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

AD-AATIC-067-2022
31 de mayo de 2022

Doctor
Roberto Cervantes Barrantes, gerente
GERENCIA GENERAL- 1100

Máster
Roberto Blanco Topping, subgerente a.i

Máster
Mayra Ulate Rodriguez, jefe
Área de Seguridad y Calidad Informática
DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES U.P. 1150

Estimados(a) señores(a):

ASUNTO: Oficio de Advertencia sobre la exposición reciente a ataques cibernéticos a la CCSS.

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, esta Auditoría advierte sobre aspectos relacionados con la exposición a ataques cibernéticos en la Institución.

Lo anterior, al ser de nuestro conocimiento el hackeo detectado la madrugada de este martes 31 de mayo en la Institución y el cual obligó a desactivar todos los sistemas informáticos de la entidad de manera preventiva.

ANTECEDENTES

Como ya es conocido Costa Rica no se encuentra exenta de ser objeto de ataques que buscan afectar, alterar, extorsionar o destruir no solo la reputación de las empresas o personas, sino también, impactar negativamente su operación o relación con los diferentes grupos de interés.

En ese sentido, recientemente se ha conocido múltiples ataques pertenecientes a la familia de los ransomware[1] y que utiliza la modalidad de extorsión con sus víctimas, según describe la nota periodística "*Grupo Conti asegura haber hackeado Ministerio de Hacienda y contar con 1 terrabyte de información de contribuyentes"* publicada por el diario La República el 18 de abril del 2022, se indicó:

> *"El grupo cibercriminal Conti, fundado en Rusia, asegura haber hackeado los sitios web del Ministerio de Hacienda y contar con 1 terrabyte de información de contribuyentes.*

[1] El ransomware es un tipo de código malicioso que secuestra su información para extorsionarlo y exigirle el pago de una suma de dinero, ya sea para recuperarla o para evitar su divulgación. **Fuente**: Página Web de ESET.

Así lo dieron a conocer a través de la red social de microblogging Twitter, donde señalan que comenzarán a exponer los datos a partir del 23 de abril.
Las plataformas que se habrían visto comprometidas son la TIC@, que utilizan importadores y exportadores nacionales, además de las agencias aduanales y el ATV, donde los grandes y pequeños contribuyentes deben presentar sus declaraciones de impuestos de la renta, de ventas, entre otras obligaciones fiscales.

A pesar de que el ataque informático trascendió hasta el día de hoy, se habría realizado desde ayer domingo de Resurección o Pascua, cuando la mayoría de personal del Gobierno y sector privado se encontraban libres producto de la celebración de la Semana Santa"

Posteriormente, se publicó ese mismo día una nota titulada "*Hackers piden $10 millones al Gobierno de Costa Rica por información del ministerio de Hacienda*", en el diario supracitado, donde se menciona:

"El grupo de hackers de origen ruso Conti, piden $10 millones al Gobierno de Costa Rica por la información sustraída aparentemente de los sitios web del ministerio de Hacienda.

Pedimos solo 10 millones de dólares por mantener los datos de sus contribuyentes" señala una publicación de la cuenta BetterCyber en Twitter, donde se reproduce el mensaje de los ciberdelincuentes, los cuales aseguran contar con 1 terabyte de información.
El ataque informático habría sido del tipo "Ransomware" que restringe el acceso a archivos de un sistema infectado al codificarlos y solicitar dinero a cambio de revertir esta situación."

No obstante, los ataques cibernéticos se seguían materializando a nivel país, en este caso afectando al Ministerio de Ciencia Tecnología y Telecomunicaciones (MICITT) tal y como lo informa la página web "*el mundo cr*" mediante la nota "*Ataque cibernético de últimas horas a entidades públicas es «un hecho sin precedentes», asegura exministro del MICITT*" del 19 de abril de 2022, citando:

"El exministro del Ministerio de Ciencia Tecnología y Telecomunicaciones (MICITT), y experto en ciberseguridad Luis Adrián Salazar, aseguró que «estamos ante un hecho sin precedentes», ante los ataques cibernéticos de las últimas horas a entidades públicas.

Según manifestó Salazar «a partir de los acontecimientos con el posible potencial hackeo del Ministerio de Hacienda y viendo el hackeo menor del Ministerio de Ciencia Tecnología y Telecomunicaciones consideró que este tema debe ser tratado de manera inmediata con la mayor atención posible del máximo nivel».

El experto señaló que «espero equivocarme estamos ante un hecho sin precedentes y es fundamental que se tomen las acciones necesarias y de manera colaborativa entre sector público y privado se analice esta situación, pues podría tener una magnitud muy importante».

De igual forma, agregó que «con pasar del tiempo y pues la digitalización de sistemas de información es total y completamente posible que los ataques hacia infraestructura crítica de los gobiernos sean objetivo de los ciberataques, estoy hablando de sistemas de información, estoy hablando de sistemas de energía, estoy hablando de diferentes tipos de infraestructura crítica».

«Aquí es importante mencionar que Costa Rica ha tenido avances importantes, se tiene un clúster de ciberseguridad, existe una estrategia de ciberseguridad se ha trabajado en alianzas internacionales, pero creo sin duda que todavía no existe la conciencia de que el tema de ciberseguridad debe priorizarse como política nacional», resaltó."

Aspecto que a la fecha aún afecta a la Institución, cumpliendo un mes y medio del ataque sufrido por parte de la banda de cibercriminales Conti, inclusive llevó al país a publicar una declaratoria de emergencia nacional sin precedentes. Lo anterior, tal y como se comentó en el programa de televisora de Costa Rica "Estado Nacional" trasmitido el pasado 29 de mato refiriéndose al tema "Hacienda bajo ataque".

En esa misma línea, pero en el en el caso particular de la CCSS, el diario La República informó el 19 de abril del 2022, la nota "Hackeo a cuenta de Twitter de la CCSS y sitio alterno del MICITT se unen al del ministerio de Hacienda", informando:

"En el caso de la cuenta de CCSS en la red de microblogging se publicaron varios mensajes de unos ciberdelincuentes que promocionaban la rifa de 5 mil bitcoins, pero la misma fue recuperada minutos después por el equipo informático de la institución."

Finalmente, *el diario La Nación el 20 de abril del 2022, informa "Portal de Recursos Humanos de CCSS sufre ataque cibernético", citando:*

"Las plataformas digitales de las entidades públicas siguen siendo objeto de ataques cibernéticos. La Caja Costarricense de Seguro Social (CCSS) sufrió este miércoles una incidencia en su portal de Recursos Humanos, que obligó a activar una revisión integral de todos sus sistemas para determinar el alcance de lo ocurrido.

El ingeniero Roberto Blanco Topping, director de Tecnologías de Información de la CCSS, detalló que una vez detectado el problema se procedió a blindar los accesos, dar de baja el portal y coordinar con los equipos técnicos para determinar si se produjo alguna extracción de información o de datos, o eventuales accesos a otras plataformas.

"Los equipos de monitoreo, humanos y en conjunto con las herramientas tecnológicas con las que se cuenta detectaron incongruencias con respecto a la gestión de datos en el portal de Recursos Humanos de la institución y se determinó que se había producido un ataque externo", detalló mediante un comunicado.

Blanco agregó que en este momento se encuentran en un proceso de análisis para determinar cuál fue el impacto y los pasos a seguir."

Finalmente, el día de hoy se dio a conocer un nuevo hackeo, según la publicación del diario "*La Nación*", titulado "*Nuevo 'hackeo' en CCSS afecta atención en hospitales y Ebáis por desactivación del EDUS*", a saber:

"La Caja Costarricense de Seguro Social (CCSS) sufrió un nuevo hackeo la madrugada de este martes 31 de mayo, el cual obligó a desactivar todos los sistemas informáticos de la entidad de manera preventiva, lo que afectará la atención de pacientes en los servicios de

hospitales, clínicas y Ebáis, debido a la desactivación del Expediente Digital Único en Salud (EDUS)(…)
El director de la Dirección de Tecnologías de Información y Comunicaciones, Roberto Blanco Topping, aseguró en un comunicado de prensa que las bases del EDUS, el Sistema Centralizado de Recaudación (SICERE), planillas y pensiones no se vieron comprometidas con el ataque cibernético.

Agregó que los equipos técnicos de la institución trabajan para tratar de restaurar servicios críticos. Blanco aclaró, sin embargo, que no es posible precisar aun cuando estarán en operación.

Estamos trabajando con todo el equipo especializado para determinar el curso y cómo levantar los sistemas críticos", dijo el funcionario."

Así mismo, en esa publicación se ejemplifica la afectación en los servicios tecnológicos que brinda la CCSS, citando:

"Varios directores de hospitales consultados por La Nación prevén retrasos en las atenciones programadas, pero aseguran que hacen lo posible para garantizar a los pacientes su cita o procedimiento. En principio, están utilizando expedientes físicos, o de papel, para asegurar la atención, confirmaron en los hospitales Nacional de Niños, San Vicente de Paúl (Heredia), San Rafael (Alajuela) y San Carlos. (…)".

Algunos pacientes y funcionarios confirmaron a La Nación los problemas en los servicios en las primeras horas de esta mañana, sobre todo porque los centros de salud han tenido que recurrir al uso de expedientes de papel para garantizar la atención programada.

(…) El director del Hospital San Carlos, Édgar Carrillo Rojas, confirmó a La Nación que también ahí se apagaron todos los equipos por indicación del nivel central de la CCSS.

"Entre las medidas de contingencia básicas se les envió un mensaje a todas las jefaturas de no encender las computadoras. La atención de la consulta de emergencias y externa (citas con médicos especialistas) se hará con expediente físico. En la parte quirúrgica también se tendrá que 'hacer a pie', con expediente físico. Esto, evidentemente, ocasionará un retraso en la atención y una sobrecarga de trabajo para el personal de Archivo, principalmente.

"El mensaje para nuestros asegurados es que por favor comprendan que es una situación de emergencia y que, por ende, mucho de sus procedimientos se verán atrasados. De igual forma, no podemos usar las plataformas que utilizamos para el ordenamiento de pacientes en la atención de emergencias", explicó Carrillo.

Por su parte, la directora médica del Hospital San Vicente de Paúl, en Heredia, Priscilla Balmaceda, dijo que han tenido que suspender algunas citas en laboratorio.

"Estamos trabajando desde buena mañana para ver cómo nos organizamos en los servicios. No podemos encender las computadoras y la situación es complicada; sin embargo, estamos tratando de organizar la atención de los pacientes usando hojas físicas tanto en Emergencias como en hospitalización y Consulta Externa. Estamos avisando por sonido que podemos tener atraso en la atención porque estamos 'a pie'.

"En el caso de laboratorio, tuvimos que suspender algunas citas en la mañana porque tampoco tenemos acceso al sistema de laboratorio y estamos haciendo un levantamiento de los casos para reprogramar después", dijo Balmaceda quien aseguró, a las 7 a . m., que aún no tienen claridad sobre el alcance de la situación."

Productos emitidos por la Auditoría Interna

Si bien es cierto la Caja ha formulado acciones relacionadas al tema, este Ente Fiscalizador ha sido insistente en diferentes momentos para señalar a la Administración las oportunidades de mejora relacionadas con la disponibilidad de estrategias avanzadas de ciberseguridad, previo a la materialización del riesgo y recientemente dando énfasis a las consideraciones pertinentes bajo el contexto actual.

Por ejemplo, la temática antes indicada ha sido señalada mediante los siguientes productos:

Cuadro No.1
Productos emitidos Auditoría Interna sobre Seguridad de la TIC y ciberseguridad

Informe / Oficio No.	Fecha	Asunto
Informe de Auditoría ATIC-049-2014	09 de mayo de 2014	Gestión de la seguridad de la información institucional y el rol que cumple el Área de Seguridad y Calidad informática.
Informe de Auditoría ATIC-127-2015	15 de junio de 2015	Avance en proyectos de adquisición e implementación de software y hardware de seguridad informática.
Informe de Auditoría ATIC-45-2016	4 de abril de 2016	Fortalecimiento de la infraestructura de seguridad en Tecnologías de Información y Comunicaciones.
Oficio 47886-2017	14 de febrero de 2017	Oficio Informativo respecto al marco normativo relacionado con la Privacidad y Confidencialidad de la Información en las Comunicaciones.
Informe de Auditoría ATIC-72-2017	9 de agosto de 2017	Avance del proyecto modelo de gobernanza de las tecnologías de información y comunicaciones y de seguridad de la información de la Caja Costarricense de Seguro Social (CCSS).
Oficio 53581-2017	22 de agosto de 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	6 de septiembre de 2017	Aspectos relacionados a la Seguridad Informática de acuerdo con temas abordados en el Convenio de Ciberdelincuencia celebrado en Budapest.
Informe de Auditoría ATIC-106-2017	29 de septiembre de 2017	Gestión del análisis integral de vulnerabilidades y riesgos de la seguridad en tecnologías de información y comunicaciones ejecutado por la Dirección de Tecnologías de Información y Comunicaciones a través de una contratación directa de servicios profesionales a la Firma Consultora Deloitte & Touche.
Oficio 6441-2018	13 de abril de 2018	Observaciones relacionadas con el Gobierno de Seguridad de la Información.
Informe de Auditoría ATIC-83-2018	23 de julio de 2018	Cumplimiento de la Ley No. 8968 "Protección de la Persona Frente al Tratamiento de sus Datos Personales" y su reglamento en la Caja Costarricense de Seguro Social (CCSS).
Oficio AD–ATIC–8137–2018	24 de septiembre de 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 No. 9125	8 de octubre de 2018	Resultado informe denominado "Evaluación de carácter especial sobre la gestión efectuada en el cumplimiento de los planes remediales del Análisis Integral de Vulnerabilidades y Riesgos en TIC de la CCSS.
Oficio No. 11069	20 de diciembre de 2018	Oficio de información sobre aspectos relacionados con la Seguridad de la Información Institucional". (Se resume un conjunto de productos realizados por este Ente Fiscalizador referente al tema).
Informe de Auditoría ATIC-246-2018	21 de diciembre de 2018	Gestión de la Gerencia de Pensiones en el cumplimiento a las Normas de Seguridad Informática Institucional.

Informe / Oficio No.	Fecha	Asunto
Oficio AI-2328-2019	9 de agosto de 2019	Dispositivos móviles institucionales.
Oficio AD-ATIC-271-2020	5 de febrero de 2020	Controles de acceso y niveles de seguridad en equipos de tecnologías de información y comunicaciones (TIC).
Oficio 292	15 de febrero de 2019	Aspectos relacionados con seguridad de la información. (Se resume un conjunto de productos realizados por este Ente Fiscalizador referente al tema)
Oficio AD-ATIC-706-2020	16 de marzo, 2020	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-896-2020	22 de abril de 2020	Controles de acceso y niveles de seguridad en equipos de tecnologías de información y comunicaciones (TIC).
AD-ATIC-1239-2020	20 de mayo de 2020	Controles de acceso y niveles de seguridad en equipos de tecnologías de información y comunicaciones (TIC).
AD-ATIC-1322-2020	25 de mayo de 2020	Controles de acceso y niveles de seguridad en equipos de tecnologías de información y comunicaciones (TIC).
AD-ATIC-1512-2020	29 junio de 2020	Oficio de advertencia sobre la contingencia de la seguridad informática en el contexto de continuidad del negocio.
AS-ASTIC-1849-2020	23 de julio del 2022	Oficio de asesoría respecto a la seguridad cibernética (ciberseguridad) ante la pandemia producida por el COVID-19.
AS-ATIC-2062-2020	13 de agosto del 2020	Oficio de asesoría respecto al uso de VPN en la CCSS.
AI-202-2021	28 de enero del 2021	Oficio que refiere a los resultados de una revisión sobre el tema de “Amenazas de Correo Electrónico”, con el objetivo de fortalecer el uso del correo electrónico bajo los principios de eficiencia, eficacia, ordenamiento jurídico y técnico.
AI-573-2021	11 de marzo del 2021	Oficio respecto a vulnerabilidad en Microsoft Exchange Server
AI-608-2021	15 de marzo del 2021	Oficio en el cual se emiten recomendaciones ante la exposición al ataque cibernético denominado “Solar Winds”
AS-ATIC-674-2021	24 de marzo del 2021	Oficio de Asesoría que refiere a las tendencias de mercado TIC para el 2021 y preparación tecnológica de la CCSS
AD-ATIC-1806-2021	26 de agosto del 2021	Oficio de Advertencia referente a evento presentado respecto de la visualización de imágenes médicas en el Hospital Nacional de Niños.
AD-ATIC-1930-2021	9 de setiembre del 2021	Oficio de Asesoría referente a la Gobernanza de Tecnologías de Información y Comunicaciones (TIC) y Seguridad de la Información en la Caja Costarricense de Seguro Social.
AS-ATIC-2298-2021	1 de noviembre del 2021	Oficio de Asesoría respecto a los tipos de amenazas que afectan a las organizaciones por medio del accionar de los ciberdelincuentes.
AS-ATIC-2313-2021	1 de noviembre del 2021	Oficio de Asesoría referente a mecanismos de control en TIC para garantizar continuidad de los servicios de salud apoyados mediante imágenes médicas.
AS-ATIC-2503-2021	30 de noviembre del 2021	Oficio de asesoría respecto a la preparación de los sistemas de información para la prevención al fraude.
AS- ATIC-052-2022	8 de abril del 2022	Oficio de Asesoría que refiere a las tendencias de mercado TIC para el 2022 y preparación tecnológica de la CCSS
AD-ATIC-038-2022	21 de abril del 2022	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.
AD-ATIC-039-2022	21 de abril del 2022	Oficio de advertencia sobre la exposición a ataques cibernéticos a la CCSS.
AD-ATIC-046-2022	3 de mayo del 2022	Oficio de Advertencia referente a la priorización de la ciberseguridad en la Caja Costarricense del Seguro Social.

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."

OBSERVACIONES

Así las cosas, es menester de este Órgano Fiscalizador hacer un recordatorio a esa Administración sobre la importancia que reviste al tema, máxime considerando los ataques cibernéticos reincidentes y reiterativos a las plataformas tecnológicas de la Institución.

A continuación, se presentan observaciones que fueron detalladas en los oficios AS- ATIC-052-2022, AD-ATIC-038-2022, AD-ATIC-039-2022, AD-ATIC-046-2022, todos relacionados con la ciberseguridad en la institución y a criterio de la Auditoría la Administración se debe revisar constantemente en el contexto actual, con el objetivo de establecer la priorización necesaria en el abordaje del tema:

- Es importante se considere la necesidad inminente de implementar estrategias y priorizar esfuerzos que coadyuven en la materialización de acciones y disposición de herramientas con la capacidad de contrarrestar la táctica de ataque guiada por los cibercriminales, los cuales buscan enganchar al mayor número de víctimas.

- Sobre el cumplimiento de políticas, normas, protocolos y directrices se debe velar en el estricto acatamiento de la directriz N° 133- MP-MICITT, Normas Técnicas para la gestión y el control de las Tecnologías de Información, Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, 2021; Ley y Normas de Control Interno para el Sector Público; Normas Institucionales de Tecnologías de Información; Políticas Institucionales de Seguridad Informática, TIC-Seguridad-001, Versión 1.0 de octubre 2007; Normas Institucionales de Seguridad Informática, TIC-ASC-SEG-0002, Versión 1.0 de abril 2008.

  Asimismo, considerar las buenas prácticas publicadas en marcos de referencia, por ejemplo: Norma de Gestión de Seguridad de la Información ISO/IEC 27001; Marco referencial COBIT 5 (Objetivos de Control para las Tecnologías de Información), marco de ciberseguridad NIST (acrónimo de Instituto Nacional de estándares y tecnología, en inglés), entre otros.

- En materia de seguridad es innegable la premisa de monitorear los activos tecnológicos de la institución, equipo, red software e información, entre otros por lo que disponer de una primera línea de defensa dedicada en tiempo completo contra cualquier incidente o intruso resaltará la función de buscar detectar y evitar ataques de forma proactiva sin afectar la contingencia y continuidad de los servicios.

- Respecto a los planes de continuidad, contingencia y/o de emergencia en el ámbito tecnológico y de negocio, es apremiante generar conciencia sobre el propósito e impacto que tienen ante un siniestro.

  Aunado a ello, se debe fortalecer la arquitectura de la plataforma tecnológica institucional que pretende asegurar la prestación de servicios conforme a criterios de disponibilidad, confiabilidad y seguridad de la información en todos los sistemas institucionales críticos, a partir del desarrollo de los entornos lógico, físico, geográfico y tecnológico necesarios.

- En virtud de la complejidad que rodea el tema de ciberseguridad y el nivel de especialización para formar profesionales expertos en la materia, la Institución debe gestionar según corresponda la participación de contratistas o terceros en la búsqueda de soluciones o acompañamiento en la implementación de soluciones aptas a las necesidades de los usuarios y bajo los criterios de oportunidad, confiabilidad, seguridad, entre otros.}

  En línea con lo anterior, podría ser necesario la contratación de servicios profesionales que puedan coadyuvar con la Institución a establecer estrategias y planes técnicos para mitigar los riesgos en materia de ciberseguridad; en ese sentido, deberá justificarse bajo el amparo del marco normativo que corresponda.

  Ahora bien, de manera gratuita se puede solicitar la retroalimentación de empresas líderes en ciberseguridad (nacional e internacional), expertos a nivel nacional (sector público y privado), suscripciones a revisas de investigación, entre otras fuentes que brinden criterios sobre el conjunto de actividades a realizar de forma preventiva y correctiva ante los ataques o interrupciones sufridos en la institución.

- A nivel técnico nos permitimos reiterar algunas recomendaciones básicas como identificar los activos críticos que necesitan protección inmediata; mantener actualizado el software vinculado a la plataforma tecnológica principal y equipamiento local; mantenerse informado de las vulnerabilidades descubiertas en hardware o software y las cuales puedan ser objeto de fallo en la seguridad informática; verificar la eficiencia y eficacia de los planes de emergencia establecidos a nivel institucional; utilizar los mecanismos de comunicación aprobados y mantener a los equipos de trabajo informados y capacitados sobre cómo atender los temas relacionados a ciberseguridad.

  Por otra parte, generar informes expeditos con el análisis de la causa impacto y reactivación correspondiente; previo al restablecimiento en servicios afectados verificar la eliminación de rastros secundarios del ataque.

- Ante el tipo de ataque ransomware, se debe asegurar a todos los equipos y sus sistemas operativos bajo la premisa de mantenerlos actualizados con los últimos parches de seguridad, evitar aplicaciones qué se tornen innecesarias y que puedan generar dudas en su origen.

En línea con lo anterior implementar factores de doble autenticación en todos los aplicativos que manejan información sensible con el fin de evitar una exposición innecesaria de accesos o privilegios a los datos.

- Considerando que la Institución ha tenido eventos similares, es necesario hacer una revisión y análisis de las actuaciones previas y posteriores a los incidentes presentados, con el propósito de generar lecciones aprendidas en torno a la gestión y tratamiento de este tipo de situaciones, de igual manera retroalimentarse de la experiencia de han sufrido otras instituciones públicas de Costa Rica.

  Es decir, estimular el análisis de las oportunidades de mejora, así como la evaluación de procesos asociados a la seguridad, principalmente considerando entre otros la capacidad de reacción y de prevención, así como el nivel de madurez en esta materia.

- Proyectar y gestionar inversión en seguridad es rentable para responder de forma ágil ante los incidentes mencionados en esta misiva, esto acompañado de iniciativas de investigación referentes a tendencias tecnológicas como Cibersecurity Mesh (malla de seguridad), Zero Tr[2]ust, entre otras con un enfoque moderno de la arquitectura de seguridad que permita a las empresas implementar y ampliar las medidas donde más las necesita.

- Considerar dentro del plan de acciones a ejecutar, el notificar a las instancias correspondientes la posible amenaza directa a la vida de los costarricenses, en virtud de la afectación que se ha tomado de forma preventiva y/o correctiva de los sistemas informáticos utilizados para la prestación de servicios médicos.

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, de ahí la necesidad de disponer de un marco de seguridad informática y de seguridad de la información apegado a la normativa, políticas, procesos, herramientas y equipos para prevenir y asegurar la disponibilidad de la plataforma tecnológica.

Bajo ese contexto, la CCSS no ha sido la excepción y está en un punto donde no hay retorno, la creciente tendencia hacia la digitalización y aumento de ciberataques se ha hecho presente en el país, en ese sentido, se impactó a la Institución y se ha hecho evidente en los diferentes procesos Institucionales, esto como reflejo del ataque de los cibercriminales y/o medidas preventivas o correctivas gestionadas por la Institución.

Ante ello, se debe resaltar la premisa de brindar continuidad al negocio y de las TIC para evitar que las actividades sustantivas permanezcan ininterrumpidas, por fallas de origen tecnológico, en este caso ocasionado por eventos de seguridad, así como activar medidas de contingencia a la altura de las necesidades de los usuarios y posibilidades de la Caja.

[2] Modelo de seguridad de red basado en la filosofía de que ninguna persona o dispositivo dentro o fuera de la red de una organización debe tener acceso para conectarse a sistemas o servicios de TI hasta que se autentique y se compruebe constantemente.

Es decir, incentivando el establecimiento de sistemas de gobernanza TI, mejora continua de los procesos y la modernización de las arquitecturas tradicionales de seguridad, de manera que se asegure un seguimiento adecuado de los niveles de acceso de una red y evitar intrusos con objetivos definidos para identificar debilidades o dejar señuelos para luego retomar sus ataques.

Para tales efectos, se destacan las observaciones inmersas en este oficio, así como los pronunciamientos emitidos por esta Auditoría en los diferentes productos relacionados a la temática, para que a nivel estratégico, táctico, operativo se minimicen riesgos. Aunado a generar esfuerzos de manera articulada y consistente para velar por la prevención, protección y recuperación ante eventos de interrupción o desastre.

En virtud de lo expuesto, se previene y advierte a esa Administración con el propósito de que se adopten las medidas pertinentes, a fin de contribuir con la divulgación de información contemplada en este oficio y así contribuir en la mitigación de vulnerabilidades, las cuales deben ser sometidas a valoración y revisión según corresponda. 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: 2022.06.01 10:02:00 -06'00'

Lic. Olger Sánchez Carrillo
Auditor

OSC/RAHM/OMG/lbc

C. Doctor Randal Álvarez Juárez, gerente, Gerencia Médica-1100
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 Tecnología - 1107
Licenciado Jaime Barrantes Espinoza, gerente, Gerencia de Pensiones-9108
Auditoría