UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

CARRERA DE INGENIERÍA DE SISTEMAS

IMPACTO DE ATAQUES RANSOMWARE EN LAS EMPRESAS DE SALUD Y MEDIDAS DE MITIGACIÓN

Trabajo de titulación previo a la obtención del
Título de Ingeniero de Sistemas

AUTOR: DAVID STEPHANO GARCIA PEREZ

TUTOR: JOE LLERENA IZQUIERDO

Guayaquil – Ecuador

2023

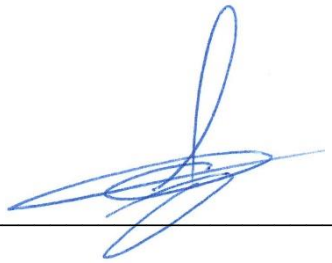
CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, David Stephano García Pérez con documento de identificación N° 0921157632 manifiesto que:

Soy el autor y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Guayaquil, 25 de agosto del año 2023

Atentamente,



David Stephano García Pérez
0921157632

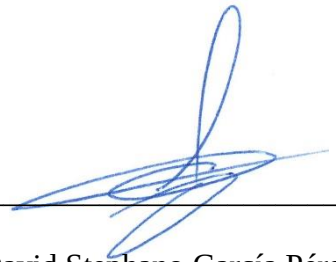
CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Yo, David Stephano García Pérez con documento de identificación No. 0921157632, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor(a) del Artículo Académico: "Impacto de ataques ransomware en las empresas de salud y medidas de mitigación", el cual ha sido desarrollado para optar por el título de: Ingeniero de Sistemas, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Guayaquil, 25 de agosto del año 2023

Atentamente,



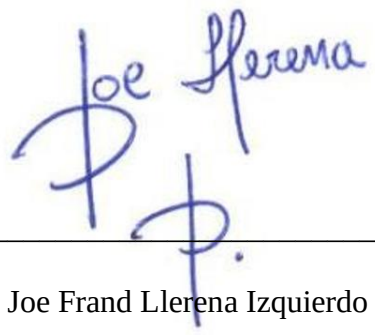
David Stephano García Pérez
0921157632

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Joe Frand Llerena Izquierdo con documento de identificación N° 0914884879, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: IMPACTO DE ATAQUES RANSOMWARE EN LAS EMPRESAS DE SALUD Y MEDIDAS DE MITIGACIÓN, realizado por David Stephano García Pérez con documento de identificación N° 0921157632, obteniendo como resultado final el trabajo de titulación bajo la opción Artículo Académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Guayaquil, 25 de agosto del año 2023

Atentamente,



Joe Frand Llerena Izquierdo
0914884879

DEDICATORIA

Dedico este trabajo a mis padres, por ser mi mayor inspiración y apoyo incondicional en todo momento. A mis amigos y familiares, por sus ánimos, paciencia y comprensión en las largas horas de estudio. A mis profesores, por guiarme en mi formación académica y brindarme las herramientas necesarias para alcanzar mis metas. Este trabajo de titulación es un reflejo de todo el esfuerzo y dedicación que puse en este camino, y se lo dedico con todo mi cariño a quienes me acompañaron en esta hermosa aventura.

AGRADECIMIENTO

Agradezco a Dios, quien ha sido mi guía y fortaleza en todo momento, le dedico este trabajo de titulación. Gracias por iluminar mi camino, por ser mi roca en los momentos difíciles y por brindarme la sabiduría y la perseverancia para alcanzar mis metas.

También quisiera agradecer a mi tutor Ing. Joe Llerena por su dedicación y paciencia en la supervisión de mi investigación. Sus comentarios y sugerencias me ayudaron a enfocar mi trabajo y a desarrollar una comprensión más profunda de mi tema de investigación.

Finalmente, me gustaría agradecer a mi familia y amigos por su apoyo incondicional durante todo el proceso. Sin su amor y aliento, este logro no habría sido posible.

RESUMEN

El valor de los datos en un contexto empresarial es crucial y esta se vuelve mucho más relevante cuando está relacionada al sector de la salud, un sector vulnerable y últimamente preferido por los ciber delincuentes debido a que el sistema de atención médica maneja datos altamente confidenciales, como información de pago, historial e información privada del paciente, medicamentos, tratamientos, etc. generando así daños significativos tanto para las organizaciones como para los pacientes.

Una de las mayores amenazas son los ransomware, ataques relacionados con el secuestro de información e inhabilitación de equipos causando la interrupción del negocio y, por supuesto, pérdidas financieras.

Este documento busca realizar un marco teórico en la cual se revise y clasifique las vulnerabilidades comunes en entornos corporativos y los riesgos asociados a ellas con el fin de establecer lineamientos y estrategias de ciberseguridad que permitan tener un ambiente de red sólido y estructurado, así como la divulgación de la información necesaria para que profesionales de TI para la salud y usuarios finales puedan prevenir, mitigar y recuperarse de estos ataques.

Palabras claves: Ransomware, Vulnerabilidades, Ciberseguridad, Red, Salud.

ABSTRACT

The importance of information in a corporate environment is crucial and this becomes much more relevant when it is related to the health sector, a vulnerable sector and ultimately preferred by cyber criminals because the health care system handles highly confidential data, such as payment information, patient history and private information, medications, treatments, etc. thus generating significant damage for both organizations and patients.

One of the biggest threats is ransomware, attacks related to hijacking information and disabling equipment causing business interruption and, of course, financial loss.

This document seeks to create a theoretical framework in which the common vulnerabilities in corporate environments and the risks associated with them are reviewed and classified in order to establish cybersecurity guidelines and strategies that allow having a solid and structured network environment, as well as the disclosure of the information necessary for health IT professionals and end users to prevent, mitigate and recover from these attacks.

Key words: Ransomware, Vulnerabilities, Cybersecurity, Network, Healthcare.

ÍNDICE DE CONTENIDO

1. INTRODUCCIÓN

El aumento de los incidentes de ciberseguridad es una amenaza creciente para la industria de la salud que en los últimos años ha experimentado una extensa y disruptiva transformación digital con el crecimiento de la conectividad, la digitalización de la información y la transición a sistemas electrónicos (Kandasamy et al., 2022)(Ayala et al., 2016)(Williams et al., 2020). Para mantener protegida la información de salud, los proveedores de atención médica deben estar al tanto de las tendencias y amenazas de ciberseguridad a medida que surgen, para ello, hay una serie de principios clave que deben tenerse en cuenta en los sistemas sanitarios dado que entornos médicos, los registros o dispositivos comprometidos pueden ralentizar o interrumpir los procedimientos, impidiendo la atención de pacientes con necesidades críticas y con potencial de muertes, así como muchas otras consecuencias (Ghayoomi et al., 2021)(Melendrez-Caicedo & Llerena-Izquierdo, 2022).

La transformación digital describe el efecto holístico donde una aplicación de software transforma fundamentalmente un dominio en particular, la transformación digital adoptada en la industria de la salud incluye la integración de sistemas de información de la salud y medidas de seguridad cibernética para dispositivos médicos en red (Nifakos et al., 2021)(Kandasamy et al., 2022).

Este proceso de transformación se ha acelerado desde 2020 debido a la pandemia de COVID-19 y junto a la necesidad de mantener una distancia física se facilitó significativamente el uso de tecnologías digitales tanto por parte de los pacientes como de los profesionales de la salud, y brindó la oportunidad de reconocer los beneficios de la salud digital volviéndose poco a poco prácticas más comunes (Zerega-Prado & Llerena-Izquierdo, 2022). Por otro lado, el sector de la salud se ha vuelto responsable de recopilar y almacenar volúmenes cada vez mayores de datos confidenciales y altamente sensibles, al mismo tiempo que debe compartirlos entre el personal médico, los pacientes y otras organizaciones (Llerena-Izquierdo & Merino-Lazo, 2021)(Llerena-Izquierdo et al., 2020). Por lo tanto, la pandemia de COVID-19 reveló no solo la necesidad de compartir datos, sino también la necesidad de protegerlos (Garcia-Perez et al., 2023)(Barberán Vizueta & Chela Criollo, 2021).

El delito cibernético surgió a finales de la década de 1970 cuando la industria de la Tecnología de la Información (TI) tomó mayor relevancia y fuerza comenzando como un correo no deseado, a lo que tenemos hoy en día donde se han observado muchas variaciones de virus informáticos y malware (McDonald et al., 2022)(Ayala Carabajo & Llerena Izquierdo, 2014).

Estos delitos tienen una fácil y rápida adaptabilidad a los cambios en la situación mundial. Al comienzo de una escalada en la pandemia de COVID-19, los ciber atacantes de malware identificaron vulnerabilidades comunes y adaptaron sus ataques para explotarlas. Los atacantes cibernéticos están aprovechando la mayor dependencia del trabajo remoto, la disminución de la movilidad y el cierre de fronteras entre diferentes países, y la mayor demanda de equipos de protección personal (EPP), como máscaras y guantes (Terán Villafuerte, 2023)(Toala Indio, 2021)(Pérez González, 2021). La compleja cadena de suministro de atención médica también es un objetivo. Como resultado, la población en general está experimentando un mayor temor, incertidumbre y duda (He et al., 2021)(Ravali & Lakshmi Priya, 2021).

El objetivo de esta revisión es reconocer las tendencias de seguridad cibernética, incluidas las amenazas recientes con respecto al ransomware y su relación con la industria de la salud a través de la literatura académica. La industria de la salud debe estar lista para enfrentar amenazas cibernéticas con el fin de salvaguardar la disponibilidad de los servicios médicos esenciales, así como la confidencialidad y la integridad de los datos relacionados con la atención médica.

2. REVISIÓN DE LITERATURA

Entre estas amenazas se encuentra el ransomware, un tipo de malware que secuestra computadoras bloqueándolas o cifrando sus archivos y le impide su correcto funcionamiento hasta que se pague un rescate (Berrueta et al., 2020)(Rameem Zahra et al., 2022). La historia del ransomware se remonta a finales de los 90, cuando se pronosticó como una amenaza potencial que utiliza criptografía de manera ofensiva (Alawida et al., 2022).

En ese sentido, los ataques de Ransomware se pueden identificar en dos categorías (Nifakos et al., 2021). El primero de ellos es el "Locker Ransomware", que como su nombre lo indica, bloquea únicamente el dispositivo haciendo imposible su uso. Sin embargo, la información interna no es vulnerada por lo que el usuario puede acceder a ella cambiando el dispositivo de almacenamiento a otro equipo (Kruse et al., 2017). En el caso del "Crypto Ransomware" hace uso de algoritmos de cifrado para cifrar los datos de la víctima mediante los enfoques simétricos y asimétricos donde la victima solo puede obtener su información cuando paga por la llave de descifrado (Kapoor et al., 2022)(Thamer & Alubady, 2021).

En el siguiente diagrama se muestra el funcionamiento típico de ataque de un ransomware.

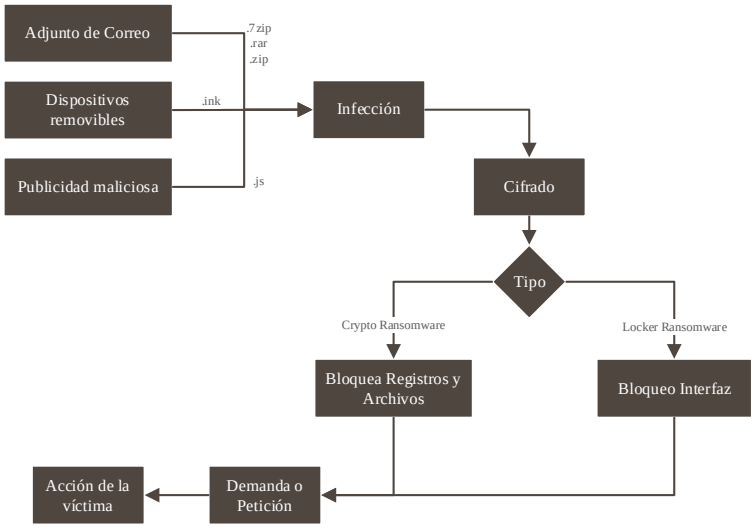


Figura 1 Secuencia de operaciones de un Ransomware

El ransomware se propaga primordialmente por razones de falta de "higiene cibernética", refiriéndose a esto como todos los aspectos de ciberseguridad, incluido la disponibilidad de antivirus, concientización del usuario, navegación, entre otras. A pesar de que a nivel organizacional se hayan mejorado los estándares y protocolos de seguridad, los ransomware han logrado penetrar exitosamente los distintos sistemas de defensas.

El sector sanitario ha sido de los objetivos primordiales de los ciberataques durante la pandemia debido a su vulnerabilidad, como el ataque del ransomware WannaCry que incapacitó el Servicio Nacional de Salud en 2017. Entre las razones principales de los ataques a estas organizaciones por considerarse una infraestructura crítica que sirve como la columna vertebral de la provisión de atención médica están los presupuestos limitados para proteger sus sistemas de TI que normalmente están sujetos controles presupuestarios muy estrictos, La rápida evolución hacia la digitalización y el crecimiento de la cantidad de dispositivos en el Internet de las Cosas (IoT). Por último, pero igualmente significativo, el mercado negro ha visto un incremento en la valoración de los datos personales de pacientes, así como de la información de propiedad intelectual y de investigación. La recuperación de la privacidad se vuelve imposible una vez que los datos privados, como el historial médico de una persona, se ven comprometidos, ya que estos registros contienen detalles como el nombre, la fecha de nacimiento, información del seguro, el proveedor de atención médica, además de información genética y de enfermedades. Esta información es lucrativa para hackers dado que es posible vender por 10 a 20 veces más que el monto de la información de una tarjeta de crédito (Argaw et al., 2020; Williams et al., 2020) (Wilner et al., 2022)(Alvarado Salazar, 2022).

Una interrupción de las soluciones digitales podría conducir, en el peor de los casos, a una inactividad total de las operaciones (Calero Manueles, 2021), lo que tendría efectos graves en el valor de la atención médica (Cruz Calero, 2022)(Arguello Lino & Coca Hidalgo, 2023). Los efectos adicionales de un ataque cibernético incluyen la interrupción de los servicios que no son de emergencia, como la programación y realización de cirugías electivas (Villamar Arellano, 2023)(Campoverde Reyes, 2023). El incidente también puede tener un impacto en el tiempo que el paciente pasa en las unidades de hospitalización afectadas. Los tiempos de servicio más largos podrían impedir la recuperación, ya que los pacientes que ingresan pueden necesitar permanecer más tiempo (Recalde Monar, 2021)(Rosero Tejada, 2021)(Acero Carrión, 2022).

En consecuencia, el impacto de un ciberataque puede volverse más severo si el aprovisionamiento de servicios depende en gran medida de las soluciones digitales para el cuidado de la salud (Alvarado-Salazar & Llerena-Izquierdo, 2022)(Wade, 2021)(Miñan Parrales, 2022)(Terán Villafuerte, 2023).

Pagar el rescate también puede tener otras consecuencias negativas. No hay garantía de que los atacantes proporcionen la clave de descifrado incluso si se paga el rescate; no hay garantía de

recuperación total; los atacantes pueden incluso exigir un segundo rescate; y el pago fomenta futuros ataques (Ghayoomi et al., 2021)(Tacuri López, 2021)(Castro Macías, 2022).

Los esfuerzos de los profesionales de la seguridad y los investigadores han convergido para luchar contra estos ataques. Se trabaja para detectar, prevenir y mitigar dichos ataques y sus posibles efectos. Pero como sabemos, los ransomware se caracterizan por su tendencia a evolucionar tanto en intensidad como en estrategias de ataque por lo que se requieren cada vez más esfuerzos para encontrar las soluciones para interrumpir su proceso de ataque (Carvajal Nagua & Solano Cedeño, 2021)(Rigchc Mero, 2022).

3. METODOLOGÍA APLICADA

Esta investigación se ha llevado a cabo para lograr una comprensión más completa de las vulnerabilidades actuales que representan una amenaza para los entornos empresariales, en particular, el sector de la salud. Para ello utilizaremos el análisis teórico descriptivo con un enfoque cuantitativo del impacto de los ataques ransomware en los diferentes procesos de las empresas de la salud, sugiriendo medidas preventivas que permitan prevenir, mitigar y recuperarse de estos ataques (ver Tabla 1).

Pregunta	Motivación
P1: ¿Cuáles son las vulnerabilidades más comunes hacia empresas de la salud?	Especificar los tipos de vulnerabilidades cibernéticos más comunes hacia empresas de la salud.
P2: ¿Cuáles son las afectaciones que presentan las organizaciones o empresas de salud al enfrentarse a ataques de ransomware?	Determinar las implicancias y afectaciones que puedan existir bajo un ataque de ransomware en empresas de salud.
P3: ¿Que estrategias pueden llevarse a cabo con el fin de disminuir el impacto de un ataque de ransomware en empresas de salud?	Documentar y especificar medidas de prevención que puedan realizarse en todos los aspectos de una empresa de salud para la correcta gestión y prevención de un ataque ransomware.

Tabla 1. Preguntas de investigación

3.1. Estrategias y procedimientos utilizados para adquirir información

Para la presente investigación se consultaron tres bases de datos diferentes en las cuales se realizó la recopilación de la literatura adecuada relacionada con el tema propuesto. Las bases de datos elegidas para ellos fueron Scopus, IEEExplore y Web of Science utilizando la cadena de búsqueda (Ransomware AND Healthcare) OR (Ransomware AND Prevention) tomándose a consideración los artículos publicados en los últimos 6 años.

3.2. Enfoques y procedimientos empleados para examinar los datos

Para la búsqueda de artículos con referencia al criterio anteriormente mencionado, se utilizaron los siguientes criterios para identificar los estudios que debían incluirse:

- Artículos que informan sobre ciberataques dirigidos a hospitales y otros entornos clínicos.
- Artículos con información relevante para la ciberseguridad en empresas de salud ya atención médica.
- Artículos que detallen medidas de mitigación y prevención de ataques ransomware.

Se utilizaron los siguientes criterios de exclusión para la selección de los artículos primarios:

- Artículos que informen sobre la seguridad del paciente a partir de dispositivos médicos y/o tecnologías de ciberseguridad relevantes.
- Estudios que informan solo sobre el desarrollo técnico (p. ej., algoritmos, software) sin la participación de profesionales de la salud.
- Artículos de estudio que no son Open Access.

3.3. Selección de estudios primarios

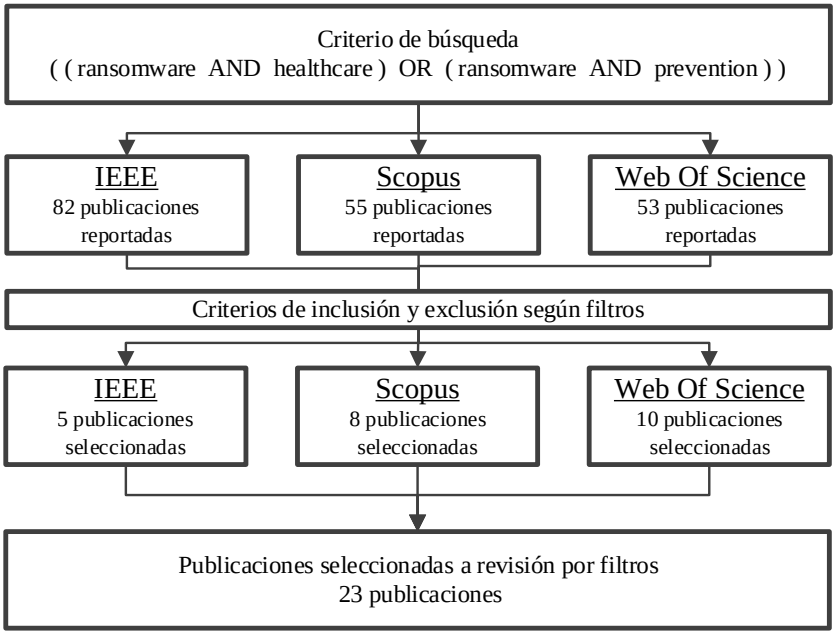


Figura 2. Flujo de selección de investigaciones

Luego de la revisión de la literatura se observaron cuatro temas principales en la bibliografía seleccionada, (ver Fig. 2): (1) cambios en las condiciones del sector de la salud debido a la COVID-19, (2) Incidentes cibernéticos en el ámbito de la atención médica durante la pandemia de COVID-19, (3) desafíos de ciberseguridad en la atención de la salud y (4) ciberseguridad en la atención de la salud. Los resultados vinculados a las transformaciones en las circunstancias del sector de la salud debidas a la COVID-19 se obtienen a partir de las preguntas de investigación detalladas en la Tabla 1, y estas respuestas se presentan en la sección de resultados.

4. RESULTADOS

Los artículos estudiados exponen que existe una creciente amenaza de los ciberataques en el sector de la salud, así como la falta de preparación para hacerles frente. Esto se debe a la rápida implementación de nuevas tecnologías, que supera la capacidad de desarrollar sistemas de seguridad para protegerlas. La investigación sugiere que la información médica de un individuo es de 20 a 50 veces más valiosas para los ciberdelincuentes ya que los mismos permite a los ciberdelincuentes cometer delitos como robo de identidad, extorsión, y la capacidad de obtener sustancias controladas de manera ilegal (Kruse et al., 2017).

Hay sugerencias como es el caso de (Kandasamy et al., 2022) que recomienda el uso de marcos de gestión de riesgos cibernéticos como ISO, MIST y HIPAAA, los cuales son estándares que tienen múltiples puntos en común en cuanto a políticas de seguridad de la información, copias de seguridad, responsabilidades, análisis y gestión de riesgo que según la naturaleza de las organizaciones de salud pueden ser aplicables en medida.

En (Pranggono & Arabo, 2021) , (Saxena & Soni, 2018) se proponen diversos métodos de mitigación de incidentes relacionados a los ataques de ransomware entre los cuales están las correcta educación del usuario, uso de redes privadas virtuales (VPN), la actualización de los dispositivos y firmwares. A su vez tener un correcto control de la infraestructura de la red médica, segmentación de las diferentes áreas, así como la seguridad física y lógica de estos.

Si bien el impacto de la ciberseguridad no es exclusivo de la industria de la salud, los esfuerzos concertados para proteger los datos de las partes interesadas se han quedado atrás y han faltado en la atención médica en comparación con otras industrias (Hofmann, 2020), (ver Fig. 3).

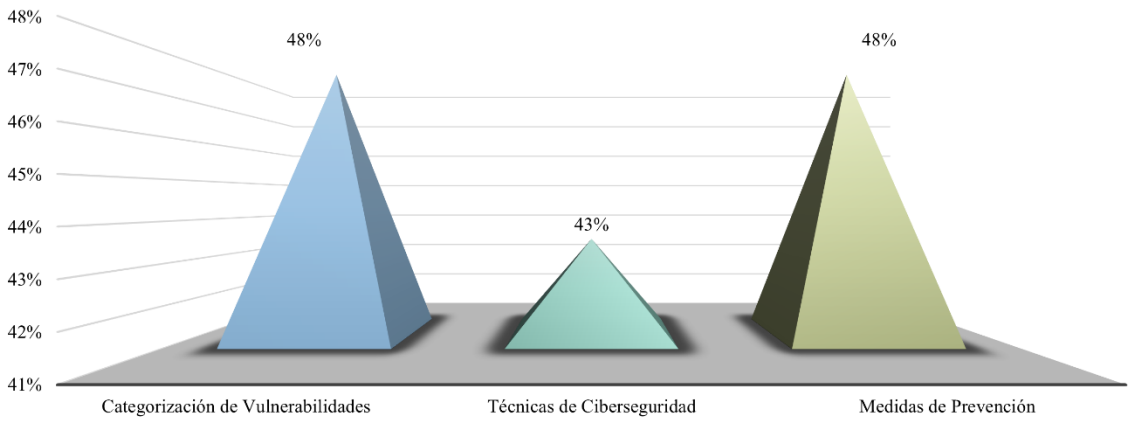


Figura 3. Porcentaje de trabajos de investigación que determinan temas y objetivos enfocadas al estudio presentado

P1: ¿Cuáles son los métodos de ataques Ransomware más comunes hacia empresas de la salud?

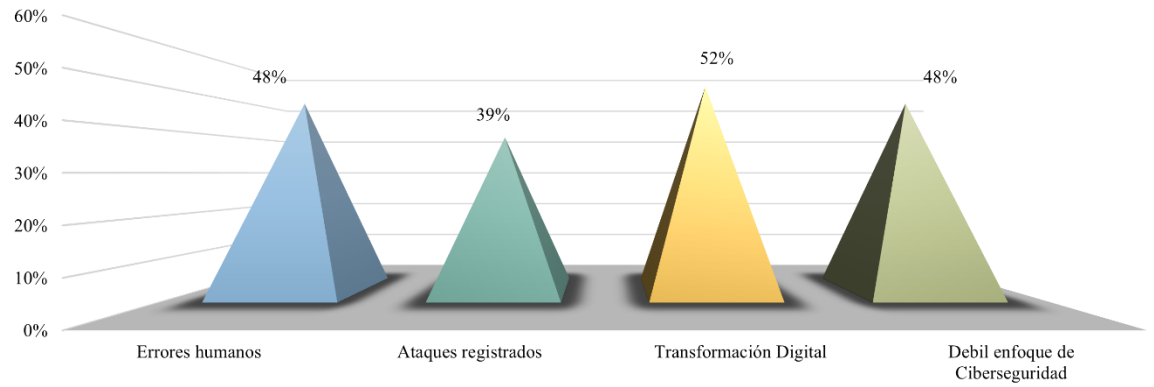


Figura 4. Porcentaje de trabajos de investigación que problemas determinados para el estudio presentado

La primera medida para mitigar los ataques ransomware es identificar las vulnerabilidades más comunes en los entornos corporativos. La mayoría de los ataques ransomware explotan las vulnerabilidades de los sistemas operativos, aplicaciones, servicios y dispositivos, (ver Fig. 4).

- Ingeniería Social y Phishing: El phishing sigue siendo una de las tácticas más habituales utilizadas por los atacantes de ransomware para infiltrarse en los sistemas y redes de las organizaciones de atención médica. Los atacantes pueden enviar correos electrónicos aparentemente legítimos con el fin de engañar a los empleados y lograr que divulguen información confidencial o descarguen software malicioso que permita a los atacantes acceder a la red de la empresa.
- Explotación de vulnerabilidades: Los atacantes pueden aprovechar la falta de actualización de software y firmware de los sistemas y dispositivos para explotar vulnerabilidades con los que puedan infiltrarse en la red y cifrar los datos. Por lo cual es importante que las empresas mantengan sus softwares actualizados con el objetivo de reducir las probabilidades de esto ataques.
- Ataques mediante proveedores externos: Los terceros proveedores de servicios de una empresa de atención médica, como contratistas o proveedores de servicios en la nube, pueden ser vulnerables a ataques y servir como punto de entrada para la infección de la red de la organización de salud.
- Ataques por fuerza bruta: Los agresores también pueden emplear métodos de fuerza bruta con el fin de descifrar contraseñas y obtener acceso no autorizado a los sistemas

de la entidad de atención médica, aprovechando la ausencia de medidas de autenticación adecuadas.

P2: ¿Cuáles son las afectaciones que presentan las organizaciones o empresas de salud al enfrentarse a ataques de ransomware?

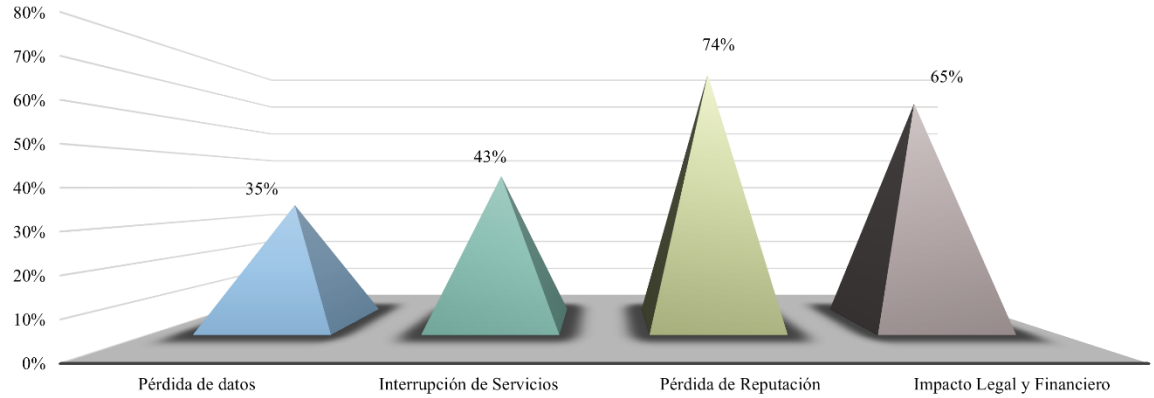


Figura 5. Porcentaje de trabajos de investigación que determinan afectaciones enfocadas al estudio presentado

- Pérdida de datos: Los ataques de ransomware pueden cifrar o eliminar archivos y datos críticos para la organización o empresa de salud, lo que puede provocar pérdidas financieras, legales y de reputación.
- Interrupción de servicios: Los ataques de ransomware pueden interrumpir los servicios y sistemas críticos de la organización o empresa de salud, lo que puede afectar la atención al paciente y los servicios médicos.
- Pérdida de reputación: Los ataques de ransomware pueden afectar la confianza de los pacientes y clientes en la organización o empresa de salud, lo que puede provocar una pérdida de reputación a largo plazo.
- Pérdidas financieras: Los costos de recuperación y respuesta a un ataque de ransomware pueden ser significativos y pueden incluir el costo de pagar el rescate, la pérdida de ingresos y la posible sanción por incumplimiento de normas.
- Impacto legal: Las organizaciones y empresas de salud pueden estar sujetas a sanciones legales y multas por incumplimiento de las normas de privacidad y seguridad de la información en caso de un ataque de ransomware.

P3: ¿Que estrategias pueden llevarse a cabo con el fin de disminuir el impacto de un ataque de ransomware en empresas de salud?

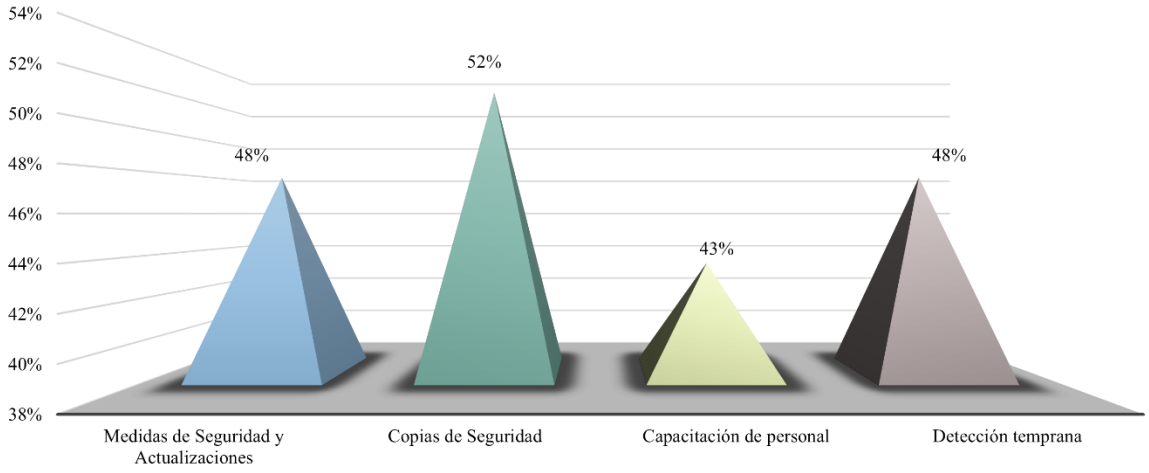


Figura 6. Porcentaje de trabajos de investigación que determinan una solución enfocada al estudio presentado

- Establecer medidas de seguridad efectivas: Las organizaciones de atención médica deben establecer medidas de seguridad efectivas para resguardarse de los ataques de ransomware, tales como la instalación de software de seguridad, la configuración de firewalls y la implementación de políticas de seguridad sólidas.
- Efectuar respaldos periódicos: Las organizaciones de atención médica deben llevar a cabo respaldos periódicos de todos los datos esenciales y sistemas para asegurar la capacidad de restaurar la información en caso de que ocurra un ataque de ransomware exitoso.
- Capacitar al personal en seguridad cibernética: Las empresas de salud deben capacitar a su personal en seguridad cibernética para identificar y prevenir posibles ataques de ransomware.
- Contar con planes de acción ante incidentes: Las empresas de salud deben tener planes de respuesta a incidentes detallados para garantizar que puedan responder rápidamente a un ataque de ransomware y minimizar el impacto del ataque.
- Mantenerse actualizado con las últimas amenazas de seguridad: Las empresas de salud deben mantenerse actualizadas con las últimas amenazas de seguridad y vulnerabilidades, para poder implementar las medidas de seguridad adecuadas y prevenir posibles ataques de ransomware.
- No pagar el rescate: A pesar de la posible tentación de pagar la suma exigida como rescate para recuperar los datos encriptados, esta acción no asegura la recuperación de los datos y podría motivar a los atacantes a seguir perpetrando ataques de ransomware.

Además, es importante tener en cuenta que el pago del rescate puede ser considerado ilegal en ciertos países.

5. DISCUSIÓN

Para contrarrestar el impacto de tales ataques de ciberseguridad, las organizaciones han adoptado estrategias de gobernanza para promover las mejores prácticas para proteger la infraestructura electrónica de los hospitales y otros entornos clínicos (Alami et al., 2019). es importante ofrecer programas de concientización y formación para el personal médico. El papel del comportamiento humano para hacer frente a los ataques cibernéticos y fortalecer las defensas cibernéticas se agrupa en el tema de los " factores humanos" en la ciberseguridad.

El análisis del malware tiene como enfoque principal comprender los componentes y comportamientos del malware, incluido el ransomware (Mayorga Muñoz, 2022). En (Thamer & Alubady, 2021), (Alotaibi & Vassilakis, 2021), (Lee et al., 2019) expone el uso de tecnologías de blockchain, Machine Learning, tecnología SDN (Software Define Network) como métodos que permitan la pronta y oportuna detección de los ataques de ransomware, así como la mejora de la recopilación y utilización de la información de salud de los pacientes. Dado que la detección temprana de estas amenazas posibilitaría la implementación de las medidas de seguridad requeridas antes de que inicie el proceso de cifrado de archivos.

Sin embargo, como fue revisado extensamente por (Alqahtani & Sheldon, 2022), estos modelos de detección temprana tienen sus limitaciones e inconvenientes. Las cuales están estrechamente relacionadas con la definición inexacta del proceso previo a la encriptación, la deficiencia de datos recopilados en esta etapa y el diseño de los componentes de detección.

6. CONCLUSIÓN

Los ataques ransomware son una amenaza importante para las empresas de salud, ya que pueden tener un impacto devastador en la atención médica y la privacidad de los pacientes. Las medidas de mitigación descritas en este artículo pueden ayudar a prevenir o reducir el impacto de estos ataques en las empresas de salud. Es esencial que las organizaciones de atención médica se mantengan al tanto de las amenazas en el ámbito de la seguridad informática y que tomen medidas apropiadas para resguardar tanto su información crítica como la de sus pacientes.

Los dos impulsores principales que exponen la atención médica a las amenazas cibernéticas incluyen el rápido avance tecnológico y la evolución de la política federal. A medida que la infraestructura de TI del cuidado de la salud lucha con la nueva tecnología y los protocolos de seguridad, la industria es un objetivo principal para el robo de información médica. A pesar de los progresos realizados por las empresas de seguridad y el gobierno para reducir la frecuencia de los ataques cibernéticos, el sector de la salud se encuentra rezagado en comparación con otras industrias líderes en la salvaguarda de datos críticos.

El cuidado de la salud debe adaptarse continuamente a las tendencias y amenazas de ciberseguridad en constante cambio, como el ransomware, donde se explota la infraestructura crítica y se extraen datos valiosos de los pacientes. Es imperativo dedicar recursos y esfuerzos para mantener y asegurar la protección de la tecnología de atención médica y la confidencialidad de la información del paciente, evitando cualquier acceso no autorizado.

Las mejores prácticas y las recomendaciones proporcionadas por expertos en organizaciones de atención médica deben promoverse entre las partes interesadas de la atención médica, incluidos médicos, enfermeras, pacientes, administradores y personal de TI porque la ciberseguridad es responsabilidad de todos.

En la actualidad, el ransomware es la principal preocupación del desarrollo tecnológico. Sin embargo, este requiere de un camino seguro para poder continuar en auge. Esperamos que en el futuro se continúen las investigaciones acerca de enfoques de mitigación y prevención de ransomware más eficientes.

REFERENCIAS

Acero Carrión, R. F. (2022). *Modelo esquema para el análisis y tratamiento de la información en empresas ecuatorianas de comercio exterior mediante el uso de BIG DATA*. http://dspace.ups.edu.ec/handle/123456789/23637

Alami, H., Gagnon, M. P., Ag Ahmed, M. A., & Fortin, J. P. (2019). Digital health: Cybersecurity is a value creation lever, not only a source of expenditure. *Health Policy and Technology*, *8*(4), 319–321. https://doi.org/10.1016/J.HLPT.2019.09.002

Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University - Computer and Information Sciences*, *34*(10, Part A), 8176–8206. https://doi.org/https://doi.org/10.1016/j.jksuci.2022.08.003

Alotaibi, F. M., & Vassilakis, V. G. (2021). SDN-Based Detection of Self-Propagating Ransomware: The Case of BadRabbit. *IEEE Access*, *9*, 28039–28058. https://doi.org/10.1109/ACCESS.2021.3058897

Alqahtani, A., & Sheldon, F. T. (2022). A Survey of Crypto Ransomware Attack Detection Methodologies: An Evolving Outlook. *Sensors*, *22*(5). https://doi.org/10.3390/S22051837

Alvarado-Salazar, R., & Llerena-Izquierdo, J. (2022). Revisión de la literatura sobre el uso de Inteligencia Artificial enfocada a la atención de la discapacidad visual. *Revista InGenio*, *5*(1), 10–21. https://doi.org/https://doi.org/10.18779/ingenio.v5i1.472

Alvarado Salazar, R. E. (2022). *Inteligencia artificial con enfoque a la discapacidad visual: un mapeo sistemático*.

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M. V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J. M., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020). Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making*, *20*(1). https://doi.org/10.1186/S12911-020-01161-7

Arguello Lino, R. E., & Coca Hidalgo, J. L. (2023). *Modelo de datos seguros para el sector inmobiliario en Ecuador utilizando tecnología Blockchain*. http://dspace.ups.edu.ec/handle/123456789/25036

Ayala Carabajo, R., & Llerena Izquierdo, J. (2014). *Primer Congreso Salesiano de Ciencia, Tecnología e Innovación para la Sociedad. Memoria Académica*. http://dspace.ups.edu.ec/handle/123456789/9506

Ayala, R., Llerena, J., Parra, P., Vega Ureta, N., Hernández, A., Romero, I., & Cueva, J. (2016). *Segundo Congreso Salesiano de Ciencia*. Tecnología e Innovación Para La Sociedad. http://dspace.ups.edu.ec/handle/123456789/12776

Barberán Vizueta, M. S., & Chela Criollo, J. K. (2021). *Prótesis impresas en 3D y aplicativo móvil de geolocalización: Caso de Estudio Novus Spem*. https://dspace.ups.edu.ec/handle/123456789/20293

Berrueta, E., Morato, D., Magana, E., & Izal, M. (2020). Open Repository for the Evaluation of Ransomware Detection Tools. *IEEE Access*, *8*, 65658–65669. https://doi.org/10.1109/ACCESS.2020.2984187

Calero Manueles, E. F. (2021). *Aplicación móvil para reconocimiento de texto sobre carnés estudiantiles utilizando visión por computadora basada en la nube*. http://dspace.ups.edu.ec/handle/123456789/20902

Campoverde Reyes, E. A. (2023). *Dispositivos inteligentes en seguridad industrial para la prevención de accidentes y enfermedades ocupacionales*.

Carvajal Nagua, K. A., & Solano Cedeño, C. S. (2021). *Desarrollo de una Aplicación Web para el Control de citas y manejo de historial médico en la Unidad Médica Family care de la ciudad de Guayaquil*. https://dspace.ups.edu.ec/handle/123456789/20905

Castro Macías, B. A. (2022). *Modelos de seguridad, acciones y protocolos para la prevención de vulnerabilidades de la seguridad de la información mediante las tecnologías IOT Y API RESTFUL*.

Cruz Calero, G. N. (2022). *Modelo de conexión y datos para el seguimiento de pacientes de hospitales en Ecuador basado en Iot y Blockchain*. http://dspace.ups.edu.ec/handle/123456789/23330

Garcia-Perez, A., Cegarra-Navarro, J. G., Sallos, M. P., Martinez-Caro, E., & Chinnaswamy, A. (2023). Resilience in healthcare systems: Cyber security and digital transformation. *Technovation*, *121*, 102583. https://doi.org/https://doi.org/10.1016/j.technovation.2022.102583

Ghayoomi, H., Laskey, K., Miller-Hooks, E., Hooks, C., & Tariverdi, M. (2021). Assessing resilience of hospitals to cyberattack. *Digital Health*, *7*. https://doi.org/10.1177/20552076211059366

He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review. *Journal of Medical Internet Research*, *23*(4), 1–18. https://doi.org/10.2196/21747

Hofmann, T. (2020). How organisations can ethically negotiate ransomware payments. *Network Security*, *2020*(10), 13–17. https://doi.org/10.1016/S1353-4858(20)30118-5

Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2022). Digital Healthcare - Cyberattacks in Asian Organizations: An Analysis of Vulnerabilities, Risks, NIST Perspectives, and Recommendations. *IEEE Access*, *10*, 12345–12364. https://doi.org/10.1109/ACCESS.2022.3145372

Kapoor, A., Gupta, A., Gupta, R., Tanwar, S., Sharma, G., & Davidson, I. E. (2022). Ransomware Detection, Avoidance, and Mitigation Scheme: A Review and Future Directions. In *Sustainability* (Vol. 14, Issue 1). https://doi.org/10.3390/su14010008

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, *25*(1), 1–10. https://doi.org/10.3233/THC-161263

Lee, K., Lee, S. Y., & Yim, K. (2019). Machine Learning Based File Entropy Analysis for Ransomware Detection in Backup Systems. *IEEE Access*, *7*, 110205–110215. https://doi.org/10.1109/ACCESS.2019.2931136

Llerena-Izquierdo, J., Barberan-Vizueta, M., & Chela-Criollo, J. (2020). Novus spem, 3D printing of upper limb prosthesis and geolocation mobile application. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, *2020*(E33), 127–140.

Llerena-Izquierdo, J., & Merino-Lazo, M. (2021). Aplicación móvil de control nutricional para prevención de la anemia ferropénica en la mujer gestante. *Revista InGenio*, *4*(1), 17–26. https://doi.org/10.18779/ingenio.v4i1.364

Mayorga Muñoz, C. J. (2022). *Amenazas en el espacio cibernético con incidencia en la información de entidades públicas y privadas*.

McDonald, G., Papadopoulos, P., Pitropakis, N., Ahmad, J., & Buchanan, W. J. (2022). Ransomware: Analysing the Impact on Windows Active Directory Domain Services. In *Sensors* (Vol. 22, Issue 3). https://doi.org/10.3390/s22030953

Melendrez-Caicedo, G., & Llerena-Izquierdo, J. (2022). Secure Data Model for the Healthcare Industry in Ecuador Using Blockchain Technology. *Smart Innovation, Systems and Technologies*, *252*, 479–489. https://doi.org/10.1007/978-981-16-4126-8_43

Miñan Parrales, W. E. (2022). *Modelo de arquitectura de gestión de la información para la cadena de suministros en empresas de consumo masivo mediante Iot y Blockchain*.

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors*, *21*(15). https://doi.org/10.3390/S21155119

Pérez González, R. F. (2021). *Softwares de penetración utilizados por los piratas informáticos: Una revisión sistemática (2015-2020)*.

Pranggono, B., & Arabo, A. (2021). COVID -19 pandemic cybersecurity issues . *Internet Technology Letters*, *4*(2). https://doi.org/10.1002/ITL2.247

Rameem Zahra, S., Ahsan Chishti, M., Iqbal Baba, A., & Wu, F. (2022). Detecting Covid-19 chaos driven phishing/malicious URL attacks by a fuzzy logic and data mining based intelligence system. *Egyptian Informatics Journal*, *23*(2), 197–214. https://doi.org/https://doi.org/10.1016/j.eij.2021.12.003

Ravali, S., & Lakshmi Priya, R. (2021). Design and Implementation of Smart Hospital using IoT. *Proceedings - 5th International Conference on Computing Methodologies and Communication, ICCMC 2021*, *Iccmc*, 460–465. https://doi.org/10.1109/ICCMC51019.2021.9418296

Recalde Monar, J. A. (2021). *El ciberacoso por redes sociales en el Ecuador*. http://dspace.ups.edu.ec/handle/123456789/20945

Rigchc Mero, A. (2022). *Determinación de los peligros en las redes sociales en entorno a niños y adolescentes para uso y prevención*. http://dspace.ups.edu.ec/handle/123456789/22843

Rosero Tejada, L. F. (2021). *El Phishing como riesgo informático, técnicas y prevención en los canales electrónicos: Un mapeo sistemático*.

Saxena, S., & Soni, H. K. (2018). Strategies for Ransomware Removal and Prevention. *2018 Fourth International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB)*, 1–4. https://doi.org/10.1109/AEEICB.2018.8480941

Tacuri López, I. L. (2021). *Acoso por medio de las tecnologías en las redes sociales durante tiempos de pandemia en Ecuador, una revisión sistemática*. http://dspace.ups.edu.ec/handle/123456789/20242

Terán Villafuerte, B. J. (2023). *Análisis de delitos informáticos relevantes en organizaciones gubernamentales de Latinoamérica*.

Thamer, N., & Alubady, R. (2021). A Survey of Ransomware Attacks for Healthcare Systems: Risks, Challenges, Solutions and Opportunity of Research. *1st Babylon International Conference on Information Technology and Science 2021, BICITS 2021, 2021*(Bicits), 210–216. https://doi.org/10.1109/BICITS51482.2021.9509877

Toala Indio, Y. I. (2021). *Delitos informáticos frecuentes en el Ecuador: casos de estudio*.

Villamar Arellano, D. A. (2023). *Estrategias de prevención frente a los ciberataques en la Unidad Educativa Luis Alfredo Noboa Icaza*.

Wade, M. (2021). Digital hostages: Leveraging ransomware attacks in cyberspace. *Business Horizons*, *64*(6), 787–797. https://doi.org/https://doi.org/10.1016/j.bushor.2021.07.014

Williams, C. M., Chaturvedi, R., & Chakravarthy, K. (2020). Cybersecurity risks in a pandemic. *Journal of Medical Internet Research*, *22*(9). https://doi.org/10.2196/23692

Wilner, A. S., Luce, H., Ouellet, E., Williams, O., & Costa, N. (2022). From public health to cyber hygiene: Cybersecurity and Canada's healthcare sector. *International Journal*. https://doi.org/10.1177/00207020211067946

Zerega-Prado, J., & Llerena-Izquierdo, J. (2022). Arquitectura de consolidación de la información para seguros de la salud mediante Big Data. *Memoria Investigaciones En Ingeniería*, *0*(23 SE-Artículos). https://doi.org/10.36561/ING.23.3