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

AS-AATIC-183-2022
31 de agosto de 2022

Doctora
Maria Eugenia Villalta Bonilla, gerente a.i
GERENCIA GENERAL –1100

Máster
Idannia Mata Serrano, subgerente a.i.
DIRECCIÓN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES – 1150

Estimadas señoras:

ASUNTO:	**Oficio de Asesoría relacionado a la gestión e implementación de la herramienta MicroCLAUDIA en el contexto del Ciberataque a la CCSS.**

En cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo para el período 2022, así como en atención del estudio "Auditoría de Carácter Especial sobre el Ataque Cibernético a la CCSS y sus efectos a partir de la desconexión de sistemas de información efectuados el 31 de mayo de 2022" comunicado mediante oficio AI-874-2022 del 6 de junio de 2022, y del artículo 5 de la sesión 9262 de la Junta Directiva del 30 de junio del 2022, esta Auditoría informa sobre lo identificado en torno a la gestión e implementación de la herramienta MicroCLAUDIA en el contexto del Ciberataque a la CCSS.

1. GENERALIDADES

1.1 Antecedentes

En el presente año, diversas Instituciones, así como Ministerios del Estado Costarricense, han sufrido ataques cibernéticos que han generado algún tipo de afectación en menor o mayor grado, por esta razón el Ministerio de Ciencia y Tecnología y Telecomunicaciones (MICITT) como ente rector en materia tecnológica a nivel nacional, gestionó la entrega del Software MicroCLAUDIA a la CCSS como parte del proceso de protección y mejora de la ciberseguridad para servidores y equipos locales Windows. Al respecto, de acuerdo con lo señalado en el oficio GG-DTIC-3001-2022 del 8 de abril de 2022 firmado por el Ing. Roberto Blanco Topping, en ese momento Subgerente a.i. de la Dirección de Tecnologías de Información y Comunicaciones, y la Ing. Vanessa Carvajal Carmona, jefe de la Subárea de Seguridad Informática, así como de otra documentación aportada por la Administración Activa, se identificó la siguiente gestión realizada:

- El 5 de mayo de 2022 el Lic. Roberto Lemaitre Picado, funcionario del Ministerio de Ciencia, Tecnología, y Telecomunicaciones (MICTT), envió correo electrónico a la Ing. Vanessa Carvajal Carmona, Ing. Mayra Ulate Rodríguez, Ing. Danilo Hernández Monge y al Ing. Roberto Blanco Topping solicitando la instalación del programa MicroCLAUDIA, bridando el api key (clave de instalación) correspondiente para su implementación.

- El 10 de mayo de 2022, la Ing. Vanessa Carvajal Carmona, le envía correo al Lic. Roberto Lemaitre Picado, indicándole que el api key aportado no está siendo reconocido en la instalación, por lo que no han podido realizar la ejecución del software. El mismo día, el Lic. Lemaitre Picado da respuesta al correo señalando que los temas relacionados con el MicroCLAUDIA deben ser enviados a la dirección microclaudia@ccn-cert.cni.es, para que sean atendidas las dudas y verifiquen el tema del api key.

- El 11 de mayo de 2022, el Lic. Roberto Lemaitre Picado, mediante correo electrónico, le informa a la Ing. Vanessa Carvajal Carmona, que, según indicación, la clave otorgada es la correcta, por lo que podría verificar si se está ingresando un espacio al final de la serie, o probar sin la etiqueta. El mismo día el Centro Criptológico Nacional de España, quien gestiona la herramienta MicroCLAUDIA, le informa mediante correo electrónico a la Ing. Vanessa Carvajal Carmona que el api key utilizado es el correcto y reitera también la recomendación de revisar si no han quedado espacios en blanco al principio o final de la línea, ante esto la Ing. Carvajal Carmona responde el mismo día, indicando que se ha probado en varios equipos que tienen salida a internet, con proxy y sin proxy, mediante línea de comando, levantando la aplicación, sin etiqueta, entre otros, persistiendo el mismo error.

- El 16 de mayo de 2022, mediante correo electrónico, el Lic. Roberto Lemaitre Picado le indica a la Ing. Vanessa Carvajal Carmona que, una vez revisado con el equipo de soporte, identificaron que al api key le falta la letra “d” al final de la serie, dicho aspecto fue reiterado también por parte del Centro Nacional Criptológico de España, mediante correo electrónico el 17 de mayo de 2022.

1.2 Implementación

Una vez solventado el problema del api key, se identificó que el 17 de mayo de 2022, se estableció una sesión de trabajo de forma remota, mediante la plataforma TEAMS con personal de la Dirección de Tecnologías y Comunicaciones, con el propósito de hacer las pruebas correspondientes en algunos equipos, y además, se definió, el plan de trabajo para el despliegue de la herramienta, el cual se estableció del 17 al 27 de mayo del 2022, incluyendo: instalación en equipos de pruebas, servidores de CODISA, servidores de Oficinas Centrales, y la implementación de equipos por dominios.

Con la implementación de dicho plan, al 31 de mayo de 2022, se efectuaron 27,610 despliegues programados a través de la herramienta System Center Configuration Manager (SCCM), de los cuales se lograron concretar un total de 22,071 equipos, para un porcentaje de 79,94%, posterior a esta fecha, de los 11,422 despliegues programados se alcanzó una cobertura de 733 equipos, para una cobertura del 6.42%, y luego se dio la orden de no encender los equipos, en tanto no se revisaran y se dieran por limpios.

2. SOBRE LA HERRAMIENTA MICROCLAUDIA Y LAS VACUNAS CONTRA EL RANSOMWARE DEL ATAQUE CIBERNÉTICO A LA CCSS

MicroCLAUDIA es una herramienta que proporciona protección ante nuevas campañas y amenazas malware del tipo ransomware, mediante el despliegue de vacunas que impiden que se infecten los equipos, esta es gestionada por el Centro Criptológico Nacional de España (CCN), y la conexión del agente al servicio central está ubicado en la nube del CCN-CERT, donde se puede descargar y ejecutar las vacunas necesarias.

Esta herramienta potencia las vacunas basadas en la simulación de los mecanismos de control de ejecución del ransomware, y se utiliza como complemento a las soluciones de antivirus y Endpoint Detection and Response (EDR) y por lo tanto no las sustituye, asimismo de acuerdo con lo señalado por la CCN-CERT, el MicroCLAUDIA no protege contra cualquier tipo de malware, ni tampoco para algún tipo de ransomware para el que este herramienta no disponga vacuna o utilice técnicas que las vacunas existentes no puedan emular.

Al respecto y ante el ataque cibernético sufrido en la CCSS el 31 de mayo de 2022, la Dirección de Tecnologías de Información y Comunicaciones realizó una revisión de la base de datos de vacunas que utiliza microCLAUDIA, específicamente la versión 1.8.0, misma que estaría instalada en los 22,071 equipos institucionales y que disponía de 103 vacunas al momento del ataque, esto según lo señalado en el oficio GG-DTIC-3001-2022 del 8 de abril de 2022 firmado por el Ing. Roberto Blanco Topping, en ese momento Subgerente a.i. de la Dirección de Tecnologías de Información y Comunicaciones, y la Ing. Vanessa Carvajal Carmona, jefe de la Subárea de Seguridad Informática, y en el cual también se indica lo siguiente:

"El 08 de junio del 2022, se realizó el análisis de las vacunas disponibles por microCLAUDA, lo cual permitió identificar 6 vacunas relacionadas con el ransomware Hive, de las cuales se constató lo siguiente:

- *Primera Vacuna, Id 87: se constató que esta actúa sobre el archivo "xxx.exe", siendo este unos de los archivos identificados como maliciosos producto del ataque del 31 de mayo del 2022, a las 01 horas con 30 minutos. Esta vacuna se generó el 31 de mayo del 2022, a las 07 horas con 42 minutos, hora de Costa Rica.*

- *Segunda Vacuna, Id 91: Esta actúa sobre el archivo "xxx.dll", también identificado por la CCSS como software malicioso al momento del ataque recibido. La vacuna se creó el 31 de mayo del 2022 al ser las 10 horas con 13 minutos, hora de Costa Rica.*

- *Tercera Vacuna, Id 92: Esta también actúa sobre el archivo "xxx.dll", esta fue creada el 01 de junio del 2022, al ser las 3 horas con 38 minutos, hora de Costa Rica.*

- *Cuarta Vacuna, Id 93: Esta vacuna actúa sobre el archivo "yyy.dll", este archivo malicioso fue identificado por la CCSS durante el ataque recibido el 31 de mayo del 2022, perpetrado a las 01 horas con 30 minutos. Esta vacuna se creó el 02 de junio del 2022, al ser las 8 horas con 21 minutos, hora de Costa Rica.*

- *Quinta Vacuna, Id 94: Esta vacuna también actúa sobre el archivo "yyy.dll", esta fue creada el 02 de junio del 2022, al ser las 8 horas con 28 minutos, hora de Costa Rica.*

- *Sexta Vacuna, Id 96: Esta es una vacuna especifica desarrollada para Costa Rica, en la base de datos se identifica con el nombre "Hive especifico CR", misma que actúa sobre el comando específico que activaba el ransomware identificado como malicioso en la madrugada del 31 de mayo 2022, esta vacuna fue creada el 02 de junio del 2022 al ser las 10 horas con 13 minutos, hora Costa Rica.*

Adicionalmente, según informó el Ing. Sergio Paz Morales, jefe del Área de Ingeniería de Sistemas, se verificó que microCLAUDIA no disponía de las vacunas necesarias para contener el ciberataque, siendo que estas fueron desarrolladas a partir del 31 de mayo del 2022, posterior de acaecido el hecho.

Por lo anterior, es menester de esta Dirección de Tecnologías de Información y Comunicaciones, señalar que los 22 071 equipos que disponía del agente microCLAUDIA instalado, no estaban protegidos contra el ransomware Hive al momento del ataque, aspecto que fue confirmado por los colaboradores del Centro Nacional Criptológico de España de manera verbal en la sesión del 9 de junio del 2022".

Así mismo, el 21 de julio de 2022 en reunión virtual efectuada con la Auditoría Interna, el personal de la empresa Deloitte que atendió el ciberataque del 31 de mayo de 2022, indicó lo siguiente:

"En relación con el programa Micro Claudia y si este pudo o ayudó a contener el ataque cibernético, el Ing. Emanuelle Bolaños explicó que el Micro Claudia es una herramienta basada en el motor de Claudia que está enfocada en la detección y/o prevención del ransomware, a su criterio teniendo la herramienta Micro Claudia es un 50% y 50%, ya que la herramienta si funciona, es la que dio el indicio para saber dónde estaba el binario que explotaba la difusión del malware, por ende se pudo iniciar con la contención del escenario.

Sin embargo Micro Claudia no va a evitar que el ataque se genere, si él no tiene la vacuna específica para ese malware en específico, por lo que si el malware que se está implantando es hecho a la medida por más Micro Claudia que se disponga, no va a servir para contenerlo ya que es una pieza de malware no conocida hasta ese momento, por esta razón Micro Claudia recolecta piezas de malware para ir creando las vacunas para que si por alguna razón uno de los comportamientos del ransomware que afecta una empresa es similar al que tuvo la Caja, ya conoce como detener ese ataque, en el caso de la Caja el malware fue creado a la medida y el Micro Claudia no lo iba a detener. De hecho, el Centro Criptológico Nacional de España (CCN-CERT) elaboró vacunas para el tipo de malware HIVE que atacó la CCSS, pues no existían, a partir de las piezas de malware que recopilaron de equipos CCSS encriptados".

Además de lo anterior, en la investigación de las vacunas de la herramienta microCLAUDIA que realizó el Ing. Sergio Paz Morales, jefe a.i. del área de Ingeniería de Sistemas de la Dirección de Tecnologías de Información y Comunicaciones, se emitieron recomendaciones con el objetivo de implementar satisfactoriamente dicha herramienta considerando la complejidad, extensión y particularidades del parque tecnológico institucional, entre las que se encuentran:

"1. Elaborar una solicitud formal a Presidencia Ejecutiva, para que nos colabore a coordinar con el MICITT y el fabricante de microCLAUDIA, las siguientes mejoras:

a) *El software debe indicar al usuario, de forma clara, que está funcionando correctamente o si tiene algún problema en su funcionamiento o configuración:*

- *El usuario solamente puede ver un ícono en la barra de tareas, que no le indica si está funcionando correctamente o no.*

b) *El software debe indicar al usuario, de forma clara, si está actualizado, o la fecha a la cual se encuentran las definiciones de vacunas.*

- *El usuario solamente puede ver el ícono del microCLAUDIA en la barra de tareas, no puede saber si se encuentra actualizado o no.*

c) *El software debe indicar al usuario, el log de eventos detectados, o bien el log en blanco si no ha detectado eventos.*

- *El usuario no puede verificar si el microCLAUDIA ha identificado actividad sospechosa, solo muestra una notificación instantánea y después no hay manera, por parte del usuario, de verificar si en su PC se ha detectado actividad sospechosa o malisiosa.*

d) *El software debe utilizar la configuración del sistema para conectarse a internet, no la configuración dentro del archivo config.json, adicionalmente debe permitir visualizar la configuración que está utilizando para conectarse al servidor de actualizaciones.*

- *La configuración de conexión al servidor de actualizaciones se realiza en el momento de la instalación, no corresponde con la configuración de conexión del sistema operativo, de manera que, si el usuario tiene distintas ubicaciones, proxy's institucionales o realiza teletrabajo, no le es posible cambiar dicha configuración.*
- *Si la instalación se realiza con el proxy institucional, ese equipo únicamente va a solicitar actualizaciones a través de la navegación por medio del proxy institucional, si el usuario teletrabaja ocasionalmente, cuando esté teletrabajando no recibirá dichas actualizaciones.*

e) La CCSS no tenía acceso a la consola de microCLAUDIA para conocer la cantidad de despliegues efectivos (validar con Vanessa)

- *Hasta hace poco tiempo, el personal de seguridad de la Institución no tenía acceso a la consola de microCLAUDIA, para observar los despligues en dicha consola y monitorear el servicio.*

f) Ocultar el archivo de configuración del sistema, con el fin de que no sea objeto de un ataque ransomware que modifique sus parámetros de configuración, invalidando o haciendo que el sistema se interrumpa o se comporte de manera errática.

- *El archivo de base de datos de vacunas y configuración del sistema (config.json), es vulnerable a un ransomware que se encargue de ubicar el archivo config.json y alterar su contenido con el fin de interrumpir, inhabilitar o corromper la información de dicho archivo o de vacunas llegando incluso a ser un riesgo para sí mismo en caso de ser alcanzado por un atacante.*

g) Las notificaciones en la consola del microCLAUDIA, deben incluir todos los datos del equipo cliente, no solo el nombre, sino también la IP, con el fin de que el administrador logre ubicar rápidamente el equipo comprometido.

- *La consola de microCLAUDIA, únicamente notifica al administrador del nombre del equipo que está siendo comprometido, no indica su IP, en el caso de equipos administrados por proveedores externos, o equipo clínico, no siempre es posible modificar el nombre del equipo, por lo que se requiere que la IP sea parte de las notificaciones, para rastrear de manera segura y efectiva la ubicación del equipo comprometido.*

2. Solicitar al MICITT el acceso al personal de Seguridad de TI de la CCSS a la consola de MicroCLAUDIA, para su correspondiente monitoreo.

3. Solicitar a Presidencia Ejecutiva la coordinación con el MICITT para crear una comisión interinstitucional que pueda aplicar mejoras al código fuente de microCLAUDIA, así como para lograr participar activamente en la generación de vacunas específicas para los ataques ransomware que presumimos que continuarán atacando a las Instituciones públicas costarricenses".

3. VIGENCIA DEL LICENCIAMIENTO DE LA HERRAMIENTA MICROCLAUDIA

Esta Auditoría tuvo conocimiento mediante un artículo periodístico del medio de comunicación digital CRHoy del 27 de agosto de 2022, que la donación recibida de la herramienta MicroCLAUDIA solo tienen un año de vigencia y así consta en el Plan General sobre los Ciberataques aprobado el 21 de julio de 2022, por la Junta Directiva de la Comisión Nacional de Emergencias, en dicho Plan se señala que es importante que el MICITT mantenga comunicación con las instituciones para que realicen las previsiones presupuestarias que les permita asumir los costos de la protección con esta o cualquier otra herramienta que resulte oportuna.

CONSIDERACIONES NORMATIVAS

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 (…).

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 (…)".

CONSIDERACIONES FINALES

Esta Auditoría identificó que el 5 de mayo de 2022, le fue suministrado a la CCSS por parte del MICITT el programa MicroCLAUDIA, con el objetivo de fortalecer la ciberseguridad en la institución, no obstante la clave de acceso dada, presentó un error y no fue hasta el 16 de mayo de 2022 que el MICITT solventó la situación presentada, entregando la clave correcta, fue así como el 17 de mayo de 2022, se inició por parte de la Dirección de Tecnologías de Información y Comunicaciones con el plan de implementación de la herramienta, generando una instalación en 22,071 equipos al 31 de mayo de 2022, cuando se presentó el ataque cibernético a la CCSS.

Así mismo, se identificó que dicha herramienta disponía de 103 vacunas al momento del ataque, no obstante, no incluía la del ransomware que afectó a la CCSS, dado que este fue creado específicamente para la Caja, por lo que no fue hasta que se dio el ataque, que la herramienta microCLAUDIA pudo crear la vacuna correspondiente.

Se evidenció, además, que el licenciamiento de dicha herramienta que fue otorgada por el MICITT en el contexto de los ataques cibernéticos que ha venido sufriendo el país, tiene una fecha de vencimiento de un año, y así consta en el Plan General sobre los Ciberataques de la Comisión Nacional de Emergencias.

Por todo lo anterior, estima pertinente esta Auditoría que la Administración Activa realice las gestiones correspondientes, para continuar y mantener una adecuada protección de los equipos y los datos institucionales ante ataques por ramsonware o algún otro tipo de malware que puedan volver a afectar a la Institución, por lo que se debe de mantener una comunicación constante con las autoridades correspondientes del MICITT, con el objetivo de coordinar la estrategia entorno a la continuidad del microCLAUDIA o la implementación de cualquier otro instrumento anti-malware, o someter en caso de que le corresponda a la Institución, realizar con la anticipación necesaria, la valoración técnica y presupuestaria de la adquisición e implementación de la herramienta que proteja a la Caja de futuros ataques por ransomware y que dispongan de las vacunas necesarias para disminuir la posibilidad de la materialización de riesgos como la presentada el pasado 31 de mayo de 2022.

Asimismo, en caso de que MicroCLAUDIA sea la herramienta que continúe brindando el servicio a la CCSS, considerar las gestiones correspondientes para que las recomendaciones emitidas en el informe de la investigación de las vacunas de la herramienta microCLAUDIA que realizó el Ing. Sergio Paz Morales, jefe a.i. del área de Ingeniería de Sistemas de la Dirección de Tecnologías de Información y Comunicaciones sean consideradas para la mejora correspondiente.

Al respecto, esta Auditoría informa sobre lo descrito, con el objetivo de que la Dirección de Tecnologías y Comunicaciones en su rol de rector y direccionamiento tecnológico, valoren dentro de sus estrategias la información expuesta y se profundice en el tema de así requerirlo, reforzando los mecanismos de ciberseguridad, y reduciendo la posibilidad de que se vuelvan a materializar riesgos que afecten las actividades sustantivas de la institución, teniendo así un efecto directo en la atención de la población que hace uso de los servicios institucionales.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.08.31 16:27:13 -06'00'

M.Sc. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/LDP/lbc

C. Doctor Álvaro Ramos Chaves, presidente, Presidencia Ejecutiva –1102.
Auditoría