios de la plataforma tecnológica de la CCSS, para garantizar la disponibilidad, confiabilidad y seguridad de la información de todos los sistemas institucionales críticos, a partir del desarrollo de los entornos lógico, físico, geográfico y tecnológico necesarios.

Al respecto, es necesario aclarar que el centro de procesamiento de datos es el lugar donde se concentran todos los recursos necesarios para la gestión de la información de una organización. Normalmente se trata de un edificio

o sala de gran tamaño, con las adecuadas condiciones físicas y lógicas, utilizado para mantener en él una gran cantidad de equipamiento electrónico que alberga soluciones.

Actualmente, el Centro de Cómputo Principal (CCP) institucional se ubica en el Parque Tecnológico CODISA en Tibás y su administración está a cargo de la Dirección de Tecnologías de Información y Comunicaciones, específicamente del Área de Soporte Técnico. En dicha Plataforma se almacenan los principales sistemas de información y las bases de datos institucionales utilizados en la prestación de servicios a los asegurados, patronos, pensionados, entre otros.

Dentro de los aplicativos y repositorios de datos resguardados en los componentes que conforman la Plataforma Tecnológica Central se encuentran el Sistema Centralizado de Recaudación (SICERE), Expediente Digital Único en Salud (EDUS), Sistema de Presupuesto Institucional (SIP), Sistema de Registro y Control de Pago de Incapacidades (RCPI), Sistema de Gestión de Suministros (SIGES), Sistema Control de Bienes Muebles (SCBM), Sistema Integrado de Comprobantes (SICO) y Módulo Integrado de Seguridad (MISE).

En ese sentido, en informe ATIC-166-2020 “Evaluación de la gestión integral de la Plataforma Tecnológica Central que soporta las soluciones informáticas de la Caja Costarricense del Seguro Social “, esta Auditoría constató que, la Institución no disponía de un sitio alterno al Centro de Datos Principal para la operación de sistemas y servicios.

Al respecto, se señalaron riesgos como no disponer de otra opción, la cual brindaría continuidad a las actividades sustantivas de la institución ante interrupciones provocadas por desastres naturales, problemas de funcionamiento de dispositivos, vulnerabilidades de seguridad, entre otros, podría ocasionar la materialización de riesgos asociados a la suspensión de los servicios brindados a los usuarios a través de la Plataforma Tecnológica Central como lo son atenciones en salud, procesos de recaudación, planillas, pensiones, entre otros.

Adicionalmente, se mencionó que ante esta situación podría generarse una pérdida de datos de salud y pensiones de la población en general provocando un impacto en la imagen de la Caja Costarricense del Seguro Social.

Lo anterior adquiere relevancia al considerar que tanto medios de prensa televisivos como Repretel y escritos como La Nación publicaron en sus espacios noticiosos, la problemática que se presentó en la atención de pacientes en establecimientos de salud, debido a la “caída de la Plataforma EDUS”.

6. Participación de contratistas o terceros en la búsqueda de la solución al evento

Sobre la intervención de contratistas o terceros durante incidencia del lunes 07 de marzo 2022, se identificó participación de los siguientes proveedores según el ámbito de sus competencias y alcance de los contratos:

- Consulting Group Corporation (Proceso de Contratación 2019CD-000021-1150, ya que es el contratista que brinda el soporte de los Detectores de Intrusos (IPS), sin embargo, al momento de su llegada la situación ya se encontraba atendida por parte de los funcionarios de la CCSS).

- SPC. Contratación: 2020LA-000001-0001101150. Objeto: Servicios de mantenimiento preventivo y correctivo de equipos de comunicación, Caso: 693188377. Como apoyo que proporcionó el ACRI en el diagnóstico de la situación, determinándose que a nivel de comunicaciones todo estaba funcionando adecuadamente.

En este sentido, es fundamental el involucramiento de los contratistas según su objeto de contratación y alcances del contrato en la planificación de la seguridad informática, con el propósito de brindar apoyo en caso de presentarse eventos como el supra citado, siempre disponiendo de los acuerdos de confidencialidad y protegiendo la información institucional bajo rigurosos protocolos.

7. Comunicación efectuada a las gerencias en torno al incidente

Si bien es cierto, la prioridad debió ser la atención de la incidencia presentada, así como la restauración de los servicios interrumpidos, es necesario definir y establecer los mecanismos de comunicación con el nivel superior: Gerencia General y Consejo Tecnológico, sobre la situación que estaba ocurriendo y deben definirse de previo, los posibles mensajes a brindar a los medios de comunicación colectiva, así como a los usuarios internos y externos.

Ante consulta efectuada por esta Auditoría, sobre la comunicación realizada a gerencia general y las gerentes, la Administración indicó lo siguiente:

> *"Esta Dirección pone en práctica actividades de comunicación al momento de la incidencia, tales como:*
>
> *- Comunicación con los Centros de Gestión Informática que consultan durante la incidencia.*
>
> *- Atención a los casos en mesa de servicios TIC, se brinda un detalle de la incidencia presentada y su solución, se comunica y valida con los usuarios, esto de acuerdo con el protocolo de Soporte Lentitud mencionado anteriormente. A las gerencias se les brinda un informe del evento ocurrido, una vez que este es corregido y los servicios vuelven a la normalidad.*
>
> *Como medida de seguridad cuando un evento es percibido con afectación a la infraestructura de seguridad, no es conveniente brindar información hasta que la incidencia sea atendida, esto con la finalidad del resguardo de la información sensible como detallar los equipos de seguridad perimetral afectados o involucrados y determinar con el análisis forense el origen del problema."*

8. Sobre las medidas correctivas aplicadas

De acuerdo con información suministrada por la DTIC mediante oficio GG-DTIC-1739-2022 del 29 de marzo de 2022, se generaron dos actividades como medidas correctivas, al respecto señalaron:

> *"Actividad uno realizada: respecto a la cantidad de tráfico anómalo que se estaba recibiendo del Hospital Nacional de Niños:*
>
> *- Bloqueo de los direccionamientos de las IPs externas a los cuales se trataban de comunicar las IPs internas de dicho nosocomio, este a nivel de los 04 IPS (Oficinas Centrales y CODISA), esto con la finalidad de salvaguardar la confidencialidad de la información, ya que los IPS que están localizados en Oficinas Centrales revisan el tráfico entrante y saliente a nivel del enlace de internet, cuando esto se aplicó, se colocaron los IPS de CODISA, para que únicamente dejaran pasar el tráfico y no bloquearan los paquetes anómalos, esto con el fin de liberar el encolamiento que se estaba generando por la inspección y bloqueo de paquetes a nivel de los mismos.*
>
> *Actividad dos realizada: Sobre los firewalls virtuales;*
>
> *- Estos equipos ubicados en Oficinas Centrales tuvieron un incremento en su procesamiento el cual llego a un 99%, no se aplicó ninguna acción para no afectar más el tráfico y se dejó que los mismos bajaran su procesamiento situación que se normalizo al momento que empezó a bajar el tráfico."*
>
> *Consideraciones generales:*
>
> *1) La medida correctiva fue temporal, ya que los IPS de CODISA se encuentran en este momento realizando su trabajo normal. Esto se logró con la reconfiguración de dicha funcionabilidad a partir de las 8pm de ese mismo día, mediante el RFC 18916, esto con la finalidad de poder monitorear el tráfico, y que no se volviera a presentar ninguna afectación.*

2) Desde la incidencia, se ha mantenido un monitoreo constante de los IPS y del tráfico, y hasta el momento no se ha vuelto a presentar dicha situación.

3) Se ha gestionado con el Hospital Nacional de Niños la actualización de sus equipos a nivel de Sistema Operativo de parches, y una revisión generalizada a nivel de malware en sus endpoints.

En ese sentido, conviene el análisis de las medidas adoptadas y revisar si su aplicación favoreció o resolvió de manera permanente la situación presentada, y cuales nuevas reglas o ajustes se requieren en la plataforma de seguridad, así como identificar si es necesario efectuar actualizaciones en otras unidades de tecnología locales como los Centros de Gestión Informática (CGI) de hospitales, establecimientos de salud, sucursales, regionales, gerenciales y unidades no formalizadas, pero con equipos TIC o médicos que acceden las redes de comunicación de datos.

Al respecto, disponer de un plan de acción con plazos y responsables contribuiría a dicha tarea, así como el involucramiento de especialistas de la institución.

Mediante oficio GG-DTIC-1368-2022 del 11 de marzo de 2022, el Ing. Danilo Hernández Monge remitió al Lic. Olger Sánchez Carrillo, Auditor Interno, respuesta a consultas efectuadas, indicando sobre las acciones a seguir en el plano de prevención para situaciones futuras, lo siguiente:

"(…) pueden ubicarse en dos líneas de acción:

I. La primera, referida al fortalecimiento de las capacidades de la Plataforma de Seguridad a nivel central. En este sentido, cabe ubicar los esfuerzos que se han venido realizando en la DTIC, entre estos, las tareas en marcha del Reforzamiento de la Infraestructura de Seguridad Perimetral.

II. La segunda, sobre el fortalecimiento de la gestión tecnológica en los niveles locales y como parte de los esfuerzos de fortalecimiento en este ámbito de gestión local, la DTIC, mediante oficio GG-DTIC-1393-2022, está informando a las Gerencias, sobre la convocatoria de los CGI's Gerenciales a fin de conformar un grupo inter-gerencial con la participación de las jefaturas de Área de la DTIC y la coordinación directa desde la Subdirección DTIC, que pueda realizar un análisis más detallado del informe en aras de identificar y generar acciones de fortalecimiento de la gestión tecnológica en los niveles locales."

9. Sobre la capacidad de la Solución de seguridad perimetral

Esta Auditoría consultó al Ing. Roberto Blanco, Subdirector de la DTIC, si se pudo haber minimizado las consecuencias del evento, y por qué la Caja no pudo anticiparlo.

Al respecto, se indicó que con el aumento de uso del mecanismo de VPN[5], el tráfico institucional había aumentado considerablemente, por lo que la solución de Seguridad Perimetral actual se encuentra en su máxima capacidad de procesamiento, señalando en oficio GG-DTIC-1739-2022 del 29 de marzo de 2022, lo siguiente:

"(…) Debido a la pandemia el tráfico institucional ha aumentado casi en un 200%, anteriormente se manejaban un aproximado de 500 VPN a nivel de teletrabajo, en este momento se cuenta con alrededor de 9 mil VPN, esto más otros servicios tecnológicos que se han generado por la atención de la pandemia han provocado que la Solución de Seguridad Perimetral actual se encuentra en su máxima capacidad de procesamiento, sin embargo se han gestionado grandes cambios a nivel de

[5] Red privada Virtual (virtual private network) Conexión cifrada a internet desde un dispositivo a una red para garantizar transmisión segura de datos.

infraestructura Tecnológica para poder solventar dicha situación, y mantenerla estable, de los ataques cibernéticos y las vulnerabilidades han aumentado en estos últimos dos años…"

(…) Para minimizar este tipo de incidencias, es necesario el cambio de la Solución de Seguridad Perimetral, que ya se encuentra en ejecución, la misma se empezó en gestión a partir del año 2020, pero por algunos procesos administrativos, su ejecución comenzó el 07 de marzo 2022, actualmente ya se gestionó la solicitud de los equipos y estamos en el proceso de diseño …"

Lo anterior adquiere relevancia si se considera que este Órgano de Fiscalización y Control en informe ATIC-045-2021 del 2 de junio del 2021, había señalado referente a la estrategia de infraestructura y seguridad informática Debido al incremento de usuarios en teletrabajo

"*Se determinó, la ausencia de una estrategia orientada al fortalecimiento de la gestión de infraestructura y seguridad informática (debido al incremento de usuarios en teletrabajo desde el inicio de la pandemia por Covid-19), donde se contemplen aspectos como: la utilización de equipos personales para realizar funciones institucionales, el acceso a información confidencial, la protección de datos, conectividad, necesidades de equipo tecnológico, mantenimiento preventivo y correctivo de activos institucionales (utilizados en teletrabajo) …"*

En oficio GG-DTIC-1587-2021 del 17 de marzo, suscrito por la Máster Mayra Ulate Rodríguez, Jefe del Área de Seguridad y Calidad Informática, el Máster Jorge Sibaja Alpízar, Jefe Área de Soporte Técnico y el Máster Christian Chacón Rodríguez, Subdirector, remitido al Máster Roberto Blanco Topping, Subgerente Dirección Tecnologías de Información y Comunicaciones, indicaron lo siguiente en torno a la capacidad de la infraestructura institucional para soportar el incremento de VPN´s:

"(…) Como parte de las acciones y herramientas tecnológicas para la sostenibilidad del teletrabajo, se ha venido recomendando a las jefaturas que todo funcionario que esté en teletrabajo debe utilizar la VPN Institucional, esto por razones de seguridad en el acceso a la plataforma de servicios en tecnologías de información de la CCSS. En ese sentido, se ha venido reforzando la plataforma de VPN, a través de varias acciones entre ellas:

A partir del 2018, se viene implementado el modelo de Gobierno y Gestión de las TIC mismo que incorpora procesos de mejores prácticas alineados con ITIL y COBIT, por lo que como parte de ese proceso, se cuenta con un procedimiento a nivel de Mesa de Servicios para la creación de usuarios a nivel de VPN, donde se definieron los procedimientos para llenar los documentos para su habilitación, un formulario que deber llenar la jefatura donde se solicita la VPN para el funcionario, con la justificación respectiva, y el Acuerdo de Uso y confidencialidad de la información, donde el funcionario asume la responsabilidad respectiva del uso adecuado de la VPN. Dicho servicio de Mesa tiene atención 24x7x365…
(...) Se han estado realizando varias mejoras en los ambientes de VPN tales como el aumento en las capacidades de tráfico en 20Gbps, lo cual ha generado que nuestra infraestructura tenga la capacidad necesaria para el trasiego de tráfico sin ningún inconveniente.
(Destacado no corresponde al original*)*

10. Sobre la actualización y revisión de los equipos de cómputo en unidades locales

En virtud de que la seguridad informática involucra a todas las unidades locales con plataformas de TIC y considerando que especialmente los Centros de Gestión Informática (CGI) disponen de servidores y soluciones tecnológicas con acceso a equipos y redes, es necesario niveles de supervisión y seguimiento que garanticen articulación y congruencia con las políticas institucionales. Al respecto, la actualización de los parches de seguridad debe efectuarse con rigurosidad.

Sobre aspectos que pudieran minimizar incidencias como la ocurrida el 7 de marzo, los profesionales de la DTIC, indicaron:

> *"(…) Otro punto importante para minimizar este tipo de incidencias es que los equipos de cómputo a nivel nacional se encuentren al día con sus parches de seguridad de Sistema Operativo, tanto equipo de oficina como equipos médicos. A nivel central mediante el System Center Configuration Manager (SCCM), se hace el envío de los parches de seguridad a todo el país, pero es responsabilidad de los Centros de Gestión Informática (CGI), estar revisando que sus equipos a cargo, se encuentren al día con dichas actualizaciones, ya que en el caso de que se encuentren desactualizados se puede coordinar mediante Mesa de Servicios con la Subárea de Soporte a Usuario Final el envío de actualizaciones masivas al sitio, o bien generar una media offline para su aplicación a cada equipo. Cabe indicar que todos los días se traslada a los CGIs Gerenciales para que bajen la información a sus colaboradores boletines sobre nuevas actualizaciones, indicando cual es la vulnerabilidad atendida y las recomendaciones que se deben de aplicar para poder mitigar dicha vulnerabilidad…"*

11. Sobre el uso de "manos remotas"

El servicio de manos remotas permite la delegación de tareas de administración y mantenimiento de TI dentro de una instalación, fuera de las oficinas donde labora, el personal técnico y especializado de una organización.

De acuerdo con la información suministrada por la DTIC, el personal de la DTIC ingresó a las instalaciones del parque tecnológico CODISA donde se encontraban ubicados los equipos IPS que requerían atención indicada conforme el siguiente cuadro:

Nombre del Colaborador	Hora de Ingreso	Tiempo transcurrido desde el inicio del incidente (8:06 am)
Ericka Sánchez Solis	8:56 am	50 min
Wilfredo Porras Morales	9:09 am	73 min
Christian Gómez Suarez	9:18 am	82 min

Lo anterior, considerando que según se señala funcionarios indicaron desconexión de la VPN, lo cual imposibilitaba el acceso a los equipos desde otros puntos diferentes de la ubicación de los IPS´s.

Tal y como lo indicó la DTIC, los equipos IPS se encuentran ubicados en instalaciones del Parque CODISA en Llorente de Tibás, es decir fuera de las oficinas de la CCSS.

Debe valorarse la necesidad de disponer de un servicio de manos remotas ya sea con personal interno, tercerizado u otra modalidad que permitan tomar acción de los equipos de forma inmediata, en virtud del impacto y costos en que incurre la CCSS ante las interrupciones como la presentada el 7 de marzo del 2022, así como el detrimento en la atención de pacientes y usuarios externos e internos.

En el caso señalado la funcionaria que llegó primero a CODISA tardó 50 minutos en apersonarse para realizar las tareas correspondientes para la atención del incidente, en virtuds de la imposibilidad de efectuarlo en forma remota.

12. Sobre los protocolos utilizados

Esta Auditoría consultó sobre los protocolos y procedimientos de seguridad aprobados para el manejo de incidentes como el presentado el 7 de marzo de 2022, trafico anómalo. Al respecto, la Administración indicó lo siguiente:

> "*Protocolo uno utilizado:*

• Protocolo "DSS02-PT-003 Protocolo de incidencia Lentitud General en Servicios v1.2.pdf" adjunto, ya que se atiende este tipo de casos en la Mesa de Servicios TIC, que es la cara principal de la gestión de servicios TIC. Este protocolo se encuentra en este momento en proceso de aprobación y divulgación de acuerdo con los lineamientos establecidos por la DTIC, para este tipo de documentos.

Protocolo dos utilizado:

• Protocolo de Servicios tercerizados: donde tenemos acceso al protocolo Deloitte para Gestión de Eventos de Seguridad TI. Este protocolo es solicitado dentro del proceso de contratación a la empresa adjudicada, el mismo no se brinda por ser un documento confidencial…"

De lo anterior, se concluye que el protocolo utilizado DSS02-PT-003 "Protocolo de incidencia Lentitud General en Servicios v1.2", no se encuentra aprobado, ni divulgado dentro de los actores que correspondan, lo cual a criterio de esta Auditoría representa riesgos asociados con ambiente de control, suficiencia del contenido del protocolo, así como la aplicación y comprensión de estos.

13. Sobre el proyecto de seguridad perimetral

El 30 de julio del 2022, la DTIC, mediante oficio GG-DTIC-4439-2020, efectuó solicitud de inicio de inicio del proceso de contratación para la adquisición de "Solución Institucional de Seguridad Perimetral" bajo la figura de seguridades calificadas, según lo dispuesto en el artículo 139 inciso h.

En ese sentido, de acuerdo con lo indicado por esa Direccion, esta compra forma parte de la atención a las brechas que se habían identificado en seguridad TI, con el Proyecto de Ciberseguridad a través del diagnóstico, análisis de vulnerabilidades y riesgos, basados en mejores prácticas y estudio de tendencias.

Es relevante indicar que el día del incidente, 7 de marzo de 2022, justamente la Direccion Jurídica otorgó el refrendo al contrato No. 0432022115000009-00, por lo cual no había iniciado su ejecución.

Al respecto, llama la atención a este órgano de Fiscalización y Control que el proceso haya tardado un año y siete meses, a pesar de lo trascendental del mismo para la seguridad institucional y lo indicado por la DTIC en cuanto a que la Solución de Seguridad Perimetral actual se encuentra en su máxima capacidad de procesamiento.

14. Importancia del plan de continuidad

Cada día la Institución utiliza las tecnologías de información y comunicación para atender los procesos de salud, pensiones y recaudación patronal que tiene a cargo, para ello debe planificar la gestión de continuidad del negocio, a fin de evitar que las actividades sustantivas permanezcan ininterrumpidas, por fallas de origen eléctrico, financiero, tecnológico (redes y comunicaciones, copias de seguridad, restauraciones de datos), desastres naturales, entre otros.

Las organizaciones deben disponer de un Plan de Continuidad del Negocio, el cual contendrá a su vez planes, como el de contingencia y/o continuidad de las TIC, así como el de comunicación, recuperación, entre otros de igual o mayor importancia.

Además, a manera de ejemplo incluye elementos de definición para la clasificación del impacto, indicadores de tolerancia ante la ausencia del funcionamiento de sus aplicaciones informáticas, todo esto con el objetivo de minimizar en la medida de lo posible la afectación al negocio.

Debido a ello, existe el Plan de Continuidad de las Tecnologías de la Información y las Comunicaciones, el cual consistiría en una estrategia planificada, constituida por un conjunto de recursos y procedimientos de actuación,

encaminados a conseguir una restauración ordenada, progresiva y ágil de los sistemas de información que soportan los procesos de negocio considerados como críticos en la Institución.

Es decir, el plan de continuidad del negocio aplica para cualquier suceso, pudiéndose afectar procesos críticos institucionales, los cuales estén vinculados o no con las tecnologías de información, principalmente porque no es un tema relacionado únicamente con la resolución que pueda dar un ente técnico en TIC1, debido a que existen particularidades en la gestión propia de las unidades de servicio y estas a su vez evalúan la pertinencia de las medidas alternas a utilizar durante la incidencia

En ese sentido, conviene comprender el significado de la continuidad de negocio y en segunda instancia lo correspondiente a tecnologías de información y comunicaciones, debido a que estas podrían no distinguirse del todo actualmente en la institución.

Finalmente, se debe considerar que las Instituciones dependen cada vez más de las tecnologías, los procesos demandan una alta disponibilidad de los servicios de TIC, en algunos casos imprescindibles para su funcionamiento, de ahí la necesidad de los planes antes indicados bajo un enfoque integral, caracterizándose por ser de índole estratégica y transversal a toda la organización, brindándose las medidas de seguridad en los diferentes ámbitos del negocio, e interrelacionándose todos los procedimientos que le conforman.

15. Sobre el nombramiento como Órgano de Investigación Preliminar expediente: IP-00125-1150-2022

Mediante GG-DTIC-1514-2022 del 17 de marzo de 2022 el Ing. Roberto Blanco Topping designó a los funcionarios de la DTIC, Ingenieros Jorge Peñaranda Guerrero y Alberto Vargas Ramírez Funcionarios del despacho de la Dirección Tecnologías de Información y Comunicaciones como miembros del Órgano de Investigación Preliminar expediente: IP-00125-1150-2022, señalando:

> *"(…) se les designa como Órgano de Investigación Preliminar con el fin de investigar un presunto hecho irregular ocurrido el lunes 07 de marzo de 2022, relacionado con "incidencia presentada en equipos de seguridad por tráfico anómalo".*
>
> *Al respecto, se les requiere que se emita el acto preparatorio, con base en los siguientes elementos:*
>
> 1. *Identificar las causas que provocaron el fallo en la infraestructura y/o servicios tecnológicos de la CCSS, por alrededor de una hora y media, entre las 8:00 a.m. y las 9:30 a.m. aproximadamente del día 07 de marzo de 2022.*
>
> 2. *Determinar el impacto en la prestación de los servicios tecnológicos, a raíz de la incidencia indicada en el punto anterior.*

Al respecto, conviene revisar la conformación de este órgano a fin de garantizar participación de especialistas y funcionarios de otras unidades, con el propósito de disponer de un panorama institucional de la situación presentada. En ese sentido debemos aclarar que al finalizar la redacción del presente documento no se ha hecho de conocimiento a la Auditoria respecto de la emisión de resolución al respecto.

Consideraciones normativas

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(...)"

Las Normas técnicas para la gestión y el control de las Tecnologías de Información emitidas pro el Ministerio de Ciencia, Tecnología y Telecomunicaciones, MICITT, señala en el Apartado XI, Seguridad y Ciberseguridad, lo siguiente:

"La institución debe tener y aplicar en forma consistente una estructura formal al nivel institucional, que permita establecer las acciones para administrar la seguridad de la información, ciberseguridad debidamente respaldada con la política de seguridad de la información / ciberseguridad y que oriente la disponibilidad de niveles de protección y salvaguarda razonables en atención a requerimientos técnicos, contractuales, legales y regulatorios asociados.

La Unidad de TI, basado en la Política de seguridad de información / ciberseguridad, debe establecer los mecanismos necesarios para asegurar una protección razonable de los activos tecnológicos, activos de información institucionales, dando énfasis en su clasificación como elemento definitorio para establecer los requerimientos de preservación de la confidencialidad, integridad y disponibilidad de la información.

La Institución debe propiciar un ambiente seguro, considerando la seguridad física y ambiental como un componente básico en el esquema de protección requerido para prevenir el acceso físico no autorizado, daños e interferencia a la información y los activos de información de la institución.

Los procesos institucionales deben considerar los requerimientos de seguridad de la información, de forma tal que proteja y propicie el cumplimiento de los objetivos institucionales, como las responsabilidades que impone el ordenamiento jurídico, normativa vigente y demás compromisos contractuales adquiridos por la institución.

La Unidad de TI debe establecer mecanismos efectivos para prevenir, detectar, impedir, valorar, evaluar y corregir transgresiones a la seguridad que pudieran generarse al nivel de acceso a sistemas, infraestructura e instalaciones en las que se almacena, procesa y transmite información, previendo que el personal y los proveedores tengan accesos mínimos necesarios para la ejecución de sus funciones; se apliquen controles para proteger la confidencialidad, autenticidad, privacidad e integridad de la información.

La Unidad de TI debe establecer un plan efectivo de capacitación, formación y actualización tecnológica para los funcionarios que se destaquen en este ámbito, el mismo debe contemplar la participación o involucramiento de los usuarios finales, dueños de procesos y responsables de los diferentes procesos y servicios institucionales."

Ese cuerpo normativo también 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.''.

Las Políticas de Seguridad Informática institucionales (octubre 2007) establecen en su apartado 10.14 Política para la elaboración de Planes de Continuidad de la Gestión, lo siguiente*:*

"Los Planes de Continuidad de la Gestión, deben mantenerse en vigencia y transformarse en una parte integral del resto de los procesos de administración y gestión.
La administración de la continuidad de la gestión debe incluir controles, procedimientos, asignación de responsable, pruebas, destinados a identificar y reducir riesgos, atenuar las consecuencias de los incidentes perjudiciales y asegurar la reanudación oportuna de las operaciones indispensables. Adicionalmente como los planes de continuidad de la gestión pueden fallar debido a suposiciones incorrectas, negligencias o cambios en el equipamiento o el personal, debe considerarse dentro de su administración la realización de pruebas periódicas para garantizar que los mismos estén actualizados y son eficaces. Las pruebas también deben garantizar que todos los miembros del equipo de recuperación y demás personal relevante estén al corriente de los planes".

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."

Productos emitidos por la Auditoría

La Auditoría Interna ha elaborado diversos productos relacionados con la seguridad informática y de la información, entre los cuales se encuentran:

- ATIC-072-2017: Evaluación sobre el avance en el Proyecto Modelo de Gobernanza de las Tecnologías de Información y Comunicaciones y de la Seguridad de la Información de la CCSS.

- ATIC-106-2017: Evaluación sobre la gestión del análisis integral de vulnerabilidades y riesgos de la seguridad en tecnologías de Información y comunicaciones ejecutado por la Subárea de Seguridad Informática a través de una contratación directa de servicios profesionales con la Firma Consultora Deloitte & Touche.

- ATIC-83-2018 Evaluación de carácter especial referente al cumplimiento de la Ley No. 8968 Protección de la Persona frente al tratamiento de sus datos personales en la CCSS

- Oficio AD-ATIC-56142-2016: Cambio de política de claves en el Directorio Activo (AD) y su posible impacto en la institución.

- Oficio 47886-2017: Oficio Informativo respecto al marco normativo relacionado con la Privacidad y Confidencialidad de la Información en las Comunicaciones

- Oficio 53581-2017: Observaciones relacionadas con la Seguridad Informática de la Información de los servicios institucionales de Tecnologías de Información y Comunicaciones (TIC) accesados a través de dispositivos móviles.

- Oficio 53708-2017: Aspectos relacionados a la Seguridad Informática de acuerdo con temas abordados en el Convenio de Ciberdelincuencia celebrado en Budapest.

- Oficio AD-ATIC-5021-2018: Oficio de advertencia sobre la vigencia actual de plataforma tecnológica Institucional y la calidad de la información almacenada en el Sistema Contable Bienes Muebles de la Caja Costarricense de Seguro Social.

- Oficio 6441-2018: Oficio sobre el Modelo de Gobierno Institucional para la seguridad de la información.

- Oficio AD–ATIC–8137–2018: Oficio de Advertencia sobre la gestión efectuada en el cumplimiento de los planes remediales para la gestión de vulnerabilidades y riesgos en TIC de la CCSS

- Oficio 292-2019: Oficio sobre aspectos relacionados con la seguridad de la información.

- Oficio AI-2328-2019: Oficio sobre la utilización de dispositivos móviles para la prestación de servicios a los usuarios de los regímenes de seguros y pensiones institucionales,

- AD-ATIC-706-2020: Oficio de advertencia sobre la continuidad de servicios bajo el contexto del evento de interrupción de los servicios tecnológicos a nivel Institucional presentado el 22 de octubre del 2019.

- AD-ATIC-1512-2020: Oficio de advertencia sobre la contingencia de la seguridad informática en el contexto de continuidad del negocio.

- ATIC-166-2020: Evaluación sobre la Plataforma TIC a nivel central.

- ATIC-068-2020: Evaluación sobre la gestión integral del Proyecto denominado “Plan de Ciberseguridad para la Caja Costarricense del Seguro Social”.

Consideraciones finales

La Caja Costarricense del Seguro Social (CCSS), dentro de su gestión y servicios que presta a la ciudadanía depende de la información, sistemas y soluciones tecnológicas que soportan esos procesos, de ahí la necesidad de disponer de un marco de seguridad informática y de seguridad de la información que incluya normativa, políticas, procesos, herramientas y equipos para prevenir y asegurar la disponibilidad de la plataforma tecnológica con capacidades para prevenir y corregir posibles amenazas, incidentes de seguridad y otros a los que está expuesta, considerando la cobertura que tiene a nivel nacional .

Es decir, la Institución en cada uno de los procesos de salud, pensiones y recaudación patronal que tiene a cargo, debe planificar la gestión de continuidad del negocio para evitar que las actividades sustantivas permanezcan ininterrumpidas, por fallas de origen eléctrico, financiero, tecnológico, eventos de seguridad, desastres naturales, entre otros.

En ese sentido, resulta fundamental el significado de la continuidad de negocio y en segunda instancia lo correspondiente a la continuidad de las tecnologías de información y comunicaciones.

Tal y como se ha señalado con anterioridad, la Caja Costarricense del Seguro Social, demanda la alta disponibilidad de los servicios tecnológicos que apoyan los procesos de salud, pensiones y otros, lo cual hace considerar la interrupción presentada el 7 de marzo requiere de un análisis técnico integral de las causas, efectos, activación de planes de contingencia, tanto en el negocio, como en TIC, funcionamiento de los protocolos, aprobados, entre otros. Asimismo, resulta relevante la realización de pruebas y simulacros que permitan mejorar los planes.

El análisis debe incluir la participación que debe tener el nivel estratégico y directivo, así como los mecanismos de comunicación a usuarios, pacientes, colaboradores, y a la prensa. Lo anterior en aras de establecer medidas que garanticen la disponibilidad de los servicios.

Al respecto, la integralidad para la gestión de la continuidad de negocio y las tecnologías de información y comunicaciones deberán minimizar riesgos, orientando esfuerzos de manera articulada, consistente para velar por la velar por la prevención, protección y recuperación ante eventos de interrupción o desastre.

En virtud de lo expuesto, esta Auditoría previene y advierte a la Administración sobre los aspectos mencionados en el presente oficio, con el propósito de evitar que se repitan este tipo de incidentes de seguridad que ocasionaron interrupciones en sistemas institucionales de impacto como lo son EDUS y SICERE, entre otros.

Lo anterior, con el objetivo de enfrentar con éxito los eventos adversos que puedan presentarse, así como coadyuvar al cumplimiento de los objetivos institucionales, garantizando un marco adecuado para el resguardo de la información institucional y de la seguridad informática.

Al respecto, se deberá informar a esta Auditoría Interna sobre las acciones ejecutadas para la administración del riesgo y atención de la situación comunicada, en el plazo de un mes a partir del recibido de este documento.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.04.21 10:20:07 -06'00'

Lic. Olger Sánchez Carrillo.
Auditor Interno

OSC/RJS/RAHM/IMSjfrc

C. Auditoría

Referencia: ID-73648