Ataque cibernético al Hospital Ciudad Neily, Caja Costarricense Seguro Social, acciones realizadas, 31 de mayo-31 de agosto 2022

Marcela Leandro Ulloa, M.D, M.Sc[1]
1:Caja Costarricense Seguro Social, Hospital Ciudad Neily, Costa Rica; mleandrou@ccss.sa.cr

ABSTRACT:

Objective. Describe the cyberattack and the actions taken to mitigate it, which occurred in the period from May 31 to August 31, 2022, in a peripheral hospital 3 the Hospital Ciudad Neily (HCN) that belongs to the Costa Rican Social Security Fund, in the city of Puntarenas, Costa Rica. **Material and methods**. It is cross-sectional observational qualitative research in the period from May 31 to August 31, 2022. **Results.** In the HCN, 90% of the servers suffered damage to their information, while in the Costa Rican Social Security Fund (CCSS) approximately 85% of the existing servers suffered damage. In the HCN of the final 315 terminals (computers, tablets, others) 120 (38%) were infected; while in the CCSS of the final 39,650 terminals, 9,600 (27%) were infected. **Conclusion.** The cyberattack affected end servers and terminals that did not have Microclaudia software, or that did not have it updated; also, those that were on at the time of the attack or during it. The actions to deal with the emergency were determination, assessment, and repercussion of the damages on the day of the cyberattack; implementation of contingency plans to allow attention to users. During the following months, the determination of inputs was made to continue the physical care, cleaning of the equipment to be able to upload the systems and upload of electronic systems. Preventive measures must be taken for future cyberattacks that were determined with experts in the field.

Key words: cyber-attack, CCSS, Ransomware, Costa Rica, Ciudad Neily Hospital.

RESUMEN:

Objetivo. Describir el ciberataque y las acciones realizadas para mitigarlo, ocurrido en el periodo del 31 de mayo al 31 de agosto del 2022, en un hospital periférico 3 el Hospital Ciudad Neily (HCN) que pertenece a la Caja Costarricense Seguro Social, en la ciudad de Puntarenas, Costa Rica. **Material y métodos.** Es una investigación cualitativa observacional transversal en el periodo de tiempo del 31 de mayo al 31 de agosto del 2022. **Resultados.** En el HCN el 90% de los servidores sufrieron daños en su información; mientras que en la Caja Costarricense del Seguro Social (CCSS) sufrieron daños aproximadamente el 85% de los servidores existentes. En el HCN de las 315 terminales finales (computadoras, tabletas, otras) fueron infectadas 120 (38%); mientras en la CCSS de las 39650 terminales finales se infectaron 9600 (27%). **Conclusión.** El ciberataque afectó los servidores y terminales finales que no tenían el software de Microclaudia, o que no lo tenían actualizado; además las que estaban encendidas en el momento del ataque o durante el mismo. Las acciones para atender la emergencia fueron determinación, valoración y repercusión de los daños el día del ciberataque; implementación

de planes de contingencia para permitir la atención de los usuarios. Durante los meses posteriores se realizó la determinación de insumos para continuar las atenciones en físico, limpieza de los equipos para poder subir los sistemas y subida de sistemas electrónicos. Se deben de tomar medidas preventivas para futuros ciberataques que se determinaron con expertos en la materia.

Palabras clave: ciberataque, CCSS, Ransomware, Costa Rica, Hospital Ciudad Neily.

INTRODUCCIÓN

Un ciberataque es un intento de desactivar ordenadores, robar datos o utilizar un sistema informático infiltrado para lanzar ataques adicionales (Unisys, 2022a). Los ciberdelincuentes utilizan diferentes métodos para lanzar un ciberataque que incluye malware, phishing, ransomware, ataque de intermediario u otros métodos. El malware es un término que describe a los programas maliciosos, incluidos programas espía, ransomware, virus y gusanos. Los programas maliciosos infringen una red a través de una vulnerabilidad, normalmente cuando un usuario hace clic en un enlace peligroso o un archivo adjunto de correo electrónico que, a continuación, instala software peligroso. El ransomware es una clase de malware que restringe el acceso al sistema informático que infecta y exige un rescate pagado al creador del malware para que se elimine la restricción. Algunas formas de ransomware cifran archivos en el disco duro del sistema, mientras que otras simplemente bloquean el sistema y muestran mensajes destinados a convencer al usuario para que pague. (Unisys, 2022b).

Costa Rica es un país que se encuentra en Centroamérica, que tiene una institución pública que presta atención de servicios de salud llamada Caja Costarricense del Seguro Social (CCSS). La CCSS tiene tres niveles de atención, el primer, segundo y tercer nivel de atención. El primer nivel de atención está conformado por áreas de salud tipo 1, 2 y 3; el segundo nivel está formado por hospitales periféricos 1, 2 y 3 y regionales; además, el tercer nivel lo conforman los hospitales nacionales y especializados.

El Hospital Ciudad Neily, es un nosocomio periférico 3, pertenece a la Red Integrada de Servicios de Salud Brunca, cuenta con 77 camas hospitalarias censables, 13 camas de observación en el servicio de emergencias, 6 salas de operaciones, 32 consultorios de atención de consulta externa. La población adscrita que tiene acceso a los servicios es de aproximadamente 50 mil habitantes. El hospital cuenta con los servicios de emergencias, consulta externa, laboratorio, radiología, sala de operaciones, hospitalización, farmacia, trabajo social, servicios administrativos-financieros. Los funcionarios que laboran en el centro son aproximadamente 567 funcionarios distribuidos en los tres turnos que cubren las 24 horas del día, los 365 días del año.

El ciberataque se realizó el 31 de mayo del 2022 por el grupo llamado Hive Ransomware Group. Este grupo apareció por primera vez en junio del año 2021 y probablemente funciona como un ransomware basado en afiliados, emplea una amplia variedad de tácticas, técnicas y procedimientos (TTP), lo que crea desafíos importantes para la defensa y la mitigación. Hive utiliza múltiples mecanismos para comprometer las redes comerciales, incluidos los correos electrónicos de *phishing* con archivos adjuntos maliciosos para obtener acceso y el Protocolo de Escritorio Remoto (RDP en inglés) para moverse una vez en la red. En el caso del ataque realizado a la CCSS y en específico al Hospital Ciudad Neily (HCN) se utilizó un ransomware que cambió las

extensiones de los archivos de los discos duros de las terminales finales del centro (servidores, computadoras, laptops, tabletas, etc.) (Unisys, 2022b).

MATERIALES Y MÉTODOS

Es una investigación cualitativa observacional transversal en el periodo de tiempo del 31 de mayo al 31 de agosto del 2022. Se realiza la recolección de los datos mediante observación cualitativa de las acciones realizadas en el Hospital Ciudad Neily por parte de las jefaturas o coordinadores de los servicios y los funcionarios del nosocomio.

El periodo de estudio y análisis del ciberataque fue entre el 31 de mayo al 31 de agosto del 2022, se analizaron todas las consecuencias del ciberataque en la atención de personas usuarios internas y externas y las acciones realizadas para poder disminuir el daño provocado.

Las afectaciones que se buscaban en las computadoras y servidores fueron información encriptada, con extensiones que no concordaran con archivos comunes de los sistemas que se utilizaban en el nosocomio; todas las computadoras de escritorio, computadoras portátiles, MIFI, tabletas fueron analizadas por el equipo de CGI (Centro de Gestión de Informática) de la institución. Se analizaron los servidores, las redes inalámbricas y las computadoras finales del centro.

Las acciones analizadas son las realizadas por las jefaturas, coordinadores o funcionarios del centro médico realizadas para mantener la atención de los usuarios Y lograr restituir los sistemas de información.

RESULTADOS

La Caja Costarricense del Seguro Social (CCSS) y el Hospital Ciudad Neily (HCN) sufrieron un ataque cibernético (ciberataque) el 31 de mayo a medianoche; los perpetradores fueron un grupo de hackers llamado Hive Ransomware Group. Las acciones que produjo el ransomware en las terminales finales y en los servidores de la CCSS y el HCN fue la encriptación de los archivos, creando extensiones no compatibles con la apertura de estos con los programas existentes, las impresoras imprimieron mucha cantidad de información que no era entendible, utilizando símbolos y letras. La información que se sincronizó en el OneDrive de los funcionarios después del ciberataque estaba infectada y encriptada. Los daños ocurridos el día del ciberataque en la red tecnológica fueron los siguientes: Servidores dañados en el HCN 90% (9) y 85 % (847) en la CCSS; terminales finales que sufrieron daños en el HCN corresponde al 38% (120) del HCN y 27% (9600) de la CCSS.

Dentro de las acciones realizadas para disminuir los daños estuvieron la desconexión de los sistemas de información como EDUS (Expediente Digital Único en Salud), SIPE (Sistema de Información del Personal), SIGES (Sistemas de Gestión en Salud), SOGER (Sistema de Recursos Humanos), SIFA (Sistema de información farmacéutica), SISVE (sistema de información de vigilancia epidemiológica), SIVA (sistema de información de vacunación), LabCore (sistema de información de laboratorio), RIS-PACS (Imágenes médicas), Cubos de información, SOCO (sistema de información de mantenimiento), SIGES (sistema de información de recursos humanos), SIPE (sistemas de información de recursos humanos), correo electrónico, office 365, RCPI (sistema de información de incapacidades), Sistemas de información de presupuesto, validación de derechos, sitios

colaborativos como SharePoint institucional. Además, se realiza desconexión de los servidores y terminales finales a las redes alámbricas e inalámbricas.

El 100% de las terminales finales infectadas tenían las siguientes características: 1. No tenían el MicroClaudia instalado y 2. tenían el programa microClaudia instalado, pero no actualizado; además habían estado encendidas durante el inicio del ciberataque, o se habían conectado a la red inalámbrica o alámbrica posterior al ataque. Las acciones realizadas posterior al ciberataque se dividieron en 1. plan de contingencia que se realizaron mientras se habilitaban los sistemas (hasta mes de agosto), 2. plan de preparación para la recuperación de los sistemas y 3. Plan de habilitación de los sistemas. En el periodo del 31 de mayo al 31 de agosto se logró habilitar EDUS, LabCore y SIFA.

DISCUSIÓN

Costa Rica desde principios del mes de abril del 2022 presentó ciberataques en diferentes instituciones como lo fue le Ministerio de Hacienda, MICITT, Instituto Meteorológico Nacional, RACSA, Ministerio de Trabajo y Seguridad Social, Caja Costarricense del Seguro Social (CCSS) (CNE, 2022).

Muchos de los ciberataques fueron perpetrados por un grupo llamado CONTI, la cual es una organización criminal de origen ruso dedicada a realizar ataques de ransomware por medio de la infección de equipos y servidores, sustrayendo archivos y documentos de servidores para luego exigir un rescate (CNE, 2022).

Con base en las acciones realizadas por estos hackers en el país, es que la CCSS comenzó la vacunación de las terminales finales y servidores con el programa microClaudia, que es una herramienta que proporciona protección ante nuevas campañas y amenazas malware del tipo ransomware mediante el despliegue de vacunas que impiden que se infecte el equipo, desarrollado en la Universidad Carlos III de España (2022).

La CCSS el 31 de mayo del 2022 sufrió un ciberataque por un grupo de hackers llamado Hive Ransomware Group, utilizando un programa ransomware que infectó algunos servidores y terminales finales de la institución en su totalidad, al igual que le ocurrió al Hospital Ciudad Neily (HCN).

La capacidad instalada tecnológica, en el momento del ciberataque de la CCSS es de 996 servidores y 10 servidores en el HCN; además, tienen 39650 terminales finales en la CCSS y 315 en el HCN. Los servidores del HCN almacenan información esencial del nosocomio, como son EDUS (Expediente Digital Único en Salud), SIPE (Sistema de Información del Personal), SIGES (Sistemas de Gestión en Salud), SOGER (Sistema de Recursos Humanos), SIFA (Sistema de información farmacéutica), SISVE (sistema de información de vigilancia epidemiológica), SIVA (sistema de información de vacunación), LabCore (sistema de información de laboratorio), RIS-PACS (Imágenes médicas), Cubos de información, SOCO (sistema de información de mantenimiento), SIGES (sistema de información de recursos humanos), SIPE (sistemas de información de recursos humanos), RCPI (sistema de información de incapacidades), Sistemas de información de presupuesto, validación de derechos, respaldos de todas las terminales finales y circuito cerrado.

Durante el ciberataque para poder disminuir los efectos producidos por el mismo, se ejecutaron las acciones que el MICITT había indicado realizar en caso de ciberataque que eran: 1. Desconexión de equipos de la red para hacer las revisiones respectivas, 2. Identificación del punto de entrada del virus, 3. Revisión de los equipos,

4. Revisión y segmentación de la red, 5. Revisión de respaldos, 6. Instalación de herramientas de seguridad (CNE, 2022).

Con base en lo anterior, las primeras acciones realizadas en el HCN fueron: 1. Deshabilitación de los sistemas de información: EDUS, SISVE, SIVA, LabCore, Imágenes médicas, Cubos de información, SOCO, SIGES, SIPE, correo electrónico, office 365, RCPI (incapacidades), reporte de laboratorios, SharePoint donde se comparte la información de Plan Presupuesto y otros, validación de derechos, presupuesto, entre otros; 2. Apagar todas computadoras , desconectarlas de la red alámbrica e inalámbrica; 3. Activación del CCO, que implica la reunión con todas las jefaturas y coordinaciones de los servicios para evaluar los daños producidos y las acciones para realizar para disminuir la vulnerabilidad del hospital y poder activar la atención de los pacientes en todos los servicios, en especial en emergencias y en hospitalización.

Los daños encontrados fueron son los siguientes: el 90% (9) de los servidores y el 38% (120) de las terminales finales del HCN y el 85% (847) de los servidores y el 27% (9600) de las terminales finales de la CCSS fueron afectados; la información se vio infectada por el ransomware provocando la encriptación de esta, el cambio en la extensión de los archivos que no podían ser abiertos con el software existente.

Las repercusiones de la desconexión de las terminales finales y los servidores en el HCN fueron los siguientes: 1. la desconexión de EDUS afectó a Consulta externa, Emergencias, Hospitalización, Trabajo Social, Sala de Operaciones, REDES, Laboratorio, Radiología y Farmacia, al no poder acceder a la información del expediente electrónico de los usuarios; 2. la desconexión de los repositorios de imágenes afectó la realización de exámenes especiales de radiología; además la realización de ultrasonidos se vio afectado por no tener computadoras para hacer los reportes, no se tenía acceso a las imágenes médicas que estaban incluidas en el receptáculo de imágenes; 3. la desconexión de SIFA afectó la gestión de los medicamentos despachados y los almacenados, con la imposibilidad de tramitar las recetas que se hicieran en electrónico anterior al ciberataque; 4. la desconexión de LabCore implicó la imposibilidad de automatización de los reportes de los exámenes realizados, ni la obtención de la información de los exámenes realizados anteriormente, además de tener que realizar los laboratorios en forma manual y no automatizada; 5. la desconexión del SIPE y SIGES produjo problemas en la solicitud y autorización de permisos para los funcionarios, la inclusión de las planillas y el pago de los salarios, los procesos de selección, los concursos en propiedad; 6. la deshabilitación del sistema de incapacidades no permitió el ingreso y pago de las incapacidades pendientes, ni de las nuevas y 7. el sistema SOCO inactivo produjo la pérdida de las solicitudes de mantenimiento de la infraestructura y de los equipos en el hospital.

Para poder dar atención a los usuarios en los servicios de emergencias, hospitalización, sala de operaciones, que eran personas que no podían ser enviados a la casa sin ser atendidos es que se realiza el plan de contingencia que es iniciar la atención de los usuarios mediante medios físicos, como expediente físico, formularios en papel para poder brindar los servicios que necesitan los usuarios. Los servicios de emergencias, hospitalización, consulta externa, trabajo social y sala de operaciones realizan las atenciones por medios físicos en papel. Radiología trabajó con las unidades de rayos equis portátiles, el fluoroscopio y ortopantógrafo no estuvieron en funcionamiento por no poder conectarse a la red institucional. El Ultrasonido se habilitó con una computadora desconectada a la red para hacer los reportes. Los exámenes de laboratorio se procesaron manualmente y se reportan individual y manualmente. En Farmacia se reciben las recetas en físico y se

despachan al día siguiente; las instrucciones en los medicamentos se imprimen individualmente en una computadora e impresora que se habilitó; el inventario de despacho no se puede llevar. Las acciones de personal que se ingresaron antes del 31 de mayo no se pudieron extraer del sistema, para contrarrestar esto se creó un lugar específico para que las secretarias en conjunto con el personal de recursos humanos realizaran y tramitaran las acciones que están pendientes para el pago de la catorcena siguiente. En consulta externa se hace el llenado de los documentos a mano, la cita del paciente no se le otorga en el momento, sino que se dejan pendientes al momento de tener los sistemas de SIAC (citación) funcionando se le llama por teléfono para otorgarle la cita. Las cirugías que se realizaron fueron las ambulatorias y prioritarias que no necesiten valoración preoperatoria y si necesitan valoración preoperatoria se le realiza el día anterior los exámenes para poder tener acceso a los resultados. Las incapacidades se realizan en físico y se registran en un archivo de Excel para llevar el control. Se utiliza el WhatsApp para enviar información a las jefaturas y los SOCO, ya que no se tiene correo electrónico activo. La información del sistema de vigilancia epidemiológica se deshabilitó por lo que se realiza la boleta VE-01 en físico, se tabula en REDES y se resguarda en Vigilancia Epidemiológica.

En los días posteriores al ciberataque se realizó el inventario de todas las terminales finales del centro para determinar la localización de las infectadas y las no infectadas, esto se realizó en conjunto con el personal del CGI (centro de gestión de informática) y las jefaturas las computadoras y tabletas que estaban infectadas y las que no estaban infectadas por parte de las jefaturas y los coordinadores de cada servicio. Con el inventario de los equipos afectados se inició los procesos previos para la habilitación de los equipos que se encuentran limpios del ransomware. Al analizar cuáles equipos fueron infectados y cuáles no encontramos que el 100% de las terminales finales infectadas tenían las siguientes características: 1. No tenían el programa microClaudia instalado y 2. tenían el programa microClaudia instalado, pero no actualizado; además habían estado encendidas durante el inicio del ciberataque, o se habían conectado a la red inalámbrica o alámbrica posterior al ataque. Lo que implicó que las computadoras que están en los servicios de atención directa a pacientes como son emergencias, hospitalización, consulta externa, sala de operaciones se vieron afectadas en el HCN.

En el mes de junio se realizaron acciones para poder habilitar la atención de los usuarios internos y externos que se habían dejado de prestar como: 1. Habilitar computadoras para que se pudieran procesar las acciones de personal y así poder estar seguros de que los trabajadores recibirían el pago en los meses siguientes al ciberataque. 2. Habilitar el Labcore en farmacia, para poder realizar los informes de los estudios en forma digital y también el procesamiento de las muestras se realiza automáticamente. 3. Habilitación de la lectura de TAC por parte de los radiólogos, mediante la compra del lector de DVD y colocación de una computadora para la lectura; 4. Actualización de las computadoras no infectadas con el programa microClaudia, Windows Defender y actualización con programas Windows con versión mayor de Windows 10 y actualización de los servidores con versión mayor o igual a SERVER 2016; 5. Formateo de todos los equipos infectados. 6. En consulta externa se hace el llenado de los documentos a mano, la cita del paciente no se le otorga en el momento, sino que se dejan pendientes al momento de tener los sistemas de SIAC (citación) funcionando se le llama por teléfono para otorgarle la cita. 7. Las cirugías que se realizaron son ambulatorias y prioritarias que no necesiten valoración preoperatoria y si necesitan valoración preoperatoria se le realizó el día anterior los exámenes para poder tener acceso a los resultados. 8. Las incapacidades se realizan en físico y se registran en un archivo de Excel para llevar el control. 9. Utilización del WhatsApp para enviar información a las jefaturas y los SOCO, ya que no se

tiene correo electrónico activo. 10. La boleta VE-01 se imprime y se llena en físico, se tabula en REDES y se resguarda en Vigilancia Epidemiológica.

En el mes de julio se inicia con el levantamiento de los sistemas realizando las siguientes medidas: 1. Corrección en la nomenclatura de las terminales para que sean visualizadas en el sistema de seguimiento de MicroClaudia en España. 2. Reinicio de las credenciales de los funcionarios para la conexión al dominio de Gerencia Médica, mediante la actualización de los correos de cada funcionario; creando claves de seguridad más robustas. 3. Reinicio de las credenciales de los funcionarios en el MISE para acceder a EDUS (cuando sea levantado). 4. Levantamiento del FARCOM, sistema de farmacia para poder imprimir las instrucciones de los medicamentos de los pacientes y el inventario de fármacos. 5. Ingreso de las terminales al dominio de la CCSS. 6. Funcionamiento del ortopantógrafo mediante la grabación del estudio en CD, ya que no se puede conectar a la red institucional.

En el mes de agosto se continúan con acciones para poder levantar los sistemas y poder prestar una mejor atención a los usuarios. Esas actividades realizadas son las siguientes: 1. Certificación de los equipos de cómputo del hospital ante la CCSS para tener autorización de levantar los sistemas digitales. 3. Funcionamiento de los sistemas de SIPE y SIGES. 4. Restablecimiento del sistema local de presupuesto. 5. Restablecimiento del EDUS en emergencias y hospitalización. 5. Utilización del SIFA sin datos pues se perdieron en el ciberataque.

Es importante describir las actividades que se tuvieron que realizar para poder utilizar el EDUS en emergencias y hospitalización, por lo que se explica a continuación:

- El 20 de agosto iniciamos EDUS emergencias a medianoche, para esto se debió tener todos los funcionarios con las acreditaciones en el EDUS emergencias, todos debían tener la clave de ingreso al dominio GMedica actualizada, al igual que la clave MISE de los sistemas EDUS actualizados. Los pacientes que quedaron en la lista de trabajo del 31 de mayo se dejaron sin tocar, ni hacer modificaciones. El trabajo en emergencias fue un éxito, pero se tenía que imprimir los expedientes si los pacientes fueran hospitalizados, ya que no estaba aún el EDUS hospitalización levantado.
- El 24 de agosto se inició el EDUS hospitalización (SIAH – ARCA QUIRURGICA) a las 6 am, los procesos que realizo REDES fue dar de alta a los pacientes que estaban ingresados el 31 de mayo, luego ingresaron los pacientes que estuvieron hospitalizados y los egresaron. Todos los funcionarios debían tener las acreditaciones en EDUS hospitalización y las claves actualizadas para el ingreso del dominio GMedica y el MISE. Los pacientes que estaban con expediente en físico se continuaron en físico hasta su egreso y los que ingresaron ese día iniciaban en digital. Los egresos de los pacientes con expediente en físico también se egresaban en digital.

En conclusión, para poder hacer frente a todas las consecuencias del ciberataque se debe de llevar a cabo un conjunto de pasos para lograr levantar los sistemas que fueron vulnerados e infectados que se enlistan a continuación: 1. Realizar análisis situacional durante el ciberataque, 2. Conformación del CCO el día del ciberataque. 3. Tener un plan contingencial para este tipo de problemas. 4. Disminución de la ansiedad de las personas mediante la información que se presentaba. 5. Reunión diaria con el CCO para analizar lo realizado el día anterior y lo que se debe valorar para el día presente y para el futuro. 6. Trabajo en Equipo para solventar los problemas que se producen durante el día del ciberataque y los 3 meses siguientes. 7. Comunicación oficial y asertiva de lo que estaba ocurriendo y lo que se pensaba realizar con todos los funcionarios del centro. 8.

Disminución de la comunicación informal. 9. Mantener al personal informado y también agradecer por las acciones que están realizando en condiciones no óptimas. 10. Siempre tener una ruta por donde transitar durante la emergencia.

Las lecciones aprendidas para disminuir el riesgo de otro ataque son: 1. Crear claves de seguridad más robustas, 2. No compartir las claves con otras personas, 3. Eliminar las claves genéricas, 4. Fortalecer la seguridad de las terminales finales con antivirus más poderosos, 5. Tener respaldos que no estén asociados a los respaldos de los servidores en la red institucional, los respaldos deben ser realizados en equipos separados de la red, 6. Hacer que cada usuario tenga respaldo de su información en dispositivos de seguridad no vinculados a la red institucional (discos duros externos).

AGRADECIMIENTOS

Personal del Hospital Ciudad Neily por su dedicación, empeño y dar la milla extra. Población del área de atracción del Hospital por su paciencia y comprensión.

REFERENCIAS

CNE (2022). *Plan General de la Emergencia por ciberataques*. Recuperado de https://www.cne.go.cr/recuperacion/declaratoria/planes/Plan%20General%20de%20la%20Emergencia%20por%20Ciberataques.pdf

Unisys (2022a). *¿Qué es un ciberataque*? Recuperado de https://www.unisys.com/es/glossary/what-is-cyber-attack/

Unisys (2022b). *¿Qué es el ransomware?* Recuperado de https://www.unisys.com/es/glossary/ransomware/

Universidad Carlos III (2022). *Protección frente a ransomware: Centro de Vacunación CCN-CERT.* Recuperado de https://www.uc3m.es/sdic/articulos/2021/microclaudia#:~:text=El%20centro%20de%20vacunaci%C3%B3n%20del,que%20se%20infecte%20el%20equipo