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

CONFIDENCIAL

AS-AATIC-152-2022
19 de julio de 2022

Doctor
Roberto Cervantes Barrantes, gerente
GERENCIA GENERAL - 1100

Máster
Idannia Mata Serrano, subgerente a.i,

Máster
Vanessa Carvajal Carmona, jefe
Subárea Seguridad de Tecnologías de Información
DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES -1150

Estimado (a) señor (a):

ASUNTO:	**Oficio Asesoría referente al establecimiento de una hoja de ruta para brindar seguimiento a las recomendaciones emitidas por Deloitte, GBM, Microsoft y el Centro Criptológico Nacional posterior al análisis e investigación del incidente suscitado 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 siendo consecuente a lo indicado en el 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 el asunto mencionado en el epígrafe.

A ese respecto, esta Auditoría Interna tuvo conocimiento del apoyo proporcionado por las compañías Deloitte Touche Tohmatsu Limited, GBM, Microsoft y el Centro Criptológico Nacional (CCN) en el análisis e investigación del incidente cibernético antes mencionado. En ese sentido, la labor supra citada fue resumida en diferentes documentos, en los cuales se detalla los resultados obtenidos, hallazgos, conclusiones y recomendaciones.

Particularmente, este Órgano Fiscalizador recopiló todas las recomendaciones supra citadas (véase Anexo 1, Anexo 2, Anexo 3 y Anexo 4); resultando un total de 99 acciones preventivas y/o correctivas a realizar, aspecto que se resumen en el siguiente cuadro:

Cuadro 1
Recomendaciones emitidas según compañía, producto del análisis e investigación del incidente suscitado el 31 de mayo del 2022

Compañía	Cantidad de recomendaciones	Fuente
Deloitte	13	Informe de análisis e investigación del "Incidente I.450 Ransomware Hive", junio 2022
Centro Criptológico Nacional (CCN)	18	Documento "Conclusiones", remitido en oficio PE-1727-2022 del 20 de junio del 2022.
GBM Cibersecurity Center	22	Boletín de Inteligencia de Amenazas – Hive Ransomware, 01 de junio del 2022
Microsoft	46	Documento "Detection and response Team del 13 de mayo del 2022 y 10 de junio del 2022
Total	**99 recomendaciones**	

Fuente: elaboración propia, a partir de la información antes indicada.

En ese orden de ideas, entre los documentos mencionados se destaca de manera generalizada, los siguientes tópicos:

- Adquisición y/o implementación de soluciones antivirus, antimalware, entre otros aplicativos de defensa disponibles en el mercado.
- Cambios masivos de contraseñas y/o privilegios en varios servicios tecnológicos.
- Utilización de múltiples factores de autenticación, así como la innovación de los mecanismos actuales.
- Actualización del software, de manera constante y remover aplicaciones innecesarias u obsoletas.
- Robustecer reglas de acceso condicional a equipamiento, redes, aplicaciones, entre otros.
- Implementación de la segmentación de red y filtrado de tráfico.
- Gestionar la configuración adecuada de hardware y software.
- Escaneo de vulnerabilidades (Detección y respuesta de amenazas), así como el monitoreo de cambios no autorizados; ambos de manera periódica.
- Actualización de políticas en seguridad de la información y ciberseguridad, considerando los aspectos mínimos ante la interacción interna y/o externa de procesos, personas y tecnologías.
- Implementar mecanismos para prevenir y/o detectar la pérdida de información.
- Disponer de planes de continuidad, recuperación de desastres, contingencia, gestión de incidentes, respaldo, entre otros.
- Mantener inventarios de recursos actualizados (servicios, red, activos), así como diagramas que apoyen su identificación.
- Políticas y mecanismos referente con la conceptualización adecuada del respaldo de información, disposición de sitio alterno, redundancia en caso de fallas en la comunicación principal, tecnología en la nube, VPN, entre otros.

Por consiguiente, es importante el énfasis en la revisión y análisis de los elementos de riesgo y advertencia indicados en estos documentos, debido a la necesidad de fortalecer la seguridad y ciberseguridad desde el ámbito que le corresponde al negocio y a la parte tecnológica.

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, en el inciso IV "Gestión de Riesgos Tecnológicos", a saber:

"La institución debe establecer un proceso formal de gestion de riesgos que responda a las amenazas que puedan afectar el logro de los objetivos institucionales, basado en una gestion continua de riesgos que este integrada al sistema especifico de valoración del riesgo institucional y considerando el Marco de Gestion de TI que le resulte aplicable.

La Unidad de TI debe aplicar el marco de gestion de riesgo tecnológico, con el fin de identificar, valorar, priorizar y gestionar los riesgos al nivel de TI en cualquiera de sus escenarios, que impliquen una eventual afectación a la continuidad operacional, así como la integridad y confidencialidad de la información y el cumplimiento regulatorio de la institución."

Bajo ese contexto, es menester de este Órgano Fiscalizador, que la Administración establezca la hoja de ruta con el detalle de actividades, plazos y responsables en atender y dar seguimiento a los hallazgos evidenciados por los especialistas consultados.

Para tales efectos, discurriendo sobre la estrategia a seguir para priorizar la ejecución de tareas e inclusive maximizar el alcance de las soluciones que permitirán fortalecer de manera efectiva las condiciones actuales de ciberseguridad en la Institución, esto desde el accionar en el ámbito estratégico, táctico y operativo según corresponda.

En ese sentido, siendo consecuente con 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", citando:

*"**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."

Así las cosas, se recuerda a esa Administración, su responsabilidad por la constante valoración de riesgos, el establecimiento de acciones que permitan mantener, perfeccionar y evaluar el sistema de control interno, y tomar de inmediato las medidas correctivas, ante cualquier evidencia de desviaciones o irregularidades, así como, implantar las observaciones, recomendaciones y disposiciones formuladas por instituciones de control y fiscalización que correspondan, conforme con lo dispuesto en los artículos 10°, 12° 14° de la Ley General de Control Interno.

Al respecto, se deberá informar a esta Auditoría Interna sobre la hoja de ruta con actividades, responsables y fechas de ejecución, en el plazo de un mes a partir del recibido de este documento.

Finalmente, es relevante manifestar la disposición de apoyar la gestión a desarrollar por esa Gerencia General en conjunto de la Dirección de Tecnologías de Información y Comunicaciones ante los argumentos citados, conforme a nuestras potestades y competencias.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.07.20 14:13:44 -06'00'

Lic. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/OMG/lbc

Anexos(4)

1- Recomendaciones emitidas por la compañía Deloitte.
2- Recomendaciones emitidas por el Centro Criptológico Nacional (CCN).
3- Recomendaciones emitidas por la compañía GBM Cibersecurity Center.
4- Recomendaciones emitidas por la compañía Microsoft.

C. Auditoría