Revista Científica General José María Córdova
ISSN: 1900-6586
ISSN: 2500-7645
Escuela Militar de Cadetes "General José María Córdova"

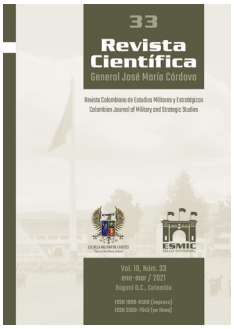
Tejo Machado, Nadjila; Rodrigues Martinez Basile, Felipe;
Cezar Amate, Flavio; Ramírez López, Leonardo Juan

Protocolo de informática forense ante ciberincidentes en telemedicina para preservar información como primera respuesta

Revista Científica General José María Córdova, vol. 19, núm. 33, 2021, pp. 181-203
Escuela Militar de Cadetes "General José María Córdova"

DOI: https://doi.org/10.21830/19006586.726

Disponible en: https://www.redalyc.org/articulo.oa?id=476268269009



Revista Científica General José María Córdova
(Revista colombiana de estudios militares y estratégicos)
Bogotá D.C., Colombia

ISSN 1900-6586 (impreso), 2500-7645 (en línea)
Web oficial: https://www.revistacientificaesmic.com

Protocolo de informática forense ante ciberincidentes en telemedicina para preservar información como primera respuesta

Nadjila Tejo Machado
https://orcid.org/0000-0001-9077-0671
nadjila.tejo@aluno.ifsp.edu.br
Instituto Federal de Educação, Ciência e Tecnologia de São Paulo, Brasil

Felipe Rodrigues Martinez Basile
https://orcid.org/0000-0002-0404-4807
felipe.basile@ifsp.edu.br
Instituto Federal de Educação, Ciência e Tecnologia de São Paulo, Brasil

Flavio Cezar Amate
https://orcid.org/0000-0002-0918-2707
amate@ifsp.edu.br
Instituto Federal de Educação, Ciência e Tecnologia de São Paulo, Brasil

Leonardo Juan Ramírez López
https://orcid.org/0000-0002-6473-5685
leonardo.ramirez@unimilitar.edu.co
Universidad Militar Nueva Granada, Bogotá D.C., Colombia

Citación: Machado, N. T., Basile, F. R. M., Amate, F. C., & Ramírez López, L. J. (2021). Protocolo de informática forense ante ciberincidentes en telemedicina para preservar información como primera respuesta. *Revista Científica General José María Córdova*, *19*(33), 181-203. http://dx.doi.org/10.21830/19006586.726

Publicado en línea: 1.º de enero de 2021

Para enviar un artículo:
https://www.revistacientificaesmic.com/index.php/esmic/about/submissions

Miles Doctus

Revista Científica General José María Córdova
(Revista colombiana de estudios militares y estratégicos)
Bogotá D.C., Colombia

Volumen 19, número 33, enero-marzo 2021, pp. 181-203
http://dx.doi.org/10.21830/19006586.726

Protocolo de informática forense ante ciberincidentes en telemedicina para preservar información como primera respuesta

Computer forensic protocol for preserving information as first response in telemedicine cyber incidents

Nadjila Tejo Machado, Felipe Rodrigues Martinez Basile y Flavio Cezar Amate
Instituto Federal de Educação, Ciência e Tecnologia de São Paulo, Brasil

Leonardo Juan Ramírez López
Universidad Militar Nueva Granada, Bogotá D.C., Colombia

Resumen. Este estudio presenta un protocolo de preservación de rastros y evidencias digitales ante ciberincidentes por medio de diferentes niveles de acceso de usuarios, con base en la informática forense. La aplicación de nuevas herramientas y sus funciones permite conservar información que puede esclarecer los tipos de ataques, la dinámica del delito, su materialidad y su autoría. Este es un protocolo que determina la primera respuesta digital, clasificada por niveles de urgencia, para apoyar la toma de decisiones manteniendo la cadena de custodia según el riesgo de volatilidad de los datos. Se concluye que este protocolo apoya el esclarecimiento de un ciberincidente y permite la correcta conservación de los datos, de manera que cada organización atacada pueda decidir qué datos debe priorizar en la identificación, el aislamiento y la protección de la información.

Palabras clave: acceso a la información; cibercrimen; informática forense; protección de datos; telemedicina

Abstract. This study presents a protocol for preserving digital traces and evidence in cyber incidents through different user access levels based on computer forensics. The implementation of new tools could preserve information that can help clarify the attack type and the crime's dynamics, its materiality, and authorship. This protocol determines the first digital response, classified by level of urgency, to support decision making while maintaining the chain of custody according to the risk of data volatility. It is concluded that this protocol helps clarify cyber incidents while respecting the correct preservation of data. Thus, each charged organization can decide which data should be prioritized in information identification, isolation, and protection.

Keywords: access to information; computer forensics; cybercrime; data protection; telemedicine

Sección: Dosier • Artículo de investigación científica y tecnológica

Recibido: 5 de octubre de 2020 • Aceptado: 1 de diciembre de 2020

Contacto: Felipe Rodrigues Martinez Basile ✉ felipe.basile@ifsp.edu.br

Introducción

El registro en papel de datos médico-clínicos ha sido reemplazado por el almacenamiento electrónico y el intercambio de información para mejorar la atención de los usuarios (Jarrett, 2017). Además de sus beneficios, los registros electrónicos también presentan desafíos y problemas de seguridad de la información (Babulak, et al., 2014). Por ello, para la gestión segura de la información, especialmente en el caso de la telemedicina, se han incrementado los estudios de los ciberataques, debido a la necesidad de brindar tecnologías seguras que estén alineadas con la normatividad de protección de datos. Así, la informática forense aparece como una estrategia para gestionar los ciberincidentes posteriores a un ciberdelito y promover que los desarrollos tecnológicos usados en telemedicina sean interoperables y mejoren la atención médica (Coventry & Branley, 2018).

La telemedicina es una aplicación de las tecnologías de las comunicaciones y de la información (TIC), ya que relaciona los registros de las historias clínicas electrónicas con los sistemas de información sanitaria (Basile et al., 2016). En este sentido, las TIC en telemedicina buscan ofrecer novedosos servicios de atención en salud que logren ampliar la cobertura, y allí el factor crítico es la distancia (Maldonado et al., 2016). Sin embargo, esta transmisión de datos en telemedicina implica el intercambio de información entre un equipo multidisciplinar que tiene puntos de seguridad débiles. Para ello, la integridad y autenticidad de los datos se asegura por diversos y robustos algoritmos de cifrado, gracias a los cuales se garantiza la confidencialidad de la privacidad de los datos trasmitidos, principalmente por la demanda de seguridad en la etapa de conectividad (Basile et al., 2019).

Está comprobado que, si ocurre un crimen cibernético, la informática forense ayuda en la investigación, y por lo mismo ahora se aplica en la gestión de la información confidencial registrada en telemedicina (Machado et al., 2019). La ciencia forense es el conjunto de conocimientos científicos y técnicos de diferentes áreas científicas (criminología, informática, medicina legal, patología, entre otras) que, aplicados interdisciplinarmente, pueden resolver las preguntas judiciales que apoyan investigaciones relacionadas con la justicia civil y penal, como la búsqueda de la verdad (Vallim, 2017).

Así, este estudio responde a la hipótesis de que la informática forense podría utilizarse en telemedicina para aclarar ciberincidentes mediante un protocolo de conservación de rastros y evidencias que, por medio de varios niveles de acceso a la información, ayude en la toma de decisiones durante una investigación.

Por lo anterior, el principal objetivo es utilizar la informática forense para validar un protocolo que logre preservar la evidencia digital, considerando varios niveles de acceso por parte de los profesionales de la salud que realicen registros en la historia clínica de pacientes. Además, se busca presentar una serie de herramientas útiles para la recopilación y adquisición de datos que ayuden al experto forense durante el postciberincidente. Finalmente, también se analiza la viabilidad de la informática forense de ciberincidentes en caso de la telemedicina para algunos escenarios.

Marco teórico

Informática forense

La informática forense desarrolla hipótesis y responde preguntas sobre el ciberincidente o delito mediante la recolección de evidencia que ayude a esclarecerlo (Carrier & Spafford, 2004), con el fin de preservar la integridad de los datos, analizarlos y resolver el delito (Kent et al., 2006). Además, la herramientas y técnicas forenses disponibles pueden aclarar los ciberincidentes, para así satisfacer la demanda proveniente de los ataques informáticos (National Institute of Standards and Technology [NIST], 2020).

Por otra parte, en el análisis de la información, debe mitigarse la volatilidad de los datos durante el proceso de recopilación y conservación de pruebas en la escena del crimen digital. Más aún durante el proceso de preservar rastros y evidencias, cuando puede haber volatilidad de la memoria, ya que los datos almacenados requieren de energía para conservarse en esta fase, denominada *post mortem* (Vallim, 2017).

Volatilidad

El término *volatilidad*, en este contexto, significa "sujeto a cambios". En otras palabras, esto significa que las pruebas pueden verse fácilmente comprometidas en su integridad y disponibilidad, e incluso pueden resultar destruidas. Por ende, minimizar la volatilidad de la fuente de la evidencia es de suma importancia al recolectar, proteger y examinar evidencia digital. Algo tan simple como apagar el dispositivo sospechoso, por ejemplo, puede comprometer información potencialmente valiosa que reside en su memoria: archivos sin terminar o eliminados; archivos abiertos; correos electrónicos o fragmentos de archivos de correos abiertos; contraseñas; nombres de usuarios; direcciones web o fragmentos de páginas web, y fragmentos o características del programa son solo algunos de los elementos que se pueden encontrar en un examen del espacio de la RAM (*random access memory*) (Bidgoli, 2006).

Método

La investigación desarrollada, analítica y exploratoria, parte de tres preguntas específicas que los autores se plantearon sobre la incidencia de los delitos cibernéticos en la telemedicina:

- ¿Cómo se podría utilizar la informática forense en la telemedicina?
- ¿Cuáles son las herramientas y funcionalidades disponibles de la informática forense?
- ¿Cómo se debe desarrollar un protocolo para preservar rastros y evidencias de los registros digitales en telemedicina con varios niveles de acceso?

Se plantean a continuación tres etapas de la investigación para responder la hipótesis y estas preguntas de investigación.

Etapa 1. Análisis de antecedentes

La revisión de literatura logró demostrar la viabilidad de la informática forense como estrategia de investigación de ciberincidentes en telemedicina. El análisis se basó en diferentes fuentes de información: primero se recurrió a Google Académico para lograr obtener un grupo amplio de referencias; luego, la búsqueda se refinó en la base de datos Pubmed usando los siguientes metadatos: "informática forense", "ciberseguridad" y "telemedicina". Como resultado, se analizaron 54 fuentes, incluidos artículos y libros de investigación.

Etapa 2. Evaluación de herramientas de la informática forense y su funcionalidad en modo *live forensics*

En esta segunda etapa, se plantearon las herramientas tecnológicas que configuran el *hardware* y el *software* para la investigación, recopilación y análisis del reporte de ciberincidentes de robo de datos en telemedicina. Se tomó como único referente al Instituto Nacional de Normas y Tecnología de Estados Unidos (NIST, 2019). El criterio de inclusión fueron las herramientas y su funcionalidad registradas hasta octubre de 2019 en su sitio web. Se logró diferenciar las herramientas y su funcionalidad de acuerdo con la volatilidad de los datos, es decir, durante la vida de estos, estrategia conocida como *live forensics*.

Etapa 3. Desarrollo del protocolo para preservar rastros y evidencias en telemedicina con varios niveles de acceso

Se partió del requerimiento de desarrollar un protocolo para preservar rastros y evidencias, destinado a ser usado en telemedicina con varios niveles de acceso de usuarios. Al respecto, se definieron nueve niveles de acceso de usuarios:

- Usuario (externo)
- Paciente (externo e interno)
- Enfermero
- Jefe de enfermeros
- Médico general
- Médico especialista
- Técnico de red informática
- Administrador de red informática

Conforme al requerimiento técnico, se usó el protocolo de Manchester como método de selección y clasificación de pacientes en el área de urgencias de la entidad de salud, lo que permite tomar decisiones sobre el nivel de atención que requiere cada paciente. De

esta forma, desde el ingreso del paciente, se decide el nivel de urgencia con base en su información, que debe preservar rastros y evidencias de acuerdo con la volatilidad de la memoria donde se almacena y si los datos necesitan energía o no para ser recolectados. En cuanto a ello, la memoria volátil es temporal y depende 100 % de la energía para registrar y almacenar los datos. Por su parte, la memoria no volátil es independiente, no requiere de la energía para registrar los datos, y, por consiguiente, una vez almacenados no se volatilizan.

El protocolo debe tener como parámetro prioritario el tipo de memoria sobre la que va a intervenir en la investigación forense; el segundo parámetro es el tipo de nivel de usuario, ya que cada uno tiene un nivel de urgencia para preservar los rastros y la evidencia en la memoria.

Desarrollo

Etapas de la informática forense

Los ciberincidentes que afectan la información de la historia clínica del paciente hacen reducir la confianza en los sistemas de salud y pueden llegar a amenazar la vida misma (Coventry & Branley, 2018). Para evitar y prevenir estos posibles efectos, la ciberseguridad requiere procesos auditados de administración de la información, con el fin de evitar el robo de información médico-clínica protegida del paciente (Jarrett, 2017). En el caso de un ciberincidente, como el robo de datos, la informática forense ayuda a explicar cómo sucedió el delito cibernético, para lo cual cuenta con procedimientos y metodologías que permiten investigar y almacenar pruebas para responder a las preguntas del juez sobre si hubo o no un delito (Queiroz & Vargas, 2010). Así, las herramientas forenses ayudan a esclarecer el ciberincidente, por lo cual sus características y técnicas deben satisfacer las necesidades de quienes las utilizan e identificar las brechas, es decir, las funciones para las que aún no existen herramientas técnicas (NIST, 2020).

Por otra parte, la identificación de datos volátiles y no volátiles es un aspecto vital de la informática forense. La validación y examen de la evidencia de volatilidad ayuda a "contar la historia" soportada en el estado de la evidencia en el momento de la recopilación. En los casos donde el código malicioso reside en la memoria, se puede contar una historia completa; de lo contrario, la volatilidad hace que se pierda parte de dicha historia por falta de datos o pruebas (Bidgoli, 2006).

Los criterios para identificar y preservar datos volátiles y no volátiles deben decidirse y documentarse con anticipación, para que las decisiones se tomen e informen lo antes posible. Las empresas deben ser proactivas en la recopilación de datos para desarrollar un plan que priorice las fuentes de información. Esto se logra al establecer una organización clara y objetiva desde la adquisición, el almacenamiento, el procesamiento, el realmacenamiento y la ubicación de los datos.

Para hacer esto, se evalúa la cantidad de esfuerzo requerido para recopilar datos (tiempo de recopilación, costo de servicios y herramientas forenses), la volatilidad de los datos y los riesgos asociados con la recopilación para determinar el potencial de recuperación de datos e información importante para la empresa. Al determinar la cadena de custodia, se evita el manejo inadecuado y la violación de la evidencia. Asimismo, la empresa decide qué datos volátiles y no volátiles son importantes, para priorizar la toma de decisiones (Kent et al., 2006).

Por esto, es necesario verificar cómo se ajusta la información forense en la información generada en la telemedicina; comprobar qué herramientas y funciones están disponibles para la informática forense y determinar la cadena de custodia para cada nivel de acceso de usuarios, con el propósito de que los administradores de la información tengan soporte para la correcta toma de decisiones en la conservación de datos en caso de un ciberincidente.

Herramientas de volatilidad en memoria RAM

Como se ha dicho, la integridad y disponibilidad de las pruebas puede verse fácilmente comprometida con algo tan simple como apagar el dispositivo sospechoso. Esto debido a que en una pesquisa del espacio RAM puede encontrarse información muy valiosa (Bidgoli, 2006).

En el estudio de volatilidad de datos se detectaron diecisiete herramientas utilizadas en el proceso de captura y análisis de memoria (NIST, 2019): Active Defense, Belkasoft Evidence Center, Belkasoft Live RAM Capture, DC3 Memory Analysis Tool (DMAT), DFF, Elcomsoft Forensic Disk Decryptor, ILookIXimager, Internet Evidence Finder (IEF), IEF Triage, Mac Memory Reader, MacQuisition, Magnet Axiom, Magnet RAM Capture, Mem Marshal, OSForensics, Responder Professional y Windows Memory Reader.

Protocolo de Manchester adaptado para primera respuesta en telemedicina

El Manchester Triage Group busca consenso entre los profesionales de la salud de emergencia sobre los estándares de evaluación de pacientes. *Emergency triage* es un sistema de gestión de riesgos clínicos empleado en las áreas de urgencias de los hospitales en todo el mundo, que permite gestionar de forma segura la atención cuando el flujo de pacientes —por ende, la necesidad clínica— supera la capacidad clínica. Este sistema tiene como objetivo asegurar que la atención se defina de acuerdo con la necesidad y prioridad de cada paciente y garantizar así que sea oportuna (Mackway-Jones et al., 2014).

En este sentido, el protocolo de Manchester es utilizado para el triaje de los pacientes. Al adquirir evidencia, el examinador o perito debe considerar el orden en que se recopilan los datos debido a su potencial volatilidad y el efecto de su recopilación en el sistema. Este orden puede cambiar según cada sistema de información. El examinador debe compren-

der las necesidades de la situación especificada y, en consecuencia, ordenar la recopilación de datos volátiles (Scientific Working Group on Digital Evidence [SWGDE], 2014).

Al analizar el protocolo de Manchester, se ha desarrollado la propuesta de toma de decisiones de tipo *primera respuesta* para la preservación de rastros y evidencias en telemedicina. En la Tabla 1 se muestra la escala de triaje basado en el protocolo de Manchester.

Tabla 1. Escala de triaje con base en el protocolo de Manchester

Prioridad	Decisión	Color	Momento	Acción
1	Ante el ciberincidente	Rojo	Ante el ciberincidente	Cadena de custodia
2	Inmediato	Naranja	0 minutos	Preservación
3	Urgente	Amarillo	10 minutos	Datos volátiles
4	Poco urgente	Verde	30 minutos	Datos no volátiles
5	No urgente	Azul	60 minutos	Almacenamiento

Fuente: Elaboración propia.

Para determinar la toma de decisiones sobre el nivel de urgencia, se debe preservar los rastros y evidencias del proceso de acuerdo con la volatilidad de la memoria. Cada institución debe diseñar la cadena de custodia para evitar un manejo inadecuado o la violación de la evidencia. Además, la empresa identifica de antemano cuáles datos son volátiles y cuáles no, con miras a su priorización; si la empresa decide que los datos volátiles no son los más importantes, puede optar por una gestión para recopilar solo datos no volátiles.

Después de identificar las posibles fuentes de datos, el analista debe hacer pruebas para adquirir la información desde dichas fuentes. La empresa determina la cantidad de esfuerzos requeridos para recopilar los datos y los riesgos asociados con la recopilación y recuperación de información. La adquisición de datos debe llevarse a cabo mediante un proceso de tres pasos: 1) se desarrolla un plan para su adquisición; 2) se adquieren los datos, y finalmente 3) se verifica su integridad.

Resultados

En una fase inicial se analizaron los errores que pueden dificultar la preservación de evidencias en los delitos cibernéticos, como apagar o reiniciar la computadora, el manejo incorrecto de la escena del crimen y la falta de documentar las acciones en la interacción con el entorno del crimen.

El error de apagar o reiniciar el sistema

Al desconectar la fuente de alimentación energética o apagar la máquina, se pierde la información de los procesos y programas en ejecución, de los datos que residen en el

espacio de archivo de intercambio o de paginación, y de la información de conexión de red, porque estas fuentes de información son volátiles. Además, la información se pierde irremediablemente cuando se apaga el sistema *host* o se corta la energía (Bidgoli, 2006).

Manejo incorrecto de dispositivos informáticos

La manipulación incorrecta de un dispositivo durante la conservación y la recopilación puede provocar la pérdida de datos digitales. Si el dispositivo no se manipula correctamente durante dichos procesos, la evidencia física puede resultar contaminada (SWGDE, 2020). Además, la documentación de todas las pruebas, incluido el sistema comprometido, ayuda al proceso de investigación (Cichonski et al., 2012). De esta manera, el hecho de no definir adecuadamente un plan de manejo de datos ante un ciberincidente puede ocasionar que no haya recursos después de un evento, lo cual define la responsabilidad en el manejo inadecuado de datos (Network Working Group [NTWG], 1997).

Documentar las acciones en interacción con el entorno del ciberincidente

El protocolo presentado en este estudio muestra la importancia de desarrollar una cadena de custodia definida con claridad. Asimismo, esta se debe seguir fielmente para evitar acusaciones de manejo inadecuado o violaciones de rastro digital, y así actuar de manera apropiada para preservar datos volátiles y no volátiles (Kent et al., 2006). En este sentido, una gestión preventiva define acciones para manejar el ciberincidente antes de que ocurra, con lo cual se logra desarrollar una cultura segura de conductas para la toma de decisiones. Esta planificación limita e incluso evita esta clase de incidentes, así como posibles daños derivados de estos.

De esta forma, la protección de la información también incluye preparar pautas de manejo de ciberincidentes como parte de un plan de contingencia, destinado a eliminar gran parte de la ambigüedad que provoca un ciberincidente y así conducir a un conjunto de respuestas apropiadas y completas. En la Tabla 2 se muestran los objetivos que debe tener dicho plan de acción.

Tabla 2. Objetivos del plan propuesto y acciones planeadas previas al ciberincidente

Plan propuesto	Acción planificada previamente
Debe aprobarse antes de que ocurra el ciberincidente para verificar la eficiencia con la simulación de conducta del equipo.	Verificar los resultados que pueden ser encontrados de acuerdo con la forma de validar el ciberincidente.
1. Proteger lo que pueda verse comprometido. 2. Proteger los recursos y planificar su uso de manera más rentable, si no hay ciberincidentes.	1. Describir cómo sucedió. 2. Describir cómo evitar las exposiciones de vulnerabilidad.

Continúa tabla...

Plan propuesto	Acción planificada previamente
3. Cumplir con las regulaciones gubernamentales y otras. 4. Evitar que los sistemas administrados sean utilizados por otros atacantes en delitos cibernéticos. Para que no haya sanciones legales. 5. Minimizar el potencial de exposición negativa.	3. Evitar otros ciberincidentes. 4. Evaluar el impacto y daño del ciberincidente. 5. Recuperarse del ciberincidente. 6. Actualizar las políticas y procedimientos según como sea necesario. 7. Averiguar quién realizó el ataque (si es apropiado y posible).

Fuente: NTWG (1997).

Debido a la naturaleza del ciberincidente, puede haber un conflicto entre analizar la fuente original de un problema y restaurar los sistemas o servicios (NTWG, 1997).

Escala de cribado para primera respuesta en tres tipos de acción

A continuación se presenta la escala de cribado para la preservación de rastros y evidencias con base en el protocolo de Manchester, que soporta las actividades durante la primera respuesta. En la Tabla 3 se muestra el conjunto de acciones para identificar, aislar y proteger la escena del ciberincidente en aras de preservar los rastros.

Tabla 3. Acción de primera respuesta de preservación para identificar, aislar y proteger la escena del ciberincidente

Acción de preservación	Identificar	Aislar	Proteger
Determinar la cadena de custodia (antes del ciberincidente) • Cada usuario identifica los datos prioritarios para su conservación • Cantidad de esfuerzo (tiempo, costos y herramientas) • Riesgo de recuperación de datos en el orden de volatilidad	X		
Preservación (inmediata) • Identificar rastros y evidencias de la fuente de datos • Fotografiar la escena con dispositivos y periféricos • Evitar tocar o manipular los dispositivos • Anotar los estados • Anotar las características (modelo, marca, año, entre otros) • Anotar el tiempo • Anotar comportamientos (calentamiento, ruido, entre otros)	X		

Continúa tabla...

Acción de preservación	Identificar	Aislar	Proteger
Datos volátiles (urgente) • Archivos de configuración: usuarios, grupos, archivos de contraseñas y trabajos programados • Historial: eventos del sistema, registros de auditoría, eventos y aplicaciones, historia de comandos, archivos accedidos y la BIOS (dispositivo) • Archivos de aplicaciones ejecutables, *scripts*, documentación, archivos de configuración, archivos de registro, archivos de configuración, archivos de registro, archivos de historial, gráficos, sonidos e íconos • Archivos de datos • Almacenar información de la aplicación: procesamientos, texto, hojas de cálculo, base de datos, archivos de audio, gráficos y archivos de impresión temporal • Archivos de intercambio: almacenamiento temporal y variedad de información sobre aplicaciones y sistema operativo. • Archivo: almacenar el contenido en caso de error para evitar un problema posterior. • Archivos de hibernación: creados para preservar el estado del sistema • Archivos temporales: archivo con actualizaciones y mejoras, archivos creados cuando se ejecutan, eliminados y terminados		X	
Datos no volátiles (no urgentes) • Espacio libre: variación de los espacios asignados • Espacio libre: datos reasignados • Configuración de red: interfaces, IP, VPN y configuración actual • Conexiones de red: conexiones de red actuales, entrada (impresora y archivos compartidos), conexiones recientes, lista de puertos e IP • Procesos en ejecución: servicios ofrecidos y activos, comandos utilizados y programas (en ejecución, desactivados o eliminados) • Archivos abiertos: usuario y procesos abiertos por cada archivo • Sesiones de inicio de sesión: usuarios y hábitos de uso • Hora del sistema operativo: zona horaria y línea de tiempo		X	
Almacenamiento (no urgente) • Inventario de rastros • Almacenamiento adecuado para no contaminar la trazabilidad • Incautación de fuentes de rastro (análisis forense): medios, dispositivos, periféricos, computadoras y portátiles, CPU			X

Fuente: Elaboración propia.

Las acciones de primera respuesta usadas para identificar, aislar y proteger la escena del ciberincidente tienen como objetivo preservar los restos digitales. Las acciones de identificación comienzan antes del ciberincidente, con la determinación de la cadena de custodia, y durante él, con acciones inmediatas para preservar los datos. Con el fin de aislar la escena del crimen, los datos volátiles (urgentes) y no volátiles (poco urgentes) son identificados, conservados y recopilados para su posterior análisis. El almacenamiento de datos para proteger los rastros se considera no urgente. Esta clasificación de poco urgente y no urgente denota mucha importancia, puesto que evidencia que la prioridad es identificar y aislar para proteger los rastros y evidencias como acción primaria.

Escenarios de ciberincidentes en telemedicina

El desarrollo de escenarios para el manejo de ciberincidentes ayuda a los miembros del equipo de respuesta a ciberincidentes a discutir sobre la toma de decisiones. Al responder al ciberincidente, los empleados de la institución de salud deben responsabilizarse de sus acciones. Sin embargo, si es un empleado subcontratado, debe tener un funcionario supervisor que evalúe su trabajo. Todos los demás modelos organizacionales generalmente tienen un jefe responsable de los equipos y uno o más corresponsables que asumen esa autoridad en ausencia del jefe.

Los miembros del equipo deben tener excelentes habilidades técnicas en administración de sistemas, administración de redes, programación, soporte técnico y detección de intrusos. Además, deben contar con habilidades blandas para resolver problemas con base en el pensamiento crítico. Sin embargo, no es necesario que todo el equipo sea de técnicos expertos; en la mayoría de casos, las consideraciones prácticas y financieras lo impiden. En lugar de ello, se requiere al menos una persona altamente competente para cada área considerada prioritaria de tecnología, como un profesional de la salud capacitado y consciente de las acciones de primera respuesta. El equipo analiza cada pregunta y determina la respuesta más viable al ciberincidente (Cichonski et al., 2012). En el protocolo de este estudio, el funcionario competente puede ser un profesional de la salud capacitado para lidiar con este tipo de eventos.

Como se ha dicho, son necesarios ciertos pasos al manejar un ciberincidente. En todas las actividades relacionadas con la seguridad, el punto más importante son las políticas institucionales vigentes. Sin política ni objetivos definidos, las actividades realizadas quedan desenfocadas. Por eso, los objetivos deben ser definidos previamente por los funcionarios del equipo de la institución y en compañía de un asesor legal. Uno de esos objetivos fundamentales es restaurar el control de los sistemas afectados y limitar así el impacto de los daños.

En el peor de los casos, apagar el sistema o desconectarlo de la red eléctrica puede ser la única solución práctica. En esas circunstancias, tratar de atrapar intrusos puede tener una prioridad muy baja en comparación con la integridad del sistema. Por ejemplo,

monitorear la actividad de un *hacker* es útil, pero puede considerarse un riesgo permitir su acceso continuo (NTWG, 1997).

Protocolo de informática forense para conservación de rastros y evidencias

Con el protocolo desarrollado en este estudio, la institución de salud debe establecer la cadena de custodia con base en recomendaciones internacionales y respetando las leyes de cada país. La institución puede tardar más en establecer la cadena de custodia ajustada a las recomendaciones internacionales, de modo que debe tener planes alternativos que consideren la toma de decisiones durante el ciberincidente.

La prioridad en el protocolo es crear la cadena de custodia que se utilizará durante el ciberincidente y que ayudará a tomar decisiones. Antes del ciberincidente, cada actor recopila los datos volátiles y no volátiles esenciales para su trabajo.

Los actores, el profesional de la salud y el experto identifican qué datos deben priorizarse durante el ciberincidente, además de determinar qué datos se respaldarán y con qué frecuencia. Los actores viabilizan la cadena de custodia comprobando sus acciones en cada etapa. En la Tabla 4 se muestran las decisiones prácticas en *prioridad 1* ante un ciberincidente.

Tabla 4. Decisión ante el ciberincidente

Indicador del protocolo	**Rojo**
Nombre de la decisión	Ante el ciberincidente
Actores	*First responder* en telemedicina Perito
Prioridad	1
Acción de los actores	
First responder	**Perito forense computacional**
Identificar los datos sensibles	1. Crear cadena de custodia de acuerdo con la legislación del país y los organismos coexistentes. 2. Recopilar y/o adquirir los datos 3. Mantener la gestión de copias de seguridad (definir qué datos y sus frecuencias de copia)
Variable forense	Datos volátiles y no volátiles (importantes para cada actor)
Artefacto forense producido	Cadena de custodia

Fuente: Elaboración propia.

Para la prioridad 2 del protocolo, se identifica la acción de la cadena de custodia que se utilizará durante el ciberincidente para una mejor toma de decisiones. A nivel inmediato, cada actor identifica su acción sobre la cadena de custodia para preservar los datos volátiles y no volátiles. Los actores denuncian el ciberincidente ante las autoridades competentes de acuerdo con la normativa de su país; anotan el comportamiento del ciberincidente y las características del equipo, e identifican la prioridad de preservación. En la Tabla 5 se muestran las decisiones prácticas en *prioridad 2*.

Tabla 5. Decisión inmediata

Indicador del protocolo	**Naranja**
Nombre de la decisión	Inmediato
Actores	*First responder* en telemedicina Perito
Prioridad	2
Acción de los actores	
First responder	**Perito forense computacional**
1. Identificar la acción sobre la cadena de custodia 2. Anotar el comportamiento del ciberincidente (tomar fotografía del equipo y de las pantallas) 3. Tener en cuenta las características del equipo (marca, modelo, año, entre otros) 4. Identificar las decisiones tomadas	1. Identificar la acción sobre la cadena de custodia 2. Denunciar al ciberincidente ante las autoridades 3. Anotar el comportamiento del ciberincidente (tomar fotografía del equipo y de las pantallas) 4. Tener en cuenta las características del equipo (marca, modelo, año, entre otros) 5. Identificar la prioridad de conservación 6. Identificar las decisiones tomadas 7. Identificar datos volátiles 8. Identificar datos no volátiles
Variable forense	Cadena de custodia
Artefacto forense producido	Preservación de datos

Fuente: Elaboración propia.

Para la prioridad 3 del protocolo, se aíslan los datos volátiles de acuerdo con la acción de la cadena de custodia. Es un nivel urgente, donde cada actor tiene como objetivo preservar los datos volátiles. Los actores analizan el comportamiento de los datos volátiles, identifican la acción de cadena de custodia para los datos volátiles, toman nota de cada manipulación de dichos datos para luego informar su manejo e identifican el *software* de recopilación de datos volátiles. Los actores también aíslan los datos volátiles para preservarlos de acuerdo con la cadena de custodia. En la Tabla 6 se muestran las decisiones prácticas ante un ciberincidente en *prioridad 3*.

Tabla 6. Decisión urgente

Indicador del protocolo	**Amarillo**
Nombre de la decisión	Urgente
Actores	*First responder* en telemedicina Perito
Prioridad	3
Acción de los actores	
First responder	**Perito forense computacional**
1. Tener en cuenta el comportamiento de los datos volátiles 2. Identificar la acción de la cadena de custodia para datos volátiles	1. Tener en cuenta el comportamiento de los datos volátiles 2. Identificar la acción de la cadena de custodia para datos volátiles 3. Tener en cuenta cada manipulación de datos volátiles 4. Identificar el *software* de recopilación de datos volátiles
Variable forense	Cadena de custodia
Artefacto forense producido	Preservación de datos volátiles

Fuente: Elaboración propia.

Para la prioridad 4 del protocolo, se aíslan los datos no volátiles de acuerdo con la acción de la cadena de custodia. Es un nivel urgente, donde cada actor tiene como objetivo preservar los datos no volátiles. Los actores describen el comportamiento de los datos no volátiles, identifican la acción de la cadena de custodia para dichos datos para informar de su manejo e identifican el *software* para su recolección. Los actores también aíslan los datos no volátiles para preservarlos de acuerdo con la cadena de custodia. En la Tabla 7 se muestran las decisiones prácticas ante un ciberincidente en *prioridad 4*.

Tabla 7. Decisión poco urgente

Indicador del protocolo	**Verde**
Nombre de la decisión	Poco urgente
Actores	*First responder* en telemedicina Perito
Prioridad	4

Continúa tabla...

Acción de los actores	
First responder	**Perito forense computacional**
1. Tener en cuenta el comportamiento de los datos no volátiles 2. Identificar la acción de la cadena de custodia para datos no volátiles	1. Tener en cuenta el comportamiento de los datos no volátiles 2. Identificar la acción de la cadena de custodia para datos no volátiles 3. Tener en cuenta cada manipulación de datos no volátiles 4. Identificar el *software* de recopilación de datos no volátiles
Variable forense	Cadena de custodia
Artefacto forense producido	Preservación de datos no volátiles

Fuente: Elaboración propia.

Para la prioridad 5 del protocolo, se protegen los datos no volátiles de acuerdo con la acción de la cadena de custodia. Es un nivel no urgente, donde cada actor tiene como objetivo almacenar datos volátiles y no volátiles. Los actores identifican la forma de almacenar ambos tipos de datos y aplican el método de almacenamiento para datos no volátiles. Los actores guardan y protegen los datos de acuerdo con la cadena de custodia. En la Tabla 8 se muestran las decisiones prácticas ante un ciberincidente en *prioridad 5*.

Tabla 8. Decisión no urgente

Indicador del protocolo	**Azul**
Nombre de la decisión	No urgente
Actores	*First responder* en telemedicina y perito
Prioridad	5
Acción de los actores	
First responder	**Perito forense computacional**
1. Identificar cómo almacenar datos volátiles 2. Identificar cómo almacenar datos no volátiles	1. Identificar cómo almacenar datos volátiles 2. Identificar cómo almacenar datos no volátiles 3. Aplicar la forma de almacenar datos volátiles 4. Aplicar la forma de almacenar datos no volátiles 5. Registrar los datos volátiles 6. Registrar los datos no volátiles
Variable forense	Cadena de custodia
Artefacto forense producido	Almacenamiento de datos volátiles y no volátiles

Fuente: Elaboración propia.

Con el protocolo sugerido en este estudio, la institución de salud puede iniciar su propia cadena de custodia, en la que analizará los puntos críticos para preservar rastros y evidencias de datos volátiles y no volátiles. Sin embargo, es necesario que la acción pueda ser modificada según el ciberincidente y de acuerdo con los actores, la institución de salud y la legislación específica de cada país.

El éxito del protocolo de preservación de evidencias depende de factores como la formación y sensibilización de los profesionales de la salud, la adecuación de las tecnologías que pueden ser utilizadas en el entorno de uso de activos computacionales, y también su compatibilidad con el uso de las herramientas forenses mencionadas en esta investigación. De esta manera, este aporte constituye un documento de referencia que sistematiza la toma de decisiones con la inclusión de niveles de urgencia del ciberincidente.

Aplicación práctica

Como escenario de la aplicación práctica del protocolo de estudio, se toma como ejemplo el ciberincidente del Hospital Oncológico de Barretos, Brasil, ocurrido en 2017. Este fue causado por una variante del virus "Petya", que infecta las computadoras con Windows y pide un "rescate" pagado con monedas digitales. El virus, de tipo *ransomware*, invade el sistema y codifica los datos y cifras de las máquinas infectadas. Restablecer el acceso requiere el uso de una clave en poder de los delincuentes, que liberan tras el pago del rescate. En este caso, el rescate solicitado era de US$300 por computador, para un total de US$360 000 por el rescate de todas las máquinas infectadas. El ciberincidente canceló aproximadamente 3000 consultas y pruebas de 350 pacientes que quedaron sin radioterapia. El equipo se turnó en régimen de 24 horas con el objetivo de restablecer el sistema, lo que tuvo consecuencias para otras unidades del hospital. La normalización de la atención de pacientes fue posible a los 6 días del ciberincidente (Guimarães, 2017).

La atención médica es un objetivo atractivo para los delitos cibernéticos por dos razones fundamentales: es una fuente rica de datos valiosos y sus defensas son débiles. En este sector, las violaciones de ciberseguridad incluyen el robo de información médica y los ataques de *ransomware* en hospitales, que pueden incluir ataques a dispositivos médicos implantados. Las Dichas violaciones pueden reducir la confianza del paciente, dañar los sistemas de salud y amenazar la vida humana (Coventry & Branley, 2018).

El *ransomware* también puede secuestrar archivos de datos enormes, lo que dificulta la atención del paciente durante periodos más prolongados. Un ataque de denegación de servicio a gran escala, en el que una red de datos está sobrecargada deliberadamente con las actividades de los médicos, impide el acceso a los registros médicos electrónicos (Jarret, 2017). Este tipo de ataques tiene más éxito cuando la víctima desconoce la seguridad del sistema. En este sentido, los usuarios pueden protegerse de posibles extorsiones simplemente aplicando las buenas prácticas y políticas de respaldo de la información o implementando *software* de restauraciones del sistema (Britz, 2013). Las instituciones de salud

que no han dispuesto copias de seguridad en la cadena de custodia digital eventualmente se ven obligadas a pagar el rescate por la necesidad de recuperar los datos, y ese pago acaba fomentando la continuación del delito (Santana et al., 2017).

El escenario de aplicación con el protocolo desarrollado en este estudio plantea la hipótesis de que el virus *ransomware* se instala y solicita el rescate por los datos secuestrados en cada computador. El virus infectó las computadoras en la sala de examen de imágenes, lo que imposibilitó el uso de la máquina que opera el equipo. Las personas que han sido programadas para el examen respectivo están esperando en la sala de espera y otras personas programadas para las próximas horas están en camino al sitio. La toma de decisiones ante el ciberincidente es decisiva, pues allí el tiempo es crítico para la solución.

De acuerdo con la escala de clasificación para preservar rastros, en la fase de identificación, el profesional que opere el equipo tendrá a disposición la cadena de custodia, con la que ya se ha decidido previamente qué datos se deben priorizar, respaldar y verificar su periodicidad. Este profesional será el *first responder* en telemedicina y debe tener en cuenta el comportamiento del sistema y las características del equipo involucrado. El ciberincidente debe informarse a las autoridades correspondientes y su identificación es responsabilidad del primer respondiente. Luego, identifica cuáles son los datos volátiles y no volátiles, su prioridad de preservación y las decisiones que se tomarán ante el ciberincidente.

De forma aislada, el *first responder* tiene como objetico preservar los datos volátiles y no volátiles para que no se pierdan e incluso contaminen durante su manipulación. Sin embargo, el *ransomware* bloquea la máquina y no es posible gestionar la preservación de datos volátiles y no volátiles. Si es posible, el primer respondiente se centrará en los datos volátiles que se pueden perder cuando se apaga el equipo, y luego de los datos no volátiles que se pueden recopilar después de apagar la máquina. Si capturar el criminal no es prioridad de la institución, el enfoque de la recolección debe estar en los datos de la institución de salud.

El presente estudio tuvo como objetivo preservar la memoria, por ser el primer paso en el análisis forense. Según *Dfir It* (2015), el *software* MoonSols DumpIt es una forma fácil de obtener memoria, incluso si el investigador no se encuentra físicamente frente al equipo o el sistema. Está diseñado para ser usado por un usuario no técnico; puede hacerlo el *first responder* en telemedicina que opera el equipo de imágenes. Basta con un doble clic en el ejecutable para generar una copia de la memoria física en el directorio actual. La versión gratuita no se ha desarrollado durante algunos años, mientras que la versión comercial tiene capacidad de comprensión LZNT1 y cifrado RC4. Durante las pruebas, DumpIt asignó 780 kb de memoria, lo que *Dfir It* califica como un gran resultado.

Discusión

La clasificación del nivel de urgencia de la toma de decisiones durante el ciberincidente estandariza acciones para preservar rastros y evidencias en telemedicina. El protocolo desarrollado es la primera respuesta digital que usa la informática forense con este fin en el contexto de la telemedicina.

Sensibilización y formación del protocolo de primera respuesta

Los pasos recomendados para identificar las fuentes de los datos parten por desarrollar un plan de adquisición, adquirirlos y verificar su integridad. El plan debe priorizar las fuentes de datos, estableciendo el orden en el que deben adquirirse los datos en función de su valor probable, la volatilidad de los datos y la cantidad de esfuerzos requeridos para recuperarlos. Antes de que comience la recopilación de datos, el analista debe tomar una decisión sobre la necesidad de recopilar y preservar rastros y pruebas para respaldar su uso en futuros procedimientos legales o disciplinarios. En tales situaciones, se debe seguir una cadena de custodia claramente definida para evitar acusaciones de manejo inadecuado o violación de los rastros (Kent et al., 2006).

El protocolo desarrollado es una versión simplificada de las acciones que se pueden tomar para preservar los datos volátiles y no volátiles. Se inspiró en las recomendaciones del NIST, la NTWG y el SWGDE, en las que señalan las conductas más adecuadas para proceder durante el ciberincidente.

De acuerdo con NTWG (1997), el ciberincidente puede ser tan complejo que es imposible hacer todo al mismo tiempo para responder a él, y es ahí donde las prioridades son esenciales. La pérdida de los datos generalmente no es un resultado aceptable. Otra gran preocupación es el efecto de la reacción en cadena del ciberincidente y, por tanto, saber qué partes se vieron afectadas. Cualquier plan para responder a ciberincidentes de seguridad debe estar guiado por políticas y regulaciones nacionales de cada país. Además, debe haber coherencia entre lo que se recopilará y lo que finalmente se utilizará; por ejemplo, solo es necesario crear mecanismos para monitorear y rastrear a los invasores si realmente se planea actuar y controlarlos, en caso de que sean capturados. Si bien las prioridades varían de una empresa a otra, las siguientes prioridades sugeridas pueden servir como punto de partida para definir la respuesta adecuada:

- *Prioridad 1*. Proteger la vida y la seguridad de las personas. La vida humana siempre tiene prioridad sobre todas las demás consideraciones.
- *Prioridad 2.* Proteger datos clasificados y/o sensibles; evitar la explotación de sistemas, redes o sitios web, e informar a los sistemas, redes o sitios web afectados o pirateados. Se debe ser consciente de las regulaciones gubernamentales.
- *Prioridad 3.* Proteger otros datos, incluidos los científicos, de gestión y otros, porque la pérdida de datos es costosa en términos de recursos. Evitar la explo-

tación de otros sistemas, redes o sitios, e informar a los ya afectados sobre las intrusiones exitosas.

- *Prioridad 4.* Evitar daños en los sistemas (por ejemplo, pérdida o alteración de archivos del sistema, daños en las unidades del disco, etc.). El daño del sistema puede resultar en costos adicionales por tiempos de inactividad y recuperación.
- *Prioridad 5.* Minimizar la interrupción de los recursos informáticos (incluidos los procesos). En muchos casos, es mejor apagar o desconectar un sistema de una red que arriesgarse a dañar datos, procesos o el sistema. Cada empresa evalúa las ventajas y desventajas entre desconectarse o mantenerse conectado.

Mitigación de errores durante la conservación de rastros por un *first responder*

Además de las acciones dañinas desencadenadas por el ciberincidente, es necesario comprender cómo las decisiones tomadas por el equipo de primera respuesta pueden ser igualmente dañinas. Las acciones del equipo pueden afectar la identificación de la fuente del ciberincidente, la protección de datos, la recopilación de rastros y la recuperación del sistema. En este sentido, la conducta eficiente durante el ciberincidente tiene beneficios económicos, por mucho que la planificación y ejecución de estas conductas requieran inversión de tiempo y recursos financieros. Los ciberincidentes suelen ser perjudiciales para la institución al alterar la relación con los clientes actuales o potenciales, por lo cual su manejo eficiente minimiza la potencial exposición negativa. Otro beneficio del manejo eficiente de los ciberincidentes tiene que ver con cuestiones legales, ya que en el futuro cercano las organizaciones pueden ser consideradas responsables de ciberincidentes y sus efectos debido a su falta de preparación para enfrentarlos (NTWG, 1997).

Impactos de la no identificación, aislamiento y protección de los datos

Como los computadores y otros dispositivos están conectados a la red, la recomendación es desconectarlos para asegurarse de que los datos no se modifiquen o destruyan de forma remota. Los dispositivos móviles generalmente tienen una función de restablecimiento que borra todo el contenido del usuario y restablece la memoria a las condiciones originales de fábrica. Dado que esto se puede hacer directamente o de forma remota, es necesario tomar precauciones inmediatas; por ejemplo, separar el dispositivo del usuario y aislarlo de la red para garantizar que los datos no se modifiquen ni se destruyan.

Históricamente, los examinadores que han aislado un dispositivo móvil de la conectividad de la red lo programan en "modo avión". Sin embargo, en las últimas versiones, esta función no desactiva *bluetooth*, wifi ni otros protocolos inalámbricos, simplemente se pueden desconectar temporalmente. Por ello, los examinadores deben confirmar manualmente que se ha desactivado la conectividad de la red o considerar medios alternativos de aislamiento, incluso colocar el dispositivo en un gabinete protegido o el aislamiento de

la red para teléfonos inteligentes. En todo caso, al desconectar el dispositivo para aislarlo de la red se corre el riesgo de afectar mecanismos de autenticación como las contraseñas o habilitar funciones de seguridad mejoradas, lo que podría hacer que los datos sean inaccesibles (SWGDE, 2020).

La estrategia de contención de ciberincidentes es importante antes de que los recursos se sobrecarguen y se aumente el daño. Tomar decisiones también es parte esencial de la contención; por ejemplo, apagar un sistema, desconectarlo de la red o deshabilitar ciertas funciones. Estas decisiones son más fáciles de tomar si existen estrategias y procedimientos predeterminados para contener el ciberincidente, como la cadena de custodia. Las organizaciones deben definir riesgos aceptables al lidiar con ciberincidentes y desarrollar estrategias de acuerdo con el tipo de ciberincidente, ya que esto hace que la efectividad de la contención varíe. Por ello, las instituciones crean diferentes estrategias de contención para cada tipo de ciberincidente, con criterios documentados para facilitar la toma de decisiones (Cichonski et al., 2012).

En cuanto a los datos volátiles del sistema operativo, estos solo se pueden recopilar en un sistema activo que no se haya reiniciado o apagado desde que ocurrió el incidente. Cualquier acción realizada en el sistema, iniciada por una persona o por el propio sistema operativo, casi con certeza los alterará de alguna manera. Por lo tanto, los analistas deben decidir lo antes posible si deben conservarse los datos volátiles en el sistema operativo.

Los criterios para tomar esta decisión deben estar documentados con anticipación, de modo que el analista pueda tomar la mejor decisión de inmediato. La importancia de esta decisión no se puede definir durante el ciberincidente porque podría ser demasiado tarde, ya que apagar el sistema o incluso desconectarlo de una red puede eliminar la oportunidad de recopilar información potencialmente importante. Por ejemplo, si un usuario ejecutó recientemente herramientas de cifrado para proteger los datos, la memoria RAM de la computadora puede contener un código *hash* de contraseña que se puede usar para proteger las contraseñas.

Por otro lado, la recopilación de datos volátiles del sistema operativo de una computadora en ejecución tiene sus propios riesgos. Por ejemplo, siempre existe la posibilidad de que los archivos y otros datos volátiles puedan cambiarse. Si el esfuerzo requerido para recopilar datos volátiles no es apropiado, los analistas pueden decidir realizar un cierre. Asimismo, deben elegir el método de apagado apropiado para cada sistema, pues cada método específico puede hacer que se conserven o corrompan diferentes tipos de datos. Así, es fundamental que los analistas conozcan el comportamiento de apagado típico de cada sistema operativo (Kent et al., 2006).

Daños materiales e inmateriales de los delitos cibernéticos en Brasil y el mundo

El Centro de Estudios Estratégicos e Internacionales de Estados Unidos (Center for Strategic and International Studies [CSIS]) estima que el costo mundial del delito ciber-

nético es de aproximadamente US$600 millones, lo que corresponde al 0,8 % del PIB mundial (CSIS, 2018). Cybersecurity Ventures (2017) estima que, para el 2021, el ciberdelito le costará al mundo US$6 billones. En el caso específico de Brasil, el 54 % de los ciberataques notificados se originó dentro del país (CSIS, 2018). El costo promedio anual de la ciberdelincuencia en Brasil fue de US$7,24 millones en 2018 (Ponemon Institute, 2019). Se han reportado 875 327 ciberincidentes al Centro de Estudios, Respuesta y Tratamiento de Ciberincidentes de Seguridad de Brasil (CERT, 2020).

Conclusiones

El protocolo desarrollado para la preservación de rastros y evidencias conforma la primera respuesta digital que, mediante informática forense, puede ayudar en la toma de decisiones frente a ciberincidentes en el contexto de la telemedicina. En este contexto —dada la importancia de la información de salud que se recoge y, por ende, la necesidad de garantizar su confidencialidad, integridad y disponibilidad—, una exigencia fundamental es contar con estrategias contra ciberincidentes. Como se ha visto, la informática forense es una valiosa herramienta para determinar la dinámica del delito, su materialidad y autoría.

La informática forense recoge el rastro digital, identifica la autenticidad de los datos, los analiza sin modificarlos, identifica el dispositivo por recoger y presenta posibles soluciones a las hipótesis del delito. De esta forma, las herramientas forenses ayudan a esclarecer los incidentes, y así sus características y técnicas satisfagan las necesidades de quienes la utilizan. La herramienta que elija el equipo de primera respuesta depende del tipo de función requerida, en la que se analiza el rastro como parte de la evidencia del delito.

Finalmente, se ha confirmado la hipótesis de esta investigación, ya que la informática forense en efecto ayuda a esclarecer delitos de medios en telemedicina. De esta forma, el protocolo para la conservación de rastros y evidencias para la primera respuesta digital, con definición de niveles de urgencia para las acciones, ayuda a tomar decisiones sobre las acciones que se deben emprender y su prioridad ante un determinado ciberincidente en el campo de la telemedicina.

Agradecimientos

Los autores desean agradecer al Instituto Federal de São Paulo, Campus São Paulo Pirituba, por su apoyo al desarrollo de esta investigación.

Declaración de divulgación

Los autores declaran que no existe ningún potencial conflicto de interés relacionado con el artículo.

Financiamiento

Los autores no declaran fuente de financiamiento para la realización de este artículo.

Sobre los autores

Nadjila Tejo Machado es magíster en ciencias de la actividad física de la Universidad de São Paulo y licenciada en educación física y salud. Es estudiante en el curso de Análisis y Desarrollo de Sistemas del Instituto Federal de São Paulo, Campus São Paulo Pirituba. Es profesora del Centro Universitario Santa Rita.
https://orcid.org/0000-0001-9077-0671 - Contacto: nadjila.tejo@aluno.ifsp.edu.br

Felipe Rodrigues Martinez Basile es doctor y magíster en ingeniería biomédica de la Universidad de Mogi das Cruzes, e ingeniero en sistemas de información. Es especialista en seguridad de la información. Es profesor e investigador en arquitectura de redes informáticas en el IFSP - Campus PTB. Realiza investigaciones multicéntricas sobre seguridad de la información en Suramérica.
https://orcid.org/0000-0002-0404-4807 - Contacto: felipe.basile@ifsp.edu.br

Flavio Cezar Amate es doctor en ingeniería eléctrica de la Universidad de São Paulo. Actualmente es profesor del Instituto Federal de São Paulo. Tiene experiencia en ingeniería biomédica con énfasis en procesamiento de señales e informática en salud. Entre otros temas, trabaja en tecnología asistencial, tecnologías de apoyo a la educación, imagen médica y redes.
https://orcid.org/0000-0002-0918-2707 - Contacto: amate@ifsp.edu.br

Leonardo Juan Ramírez López es doctor en ingeniería biomédica de la Universidad de Mogi das Cruzes de São Paulo (Brasil), magíster en ingeniería de sistemas de la Universidad Nacional de Colombia, especialista en instrumentación electrónica e ingeniero electrónico. Es profesor e investigador senior de la Universidad Militar Nueva Granada, Bogotá, Colombia.
https://orcid.org/0000-0002-6473-5685 - Contacto: leonardo.ramirez@unimilitar.edu.co

Referencias

Babulak, E., Jin, M., & Kim, Y. S. (2014). Future e-Health, QoS provision and cybersecurity challenges. *Journal of the Institute of Industrial Applications Engineers, 2*(3), 113-121.

Basile, F. R., Ramírez, L. J., & Amate, F. C. (2019). Método para realizar copias de seguridad de imágenes médicas basado en tareas automatizadas. *JINT. Journal of Industrial Neo-Technologies, 6*(1), 26-33.

Basile, F. R., Thomé, M., Amate, F. C., Rodrigues, R., Bastos, S., & Goroso, D. G. (2016). Segurança de transferência de dados em Telessaúde e Telemedicina. En *Proteção à privacidade e acesso às informações em saúde: tecnologias, direitos e ética* (pp. 279-298). Instituto de Saúde.

Bidgoli, H (2006). *Handbook of information security: Key concepts, infrastructure, standards, and protocols* (vol. 2). John Wiley & Sons.

Britz, M. T. (2013). *Computer forensics and cyber crime: An introduction* (3rd ed.). Pearson Education.

Carrier, B., & Spafford, E. H. (2004). An event-based digital forensic investigation framework. En *Proceedings of the Fourth Digital Forensics Research Workshop* (pp. 11-13).

Center for Strategic and International Studies (CSIS). (2018). *Economic impact of cybercrime — No slowing down* [report]. https://bit.ly/3rQLoVF

Centro de Estudos, Resposta e Tratamento de Ciberincidentes de Segurança no Brasil (CERT). (2020). *Estatísticas dos ciberincidentes reportados ao CERT.br*. https://www.cert.br/stats/incidentes/

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer security incident handling guide* [NIST Special Publications, 800-61]. NIST. http://dx.doi.org/10.6028/NIST.SP.800-61r2

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas, 113*, 48-52. https://doi.org/10.1016/j.maturitas.2018.04.008

Cybersecurity Ventures. (2017). *2017 Cybercrime Report*. Herjavec Group. https://bit.ly/389xV3N

Dfir it! (2015, 20 de abril). Memory acquisition tools for Windows. https://bit.ly/3bMfvYO

Guimarães, K. (2017, 10 de agosto). Os crimes dos hackers que interrompem até quimioterapia em sequestros virtuais de hospitais. *BBC Brasil*. 2017. https://www.bbc.com/portuguese/brasil-40870377

Jarrett, M. P. (2017). Cybersecurity—A serious patient care concern. *JAMA, 318*(14), 1319-1320. https://doi.org/10.1001/jama.2017.11986

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to integrating forensic techniques into incident response* [NIST Special Publications, 800-86]. NIST. https://bit.ly/3n8DALx

Machado, N. T., Ramírez, L. J., & Basile, F. R. M. (2019). *Forense computacional como estratégia para investigação em crimes cibernéticos* [ponencia]. 10.º Congresso de Inovação, Ciência e Tecnologia do IFSP, Sorocaba, Brasil.

Mackway-Jones, K., Marsden, J., & Windle, J. (2014). *Emergency triage: Manchester Triage Group* (3th ed.). John Wiley & Sons.

Maldonado, J. M. S. V., Marques, A. B., & Cruz, A. (2016). Telemedicina: desafios à sua difusão no Brasil. *Cadernos de Saúde Pública, 32*(2). https://doi.org/10.1590/0102-311X00155615

National Institute of Standards and Technology (NIST). (2019). *Searching for forensic tools and techniques by functionality* [database]. https://toolcatalog.nist.gov/search

National Institute of Standards and Technology (NIST). (2020). *Computer Forensics Tools & Techniques Catalog*. https://toolcatalog.nist.gov

Ponemon Institute. (2019). *The cost of cybercrime. Ninth annual cost of cybercrime study*. Accenture. htA tps://accntu.re/38XZWug

Queiroz, C., & Vargas, R. (2010). *Investigação e perícia forense computacional: certificações, leis processuais e estudos de caso*. Brasport.

Network Working Group (NTWG). (1997, septiembre). *Site security handbook* [RFC 2196]. https://tools.ietf.org/html/rfc2196.

Santana, K. G., Oliveira, P. R. L., Ramos, D. R. (2017). Perícia cibernética: a evolução do trabalho científico pericial informatizado ante aos desafios tecnológicos de ataques virtuais nos sistemas de segurança. *Revista Dat@venia, 9*(1), 101-111.

Scientific Working Group on Digital Evidence (SWGDE). (2020). *SWGDE best practices for mobile device evidence collection & preservation, handling, and acquisition* (version 1.2). https://bit.ly/3b5taK7

Scientific Working Group on Digital Evidence (SWGDE). (2014). *SWGDE capture of live systems* (version 2.0). https://bit.ly/3n41XKo

Vallim, A. P. (2017). *Forense computacional e criptografia*. Senac São Paulo.