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

AS-AATIC-113-2022
27 de junio de 2022

Doctor
Roberto Cervantes Barrantes, gerente
GERENCIA GENERAL-1100

Doctor
Randal 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 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 restablecimiento en la operación de sistemas de información y bases de datos.**

Esta Auditoría en cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo para el período 2022 y con fundamento en los artículos N.º 21 y 22 de la Ley General de Control Interno y consecuente al oficio AI-874-2022 del 6 de junio del 2022, en el cual se comunicó el inicio de la evaluación concerniente al ataque cibernético a la CCSS y sus efectos a partir de la desconexión de sistemas de información efectuada el 31 de mayo del 2022, emite la siguiente asesoría sobre el restablecimiento en la operación de sistemas de información y bases de datos.

ANTECEDENTES

Como es ya conocido, la Caja Costarricense de Seguro Social (CCSS), recibió ciberataques que le obligaron a desactivar todos los sistemas informáticos de la Institución de manera preventiva.

Ahora bien, tras cumplirse más de 20 días de ese incidente, la Institución restableció el funcionamiento de algunos sistemas de información, tal y como lo anuncia el medio de comunicación nacional "amprensa" en el titular "CCSS anuncia que su página web y plataforma de pagos ya fueron restablecidas" publicado el 21 de junio del 2022, citando:

> *"Este martes la Caja Costarricense de Seguro Social, CCSS, anunció que la Presidencia Ejecutiva y la Gerencia General agradecían el trabajo realizado que permitió restablecer la página web de la Caja y la plataforma de SICERE.*
>
> *La plataforma de pagos de Sistema Centralizado de Recaudación, SICERE, permite a los patronos mensualmente presentar y facturar planillas.*
>
> *¿Y los otros sistemas?*
> *La Caja ha anunciado que se encuentran trabajando arduamente en restablecer los sistemas pero que irán poco a poco."*

OBSERVACIONES

Así las cosas, esta Auditoría Interna se refiere al argumento citado en el epígrafe, con el objetivo de hacer de su conocimiento las siguientes observaciones que pretenden generar valor agregado a las labores encomendadas. A ese respecto, considerándolas al definir una estrategia para asegurar el restablecimiento paulatino en la operación de sistemas de información institucionales y por supuesto el de sus bases de datos (DB).

- Según las recomendaciones de los expertos, se deberá previo a la recuperación de los servicios tecnológicos, evaluar la exposición al riesgo que podrían tener las credenciales de acceso, tanto para sistemas de información, como bases de datos.

  En ese sentido, al examinar las condiciones de los activos TIC[1] se debe identificar si existe la posibilidad de haber sido comprometidas las credenciales de acceso, de ser así, proceder con el cambio de contraseñas, verificación de perfiles en cada solución de software, y mantenerse alerta ante el riesgo inminente de un ingreso no autorizado a las soluciones informáticas.

  Tal y como lo informa el medio de comunicación español "eldiario.es" en su titular "España pide a los funcionarios que cambien contraseñas y apaguen equipos no esenciales ante la crisis de Ucrania", publicado el 25 de febrero del 2022, donde se cita la siguiente recomendación dictada a nivel de gobierno:

  > *"El Gobierno llama a los trabajadores públicos y diplomáticos a tomar medidas de seguridad "en previsión de posibles ciberataques"*

[1] TIC es la abreviatura de Tecnologías de la Información y la Comunicación.

(…) España ha pedido a sus funcionarios y diplomáticos que cambien sus contraseñas "a la mayor brevedad" y que, en la medida de lo posible, "se proceda al apagado de equipos cuyo encendido sea prescindible durante este fin de semana". En varios comunicados a organismos públicos y embajadas a los que ha tenido acceso el Diario.es, Exteriores, la secretaria de Estado de Administración Digital y el Centro de Operaciones de Ciberseguridad de la Administración General del Estado han recomendado llevar a cabo estas prácticas "en previsión de posibles ciberataques" ante el peligro de que la guerra en Ucrania contagie infecciones informáticas por el continente

(…) "En el marco de actuaciones realizadas para garantizar la seguridad de los sistemas de información del Ministerio, se requiere que realice el cambio de contraseña de su usuario de acceso", solicita uno de los mensajes enviados a altos funcionarios y diplomáticos. "Este cambio es obligatorio y le recomendamos que lo realice voluntariamente a la mayor brevedad", añade: "En caso de no efectuar la actualización voluntaria, ésta expirará en los próximos días".

Así mismo, como oportunidad de mejora se podría implementar el doble factor de autenticación, utilizar accesos seguros, automatizar el proceso correspondiente a cambios periódicos de contraseña, gestionar la política para la inactivación de usuarios, entre otras prácticas en materia de seguridad.

- A criterio de cada responsable de los sistemas de información y procesos de negocio, debe existir una valoración formal sobre la necesidad de digitalizar los datos generados mediante mecanismos contingenciales (en su gran mayoría de forma física) e informar ante el conjunto de involucrados la decisión acordada.

  Un ejemplo de los casos por analizar corresponde a la información gestionada para la atención médica o farmacéutica de usuarios en los centros de salud y que se mantienen utilizando mecanismos contingenciales apartados del registro de datos digital en las aplicaciones de software estandarizadas a nivel institucional. Lo anterior, tal y como cita el periódico "La Nación" el 01 de junio del 2022 a través de la nota "Hospitales de CCSS vuelven a usar expedientes médicos de papel por 'hackeo'", a saber:

  "Los hospitales volvieron a usar el expediente de papel, o físico, como única salida para garantizar la atención básica de miles de asegurados, luego de detectar un intento de hackeo, este martes, que obligó a la Caja Costarricense de Seguro Social (CCSS) a apagar todos sus sistemas, incluido el Expediente Digital Único en Salud (EDUS), donde se registran las consultas médicas de los asegurados

  (…) "Tenemos que retroceder por unos días al papel, esperamos que no mucho, pero le pedimos paciencia a la población en el sentido de que este fue un intento muy violento de vulnerar los sistemas de la Caja y del país, en un proceso que lleva varios días. El diagnóstico de la afectación final solo lo podremos hacer a posteriori", agregó."

  Lo anterior, con el objetivo de evitar brechas en la información guardada en la BD y garantizar la trazabilidad esperada por los usuarios digitales, principalmente en procesos críticos donde es indispensable el historial de atenciones o trámites en materia de salud, pensiones y recaudación patronal.

- Es trascendental examinar detalladamente la información contenida en las bases de datos, con el objetivo de diagnosticar y certificar que los repositorios no tengan una exposición a riesgo descontrolada.

  En ese sentido, esa labor podría ser realizada a través de herramientas de software, técnicas forenses o inclusive el hacking ético, las cuales valoran las intenciones de los cibercriminales al considerar las bases de datos, como un terreno fértil para actividades maliciosas.

  Aunado a lo anterior, se justifica esa labor a raíz del aumento de ataques y posiblemente la reincidencia de intentos por vulnerar las plataformas de la Caja, tal y como lo generaliza la revista "Forbes[2]" en su artículo "Los ciberataques se multiplicaron en el sector médico: cómo deben protegerse las empresas", publicado el 9 de junio del 2022, en el cual cita:

  "La compañía de ciberseguridad Sophos publicó el informe sectorial del Estado del Ransomware 2022, enfocado en las empresas del sector médico, que indica que en 2021 hubo un incremento de 94% en los ataques de ransomware hacia las organizaciones encuestadas en este sector.

  El informe titulado El estado del ransomware en el cuidado de la salud 2022 indica que el 66% de las organizaciones de atención médica se vieron afectadas; de ellas, el 34% también fueron vulneradas en 2020.

  Sin embargo, el lado positivo radica en que las organizaciones de atención médica están mejorando en el manejo de la situación posterior al ataque, según los datos de la encuesta. El informe muestra que el 99% de las organizaciones de atención médica afectadas por el ransomware recuperaron al menos algunos de sus datos."

- Se recomienda que los sistemas operativos, motores de bases de datos y equipos donde se encuentran instalados los aplicativos y BD se encuentren debidamente actualizados y con el soporte por parte del personal técnico, proveedor o fabricante (según corresponda).

  Lo anterior, previendo vulnerabilidades que puedan ser aprovechadas por el cibercrimen. A ese respecto, en la página web del noticiero CNN[3] se publicó la nota "Por qué no deberías de ignorar las actualizaciones de software" publicada el 7 de junio del 2021, refiriéndose a esta tarea, a realizar como parte de la gestión diaria de las TIC de las organizaciones, a saber:

  "Si más de una vez has ignorado las ventanas emergentes que te invitan a instalar una actualización de software en tu computadora o teléfono, esta información te interesa. Y es que si bien, postergar las actualizaciones de software es algo fácil, la realidad es que al no actualizar el software de tus dispositivos electrónicos podrías abrirles una puerta a los hackers para que accedan a tu información privada.

  Según un estudio realizado por la compañía de ciberseguridad Kaspersky en abril de 2021, 50% de las más de 15.000 personas encuestadas, dijo que presionan el botón "recordarme más tarde" al recibir una notificación para actualizar su sistema operativo bajo la justificación de que están ocupadas con otras cosas.

[2] Forbes es una revista especializada en el mundo de los negocios y las finanzas fundada en 1917.
[3] CNN (Cable News Network) es un canal de televisión por suscripción estadounidense de noticias fundado en 1980.

"Actualizar tu sistema operativo puede parecer una molestia para muchos, pero las actualizaciones del sistema operativo no están ahí solo para corregir errores o para habilitar la interfaz más nueva", indica Oleg Gorobets, gerente senior de marketing de productos de Kaspersky en un comunicado, quien dijo que las actualizaciones proveen soluciones para esos errores, que de no aplicarse, pueden abrir una puerta para que entren los ciberdelincuentes.

Kaspersky también encontró que un 22% de usuarios de PC continúan utilizando Windows 7, un software que dejó de recibir soporte general en enero de 2020. "Afortunadamente, el 72% de los usuarios utilizan Windows 10, la última versión del sistema operativo Windows, que parece ser la opción más segura", se lee en un comunicado de prensa.

Gorobets indica que, aunque un sistema operativo parezca funcional, es fundamental realizar estas actualizaciones para protegernos de vulnerabilidades.

(…) Por su parte, la empresa de ciberseguridad McAfee, indica que muchos de los peores ataques de malware se aprovechan de las vulnerabilidades de software en sistemas operativos y navegadores. Por ello, es que recomiendan no postergar las actualizaciones de software, ya que son un paso esencial para proteger la información de los usuarios.

Tanto Kaspersky como McAfee recomiendan habilitar la función de actualización automática, y descargar las actualizaciones de software desde la página oficial del desarrollador."

- En cuanto a información utilizada para la toma de decisiones, es importante generar reportes debidamente oficializados y socializados con las instancias correspondientes, en los cuales brinden los detalles a considerar sobre la temática tratada en esta misiva, entre ellos:

  - Tipo de amenaza que afecta la información contenida en la BD o repositorios locales, origen del software malicioso, fecha de infección inicial, medios de transmisión utilizado, entre otros aspectos para ser valorados.
  - Pormenorizar si los datos fueron cifrados, alterados, robados, copiados, entre otras variantes.
  - Certificar la revisión e inmunización de equipos, esto previo al restablecimiento de sistemas de información y bases de datos.
  - Especificar o certificar las acciones llevadas a cabo en equipamiento e información afectada por ransomware[4].
  - Referenciar sí se está accionando conforme al plan de continuidad del negocio, contingencia, recuperación, entre otros; con el objetivo de orientar a los interesados sobre el nivel de madurez de la organización y/o la etapa en la cual se encuentra la atención del incidente de ciberseguridad.
  - Explicar el plan de acción llevado a cabo actualmente, las mejoras a futuro para remediar o minimizar la exposición al riesgo.

  Lo anterior, para cada repositorio de los diferentes sistemas de información de la Caja.

[4] El ransomware es una forma de malware que está en auge; bloquea los archivos o dispositivos del usuario y luego reclama un pago online anónimo para restaurar el acceso.

- Finalmente, este Ente Fiscalizador hace recordatorio de las observaciones que pueden ser estimadas para desarrollar una estrategia alineada al restablecimiento en la operación de sistemas de información y bases de datos, concretamente al considerar las reseñas emitidas en los productos:

  - AS-AATIC-072-2022 del 10 de junio del 2022, sobre la gestión de crisis
  - AS-AATIC-088-2022 del 16 de junio del 2022, referente a la continuidad del negocio
  - AS-AATIC-108-2022 del 22 de junio del 2022, referente a estrategia de recuperación ante amenazas o desastres de origen tecnológico.

CONSIDERACIONES FINALES

Ante el ciberataque perpetrado en la Institución, se debe expandir su capacidad de garantizar seguridad sobre el restablecimiento de servicios tecnológicos, entre ellos, los correspondientes a la puesta en operación de sistemas de información y sus respectivas bases de datos.

Aunado a lo anterior, fortalecer la defensa contra el ransomware al combinar la tecnología de seguridad con la búsqueda de amenazas. En ese sentido, esta misiva incluye observaciones para incentivar la implementación de valoraciones de alta calidad, reforzar el entorno TIC buscando y cerrando brechas.

Es decir, complementando esa premisa con la seguridad de haber mitigado los riesgos materializados en los dispositivos y/o redes informáticas, al instalar las actualizaciones correspondientes y soluciones de protección especializadas, necesarias de forma preliminar para determinar si es el momento de proceder con el restablecimiento de servicios tecnológicos en un ambiente controlado.

Finalmente, habiendo examinado los aspectos de ciberseguridad citados, se debe proceder a la valoración por parte de cada estructura organizacional, la directriz a seguir para la migración de información generada en los mecanismos contingenciales (durante la interrupción de servicios tecnológicos) a las bases de datos vinculadas a sus respectivos sistemas de información estandarizados para apoyar los procesos sustantivos de la Institución.

Bajo ese contexto, en acatamiento a lo indicado en las Normas técnicas para la gestión y el control de las Tecnologías de Información emitidas por el Ministerio de Ciencia, innovación, Tecnología y Telecomunicaciones (MICITT), 2021, apartado “Continuidad y Disponibilidad Operativa de los Servicios Tecnológicos”, donde cita:

> *“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."

Todo lo anterior, con el objetivo de ser resilientes y generar confianza en los servicios que obtienen apoyo por parte de las TIC, manteniendo la continuidad de las operaciones, pese al costo en inversión necesaria para prever este tipo de eventos (mínimo, en comparación a una nueva materialización del riesgo).

En virtud de lo mencionado, esta Auditoría hace de conocimiento de esa Administración los aspectos mencionados en la presente, con el objetivo de incentivar la capacidad de la Institución para recuperar y restablecer el componente TIC 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: 2022.07.04 11:49:37 -06'00'

Lic. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/OMG/lbc

C. Ingeniero Esteban Zúñiga Chacón, jefe, CGI, Gerencia Médica-2901
Ingeniero Alexander Solís Abarca, jefe, CGI, Gerencia Financiera -1103
Ingeniera Giselle Tenorio Chacón, jefe, CGI, Gerencia Administrativa-1104
Ingeniero Roy Armando Ovares Valerio, jefe, CGI, Gerencia Logística -1106
Ingeniero Giovanni Campos Alvarado, jefe, CGI, Gerencia de Infraestructura y Tecnologías-1107
Ingeniero Eithel Giovanni Corea Baltodano, jefe, CGI, Gerencia de Pensiones- 9108
Auditoría