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

Al contestar refiérase a: **ID-99719**

AS-ATIC-0090-2023
25 de septiembre de 2023

Máster
Marta Eugenia Esquivel Rodríguez, presidenta ejecutiva
PRESIDENCIA EJECUTIVA – 1102

Máster
Marta Eugenia Esquivel Rodríguez, presidente ejecutiva con cargo de gerente
GERENCIA GENERAL–1100

Doctor
Wilburg Díaz Cruz, gerente a.i.
GERENCIA MEDICA-2901

Máster
Gabriela Artavia Monge, gerente a.i.
GERENCIA FINANCIERA-1103

Máster
Vilma María Campos Gómez, gerente a.i.
GERENCIA ADMINISTRATIVA- 1104

Doctor
Esteban Vega de la O, gerente
GERENCIA LOGÍSTICA-1106

Ingeniera
María de los Ángeles Gutiérrez Brenes, gerente a.i.
GERENCIA INFRAESTRUCTURA Y TECNOLOGÍAS-1107

Licenciado
Jaime Barrantes Espinoza, gerente
GERENCIA DE PENSIONES -9108

Máster
Danilo Hernández Monge, subdirector, subgerente a/c
DIRECCIÓN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES - 1150

Estimados (as) señores (as):

ASUNTO:	**Oficio de Asesoría respecto al ransomware del grupo cibercriminal autodenominado "RansomHouse" y el riesgo de filtración de datos sensibles.**

En cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo para el período 2023 y con fundamento en los artículos N.º 21 y 22 de la Ley General de Control Interno específicamente en su rol de asesor, esta Auditoría informa sobre la importancia de implementar acciones preventivas, a fin de evitar la materialización de riesgos en materia de Ciberseguridad y protección de datos, generados por el ransomware del grupo denominado *"RansomHouse"* que ha afectado recientemente a instituciones de la República de Colombia, y quienes también se atribuyeron los ciberataques efectuados a varios centros de salud en España en marzo del 2023.

Al respecto, *"RansomHouse"* es un grupo de delincuentes informáticos que aparecieron en el 2021, dedicados al secuestro de la información para encriptarla y posteriormente solicitar dinero para su rescate, o eventualmente demostrar y evidenciar las debilidades en los controles de ciberseguridad que tienen las organizaciones. Lo anterior, mediante infiltraciones en sistemas informáticos vulnerables, cifrando la información almacenada en estos.

Al grupo *"RansomHouse"* recientemente se le ha relacionado con los ciberataques sufridos en Colombia, en instituciones como las Entidades Promotoras de Salud (EPS) y Colsanitas (compañía de medicina prepagada) eventos donde se expusieron datos privados de los pacientes, asimismo del ciberataque masivo en dicho país sufrido el 12 de setiembre de 2023, donde varias infraestructuras críticas y entidades del Estado se vieron afectadas, como las Superintendencias de Industria y Comercio, de Salud, Consejo Superior de la Judicatura, Ministerio de Salud y Protección Social, entre otras.

Al respecto, el Gobierno de la República de Colombia, ha informado que en dichos eventos hubo fuga de datos de diferentes entidades del Estado, mismas que se han encontrado en la *"Dark Web"*[1], donde se vende la información robada a otras organizaciones ciber delictivas.

Este grupo criminal, también fue el responsable del ciberataque sufrido el 5 de marzo de 2023 en el hospital Clínic de Barcelona, España, el cual se vio obligado a desprogramar 150 operaciones no urgentes y cancelar entre 2,000 y 3,000 citas de Consulta Externa, asimismo intentaron extorsionar al centro médico con la liberación de 4.4 terabytes de datos que sustrajeron y que contenía información confidencial de pacientes, trabajadores, directivos y proveedores, ensayos clínicos de cáncer y enfermedades autoinmunes, con la amenaza de ser publicada en la *"Dark Web*".

Por lo anterior, es importante que la Institución esté vigilante ante la situación presentada con esta organización delictiva, donde sus objetivos de ataque han estado relacionados con instituciones del sector Salud, con el fin de que se fortalezcan las medidas preventivas de seguridad y ciberseguridad, disminuyendo así el riesgo de que se materialice en la CCSS, un nuevo ciberataque que afecte la continuidad en la prestación de los servicios y la divulgación de información de carácter confidencial que ponga a la Institución en una situación irregular en materia de legalidad, considerando además que el mecanismo utilizado para vulnerar la seguridad es mediante ransomware, por lo que esta Auditoría informa sobre este grupo criminal, como lo hizo anteriormente con "Black Cat", "Dead Bolt", "Red Alert", y Ransomware en office 365, en los productos: AS-AATIC-089-2022, AS-AATIC-155-2022, AI-1151-2022, AI-1043-2022 respectivamente.

Por esta razón, para contrarrestar las posibilidades de que se materialicen nuevas vulnerabilidades, esta Auditoría recuerda que, entre otros aspectos, como medidas preventivas se considere:

1. Atender oportunamente las alertas emitidas por el Ministerio de Ciencia, Innovación y Tecnología, así como de las empresas contratadas que brindan servicios de Ciberseguridad a la Institución.
2. Mantener los Sistemas Operativos actualizados y aplicaciones al día, con sus respectivos parches y actualizaciones correspondientes.
3. Utilizar software de seguridad que detecten y bloqueen amenazas antes de que se genere un daño
4. Limitar los privilegios de administrador, ya que al reducir al máximo el número de privilegios otorgados se reduce la posibilidad de la materialización del evento.
5. Fortalecer los mecanismos de educación y concientización en los usuarios, entorno al uso adecuado de la tecnología, reconocer correos electrónicos y enlaces sospechosos.
6. Monitoreo de la Red.
7. Pruebas para identificar vulnerabilidades.

En este sentido, esta Auditoría informa sobre lo descrito con el objetivo de que se analice la información expuesta y se profundice en el tema de considerarlo necesario, reforzando así los mecanismos de ciberseguridad, de tal forma que se reduzca la posibilidad de que se vuelvan a materializar riesgos como el sucedido el 31 de mayo del 2022.

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.*

[1] Parte de Internet que no está indexada por los motores de búsqueda y solo se puede acceder mediante un navegador Web especializado

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 (…).

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 (…)".

En virtud de lo expuesto, se da conocer la información descrita, con el propósito de ser sometidas a valoración y revisión por esa Administración 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: 2023.09.26 15:34:00 -06'00'

M.S. c. Olger Sánchez Carrillo
Auditor

OSC/RJS/EZCH/LDP/lbc

C. Auditoría-1111

Referencia: ID-99719