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

AS-ATIC-006-2023
26 de enero de 2023

Máster
Marta Eugenia Esquivel Rodríguez, presidenta ejecutiva con recargo a la Gerencia General y coordinadora del Consejo Tecnológico
PRESIDENCIA EJECUTIVA -1102

Máster
Eithel Corea Baltodano, Sub-Gerente a.i.
DIRECCIÓN DE TECNOLOGÍAS Y COMUNICACIONES - 1150

Estimados señores:

ASUNTO:	**Oficio de Asesoría relacionado con la necesidad de brindar seguimiento a los productos de auditoría emitidos en torno al ciberataque a la Institución que llevó a la desconexión de servicios tecnológicos el 31 de mayo del 2022.**

La Auditoría Interna de conformidad con sus competencias y facultades conferidas en la Ley General de Control Interno No. 8292, así como las disposiciones emitidas por la Contraloría General de la República en las Normas para el Ejercicio de la Auditoría Interna en el Sector Público sección 1.1.4, y los Lineamientos Generales para el análisis de presuntos hechos irregulares atendió lo solicitado por Junta Directiva en el artículo 5, de la sesión No. 9262 del 30 de junio del 2022, en el cual se acordó:

> *"(…)*
> *ACUERDO ÚNICO: Se instruye a la Auditoria Interna para que efectúe una investigación, en el ámbito de sus competencias y potestades. Emitido el producto correspondiente, este se traslade a la autoridad competente para que, si corresponde, ulteriormente, se establezcan las responsabilidades administrativas y de otra índole, con respecto al ciber ataque perpetrado en la Institución el pasado 31 de mayo de 2022".*

Como consecuencia de las investigaciones desarrolladas, el 18 de agosto de 2022, mediante oficio AI-1255-2022, se informó a la Junta Directiva que se procedió a la emisión de la relación de hechos AATIC-RH-046-2022 del 17 de agosto del 2022, referente al uso irregular de las tecnologías de información por parte de un funcionario, que en apariencia habría originado la vulnerabilidad para propiciar el ataque cibernético contra la Caja Costarricense de Seguro Social.

Aunado a lo anterior, se informó que posterior a la emisión de la relación de hechos mencionada, se emitió la denuncia penal AATIC-DP-047-2022 referente a los mismos hechos sobre el uso irregular de las tecnologías de información por parte de un funcionario, que en apariencia habría originado la vulnerabilidad para propiciar el ataque cibernético contra la Caja Costarricense de Seguro Social, el mismo fue interpuesto ante la Fiscalía Adjunta de Fraudes y Cibercrimen del Ministerio Público.

Asimismo, el 13 de diciembre de 2022, se emitió la relación de hechos ATIC-RH-109-2022 relacionado con el debilitamiento del Control Interno en materia de Ciberseguridad y Seguridad Informática. Lo anterior, por cuanto se evidenciaron hechos que hacen presumir la existencia de posibles responsabilidades en sede administrativa.

Además de lo anterior, esta Auditoría Interna en cumplimiento al acuerdo de junta directiva supracitado, emitió los siguientes oficios de asesoría y de advertencia donde se abordaron diferentes temas con el objetivo de que fuera de conocimiento de la Administración Activa y se procediera a las acciones pertinentes:

Tabla 1. Productos emitidos por parte de la Auditoría Interna en torno al ciberataque del 30 de mayo de 2022

No. OFICIO	TEMA
AD-AATIC-067-2022	Oficio de Advertencia sobre la exposición reciente a ataques cibernéticos a la CCSS.
AI-884-2022	Oficio de información en relación con el acceso a la página Web de la Biblioteca Nacional de Salud y Seguridad Social (BINASSS) en el contexto de los ataques cibernéticos a la CCSS.
AS-AATIC-072-2022	Oficio de Asesoría sobre la gestión de crisis en materia de ciberseguridad como resultado del ataque cibernético ocurrido el 31 de mayo del 2022.
AI-905-2022	Oficio de información en relación con acciones preventivas para minimizar la materialización de riesgos generadas por la herramienta "Mimikatz".
AS-AATIC-088-2022	Oficio de Asesoría sobre la continuidad del negocio ante amenazas o desastres de origen tecnológico.
AS-ATIC-101-2022	Oficio de asesoría en torno al cambio jerárquico del proceso Gestión de Tecnologías de Información y Comunicaciones propuesto en el oficio GG-1067-2022.
AS-AATIC-102-2022	Oficio de Asesoría en torno a los equipos tecnológicos utilizados para el Expediente Digital Único en Salud (EDUS) como parte de los contratos de servicios administrados suscritos entre la Caja Costarricense de Seguro Social (CCSS) y el Instituto Costarricense de Electricidad (ICE), afectados por el ciberataque del 31 de mayo del 2022.
AS-AATIC-093-2022	Oficio de asesoría referente a las previsiones relacionadas con los contratos de prestación de servicios por terceros eventualmente afectados por el ciberataque sufrido el 31 de mayo de 2022. En cumplimiento de las actividades
AS-AATIC-103-2022	Oficio de asesoría referente a la instalación de una red WIFI en el Dirección General del hospital Guápiles, con la finalidad de acceder a servicios web externos como contingencia por el ciberataque sufrido el 31 de mayo de 2022.
AS-AATIC-089-2022	Oficio de Asesoría en relación con acciones preventivas para minimizar la materialización de riesgos generados por eventuales debilidades en el Active Directory y servidores Exchange que permita la ejecución del ransomware "BlackCat".
AS-AATIC-108-2022	Oficio de asesoría sobre la estrategia de recuperación ante amenazas o desastres de origen tecnológico.
AS-AATIC-107-2022	Oficio de Asesoría referente al tratamiento de los datos personales y medidas de seguridad.
AS-AATIC-113-2022	Oficio de Asesoría sobre el restablecimiento en la operación de sistemas de información y bases de datos.
AS-AATIC-112-2022	Oficio de Asesoría referente a la gestión del Consejo Tecnológico.
ASS-AATIC-122-2022	Oficio asesoría referente a las acciones preventivas para minimizar la materialización de riesgos generadas por la herramienta "Log4J".
AS-AATIC-124-2022	Oficio de Asesoría en relación con riesgos identificados en materia de protección de datos por la implementación de mecanismos contingentes en la atención de pacientes.
AD-AATIC-063-2022	Oficio de Advertencia sobre gobierno y gestión de la ciberseguridad en la CCSS.
AS-AATIC-087-2022	Oficio de Asesoría referente a la afectación en la gestión de Telesalud como resultado de los ataques cibernéticos ocurridos contra la Caja Costarricense de Seguro Social.
AS-AATIC-125-2022	Oficio de Asesoría sobre el comportamiento, tácticas y herramientas utilizadas por los ciber atacantes.
AS-AATIC-114-2022	Oficio de Asesoría referente al uso de WhatsApp para el envío y recepción de información institucional.
AD-AATIC-074-2022	Oficio de Advertencia sobre equipos de laboratorio pertenecientes a los contratos de laboratorio (CAPRIS-ROCHE) afectados por el ciberataque del 31 de mayo del 2022.

AS-AATIC-127-2022	Oficio de Asesoría sobre la actualización del software y la infraestructura en TIC.
AS-AATIC-130-2022	Oficio de asesoría referente a la gestión del Directorio Activo
AS-AATIC-131-2022	Oficio de Asesoría referente soluciones de autenticación en sistemas informáticos.
AI-1043-2022	Oficio de información relacionado con el riesgo de ransomware detectado en la plataforma de Microsoft 365.
AS-AATIC-116-2022	Oficio de Asesoría referente a los Planes de Continuidad de TIC.
AS-AATIC-137-2022	Oficio de Asesoría relacionado con la gestión de Bases de Datos y sus mecanismos de seguridad.
AS-AATIC-135-2022	Oficio de Asesoría sobre el impacto en la prestación de servicios y medidas de contingencia, producto del ataque cibernético en la plataforma tecnológica institucional.
AS-AATIC-138-2022	Oficio de Asesoría referente al uso de servicio de internet (MIFI) en la Dirección de Inspección como contingencia al ataque cibernético sufrido el 31 de mayo de 2022
AD-AATIC-078- 2022	Oficio de Advertencia sobre la urgente necesidad de disponer de un sitio alterno de procesamiento de datos, dada la afectación sufrida en la prestación de servicios por el ciberataque del 31 de mayo de 2022.
AS-AATIC-146-2022	Oficio de Asesoría referente al procedimiento de registro y pago de incapacidades descrito en el oficio GF-0410-06-2022/GM-8071-2022 del 5 de julio del 2022.
AS-AATIC-147-2022	Oficio de Asesoría sobre los roles y responsabilidades de ciberseguridad a considerar en la Caja Costarricense del Seguro Social.
AS-AATIC-155-2022	Oficio de Asesoría relacionado con amenazas generadas por el ransomware DeadBolt que afecta los almacenamientos en dispositivos NAS.
AS-AATIC-152-2022	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.
AS-AATIC-160-2022	Oficio de Asesoría referente a la finalización del ciclo de vida del software de desarrollo SQL Server 2012
AI-1151-2022	Oficio de información relacionado con amenazas generadas a los servidores virtuales por el ransomware Red Alert.
AS-AATIC-167-2022	Oficio de Asesoría sobre la importancia de establecer una estrategia integral que promueva la formación, capacitación y concientización en seguridad informática, seguridad de la información y ciberseguridad.
AS-AATIC-169-2022	Oficio de Asesoría sobre la gestión de ciberseguridad en el uso de dispositivos móviles.
AS-AATIC-168-2022	Oficio de Asesoría sobre la protección de datos adaptable al riesgo con un enfoque basado en el comportamiento.
AS-AATIC-175-2022	Oficio de Asesoría relacionado con los Sistemas de Gestión de Privacidad de la Información en el contexto actual de la Caja Costarricense de Seguro Social.
AS-AATIC-174-2022	Oficio de Asesoría sobre ciberseguridad hospitalaria.
AS-AATIC-177-2022	Oficio de Asesoría sobre la gestión de servicios de computación en la nube como mecanismo de contingencia.
AS-AATIC-183-2022	Oficio de Asesoría relacionado a la gestión e implementación de la herramienta MicroCLAUDIA en el contexto del Ciberataque a la CCSS.
AS-AATIC-184-2022	Oficio de Asesoría sobre la importancia del desarrollo seguro de sistemas y aplicaciones institucionales.
AS-AATIC-186-2022	Oficio de Asesoría Referente a Aplicaciones que Originan Descargas de Malware.
AS-AATIC-185-2022	Oficio de Asesoría relacionado con los riesgos detectados en materia de Seguridad de la Información y Ciberseguridad en instrumento elaborado por la Contraloría General de la República.
AS-AATIC-182-2022	Oficio de Asesoría Referente a Nuevas Vulnerabilidades Explotadas Activamente que han sido incorporadas al Catálogo de Vulnerabilidades Conocidas.

AS-AATIC-190-2022	Oficio de Asesoría sobre las capacidades asociadas con la gestión de incidentes de ciberseguridad.
AS-AATIC-194- 2022	Oficio de Asesoría referente al sitio alterno de procesamiento de datos de la Gerencia de Pensiones, dada la afectación sufrida en la prestación de servicios por el ciberataque del 31 de mayo de 2022.
AS-AATIC-198-2022	Oficio de Asesoría sobre ciberseguridad para dispositivos y equipos médicos.

Al respecto, es importante señalar y recordar que el artículo 10° de la Ley General de Control Interno, establece que es responsabilidad del jerarca y el titular subordinado establecer, mantener, perfeccionar y evaluar el sistema de control interno y realizar las acciones necesarias para garantizar su efectivo funcionamiento.

De igual manera el artículo 17° de la Ley General de Control Interno, establece la obligación de la administración activa, de realizar actividades de seguimiento para valorar el funcionamiento del sistema de control interno y asegurar que los hallazgos de la auditoría y los resultados de otras revisiones sean atendidas con prontitud, asimismo el inciso C de ese mismo artículo, menciona que es deber del jerarca y los titulares subordinados implantar los resultados de las evaluaciones periódicas que realiza la auditoría interna, así como otros entes de fiscalización y control.

Además, el artículo 12° de la Ley General de Control Interno inciso C dispone que la Administración Activa debe analizar e implantar de inmediato, las observaciones, recomendaciones y disposiciones formuladas por la auditoría interna y demás instituciones de control y fiscalización que correspondan.

Por lo anterior, se insta a la Administración Activa a continuar con las medidas de fortalecimiento de los mecanismos de control en torno a la Ciberseguridad y Seguridad de la Información, de tal forma que se minimicen la posibilidad de materialización de riesgos en esta materia, y que la Institución no se vea afectado ante nuevos ataques por parte de organizaciones criminales, considerando además que el país continua presentando este tipo de eventos, como el sucedido el pasado 17 de enero del 2023 que tuvo como resultado la encriptación de 12 servidores en el Ministerio de Obras Públicas y Transportes (MOPT).

En virtud de lo expuesto, se da conocer los productos emitidos por parte de esta Auditoría, que están relacionados con temas de vital importancia como lo es la ciberseguridad y Seguridad de la Información, así como la protección de los datos, medidas de contingencia, continuidad de los servicios, entre otros. El propósito de informar y actualizar a la Administración sobre estos productos es que se adopten las acciones de seguimiento, en especial de los productos que están relacionados con el fortalecimiento de los temas mencionados, así como las brechas identificadas en los diferentes productos emitidos, de manera que se adopten las medidas que estimen pertinentes y así coadyuvar a la mitigación de las vulnerabilidades identificadas, cumpliendo con los objetivos institucionales.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)
Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2023.01.26 11:47:19 -06'00'

M. Sc. Olger Sánchez Carrillo
Auditor Interno

OSC/RJS/RAHM/LDP/jfrc

C. Auditoría

Referencia: ID-80685