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

AS-AATIC-072-2022
10 de junio de 2022

Doctor
Álvaro Ramos Chaves, presidente
PRESIDENCIA EJECUTIVA-1102

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 TECNOLOGÍA-1107

Licenciado
Jaime Barrantes Espinoza, gerente
GERENCIA DE PENSIONES-9108

Máster
Roberto Blanco Topping, subgerente a.i.
DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES-1150

Licenciada
Xinia Fernández Delgado, directora
DIRECCIÓN DE COMUNICACIÓN ORGANIZACIONAL- 1115

Ingeniera
Susan Peraza Solano, directora
DIRECCIÓN DE PLANIFICACIÓN INSTITUCIONAL- 2902

Estimados(as) señores (as):

ASUNTO: Oficio de Asesoría sobre la gestión de crisis en materia de ciberseguridad como resultado del ataque cibernético ocurrido el 31 de mayo del 2022.

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, se asesora sobre los siguientes aspectos que refieren a la gestión de crisis en materia de ciberseguridad.

ANTECEDENTES

Términos y definiciones

Por crisis se entiende cualquier circunstancia, deliberada o fortuita, ocasionada internamente o no, que produce un desequilibrio en una organización y cuando sucede genera impacto y su efecto perdura en el tiempo, sin ser la excepción lo correspondiente a ciberseguridad.

En ese sentido, la gestión de todo tipo de crisis es una disciplina que ha tenido un significativo desarrollo en la última década y desde muy distintos campos, particularmente los relacionados con la seguridad de la información. Ahora bien, al tratarse de situaciones de especial gravedad, que puede llegar a comprometer, no solo el funcionamiento de la organización, sino incluso su futuro; por ello, esa práctica ha pasado a ser una capacidad imprescindible para un número creciente de organizaciones.

Por ejemplo, en el diario español la “Vanguardia” se publicó el 15 de febrero del 2018, la nota “Una cibercrisis global es posible y las empresas deben prepararse”, refiriéndose a los ciberataques cometidos a nivel internacional y que han provocado la caída de todos o muchos de sus sistemas informáticos, aspecto que podría considerarse como una crisis, pero más allá de esa apreciación, resalta la responsabilidad de un país y de la organización por gestionar lo correspondiente, a saber:

"La gran amenaza en internet no son los ciberdelincuentes ni grupos aislados de cibercriminales sino "los gobiernos", que son los que contarían con los recursos y la sofisticada organización que requeriría un plan para hacer caer millones de ordenadores en el mundo, ha añadido Ramírez.

El director de Seguridad de Gas Natural Fenosa, José Luis Bolaños, ha advertido de la falta de "preparación" que existe en general en las empresas para afrontar las nuevas cibercrisis que acechan, con amenazas mucho más sofisticadas de las que ha habido hasta ahora dada la rapidez con la que la información se despliega en una red de internet "sin fronteras ni leyes".

En ese contexto, existen fuentes de conocimiento que proponen cuáles podrían ser los recursos más adecuados para las organizaciones, con el objetivo de desarrollar metodologías o protocolos enfocados en apoyar al negocio y las TIC ante la posible crisis causadas por la materialización de ataques cibernéticos, dirigidos por 'hackers', quienes amenazan con alterar documentos valiosos o hacer mal uso de estos.

Contexto institucional

El 31 de mayo del 2022 se dio a conocer un nuevo hackeo, según la publicación del diario "La Nación", titulado "Nuevo 'hackeo' en CCSS afecta atención en hospitales y EBAIS 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 (…)"

Ese mismo día, las autoridades de la Caja Costarricense de Seguro Social (CCSS) informan formalmente a la prensa que el hackeo registrado fue "excepcionalmente violento" y el Dr. Alvaro Ramos Chaves, presidente ejecutivo de la Institución, hizo el siguiente llamado ante la situación de marras, citando:

"Pedimos paciencia porque tenemos mucho trabajo por delante. La gente razonablemente se ha acostumbrado a la agilidad con la que podemos hacer las cosas cuando tenemos recursos digitales, pero tendremos que recurrir por unos días al papel. Este fue un intento muy violento de vulnerar bases de datos, los sistemas de la Caja, tenemos que pedir paciencia en ese sentido."

En línea con lo anterior, el Dr. Ramos insistió en que no fueron los hackers los que cerraron las bases de datos ni apagaron los sistemas, mencionando la medida tomada a nivel interno de la CCSS:

"Fuimos nosotros mismos, eso que quede muy claro, para que los hackers no pudieran acceder a ella. Naturalmente no tenemos certeza absoluta de que no haya exfiltración de una parte parcial de estos datos, pero estamos bastante confiados en que no fue así. Nuestros datos preliminares es que no pudieron sacar esa información, con una investigación profunda terminaremos de saberlo con certeza."

No obstante, el 2 de junio del 2022, se dio a conocer la noticia "'Hackers' infiltraron la CCSS desde febrero" publicada por el diario la Nación, donde se amplía con mayor precisión la afectación dada en el equipo tecnológico de la CCSS y la eventual respuesta al restablecimiento de los servicios, citando:

"Todos los indicios apuntan a que los hackers empezaron a gestar su ciberataque a los sistemas de la Caja Costarricense de Seguro Social (CCSS) desde febrero, pues, desde ese mes, en la llamada Internet oscura ("dark web"), comenzaron a ofrecer accesos a los sistemas informáticos de la entidad, reveló el presidente ejecutivo, Álvaro Ramos Chaves, al admitir que el daño es mayor al que calcularon el martes.

Se sospecha que el "software" hostil que inyectaron los extorsionadores entró por alguna terminal o computadora y logró infectar a otras 9.000 (22%) de las 40.000 unidades que tiene la institución. También logró penetrar no a 30, como se dijo inicialmente, sino a 800 servidores (53%) de los 1.500 que tiene la CCSS y, ya una vez adentro, asestó el zarpazo final este 31 de mayo cuando se activó y alteró los sistemas.

(…) "Los técnicos, no necesariamente de la Caja, me han estado informando de que, por ejemplo, hay evidencia en lo que llaman las redes oscuras de que había actores conocidos en ese tipo de redes ofreciendo accesos a la Caja, y que posiblemente hubo múltiples intentos de acceso (…) Ahora que se hace la revisión forense en la dark web encuentran que había gente ofreciendo (información)", explicó.

Admitió que, desafortunadamente, la dimensión del daño es mayor a la que se dijo en un inicio. No se atrevió a dar un plazo para restablecer todos los sistemas, aunque espera que el Expediente Digital Único en Salud (EDUS), en su versión de respaldo para situaciones de emergencia –conocido como EDUS desconectado– pueda estar disponible en no menos de una semana."

OBSERVACIONES

En virtud de lo anterior y bajo el contexto actual de la CCSS, es menester de este Órgano Fiscalizador hacer recordatorio a la Administración sobre la importancia que reviste al tema de gestionar la crisis ante los ciberataques, principalmente considerando el impacto y la exposición prolongada a la desconexión de los sistemas de información en la institución.

En ese sentido, mediante las siguientes observaciones se exponen buenas prácticas al gestionar las cibercrisis. Lo anterior, para que sea examinado y discurrido por el conjunto de involucrados en el asunto, a saber:

- Considerando que toda crisis implica una toma de decisiones bajo presión, con tiempo e información "limitada", desde los diferentes frentes e incluyendo personas, resulta relevante dotar de capacidades y estructuras dedicada al abordaje del asunto mencionado en el epígrafe.

  Por ejemplo, al conformar o activar la comisión de crisis, integrada por conocedores de las dos esferas de actuación, la primera de ellas referente a la operativa y de respuesta técnica y la segunda desde el punto de vista organizativo o estratégico, enfocado en gestionar el impacto desde los diferentes ámbitos de la organización (servicio, operativa, imagen y reputación, proveedores externos, etc.) y que requiere de una respuesta coordinada a alto nivel, determinando los canales de comunicación con otras unidades o entidades, propias y/o ajenas

  Particularmente, este tipo de agrupaciones debe estar compuesta por personas con distintos perfiles (multidisciplinario e integral), incluyendo niveles ejecutivos y gerenciales, asesores a nivel legal, responsable de equipos técnicos, equipo de comunicación, expertos en TIC[1], entre otros; dichos funcionarios deben ser resolutivos, es decir, con la capacidad de reacción ante situaciones de estrés y agilidad en la dirección de los equipos y toma de decisiones.

- Como parte del propósito de gestionar la crisis mediante estructuras adecuadas, se destaca el poder tomar decisiones y planificar medidas contingentes de forma coordinada, incorporando a la alta dirección quien tiene la capacidad de asegurar los recursos materiales y humanos necesarios, así como la jerarquía para proceder con el liderazgo y control necesario.

  No obstante, esa labor a nivel estratégico debe estar apoyada por los responsables de la seguridad de la Información, quienes son los que categorizan el evento, identifican el plan de acción y la idoneidad o no de convocar al comité de crisis, valorando razonablemente el impacto, los tiempos de respuesta y tolerancia, los servicios paralizados (total o parcial) e inclusive midiendo la efectividad de la organización para restablecerse paulatinamente.

- Ante la complejidad de las acciones por implementar o incertidumbre generada por el evento, es relevante supervisar el desarrollo de actividades a nivel central, regional y local, de forma tal que se compruebe el acatamiento de directrices y si estas se ajustan a los diferentes escenarios de la Institución.

[1] Las Tecnologías de la Información y las Comunicaciones (TIC)

Aunado a esa labor, se apoyaría la premisa de identificar y planificar constantemente el impacto y alcance de las medidas contingentes, en aras de identificar si son suficientes para garantizar la continuidad de servicios.

De esa manera, promoviendo la continuidad del negocio o en su defecto el restablecimiento de servicios de manera segura, garantizando que la superficie de exposición a la ciber amenaza es medible, controlada y adaptada a los planes atinentes al negocio y TI[2].

- En cuanto a la gestión de los grupos de interés es relevante mencionar que debe prevalecer una línea activa de comunicación y participación, pese a la complejidad del incidente y ocupación de los lideres; en ese sentido, los diferentes responsables deben informar según corresponda, el impacto del ataque, tipo de afectación, plan de acción, avance en el desarrollo de las iniciativas, entre otras acciones.

  Principalmente, considerando los grupos en función a su actividad, tales como: Internos, donde se incluye la Junta Directiva, Consejo Tecnológico, Comités, Auditoría Interna, responsables de equipos estratégicos y técnicos, conjunto de funcionarios involucrados o afectados por el incidente en ciberseguridad, entre otros; Externos, conteniendo autoridades gubernamentales, organismos reguladores y supervisores, agencias especializadas, CERT o CSIRT[3], usuarios, proveedores, compañías de seguros, asociaciones, comisiones especializadas, colegios profesionales, grupos sindicales o representantes de distintos grupos ocupacionales; y medios de comunicación incluyendo los tradicionales y los online.

- Ante las oportunidades de mejora que se deban atender sobre el incidente o al considerar la necesidad de gestionar procesos para el manejo de crisis en la Institución, se estima conveniente examinar los marcos de referencia y estándares de calidad que proponen metodologías debidamente aprobadas, las cuales comparten recomendaciones y herramientas de utilidad.

  Al respecto, la temática de gestión de crisis no es una excepción (así lo refieren los estándares internacionales como la ISO 27001[4] y 22301[5] para la implantación de un SGSI[6], entre otros) por lo cual se podría revisar y extraer las prácticas que sean de utilidad en el contexto actual de la Institución. Particularmente, las correspondientes a adoptar acciones en materia de continuidad, contingencia, comunicación, administración de recursos, humanos, servicios tercerizados, asignación de roles y responsabilidades, entre otros componentes notables.

[2] Tecnologías de la Información (TI)
[3] CERT (Computer Emergency Response Team) y CSIRT (Computer Security Incident Response Team)
[4] Norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información.
[5] Norma internacional de gestión de continuidad de negocio.
[6] Sistema de Gestión de la Seguridad de Información que recoge un conjunto de políticas, procedimientos y directrices para una correcta protección de los activos de la información de cualquier organización.

- Como parte de la gestión de crisis llevada a cabo en una organización, la estructura correspondiente analiza a detalle el diagnóstico inicial y los posibles escenarios de riesgo para tener certeza sobre lo que está sucediendo, el recuento de daños y el compromiso requerido en atención al incidente.

  Lo anterior, alineado a un plan de respuesta de incidentes en ciberseguridad, tal y como lo menciona el artículo posteado en Blog "Netdata" el 9 de diciembre del 2020, titulado "¿qué hacer en caso de un ciberataque?":

  "Es muy importante contar con un Plan de Respuesta a Incidentes de Ciberseguridad, que te permita tener una metodología a llevar a cabo ante un ciberataque. Este plan debe ser socializado con toda la organización y probado constantemente para evaluar su efectividad. (…)

  De esta manera, podrás desarrollar tu plan en base a cuatro fases:

  Planificación y Preparación.
  Detección y Análisis.
  Respuesta: Contención, Erradicación y Recuperación.
  Acciones Post-Incidentes."

  Además, logrando comprender que terminada la crisis no se resuelve el nivel de exposición, sino el inicio de una etapa llamada "Acciones Post-Incidentes", "Plan de Cierre", "Lecciones aprendidas" entre otros nombres enfocados en sintetizar el conjunto de actividades para tratar de manera integral las implicaciones del incidente.

- Aunado a la observación anterior, una vez superado el momento crítico de la crisis, se extrae las experiencias del conjunto de involucrados al desarrollar acciones en atención al incidente, para posteriormente determinar cuáles tareas se deben implementar o priorizar basado en las lecciones aprendidas, es decir, corresponde a una reacción de análisis a profundidad que pretende establecer planes de mejora con objetivos concretos y una evolución medible.

  En ese sentido. no estando satisfechos con las relaciones causa-efecto más inmediatas, sino buscando también orígenes sistémicos del problema que puedan solventarlo con legislaciones, estrategias, modelos, modernización de procesos, planes de acción e inversión.

Consideraciones finales

La Caja Costarricense del Seguro Social (CCSS), se encuentra ante un incidente donde se infectó con Ransomware los computadores y servidores que respaldan las labores de las diferentes unidades de trabajo en la Institución, lo cual afectó la dinámica habitual de los procesos.

En ese sentido, la situación no es exclusiva de la Caja ya que otras instituciones públicas habían sido atacadas por los cibercriminales. No obstante, tanto el país como la institución denotan la necesidad de disponer de una estrategia en ciberseguridad capaz de mitigar esa exposición al riesgo. A ese respecto, cabe destacar que las inversiones en seguridad debe ser una prioridad para las organizaciones. A pesar de la dificultad en calcular su retorno financiero, dada la cada vez mayor frecuencia de los ciberataques y el gran impacto que tienen tanto en afectación al servicio prestado como en salvaguarda de la información y reputación de la CCSS.

Lo anterior, en apego a lo indicado en las Normas técnicas para la gestión y el control de las Tecnologías de Información del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, que establecen dentro de los procesos del marco de gestión de TI, lo correspondiente a la "Seguridad y Ciberseguridad", a saber:

> *"**XI. SEGURIDAD Y CIBERSEGURIDAD***
>
> *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."

Sin embargo, mediante las observaciones descritas anteriormente se pretende reflejar cuáles aspectos de gobierno y gestión pueden ser considerados de forma inmediata, sin necesidad de un modelo de ciberseguridad, pero sin obviar el manejo de una cibercrisis.

De esa manera, incentivando el análisis desde la alta dirección, equipos técnicos, rectoría en TIC, servicios de apoyo, comunicación organizacional, entre otros involucrados, en beneficio de la institución y concretamente generando resiliencia en medio del evento acontecido el 31 de mayo, mismo que aún afecta a la CCSS.

A ese respecto, verificándose la existencia de capacidades y estructuras que aborden integralmente el tipo de la amenaza, impacto sobre el servicio, pertinencia o suficiencia de acciones implementadas, grado de preparación de la Caja, así como sus carencias. Es decir, esfuerzos y acciones realizadas a través de una estrategia integrada, coordinada y organizada desde la Presidencia Ejecutiva y Gerencia General, garantizando la gestión de interesados y su eventual alineamiento con las iniciativas de contingencia propuestas desde el ámbito de negocio y TIC.

Adicionalmente, disponiéndose de una gestión de crisis consciente de la capacidad de respuesta alineada con la administración de recursos, pendiente de alertas, generando criterios, tomado decisiones rápidas, considerando las lecciones aprendidas, entre otras actividades. Claro está, basando esa labor a partir de marcos regulatorios, guías de mejores prácticas o estándares de calidad, especializados en la temática de ciberseguridad, manejo crisis, continuidad, prestación de servicios TIC, mecanismos de contingencia, entre otros tópicos.

Así las cosas y de conformidad con expuesto en el artículo 8 de la Ley General de Control Interno, referente al deber de garantizar la eficiencia y eficacia de las operaciones ejecutadas, resulta fundamental que la Administración Activa se mantenga vigilante en la adopción de acciones pertinentes y suficientes en la materia abordada en esta misiva.

Asimismo, es importante que las acciones ejecutadas incluyan los mecanismos básicos de control que aseguren la legalidad de las operaciones y a su vez acrediten documentalmente los lineamientos y directrices considerados para dirigir adecuadamente la gestión de negocio y TI. Aunado a lo anterior, resaltando la necesidad de rendir cuentas o mantener informados al grupo interesados o involucrados en el incidente.

En virtud de lo expuesto, se da conocer las observaciones insertas en el oficio, con el propósito de ser sometidas a valoración y revisión por esa Administración. Lo anterior, con el objetivo de enfrentar con éxito los eventos adversos que puedan presentarse, la mitigación de vulnerabilidades y así coadyuvar al cumplimiento de los objetivos institucionales, garantizando un marco adecuado para el resguardo de la información institucional y de la seguridad informática.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.06.10 11:51:47 -06'00'

Lic. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/OMG/lbc

C. Doctor Wilman Rojas Molina, director regional, Dirección de Redes Integradas Prestación de Servicios de Salud Región Central Norte- 2299.
Doctor Albert Méndez Vega, director regional, Dirección de Redes Integradas Prestación de Servicios de Salud Región Central Sur -2399.
Doctor Warner Picado Camareno, director regional, Dirección de Redes Integradas Prestación de Servicios de Salud Chorotega- 2599.
Doctora Silene María Aguilar Orias, directora regional, Dirección de Redes Integradas Prestación de Servicios de Salud Huetar Atlántica- 2699.
Doctor Gustavo Zeledón Donzo, director regional, Dirección de Redes Integradas Prestación de Servicios de Salud Huetar Norte – 2499.
Doctor Wilburg Díaz Cruz, director regional, Dirección de Redes Integradas Prestación de Servicios de Salud Pacífico Central- 2598.
Doctor Arturo Enrique Borbón Marks, director regional, Dirección de Redes Integradas Prestación de Servicios de Salud Brunca -2799.
Licenciado Olman Arturo Mora Valverde, director regional, Dirección Regional Brunca Sucursales -1601.
Licenciado Alfredo Vindas Evans, director regional, Dirección Regional Central de Sucursales – 1201.
Licenciada Maylen Herrera Araya, directora regional, Dirección Regional Huetar Atlántica Sucursales -1501.
Licenciada Xiomara Poyser Watson, directora regional, Dirección Regional Huetar Norte Sucursales -1301.
Licenciado Luis Mario Carvajal Torre, director regional, Dirección Regional Chorotega Sucursales-1401.
Auditoría