Artículo original

Telesalud y seguridad de la gestión de la información para los entornos médicos actuales

Telehealth and information management security for today's medical environments

Inglis Pavón de la Tejera*[1] 0000-0001-7464-4640
Nubia de la Tejera Chillón[2] 0000-0002-1635-9304
Germán Del Rio Caballero[1] 0000-0002-9857-9596
Sergio Daniel Cano Ortiz[3] 0000-0003-0049-6256
Lesbia Eloina Rodríguez Baez[1] 0000-0003-1289-0605

1. Universidad de Ciencias Médicas, Santiago de Cuba*
2. Universidad Latinoamericana de Medicina, La Habana
3. Universidad de Oriente, Santiago de Cuba.

*Autor para la correspondencia: iptcuba@infomed.sld.cu

RESUMEN

Introducción: La información médica es sensible, clasificada y confidencial; está expuesta a diferentes formas de riesgos y vulnerabilidades, por lo que se hace necesario crear políticas y mecanismos para protegerla y hacerla segura. Para lograr esta confianza en los sistemas informáticos de salud, se requiere establecer principios y normas de seguridad de la información.

Objetivo: Analizar los procesos tecnológicos de la salud en los actuales escenarios de la seguridad de la Información y el impacto de las diferentes variantes de ciberataques.

Métodos: Se realizó un estudio del uso de las diferentes tecnologías telemáticas sanitarias actuales, en relación a los ciberataques a las que están sometidas en los diferentes escenarios sanitarios. Se analizaron diversas regulaciones y aspectos legislativos nacionales e internacionales, para evaluar los impactos negativos, así como las posibles variantes o alternativas de enfrentamiento y solución.

Conclusiones: El factor determinante en las políticas y normas de ciberseguridad y seguridad en la gestión de la información es el recurso humano, al cual hay que prestarle la mayor atención, seguido por los procesos tecnológicos, las proyecciones de contingencia para la minimización de los riesgos y amenazas latentes contra los sistemas e infraestructuras tecnológicas en la salud. El Estado Cubano ha establecido

los instrumentos legales y regulatorios para el buen desempeño de las actividades de enfrentamiento, ciberseguridad y seguridad de la gestión de la información, en la protección y las garantías legales para su desarrollo actual.
Palabras clave: ciberseguridad; seguridad de la información; seguridad de la gestión de la información; tecnologías sanitarias; cibercrimen; riesgos; amenazas.

ABSTRACT
Introduction: The medical information is sensitive, classified and confidential; it is always exposed to different risks and vulnerabilities, so it is necessary to create policies and mechanisms to protect and make it secure. To achieve confidence in health information systems, it is necessary to establish information security principles and standards.
Objective: To analyze the technological processes of health in the current scenarios of Information Security and the impact of the different variants of cyberattacks.
Methods: A retrospective, historical and analytical study of the use of different current health telematics technologies was carried out, in relation to the cyberattacks to which they are subjected in different health scenarios. Various national and international regulatory and legislative aspects were analyzed to carry out a meridian evaluation of the negative impacts, as well as the possible variants or alternatives to face them and give them a solution.
Conclusions: It is concluded that the determining factor in cybersecurity and security policies and standards in the management of information in human resources, to which the greatest attention must be paid, followed by technological processes, contingency projections for the minimization of the risks and latent threats against technological systems and infrastructures in health. The Cuban State has established the legal and regulatory instruments for the proper performance of confrontation, cybersecurity and information management security activities, in the protection and legal guarantees for its current development.
Keywords: cybersecurity; safety; health technologies; health; cybercrime; risks; threats.

Recibido: 04/01/2023
Aprobado: 31/08/2023

Introducción

Con el desarrollo científico tecnológico actual aparecen cambios en los procesos tradicionales de la sociedad. Con la introducción de la Internet se transforman los procesos sociales, lo que da lugar a una nueva dimensión de integración para el hombre, denominada Sociedad de la Información y el Conocimiento (SIC).

Este desarrollo propiciado por las diferentes revoluciones industriales, donde suceden saltos cualitativos y cuantitativos que modifican y cambian las maneras de actuación, es un fenómeno social que ha evolucionado de manera exponencial en los últimos treinta años.

Según Barnett, "...la práctica de la medicina es dominada por la forma en que procesamos la información, en cómo registramos la información, cómo recuperamos la información, y cómo comunicamos la información".[1] Pero la información médica es sensible, clasificada y confidencial, siempre está expuesta a diferentes formas de riesgos y vulnerabilidades, por lo que se hace necesario crear políticas y mecanismos para protegerla y hacerla segura. Para lograr la necesaria confianza en los sistemas informáticos de salud, se requiere establecer principios y normas de seguridad de la información.

Antes de la aparición de los sistemas informáticos toda la información importante se guardaba en formato de papel, en esta actividad se concentraba y registraba una gran cantidad y variedad de documentación. En el caso del sector de la salud, los procedimientos de seguridad, custodia y acceso a la información han estado descritos por legislaciones, manuales y normas de acceso y seguridad. Con la digitalización de la información se aprecia un beneficio en el acceso, análisis, procesamiento y reducción de espacio, entre otros aportes; pero surgen problemas relativos a la protección de la información, proceso que ha cambiado en correspondencia con los actuales requerimientos tecnológicos.

Hasta la segunda mitad del pasado siglo en general existía gran privacidad tanto de los datos como del tratamiento de los pacientes, debido por una parte a normas legales, pero también a la generalmente difícil caligrafía de los médicos y a la manera como se protegía la información de los pacientes y se puede plantear que influía la reticencia que mostraban las instituciones con la introducción de las TIC, debido a la exposición a nuevas vulnerabilidades y riesgos que estas pueden introducir en los sistemas de salud.

El objetivo del presente trabajo es analizar los procesos tecnológicos de la salud en los actuales escenarios de la seguridad de la Información y el efecto posible de las diferentes variantes de ciberataques.

Métodos

Se realizó un estudio retrospectivo, histórico y analítico del uso de las diferentes tecnologías telemáticas sanitarias actuales, en relación a los ciberataques a las que están sometidas en los diferentes escenarios sanitarios. Se analizaron diversos aspectos regulatorios y legislativos nacionales e internacionales para realizar una evaluación objetiva de los impactos negativos, así como de las posibles variantes o alternativas para enfrentarlos y darle solución.

Desarrollo

Desde la literatura ¨la seguridad se analiza y se proyecta de muchas maneras diferentes; dentro de los cuales se presentan algunos tipos de ambientes o criterios de seguridad: [2-4]

- Seguridad industrial o empresarial.
- Seguridad privada o personal.
- Seguridad ambiental.
- Seguridad nacional o de estado.
- Seguridad informática (SI) o ciberseguridad.[5]
- Seguridad de la información o seguridad de la gestión de la información(SGI).[6]

La seguridad informática (SI) es la especialidad o disciplina que se enfoca en proteger la integridad y la privacidad de los sistemas informáticos y sus componentes, así como de prevenir y detectar el uso no autorizado de los sistemas, equipos y sus datos.[7],[8]

Es difícil garantizar la inviolabilidad de un sistema informático o la seguridad de sus aplicaciones e información; aunque se generan herramientas, así como técnicas lógicas y físicas para minimizar sus afectaciones, vulnerabilidades y riesgos. [9]

Fig. 1- Los activos, el cibercrimen y la gestión de la seguridad de la información.

Fuente: Creado por el investigador

La computadora como dispositivo digital es condicionada para realizar determinadas acciones; por este hecho, ella no comete delito, ni violación, es un medio o herramienta de apoyo. A partir de este criterio se afirma que la amenaza la constituye el usuario que es de donde proviene la mayor vulnerabilidad por ser el que accede, manipula y procesa la información.

La SGI comprende un conjunto de herramientas, técnicas y medidas para controlar todos los datos (en formato digital o no), que se manejan dentro de una institución y asegurar que no se afecten o salgan de ese sistema; por tal razón su base está en el resguardo de los datos disponibles y su modificación será posible solo por el personal autorizado y con los roles correspondientes.

Un sistema de información se articula en cinco dimensiones o propiedades:

-Disponibilidad (habilitado, estable y utilizable).
-Confidencialidad (los datos deben ser legibles, no manipulables y no ser divulgada).
-Autenticidad (la fuente debe ser accedida y modificada solo por personal autorizado).
-Integridad(toda la información conserva su precisión y veracidad).
-Verificabilidad (puede ser controlada y aplicarle trazabilidad).

En los pilares anteriores se sustentan cuatro cualidades principales, que son:

-Crítica (por hacer sus fundamentos y llevar a cabo las operaciones sin asumir demasiados riesgos para la entidad).
-Valiosa (los datos que se manipulan son vitales y esenciales para el buen funcionamiento de la institución).
-Sensible (el sistema solo puede ser accedido por personas que estén debidamente autorizadas).
-Irrefutable (el usuario no puede negar las acciones que realizó).

La meta de los procedimientos de seguridad informática es garantizar que los recursos físicos y lógicos sean explotados con protección y sin afectaciones; es común confundir los conceptos de la SGI con los de la SI; la información se procesa desde muchos contextos, por lo que no solo se limita a los sistemas digitales, todo proceso productivo o de servicio genera información.[10-12]

En la toma de decisiones para impedir o minimizar los riesgos y amenazas sobre la gestión de la información, el estado cubano define un compendio de medidas legales para la seguridad, la contingencia para la información y la protección de los datos personales.

Para dar respuesta a estos problemas el sector de la salud cubana contó, desde sus inicios con sus propias regulaciones legales registradas en la Ley No. 41/1983 “Ley de

la Salud Pública", además del amparo del Decreto-Ley 199/1999 "Sobre la Seguridad y Protección de la Información Oficial" del Ministerio del Interior.[13],[14]

A partir de la aprobación de la nueva constitución, se declaran por el Ministerio de las Comunicaciones, los instrumentos legales asociados con las TIC:[15-18]

1. Ley 149/2022 "De Protección de Datos Personales".
2. Decreto-Ley 370/2018 "Sobre la Informatización de la Sociedad de Cuba".
3. Decreto 360/2019 "Sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional".
4. Decreto 42/2021 "Reglamento General de Telecomunicaciones y las Tecnologías de la Información y la Comunicación".
5. Resolución 126/2019 "Medidas de Control y los tipos de Herramientas de Seguridad que se implementan en las Redes Privadas de Datos".
6. Resolución 128/2019 "Reglamento de Seguridad de las Tecnologías de la Información y la Comunicación".
7. Resolución 129/2019 "Metodología para la Gestión de la Seguridad Informática".
8. Resolución 105/2021 "Reglamento sobre el Modelo de Actuación Nacional para la Respuesta a Incidentes de Ciberseguridad".
9. Resolución 58/2022 "Reglamento para la Seguridad y Protección de los Datos Personales en Soporte Electrónico".

Entre las afectaciones por ataques a los sistemas telemáticos en instituciones hospitalarias está el robo de datos sensibles de pacientes.[19] La realización de estos hechos no es solo por poseer el historial médico o demostrar las vulnerabilidades de los sistemas de ciberseguridad de los hospitales; la intención se centra en el acceso a números de la seguridad social, direcciones, cuentas de redes sociales, datos bancarios, entre otras informaciones, lo que facilita la suplantación de identidad, la extorsión, así como el chantaje privado y empresarial.

En la actualidad existen metodologías para establecer medidas de seguridad para todos los procesos en los que intervienen las tecnológicas telemáticas. Desde una óptica global están definidas las directivas internacionales sobre ciberseguridad y seguridad de la información; además los gobiernos, empresas e instituciones proclaman sus políticas y métodos de enfrentar los diferentes riesgos, amenazas y vulnerabilidades.

En la medida en que se actualizan los sistemas digitales y de transmisión se hace necesario una revisión de los mencionados procesos para minimizarlos o prevenirlos, por lo tanto, para el sector de la salud, se hace necesario un continuo análisis y estudio de todas las posibilidades de ataques y afectaciones que puedan comprometer los procesos sanitarios.

Para las instituciones de salud los riesgos y amenazas son tangibles y en incremento, ya que en muchos casos sus infraestructuras actuales y sistemas no están preparados para soportar los ataques, entre las causas que generan el peligro se encuentran:

- El uso de las historias clínicas digitales.
- Las dispensarizaciones farmacéuticas digitales.
- La significativa cantidad de dispositivos conectados a las redes intrahospitalarias.
- El intercambio de información extrahospitalaria, entre otros.

Estas causas proporcionan una oportunidad para que los piratas informáticos, usuarios y personal, mal intencionado propio del sector de la salud, aprovechen las brechas creadas por las actividades asistenciales.

Entre los ataques más comunes se encuentran: ransomware, malware, phishing. [20-24]

Para enfrentarse a estas situaciones las instituciones hospitalarias deben establecer principios cardinales entre la SI y la SGI. Por el alto volumen de información médica, gerencial y de pacientes, las acciones de protección y seguridad deben constituirse como un componente esencial para las transformaciones tecnológicas sanitarias.

Existen muchas propuestas y mecanismos para minimizar los riesgos y amenazas, algunos pueden ser de uso común, pero no satisfacen las necesidades para proteger los sistemas tecnológicos sanitarios. Entre las líneas de ciberseguridad y de seguridad de la información que se evalúan en la actualidad se cuentan:

- Evitar descargas de aplicaciones e información no autorizadas en los ordenadores.
- Evitar acceder a información de sitios dudosos o ventanas emergentes.
- Evitar el llenado de formularios de sitios ajenos con información personal e institucional.
- El uso de algoritmos criptográficos más complejos
- El uso de las cadenas de bloque (blokchain) como mecanismo de protección avanzado contra los ataques informáticos y la perdida de información médica institucional.[25]
- La utilización de barreras lógicas a nivel de aplicaciones (cortafuegos digitales - proxy) y de filtrado de paquetes.
- La implementación de barreras físicas a nivel de circuito (cortafuegos físicos - servidores) y direccionamiento múltiple con el uso de tramado físico de red mediante cascadas por niveles de actividad.

Los ciberataques generan grandes pérdidas, además de que afectan seriamente al sistema de salud. Solo por mencionar un dato, para septiembre del 2020 se registraron nueve millones de robos de registros médicos por piratas informáticos según la Revista HIPAA.[26]

La intención de lograr un entorno seguro exige calidad en los servicios de salud, los cuales se proyectan desde la formación de una conciencia individual y colectiva de los factores actuantes directa o indirectamente, donde la discreción, la ética médica, la garantía de los derechos de los pacientes y el control de la información se resumen en las buenas prácticas médicas y en las políticas de ciberseguridad en la gestión de la información.

Estas garantías se resumen en la protección del derecho al honor del paciente, a la intimidad personal, familiar y a la de la institución, a saber:

- Secreto en las transmisiones de las comunicaciones.
- Protección de los datos de carácter personal e institucional.
- Protección de derechos digitales.
- Protección de los derechos de propiedad intelectual sobre los contenidos.
- Protección de los derechos médicos y hospitalarios.

En el caso de las ciencias de la salud se exigen reglas y normas morales que se resumen en las concepciones de la ética médica y la bioética. Pero estos modelos de conducta también se aplican al uso de las tecnologías, acción que declara un dinámico campo de estudio e investigación, el cual se define como la ética de la información, ética informática o infoética.[27] Esta nueva disciplina se orienta en el estudio de la ética informática y los avances científicos-tecnológicos y su integración a otros escenarios y entornos científicos.

Todos estos procedimientos se instrumentan en una armónica coordinación entre las normas éticas, bioéticas e infoéticas, los principios de seguridad de la gestión de la información y las políticas de ciberseguridad. Además, en la primacía de la protección, integralidad, veracidad y confiabilidad de la información del paciente, el médico, la institución y el sector de la salud.

Al realizar un examen sobre el tema de la seguridad, las ideas comunes que se evalúan están relacionadas con la protección, cuidado o tranquilidad; pero este término pude conceptualizarse según el entorno o campo en que se desee emplear.

Lo mismo ocurre con el tema de la seguridad informática o ciberseguridad; en los que se exponen diversos juicios según el radio de acción o entorno, por estas razones y a interés de la investigación, se analizará el concepto seguridad y dos de sus manifestaciones, que son la seguridad informática y la seguridad de la gestión de la información.

La intención manifiesta se dirige a minimizar riesgos, daños y amenazas a las que puede estar sometido algún proceso o individuo, y las acciones están encaminadas a medidas organizativas, de control del personal, uso de medios de seguridad

destinados para garantizar la integridad y custodia de recursos humanos o materiales ante posibles amenazas o peligros.

Las medidas organizativas y de control se adoptan para garantizar el mantenimiento del orden y la eficiencia en los sistemas de seguridad y protección, los mismos pueden ser accesorios, instrumentos, barreras físicas o lógicas y dispositivos aislados o integrados en un sistema, todos ellos destinados a la vigilancia y protección física de los recursos humanos y materiales.

Conclusiones

A partir de lo expuesto, se puede concluir que el factor determinante en las políticas y normas de ciberseguridad y seguridad en la gestión de la información es el recurso humano, al cual hay que prestarle la mayor atención; seguido por los procesos tecnológicos, proyecciones de contingencia para la minimización de los riesgos y amenazas latentes contra los sistemas e infraestructuras tecnológicas en la salud. El Estado Cubano ha establecido los instrumentos legales y regulatorios para el buen desempeño de las actividades de enfrentamiento, ciberseguridad y seguridad de la gestión de la información, en la protección y las garantías legales para su desarrollo actual.

Referencias

1. Indarte S, Pazos Gutiérrez P. Estándares e interoperabilidad en salud electrónica: Requisitos para una gestión sanitaria efectiva y eficiente [Internet]. Santiago de Chile: CEPAL; 2011 [Citado 04/07/2022]. Disponible en: https://www.cepal.org/sites/default/files/publication/files/3938/S2011120_es.pdf
2. Tickner AB. El Concepto De La Seguridad: Aportes Críticos [Internet]. Colombia: Friedrich-Ebert-Stiftung; 2020 [Citado 19/04/2022]. Disponible en: http://library.fes.de/pdf-files/bueros/la-seguridad/16914.pdf
3. DocuSing. Entiende el concepto de seguridad digital [Internet]. Mexico: DocuSign ; 2021 [Citado 19/04/2022]. Disponible en: https://www.docusign.mx/blog/seguridad-digital
4. Bogantes A. El rol de la seguridad informática en el ámbito académico y los sistemas de información asociados. SISTEMAS CIBERNÉTICAE INFORMÁTICA [Internet]. 2020 [Citado 19/04/2022]; 17(1): 57-62. Disponible en: http://www.iiisci.org/journal/pdv/risci/pdfs/CB294NT20.pdf
5. GCF Global. Concepto de seguridad [Internet]. EE UU: GCF Global; 2021 [Citado 19/04/2022]. Disponible en: http://epn.gov.co/elearning/distinguidos/SEGURIDAD/1_conceptos_de_seguridad.htmlhttps://definicion.de/seguridad/
6. Perez Porto J, Gardey A. Definición de Seguridad [Internet]. EE UU: conceptodefinicion.de; 2022 [Citado 19/04/2022] disponible en: https://conceptodefinicion.de/seguridad/

7. Sain G. ¿Qué es la seguridad informatica?. Revista Pensamiento Penal [Internet]. 2021 [Citado 19/04/2022]; 48. Disponible en: http://www.pensamientopenal.com.ar/system/files/2021/05/doctrina46557.pdf
8. Moreno Heredia A, Oré Crisóstomo WR. Formulación de Políticas de Seguridad Informática Basado en la Norma ISO/IEC 17799 para la Gestión de la Información de la Unidad de Gestión Educativa Local en Chincha en el Año 2018 [Tesis Especialidad]. Perú: Universidad Autónoma de Ica; 2020 [Citado 19/04/2022]. Disponible en: http://repositorio.autonomadeica.edu.pe/handle/autonomadeica/563
9. CUPUE. ¿Cuáles son los tipos de seguridad informática? [Internet]. Argentina: CUPUE; 2020 [Citado 19/04/2022] . Disponible en: https://ceupe.com.ar/blog/cuales-son-los-tipos-de-seguridad-informatica/
10. Triana EJ. Capacidades técnicas , legales y de gestión para equipos BLUE TEAM Y RED TEAM [Tesis Maestría]. Colombia: Universidad Nacional Abierta y a Distancia – UNAD; 2020 Citado 19/04/2022]. Disponible en: https://repository.unad.edu.co/handle/10596/48117
11. Grupo ESGinnova. ISO 27001: ¿Qué significa la Seguridad de la Información? [Internet]. Córdova: Grupo ESGinnova; 2015 [Citado 19/04/2022]. Disponible en: https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/
12. Franco Reyes WA. Diseño administrativo para la creación de un centro de respuesta a incidentes de seguridad informática CSIRT en la empresa platino sistemas [Tesis Maestría]. Colombia: Universidad Nacional Abierta y a Distancia – UNAD; 2021 [Citado 19/04/2022]. Disponible en: https://repository.unad.edu.co/handle/10596/39392
13. Gaceta Oficial No. 061 / 1983 Ordinaria; Ley No. 41, "Ley De La Salud Pública". [Internet] 1983 Ago 15 [Citado 19/04/2022], GOC-1983-061-O pág. 967-982. Disponible en: http://www.parlamentocubano.gob.cu/index.php/documento/ley-de-la-salud-publica/
14. Gaceta oficial No. 078 Ordinaria de 1999 [Internet]. La Habana: GOC-1999-078-O:1259-1273 ; 1999 [Citado 19/04/2022]. Disponible en: https://vuceregulaciones.mincex.gob.cu/media/Decreto-Ley%20199-99%202.pdf
15. Gaceta oficial No. 5 Extraordinaria de 2019 [Internet]. La Habana: GOC-2019-406-EX5; 2019 [Citado 19/04/2022]. Disponible en: https://www.gacetaoficial.gob.cu/sites/default/files/goc-2019-ex5.pdf
16. Gaceta oficial No. 90 Ordinaria de 2022 [Internet]. La Habana: GOC-2022-832-090-O; 2022 [Citado 19/04/2022]. Disponible en: https://www.gacetaoficial.gob.cu/sites/default/files/goc-2022-o90_0.pdf
17. Gaceta oficial No. 45 Ordinaria de 2019 [Internet]. La Habana: GOC-2019-547-045-O; 2019 [Citado 19/04/2022]. Disponible en: https://www.gacetaoficial.gob.cu/sites/default/files/goc-2019-o45.pdf
18. Gaceta oficial No. 92 Ordinaria de 2021 [Internet]. La Habana: GOC-2021-760-092-O; 2021 [Citado 19/04/2022]. Disponible en: https://www.gacetaoficial.gob.cu/sites/default/files/goc-2021-o92.pdf
19. Madariaga B. Los ataques informáticos a hospitales se incrementan un 600 por ciento [Internet]. España: CSO Computer World; 2014 [Citado 19/04/2022]. Disponible en: https://cso.computerworld.es/seguridad-en-cifras/los-ataques-informaticos-a-hospitales-se-incrementan-un-600-por-ciento
20. Oz H, Aris A, Levi A, Levi A, Uluagac AS. A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions. ACM *COMPUTING SURVEYS* [Internet] 2022 [Citado 19/04/2022]; 54(11s):1-37. Disponible en: https://doi.org/10.1145/3514229

21. Humayun M, Jhanjhi NZ, Alsayat A, Ponnusamy V. Internet de las cosas y ransomware: evolución, mitigación y prevención. Revista de informática egipcia [Internet]. 2021 [Citado 19/04/2022]; 22(1):105-17. Disponible en: https://doi.org/10.1016/j.eij.2020.05.003
22. Aslan ÖA, Samet R. Una revisión exhaustiva de los enfoques de detección de malware. IEEE Access [Internet]. 2020 [Citado 19/04/2022]; 8:6249-71. Disponible en: https://doi.org/10.1109/ACCESS.2019.2963724
23. Zuraiq AA, Alkasassbeh M. Enfoques de detección de phishing [Internet]. EE UU: Conference: 2019 2nd International Conference on new Trends in Computing Sciences (ICTCS); 2020 [Citado 19/04/2022] *disponible en: https://doi.org/10.1109/ACCESS.2019.2963724*
24. HIPAA JOURNAL. Informe de violación de datos de atención médica de septiembre de 2020: 9,7 millones de registros comprometidos [Internet]. Texas: HIPAA; 2020 [Citado 19/04/2022]. Disponible en: https://www.hipaajournal.com/september-2020-healthcare-data-breach-report-9-7-million-records-compromised/
25. Matesanz V. Qué es el blockchain, cómo funciona y cuál es su relación con las criptos, [Internet]. Madrid: FINECT; 2022 [Citado 19/04/2022]. Disponible en: https://www.finect.com/usuario/vanesamatesanz/articulos/que-blockchain-criptomonedas-guia-facil
26. HIPAA JOURNAL. Informe de violación de datos de atención médica de septiembre de 2020: 9,7 millones de registros comprometidos [Internet]. 2020 Oct 22 [Citado 19/04/2022]. Disponible en: https://www.hipaajournal.com/september-2020-healthcare-data-breach-report-9-7-million-records-compromised/
27. Amoroso Fernandez Y. Infoética. Ciberespacio y Derecho. Reflexiones [Internet]. 2014 [Citado 19/04/2022]; 10(10). Disponible en: http://revistas.bnjm.cu/index.php/BAI/article/download/243/256

Conflicto de interés

No existe ningún conflicto en esta publicación por parte de los autores.

Declaración de autoría

Lic. Inglis Pavón de la Tejera: Conceptualización, Curación de datos, Investigación, Redacción, Administración del proyecto**.**

Dr.C. Lesbia Eloina Rodriguez Baez: Redacción, Revisión y Edición**.**

Ms.C. Nubia de la Tejera Chillón; Dr.C. Germán Del Rio Caballero; Dr.C. Sergio Daniel Cano Ortiz: Supervisión, Revisión y Validación.