

---

Metodologías de la Investigación

## **Sistemas de seguridad empresarial**

# **Tema de Investigación: "Vulnerabilidades y Mitigación de Riesgos en los Sistemas de Seguridad Empresarial: Un Estudio de Caso del Ataque de Ransomware en PAMI"**



ÁREA DE INTERÉS: Tecnología y Ciberseguridad

**Motivaciones/Razones:**

Este tema de investigación me interesa debido a la creciente importancia de la ciberseguridad en el entorno empresarial actual. Los ataques de Ransomware, como el que afectó a PAMI, representan una amenaza seria para la seguridad de la información y la continuidad de las operaciones empresariales. A través de esta investigación, deseo comprender mejor las vulnerabilidades subyacentes en los sistemas de seguridad empresarial y explorar formas efectivas de mitigar los riesgos asociados con estos ataques.

**Factibilidad/Dudas:**

A FAVOR: Tengo acceso a una amplia gama de recursos en línea y literatura académica que abordan temas de ciberseguridad y ataques de Ransomware. Además, el estudio de caso de PAMI proporciona un ejemplo concreto para analizar las vulnerabilidades y las medidas de mitigación.

DUDAS/DIFICULTADES: Puede ser un desafío acceder a información específica sobre los detalles técnicos del ataque de Ransomware en PAMI debido a la naturaleza sensible del incidente. Además, podría ser difícil evaluar completamente las medidas de mitigación implementadas por PAMI sin acceso directo a su infraestructura de seguridad.

**Fuentes de interés:**

Mi interés en el tema de la ciberseguridad ha sido alimentado por diversas fuentes que han influido en mi ruta de aprendizaje. Algunas de estas influencias incluyen:

- **Experiencias personales:** Mi interés en el tema de la ciberseguridad se ha forjado a lo largo del tiempo, pero adquirió mayor relevancia cuando experimenté en carne propia la vulnerabilidad digital. El año pasado, mi cuenta de Twitter e Instagram fue hackeada, lo cual me llevó a tomar medidas más rigurosas para asegurar mi presencia en línea. Este evento personal subrayó la necesidad apremiante de comprender y abordar las amenazas cibernéticas, impulsándome a investigar y aprender en profundidad sobre la ciberseguridad.
- **Formación personal:** Mi formación se centra en los fundamentos de Linux y redes, y estoy en medio de un curso de preparación para la certificación en ciberseguridad (eJPT). Esta certificación abarcará conceptos profundos de redes, habilidades manuales de seguridad en aplicaciones web, el uso de Metasploit para ataques simples y análisis de protocolos en capturas de tráfico. Además, aprenderé técnicas de recopilación de información y entenderé el proceso de pruebas de penetración. Este proceso de formación está fortaleciendo mi comprensión de la ciberseguridad y me está preparando para enfrentar los desafíos del entorno digital actual. Estoy entusiasmado por aplicar estos conocimientos y contribuir al campo de la ciberseguridad en el futuro.

**Producir Conocimiento:**

Ítems de interés que me gustaría explorar para producir conocimientos:

1. ¿Cómo han evolucionado los grupos de Ransomware, como Rhysida, desde su aparición reciente y cómo se están adaptando para atacar a entidades públicas y organizaciones de diferentes países y sectores, como se evidencia en el ataque al PAMI?
2. En base a los métodos de propagación del Ransomware y el reciente ataque al PAMI, ¿cómo podrían las organizaciones mejorar sus estrategias de educación y capacitación para sus empleados, con el objetivo de prevenir y detectar con éxito intentos de phishing y otros vectores de ataque similares?
3. ¿Cuál es el impacto real y potencial de un ataque Ransomware en una organización, como se observa en el caso del PAMI, en términos de la pérdida de datos, la interrupción de servicios esenciales y la exposición de información confidencial? ¿Qué medidas concretas pueden implementarse para mitigar estos riesgos y responder de manera efectiva a tales incidentes de seguridad cibernética?

Estas preguntas exploran diferentes aspectos del ataque Ransomware al PAMI y brindan la oportunidad de profundizar en la comprensión de las amenazas cibernéticas y las estrategias de defensa.

**Enunciados que expresen algunos temas de investigación identificados en las fuentes abordadas:**

1. Vulnerabilidades y mitigación de riesgos en sistemas de seguridad empresarial.
2. Amenazas y ataques de Ransomware en instituciones de salud.
3. Ciberseguridad en el sector de la salud y sus desafíos.
4. Grupos cibercriminales y su impacto en la seguridad digital.
5. Riesgos y consecuencias de la filtración de datos sensibles en ataques de Ransomware.

**Situación problemática identificada a partir de uno de los temas de investigación**

Voy a describir la situación problemática relacionada con el tema de investigación número 2: "Amenazas y ataques de Ransomware en instituciones de salud."

- Situación Problemática:
  - En el contexto actual, las instituciones de salud se han convertido en un blanco cada vez más frecuente de ataques de Ransomware. Estos ataques, como se ha visto en el caso del PAMI en Argentina, involucran a grupos cibercriminales que comprometen la infraestructura de sistemas de salud y exigen rescates económicos a cambio de proporcionar las claves para desbloquear los datos. Esta situación problemática es altamente preocupante debido a las siguientes razones:
- Contexto Socio-Histórico:
  - Dependencia de la Tecnología: En los últimos años, las instituciones de salud han dependido cada vez más de la tecnología para gestionar registros médicos, información de pacientes y operaciones clínicas. Este aumento en la digitalización de datos ha creado una superficie de amenaza expandida.
  - Regulaciones de Privacidad de Datos: Con el aumento de la conciencia sobre la privacidad de los datos de salud, se han introducido regulaciones más estrictas, como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea. Los ataques de Ransomware que resultan en la filtración de datos de pacientes pueden llevar a sanciones legales significativas.
- Proceso Social/Económico/Político Amplio:
  - Impacto en la Atención al Paciente: Los ataques de Ransomware pueden interrumpir gravemente la atención médica, retrasando tratamientos, cirugías y la

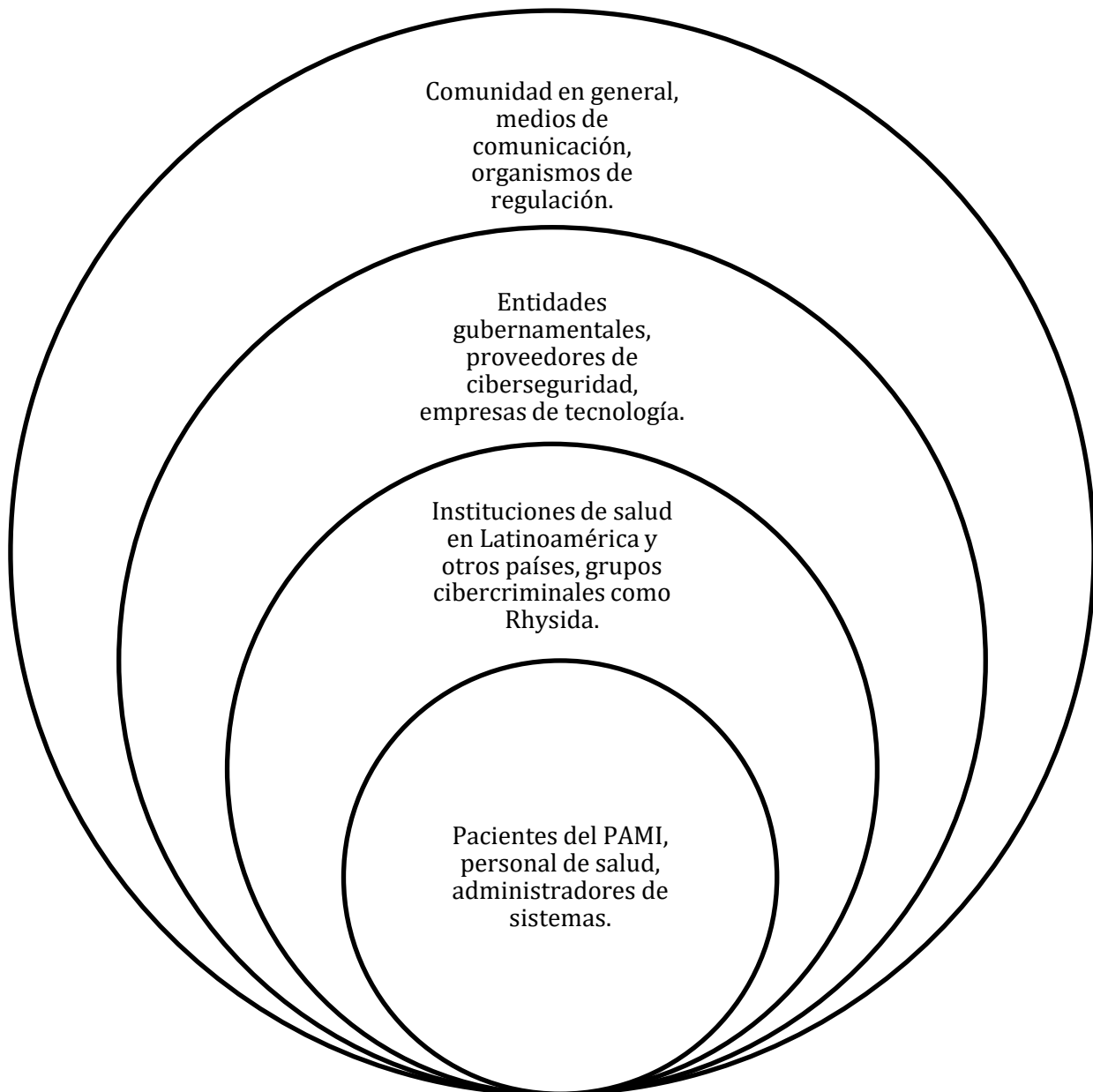
entrega de resultados de pruebas médicas. Esto puede poner en riesgo la salud y la vida de los pacientes.

- Costos Financieros: El pago de rescates y la recuperación de sistemas después de un ataque de Ransomware pueden generar costos financieros significativos para las instituciones de salud. Estos costos pueden desviar recursos que podrían haberse utilizado para la atención médica.
- Consecuencias Políticas: Los ataques exitosos de Ransomware en instituciones de salud pueden tener consecuencias políticas, ya que los gobiernos y las autoridades de salud pública pueden enfrentar críticas por no garantizar la seguridad de los datos de los ciudadanos y por no tomar medidas adecuadas para prevenir tales ataques.

En resumen, la situación problemática identificada es que las instituciones de salud se enfrentan a un creciente número de ataques de Ransomware que amenazan tanto la seguridad de los datos de los pacientes como la prestación de atención médica. Este problema se enmarca en un contexto socio-histórico de creciente dependencia tecnológica y regulaciones de privacidad más estrictas, y tiene impactos significativos en la atención al paciente, los costos financieros y las consideraciones políticas.

---

**Actores/sujetos que forman parte de esa situación problemática de acuerdo al grado de incidencia**



- Grado 1 (más afectados): Pacientes del PAMI, personal de salud, administradores de sistemas.
- Grado 2: Instituciones de salud en Latinoamérica y otros países, grupos cibercriminales como Rhysida.
- Grado 3: Entidades gubernamentales, proveedores de ciberseguridad, empresas de tecnología.
- Grado 4 (menos afectados): Comunidad en general, medios de comunicación, organismos de regulación.

En esta perspectiva, los sujetos más directamente afectados por el ataque de Ransomware estarían en el **Grado 1**. Esto incluiría a los pacientes del PAMI, ya que podrían enfrentar interrupciones en la atención médica y en el acceso a sus registros médicos. El personal de salud también sería gravemente afectado, ya que su capacidad para proporcionar atención adecuada se vería comprometida. Los administradores de sistemas estarían en el Grado 1 ya que serían responsables de la mitigación y recuperación del ataque.

Las instituciones de salud en el **Grado 2** también se verían afectadas, pero de manera menos inmediata y directa. Los grupos cibercriminales como Rhysida estarían en el Grado 2 ya que son responsables del ataque, pero su impacto sería principalmente a través de sus acciones maliciosas.

Entidades gubernamentales, proveedores de ciberseguridad y empresas de tecnología estarían en el **Grado 3**, ya que podrían estar involucrados en la respuesta al ataque y en la implementación de medidas de seguridad para prevenir futuros incidentes.

La comunidad en general, los medios de comunicación y los organismos de regulación estarían en el **Grado 4**, ya que su impacto directo sería menor y estarían más alejados de la situación problemática en términos de consecuencias inmediatas.

### Cuestiones que se desea saber sobre esta situación problemática que aún no sabe

1. ¿Cómo evolucionó Rhysida desde su aparición y qué estrategias utiliza para atacar a instituciones de salud?

Rhysida es un grupo de ciberdelincuencia que emergió a fines de mayo de un año determinado. Desde su aparición, el grupo ha ganado notoriedad por sus ataques a gran escala. Inicialmente dirigidos a objetivos en Latinoamérica, como el ejército chileno, su enfoque se expandió hacia Europa y los Estados Unidos, afectando a hospitales y clínicas. Utilizan tácticas modernas y están vinculados con Vice Society, otro grupo de Ransomware. Sus estrategias incluyen el movimiento lateral para control de red, acceso a credenciales, conexiones a comandos y control, evasión de defensa y el impacto que involucra el cambio de contraseñas y el cifrado de archivos.

2. ¿Cuáles son las medidas de seguridad más efectivas para prevenir y detectar ataques de Ransomware en instituciones de salud?

Algunas medidas efectivas incluyen mantener el software actualizado, utilizar soluciones de seguridad confiables, realizar copias de seguridad regulares, educar al personal sobre riesgos

de ciberataques, implementar políticas de seguridad sólidas y establecer un plan de respuesta a incidentes. Además, es vital capacitar a los empleados sobre el phishing y verificar la procedencia de archivos adjuntos y enlaces antes de abrirlos.

3. ¿Cuáles son las principales consecuencias económicas y sociales de un ataque de Ransomware en el sector de la salud?

Un ataque de Ransomware en el sector de la salud puede interrumpir servicios vitales, afectar la atención médica y la tramitación de medicamentos y tratamientos. La dependencia de sistemas electrónicos se ve comprometida, y en algunos casos, se pueden paralizar operaciones médicas. Esto puede resultar en costos económicos significativos para recuperar sistemas y datos, pérdida de confianza del público y daño a la reputación de la institución médica.

4. ¿Cómo pueden las organizaciones mejorar la educación y capacitación de su personal para evitar intentos de phishing y otros vectores de ataque?

Las organizaciones pueden implementar programas de capacitación en seguridad cibernética que incluyan formación en reconocimiento de intentos de phishing, métodos de prevención y buenas prácticas de seguridad. También pueden llevar a cabo simulacros de ataques de phishing y ofrecer material educativo regular para mantener al personal informado sobre las últimas tácticas utilizadas por los ciberdelincuentes.

5. ¿Qué enfoques teóricos y conceptos son esenciales para entender la complejidad de los ataques de Ransomware y su impacto en la seguridad digital?

Para entender los ataques de Ransomware, es importante comprender conceptos como Ransomware, ciberseguridad, criptografía, ingeniería social, malware y técnicas de mitigación. Los enfoques teóricos podrían incluir el análisis de amenazas, el estudio de los incentivos económicos detrás de los ciberataques y la relación entre las vulnerabilidades del sistema y la ejecución de ataques exitosos.

### **Conceptos teóricos necesarios para estudiar la problemática (palabras clave)**

**Ransomware:** El Ransomware es un tipo de programa malicioso utilizado por grupos ciberdelincuenciales como Rhysida. Este programa encripta los sistemas y archivos de una organización, haciendo que sean inaccesibles para sus usuarios. Los atacantes exigen un rescate económico en forma de criptomonedas a cambio de proporcionar la clave necesaria para desbloquear los sistemas afectados. En caso de que la víctima no pague, los ciberdelincuentes amenazan con publicar los datos robados, lo que puede resultar en daños a la reputación y en riesgos para la seguridad de la información.

- **Dark Web:** La dark web es una parte de Internet que no es indexada por los motores de búsqueda convencionales y que requiere software específico para acceder. Es utilizada por ciberdelincuentes para llevar a cabo actividades ilícitas, como la venta de



datos robados, herramientas de hacking y otros servicios relacionados con el cibercrimen. En los artículos se menciona que Rhysida listó a la entidad PAMI como víctima en su sitio en la dark web, donde amenazan con publicar los datos robados si no se paga el rescate.

- **Tácticas, Técnicas y Procedimientos (TTPs):** Las tácticas, técnicas y procedimientos son métodos específicos utilizados por grupos ciberdelinquentes para llevar a cabo sus ataques. En el caso de Rhysida, se menciona que sus TTPs están saliendo a la luz gradualmente a medida que se analizan sus operaciones y métodos. Estos métodos pueden incluir movimientos laterales en la red, acceso a credenciales, conexiones a command & control, evasión de la detección y el impacto, como el cifrado de archivos.
- **Superficie de Amenaza:** La superficie de amenaza se refiere a todas las posibles vulnerabilidades y puntos de entrada que podrían ser aprovechados por ciberdelinquentes para llevar a cabo ataques. En el contexto de la atención médica, como mencionado en el artículo, la superficie de amenaza es particularmente alta debido a la naturaleza esencial de los servicios de salud y a la gran cantidad de datos médicos confidenciales almacenados. La adopción de dispositivos IoT en entornos médicos también agrega complejidad y posibles vulnerabilidades.
- **Doble Extorsión:** La doble extorsión es una estrategia utilizada por ciberdelinquentes que involucra amenazar a las víctimas con publicar los datos robados además de encriptarlos. Incluso si las víctimas tienen copias de respaldo de sus datos, la amenaza de publicación puede ser suficiente para ejercer presión y obtener el pago del rescate. En el caso del PAMI, a pesar de que afirmaron haber mitigado el ataque, los atacantes podrían intentar utilizar la doble extorsión para forzar el pago del rescate y evitar la publicación de datos robados.

**Fuentes de información (Google Académico)****Artículo 1: "Ransomware y Seguridad Informática"**

Este artículo se enfoca en el Ransomware y su impacto en la seguridad informática. Los aspectos destacados y desarrollados por otros investigadores incluyen:

- Definición del Ransomware y sus modalidades de ataque.
- Implicaciones legales y técnicas de los ataques de Ransomware.
- Estrategias de prevención y respuesta a los ataques.

Aspectos adicionales que podrían ser abordados, como:

- Un enfoque más detallado en técnicas específicas utilizadas por los ciberdelincuentes.
- Estadísticas actualizadas sobre la prevalencia y la evolución del Ransomware.
- Desarrollo de soluciones técnicas avanzadas para la detección y prevención.

**Artículo 2: "Formación y Concienciación en Ciberseguridad"**

Este artículo resalta la importancia de capacitar al personal no técnico en ciberseguridad. Aspectos destacados y desarrollados por otros investigadores incluyen:

- La necesidad de concienciación en ciberseguridad en todos los niveles de la organización.
- La identificación de errores humanos como una amenaza importante.
- La propuesta de modelos de competencias como enfoque.

Sin embargo, aún hay oportunidades para innovar:

- Desarrollo de métodos de formación más efectivos y personalizados.
- Investigación sobre la eficacia a largo plazo de la concienciación en ciberseguridad.
- Evaluación de la adaptabilidad de los modelos de competencias en diferentes contextos organizativos.

**Artículo 3: "Modelo de Auditoría de Ciberseguridad (CSAM)"**

Este artículo propone un modelo de auditoría de ciberseguridad integral. Aspectos destacados y desarrollados por otros investigadores incluyen:

- La importancia de la gestión de riesgos en ciberseguridad.
- La aplicación del modelo en diferentes contextos organizativos.
- Resultados que respaldan la efectividad del CSAM.

Para avanzar en esta área, podría considerar:

- Desarrollar herramientas o software específicos para implementar y automatizar el CSAM.
- Investigar cómo el CSAM podría aplicarse a nivel nacional y en diferentes industrias.
- Explorar métricas de ciberseguridad más avanzadas para evaluar la madurez cibernética.

**Innovación Propia:**

Dado el panorama actual de amenazas cibernéticas en constante evolución, podría considerar enfocarme en el desarrollo de sistemas de detección y respuesta temprana de Ransomware que utilicen técnicas avanzadas de inteligencia artificial y aprendizaje automático. Esto podría incluir la detección de comportamientos anómalos en tiempo real y la identificación de patrones de Ransomware antes de que causen un daño significativo.

Además, podría investigar la creación de un marco de gestión de incidentes de Ransomware que permita una respuesta coordinada y eficiente ante un ataque, incluyendo la comunicación con las autoridades pertinentes y la preservación de evidencia digital para futuras investigaciones.

En resumen, esta innovación podría centrarse en el desarrollo de soluciones técnicas avanzadas y enfoques más efectivos para prevenir, detectar y responder a ataques de Ransomware, teniendo en cuenta la dinámica cambiante de las amenazas cibernéticas y la necesidad de una respuesta rápida y coordinada.

**Objetivos:****Objetivos Generales:**

"Analizar las vulnerabilidades y las estrategias de mitigación de riesgos en los sistemas de seguridad empresarial, centrándose en el estudio de caso del ataque de Ransomware que afectó a PAMI, con el propósito de mejorar la comprensión de las amenazas cibernéticas en el sector de la salud y proponer medidas efectivas para la prevención y respuesta a futuros ataques."

**Objetivos Específicos:**

- Investigar la evolución y las tácticas utilizadas por grupos de Ransomware, como Rhysida, desde su aparición hasta la fecha, con un enfoque en los ataques dirigidos a instituciones de salud.
- Evaluar las implicaciones legales y técnicas de los ataques de Ransomware en el contexto de las instituciones de salud, centrándose en el caso del ataque a PAMI en Argentina.
- Analizar estrategias efectivas de formación y concienciación en ciberseguridad para el personal de las instituciones de salud, con el objetivo de prevenir y detectar intentos de phishing y otros vectores de ataque similares.
- Cuantificar y comprender el impacto económico y social de un ataque de Ransomware en una institución de salud, incluyendo la pérdida de datos, la interrupción de servicios y la exposición de información confidencial.
- Proponer un marco de gestión de incidentes de Ransomware que permita una respuesta coordinada y eficiente en caso de un ataque, considerando la dinámica cambiante de las amenazas cibernéticas y la necesidad de una respuesta rápida.

**Hipótesis:**

Dado el crecimiento continuo de ataques de Ransomware, como el que afectó al PAMI, y la creciente dependencia tecnológica en el sector de la salud, existe la hipótesis de que mejorar la comprensión de las vulnerabilidades y las estrategias de mitigación de riesgos en los sistemas de seguridad empresarial, así como la implementación efectiva de medidas de formación y concienciación en ciberseguridad, puede reducir significativamente el impacto y la frecuencia de ataques de Ransomware en instituciones de salud. Además, la implementación de un marco de gestión de incidentes de Ransomware permitiría una respuesta más eficiente y coordinada en casos de ataques, disminuyendo las consecuencias negativas en la atención médica y la seguridad de la información.

### **Sección de Metodología:**

#### **1. Diseño de la Investigación**

Mi investigación se basa en un enfoque cualitativo. El alcance de esta investigación se limita al sector de la salud en instituciones de atención médica, centrándose en el estudio de caso del ataque de Ransomware que afectó a PAMI en Argentina. Se trata de un estudio no experimental, ya que los datos se obtienen en su contexto natural. Además, es de tipo exploratorio, ya que tiene como objetivo comprender las vulnerabilidades y estrategias de mitigación de riesgos en los sistemas de seguridad empresarial relacionados con amenazas cibernéticas, específicamente ataques de Ransomware, con el propósito de mejorar la comprensión de las amenazas cibernéticas en el sector de la salud y proponer medidas efectivas para la prevención y respuesta a futuros ataques.

#### **2. Muestra y Recolección de Datos**

La población objetivo de esta investigación consiste en instituciones de salud en Latinoamérica, con un enfoque especial en casos de ataques de Ransomware. Para seleccionar la muestra, se utilizará un muestreo por conveniencia, ya que se trabajará con casos de estudio específicos disponibles en la literatura y en fuentes de información en línea. El tamaño de la muestra se determinará mediante la revisión de casos relevantes y la disponibilidad de datos.

La recolección de datos se llevará a cabo utilizando métodos de revisión documental en línea. Se recopilarán datos y estudios de casos previamente publicados que se relacionen con ataques de Ransomware en instituciones de salud.

#### **3. Instrumentos y Herramientas**

Se utilizarán los siguientes instrumentos para recopilar datos:

- Revisión de informes y estudios de casos relacionados con ataques de Ransomware en instituciones de salud.
- Recopilación de datos de fuentes de noticias y publicaciones especializadas en ciberseguridad.

#### **4. Procedimientos**

El proceso de investigación se llevará a cabo en las siguientes etapas:

- Selección de casos de estudio relacionados con ataques de Ransomware en instituciones de salud, a partir de fuentes disponibles en línea como noticias, informes y artículos académicos.
- Recopilación de datos mediante la revisión y extracción de información relevante de las fuentes mencionadas.
- Análisis de los datos recopilados para identificar vulnerabilidades, estrategias de mitigación de riesgos y las implicaciones legales y técnicas de los ataques de Ransomware en el contexto de las instituciones de salud.
- Síntesis de los hallazgos y resultados en relación con los objetivos específicos de la investigación.

#### **5. Análisis de Datos**

Los datos recopilados se analizarán mediante la revisión y síntesis de información relevante de las fuentes disponibles en línea, que incluyen noticias, estudios de casos y artículos académicos. El análisis se centrará en identificar las vulnerabilidades, estrategias de mitigación de riesgos y las implicaciones legales y técnicas de los ataques de Ransomware en el contexto de las instituciones de salud. Se utilizará un enfoque de análisis cualitativo para examinar las tendencias y patrones emergentes en los datos.

## 6. Aspectos Éticos

Dado que la investigación se basa en la revisión de datos disponibles públicamente en línea y no involucra la participación directa de sujetos humanos, no se requerirá consentimiento informado. Se garantizará la confidencialidad de la información recopilada de acuerdo con las prácticas estándar de investigación.

## 7. Consideraciones Temporales

Se espera que esta investigación se lleve a cabo en un período estimado de 1 semana. Dado el enfoque en la revisión de datos en línea y la naturaleza limitada de la recopilación de información, la temporalidad se simplificará de la siguiente manera:

Selección de casos de estudio y recopilación de datos: 1 semana.

Análisis de datos y síntesis de resultados: 1 semana.

**Bibliografía:**

[Ransomware: seguridad, investigación y tareas forenses](#)

[Auditorías en ciberseguridad: un modelo de aplicación general para empresas y naciones](#)

[Formación y concienciación en ciberseguridad basada en competencias: una revisión sistemática de literatura](#)

[Glosario de términos de ciberseguridad: una guía de aproximación para el empresario](#)