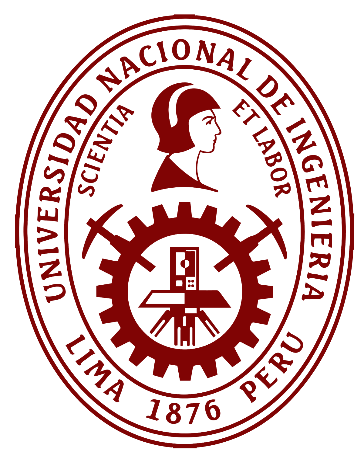
**UNIVERSIDAD NACIONAL DE INGENIERÍA**

**FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS**



**TESIS**

**DISEÑO DE UN SISTEMA DE CIBERSEGURIDAD PARA LA PROTECCIÓN DE ACTIVOS CON INFORMACIÓN SENSIBLE DE PACIENTES EN EMPRESAS DEL SECTOR SALUD**

**PARA OBTENER EL TÍTULO PROFESIONAL DE**

**INGENIERO DE SISTEMAS**

**ELABORADO POR**

**JOHAN HENRY ROBLES BENITES**

**ASESOR**

**DR. EMILIO ALBERTO UN JAN LIAU HING**

**LIMA - PERÚ**

**2024**

**Tabla de Contenido**

Pág.

[Introducción 1](#_Toc169571866)

[Capítulo I. Parte introductoria 2](#_Toc169571867)

[1.1. Generalidades 2](#_Toc169571868)

[1.2. Descripción del problema de investigación 3](#_Toc169571869)

[1.2.1. Problema General 8](#_Toc169571870)

[1.2.2. Problemas específicos 8](#_Toc169571871)

[1.3. Objetivos del estudio 10](#_Toc169571872)

[1.3.1. Objetivo General 10](#_Toc169571873)

[1.3.2. Objetivos Específicos 11](#_Toc169571874)

[1.4. Hipótesis 11](#_Toc169571875)

[1.4.1. Hipótesis General 12](#_Toc169571876)

[1.4.2. Hipótesis especificas 12](#_Toc169571877)

[1.5. Antecedentes investigativos 15](#_Toc169571878)

[Capítulo II. Marcos Teóricos y conceptuales 17](#_Toc169571879)

[2.1. Marco teórico 17](#_Toc169571880)

[2.1.2. Defensa en profundidad 17](#_Toc169571881)

[2.1.3. Confianza cero 18](#_Toc169571882)

[2.1.4. Gestión de identidades y roles 18](#_Toc169571883)

[2.1.5. Sistema de gestión de eventos de seguridad 18](#_Toc169571884)

[2.2. Marco conceptual 18](#_Toc169571885)

[2.2.1. Activo de Información 19](#_Toc169571886)

[2.2.2. Sistema de información de salud 19](#_Toc169571887)

[2.2.3. Ataques informáticos 19](#_Toc169571888)

[2.2.4. Gestión de vulnerabilidades de ciberseguridad 19](#_Toc169571889)

[2.3. Marco sistémico 20](#_Toc169571890)

[2.4. Marco ético 20](#_Toc169571891)

[Referencias bibliográficas 21](#_Toc169571892)

Lista de Tablas

Pág.

[**Tabla 1** Preguntas de investigación en artículos relacionados protección de datos de los pacientes 2](#_Toc166577598)

[**Tabla 2** Matriz de consistencia 11](#_Toc166577599)

Lista de Figuras

Pág.

[**Figura 1** Cantidad de ciberataques semanales a nivel global por sector en el tercer trimestre del 2022 5](#_Toc169491541)

[**Figura 2** Cantidad de notificaciones de robos y secuestro de información en el mes de abril y mayo del 2024 6](#_Toc169491542)

[**Figura 3** Número de hospitales peruanos que no presentan equipo de respuesta ante incidentes de ciberseguridad 7](#_Toc169491543)

[**Figura 4** Porcentaje de clínicas en Lima que tiene prácticas de ciberseguridad para proteger la información de sus pacientes 7](#_Toc169491544)

[**Figura 5** Árbol de problemas 9](#_Toc169491545)

[**Figura 6** Modelo de registros médicos electrónicos de autoprotección 15](#_Toc169491546)

[**Figura 7** Caso de ataque al sistema de información medica 16](#_Toc169491547)

# Introducción

# Capítulo I. Parte introductoria

## Generalidades

La necesidad de la ciberseguridad en el sector salud se ha vuelto una prioridad, ya que actualmente gracias a las innovaciones tecnológicas existen equipos y aplicaciones que son vitales para la atención de los pacientes (Javaid et al., 2023), pero estos dispositivos tecnológicos a menudo son el objetivo de muchos piratas informáticos, ya que estos contienen datos muy sensibles y privados de la salud de los pacientes (Kim, 2018). Existen diversos vectores por los que podrían obtener esta información de los pacientes, los más comunes son fuga de información por personal de salud y el infectar algún dispositivo para extraer la información de los pacientes (Brantly y Brantly, 2020). Por ello es importante analizar los factores involucrados en los sistemas de información médico y las tecnologías asociadas ya que esto permite desarrollar un modelo de seguridad de información de calidad (Handayani et al., 2018), basado en esos factores relacionados a los sistemas de información se plantea el diseño de un sistema para la protección de la información sensible de los pacientes.

Actualmente el compartir datos entre los diversos sistemas de información en el sector salud son cada vez más comunes e incluso con tecnologías emergentes, por ejemplo, con el internet de las cosas se produce una gran interoperabilidad ya que este permite una conexión a tiempo real de los datos de cada sistema con interfaces y aplicaciones web (Balasamy et al., 2022; Salahuddin et al., 2020), de esta manera se tienen los datos de los pacientes a tiempo real. El hecho de que los datos se envíen por internet y muchas veces por medios que no están controlados por una red empresarial provocan filtración de estos datos (Bones et al., 2007; Yeole y Kalbande, 2021).

El aumento en el uso de los sistemas de información en las empresas del sector salud plantea un riesgo latente para la seguridad de los pacientes si no se realiza un correcto diseño e implementación de los softwares que se utilizan (Salahuddin et al., 2020), por lo que es necesario tener un marco de referencial el cual seguir para la implementación de estos sistemas. Existen marcos de referencia que permiten la seguridad de los datos, uno de esos marcos de referencia es el de una arquitectura informática basada en la gestión de claves el cual permite tener seguro los datos que se comparte entre sistemas de información (Perumal y Nadar, 2020), este marco de trabajo se puede adoptar en las instituciones de salud para tener una mejor protección de los datos de los pacientes.

## Descripción del problema de investigación

Para poder describir el problema de investigación, debemos tener en cuenta que plantear el problema es definir la idea de investigación esto mediante la precisión y estructuración del caso que vamos a investigar (Hernández y Mendoza, 2018) para realizar esta precisión es necesario revisar fuentes especializadas. Por eso en la tabla 1 se especifican cuáles son las principales fuentes que se revisaron para poder plantear el problema de investigación.

**Tabla 1**Preguntas de investigación en artículos relacionados protección de datos de los pacientes

|  |  |
| --- | --- |
| **Cita** | **Preguntas de investigación** |
| Javaid et al. (2023) | ¿Cuáles son las prácticas de ciberseguridad que se están implementando en los hospitales para la protección ante posibles ciberataques? |
| Ahmed et al. (2024) | 1) ¿Cuáles son los retos de ciberseguridad a los que se enfrentan las organizaciones? 2) ¿Qué medidas se pueden adoptar para reducir la pérdida de datos y ciberataques en las organizaciones? |
| Čaušević et al. (2017) | 1) ¿Qué nuevas amenazas se presentan los sistemas médicos autocontrolados en la atención sanitaria? 2) ¿Cómo se puede hacer más seguro la comunicación de los datos por medios inalámbricos entre estos sistemas médicos? |
| Angafor et al. (2020) | ¿Cómo realizar una correcta capacitación en respuesta a incidentes a los trabajadores de las organizaciones? |
| Cervera y Goussens (2024) | ¿Cuáles son los peligros y amenazas que enfrentan las tecnologías de la información y la comunicación (TIC)? |

*Nota:* Elaboración propia de los principales artículos que se utilizaron para poder plantear el problema de investigación.

Con el incremento de las nuevas tecnologías a nivel mundial de los últimos años se ha hecho cada vez más grande la cantidad de procesos que se soportan en sistemas de información esto generando un incremento en casos de ciberataques (Madnick et al., 2023) estos procesos al estar relacionados de forma holística y formar una cadena de suministro generan la necesidad de que se proteja la cadena de suministro ya que si alguna parte se ve vulnerada puede tener acceso a la información del resto de procesos (Ahmed et al., 2024). En el sector salud al tener cadenas de suministro con entidades externas y compartir información con estas entidades genera brechas de seguridad externas (Kim et al., 2022) lo cual lleva a la pérdida de los datos de los pacientes y una mala reputación de la empresa.

Tener en cuenta que no siempre los ataques deben estar dirigidos de forma directa para el sector salud para que este sector se vea afectado, un claro ejemplo es el de WannaCry un ataque de secuestro de datos el cual llegó a encriptar un total de 230000 computadoras con información sensible en 150 países y que, a pesar de no ser dirigido al Servicio Nacional de Salud de Inglaterra, este ataque perjudicó su funcionamiento (Ghafur et al., 2019) lo sistemas que se vieron comprometidos y que tenían datos sensibles del historial médico de los pacientes tuvieron un precio de recuperación de entre $300 y $600 dólares (Zhao et al., 2019) demostrando de esta manera que los ciberataques muchas veces tienen un alcance global y que afecta a las industrias de forma conjunta.

Ahora viendo datos más recientes podemos ver que cada organización recibe en promedio un total de 1130 ataques semanales lo cual representaría un incremento interanual de un 28% del número de casos de ciberataque (Mariano y Núñez, 2023) por lo que es necesario hacerles frente a estos ataques y lograr una mayor protección de los datos. Los principales vectores de ataque son el de suplantación de identidad y robo de información (Zhan et al., 2024) los cuales se presentan en diversos sectores, pero en el Figura 1 se muestra que el principal sector es el de educación seguido de gobiernos y las empresas proveedoras de internet; no obstante, en cuarto lugar, están las empresas del sector salud con uno de los incrementos más grandes con respecto al trimestre anterior (Mariano y Núñez, 2023).

**Figura 1**Cantidad de ciberataques semanales a nivel global por sector en el tercer trimestre del 2022

Imagen que contiene Interfaz de usuario gráfica

Descripción generada automáticamente

*Nota:* Se muestra el aumento de cantidad de ciberataques por sector a nivel mundial por Mariano y Núñez, 2023 (<https://repositorio.cepal.org/server/api/core/bitstreams/2db8feef-29d6-4981-9741-9ad3154d3789/content>)

Centrándonos en Perú, se aprecia que la situación de seguridad informática tiene la misma problemática que las empresas de forma global. Aproximadamente el 51% de las empresas en el Perú no tiene una correcta seguridad informática en sus líneas de negocio (Cama, 2020) esto sucede principalmente a que no hay una política que estandarice los controles de seguridad que deberían tener los procesos y que tampoco existen indicadores que sirvan para poder hacer frente a estos ataques (Leszczyna, 2019). Además, podemos ver que actualmente uno de los ataques más críticos es el de secuestro de información el cual se aprecia en la Figura 2, en el mes de abril y mayo del 2024 el número de ataques de secuestro de información que recibieron las empresas peruanas en ese mes fue de 3000 aproximadamente (Kaspersky Lab, 2024) basados en esta cantidad de incidentes se observa la necesidad de tener un sistema que evite esta gran cantidad de casos.

**Figura 2**Cantidad de notificaciones de robos y secuestro de información en el mes de abril y mayo del 2024

Interfaz de usuario gráfica, Gráfico, Gráfico de líneas

Descripción generada automáticamente

*Nota:* La imagen muestra la cantidad de ataques de secuestro de información registradas en el mes de abril y mayo fue elaborada a partir del reporte mensual de por Kaspersky Labs, (2024).

Mientras que en empresas peruanas del sector salud, se puede observar que sigue la tendencia de las empresas peruanas en general, ya que se observó que tan solo 2 de los 83 centros de salud revisados tienen un equipo y procesos para la respuesta de incidentes de ciberseguridad (Presidencia de Consejo de ministros, 2024), esto se aprecia en la Figura 3. Además, si vamos por el lado privado en clínicas de apoyo se observa que el porcentaje de empresas con actividades de ciberseguridad es mayor, en la Figura 4, solo el 39.3% aproximadamente no implementa actividades de ciberseguridad (Gomero y Sánchez, 2024), pero aun así el dejar estos puntos de lado deja expuesto a que estas empresas de salud puedan ser víctimas de ciberataques.

**Figura 3**Número de hospitales peruanos que no presentan equipo de respuesta ante incidentes de ciberseguridad

Diagrama

Descripción generada automáticamente

*Nota:* La figura fue elaborada a partir de la información registrada por la secretaría de gobierno y transformación digital de la presidencia del consejo de ministros PCM (2024).

**Figura 4**Porcentaje de clínicas en Lima que tiene prácticas de ciberseguridad para proteger la información de sus pacientes

Gráfico, Gráfico de barras

Descripción generada automáticamente

*Nota:* La imagen fue elaborada en base a la información de las 11 encuestas a las clínicas de Gomero y Sánchez (2024).

En base a estos datos podemos ver que, si hay una tendencia creciente al aumento de ciberataques en el sector salud, además el hecho de que no posean sistemas, procesos y actividades para hacer frente a estos posibles ataques incrementa más esta problemática (Čaušević et al., 2017).

### Problema General

Actualmente la falta de una protección de ciberseguridad en los sistemas de información del sector salud es el principal motivo de la gran cantidad de casos de ciberseguridad que actualmente existen, ya que la mayoría de las empresas consideran que para realizar una protección frente a los ataques de ciberseguridad es solo necesario dispositivos de protección usando antivirus o algún cortafuegos (Ahmed et al., 2024) pero es necesario más que solo implementar un dispositivo de protección es necesario realizar una revisión holística e implementar una protección de ciberseguridad centrado en la protección de datos de los pacientes (Brantly y Brantly, 2020) que busque que los involucrados en el manejo de información sensible conozcan los procesos de ciberseguridad de la empresa.

La información del sector salud es muy sensible ya que los datos de los pacientes que estas empresas manejan van desde diagnósticos médicos hasta algunos datos más comprometedores cómo información financiera de los pacientes (Cervera y Goussens, 2024) es por ello que el problema general que se abordará en la investigación es que las empresas del sector salud no conocen cómo proteger la información sensible de los pacientes ante posibles ciberataques en empresas del sector salud de Lima

### Problemas específicos

El problema general de que no se conoce cómo proteger la información sensible de los pacientes ante posibles ciberataques, uno de los factores es que actualmente los sistemas de información son cada vez más complejos y con el uso de nuevas tecnologías son cada vez más autocontrolados lo cual presenta un nuevo problema para la ciberseguridad de la empresa (Čaušević et al., 2017) de esto podemos deducir que un problema específico a analizar es el de no se conoce cómo asegurar los equipos informáticos del sector salud y el problema que se busca resolver en la investigación es el de ¿Cómo asegurar los equipos informáticos en empresas del sector salud de Lima?

Otro punto para tener en cuenta es la respuesta en caso de que suceda un ataque de ciberseguridad es necesario que sea inmediata y que el personal conozca los procedimientos que se deben de seguir, así cómo de tener un sistema que maneje indicadores que permitan una respuesta inmediata (Angafor et al., 2020) por tanto otro problema específico a revisar en la investigación es el de ¿Cómo realiza una adecuada procedimiento de respuesta ante incidentes de ciberseguridad en empresas del sector salud de Lima?

De esta manera siguiendo la teoría general de sistemas podemos de un problema complejo que teníamos en el problema general reducir esta complejidad dividiéndolo en subproblemas más específicos (Ossa, 2017) por lo que en la Figura 5 podemos ver el árbol de problemas que además de los problemas específicos podemos ver las causas de este problema.

**Figura 5**Árbol de problemas

Diagrama

Descripción generada automáticamente

*Nota*: Elaboración propia de los problemas y causas para la investigación en base a los problemas identificados en los artículos leídos durante la investigación

## Objetivos del estudio

Una vez que ya tenemos definido el problema de investigación debemos de establecer el propósito o finalidad de la investigación el cual es el objetivo del estudio (Bernal, 2010). En el caso de esta tesis el objetivo que se busca es el de proteger la información sensible de los pacientes de tal manera que este sistema de ciberseguridad que se propone permita gestionar las vulnerabilidades de forma holística y de esta manera corregir la actual incapacidad que tienen los centros de salud para gestionar sus problemas de ciberseguridad (Brantly y Brantly, 2020) para poder tener una mejor protección de los datos sensibles.

### 1.3.1. Objetivo General

La mayoría de los procesos de los hospitales al estar sustentados en sistemas de información hacen que la cadena de suministro sea compleja pero que al mismo tiempo tenga que atender a múltiples pacientes y actores (Hossain et al., 2023) esto hace que para lograr el objetivo de proteger la información sensible de los pacientes sea necesario proteger el componente de sistemas de la información y humano. Teniendo en cuenta la creciente demanda de los servicios y el deterioro de la calidad de los servicios de los sistemas de salud (Jiang et al., 2023) es necesario hacerle frente a este problema para evitar un desafío mayor a futuro.

La fuga de información es un problema que tiene un impacto económico muy grande en las empresas el costo de compromiso de datos en 2023 fue de 4.45 millones de dólares, pero en el sector salud este coste se incrementa a casi el doble llegando a una media de 10.93 millones de dólares (Cervera y Goussens, 2024) además de que en muchas ocasiones las empresas del sector salud no invierten lo necesario para poder cerrar la brecha de ciberseguridad (Dugar, 2021) es por ello que al ser un problema que engloba muchas activos de información tanto tecnológicos cómo humanos y tener un gran impacto económico planteamos cómo objetivo de la investigación el proteger la información sensible de los pacientes ante posibles ciberataques en las empresas del sector salud de Lima.

### 1.3.2. Objetivos Específicos

Para lograr el objetivo general de proteger la información sensible de los pacientes ante posibles ciberataques es necesario dividirlo en otros objetivos específicos que permitan de esta manera poder reducir la complejidad (Ossa, 2017) uno de estos es el de la protección de los sistemas de información ya que estos sistemas de información sanitarios permiten que la atención a los usuarios sea mejor ya que permite que los datos sean de conocimiento del usuario a tiempo real y que los doctores tomen decisiones en base a esta información (Handayani et al., 2018) es por este motivo que uno de los objetivos específicos que se plantea en el trabajo de investigación es el de asegurar los equipos de seguridad informáticos de las empresas del sector salud de Lima.

Adicionalmente no solo basta con una seguridad preventiva en los sistemas de información, también es necesario tener un buen equipo de respuesta ante incidentes, la ciberseguridad es una de las principales áreas en las que hay una brecha muy grande entre demanda y la cantidad de personal calificado para cubrir estos puestos (Angafor et al., 2020) esto sumado al hecho de que las empresas de salud buscan perfiles con mucha experiencia para cubrir su brecha de seguridad que tienen (Dugar, 2021) dan de resultado una mala respuesta ante incidentes, es por este motivo que otro de nuestros objetivos específicos es el de realizar una adecuada procedimiento de respuesta ante incidentes de ciberseguridad en empresas del sector salud de Lima.

## Hipótesis

Una vez teniendo en claro el objetivo el problema y el objetivo de la investigación, se puede realizar la hipótesis la cual indica lo que tratamos de probar, se les puede considerar respuestas provisionales a las preguntas de investigación (Hernández y Mendoza, 2018). Esta tesis lo que busca probar es que con un sistema de ciberseguridad se puede proteger los activos con información sensible del sector salud, ya que el sector salud actualmente no tiene una seguridad de que sus datos de los activos de información sean íntegros debido a que hay brechas de seguridad frecuentemente que tienen por objetivos estos datos (Mohammed et al., 2024) por lo que es necesario hacer frente a este problema y se plante que una manera de hacerlo es con un sistema de ciberseguridad.

### Hipótesis General

Actualmente no existe un estándar especifico de ciberseguridad que se adapte a las empresas esto incluye a empresas del sector salud (Kim et al., 2022), ya que siempre existirá controles que no se relacionen con la necesidad de seguridad de las empresas (Leszczyna, 2019) por lo que es necesario poder seleccionar solo los controles que necesite la empresa y aplicarlos. Adicional a una seguridad preventiva es necesario tener un correcto procedimiento de respuesta ante incidentes ya que en caso de que ya se dio un ataque en algún sistema es necesario la resiliencia y buscar frenar al atacante lo más pronto posible (Hossain et al., 2023) ambas necesidades de protección se pueden cubrir si se implementará un sistema de ciberseguridad que en base a controles y registro de eventos pueda seleccionar los controles adecuados y responder ante cualquier sospecha de ciberataque.

Adicionalmente los sistemas de información en el sector salud son indispensables puesto que cumplen funciones vitales por ejemplo mostrar estadísticas vitales de los pacientes y guardar información de padecimientos los cuales son vitales para la atención adecuada (Zarour et al., 2021) por lo que es necesario asegurarlos, por lo que la tesis plantea la hipótesis nula de que con un sistema de ciberseguridad no se protegerá los activos con información sensible de los pacientes protegidos ante posibles ciberataques, en consecuencia la hipótesis que tratamos de probar es la hipótesis alterna la cual es que con un sistema de ciberseguridad si se protegerá los activos con información sensible de los pacientes protegidos ante posibles ciberataques.

### Hipótesis especificas

Los equipos que actualmente se están usando en las empresas del sector salud son cada vez más complejos y muchos de estos ya son autocontrolados, por lo que al tener menor intervención humana y estar en uso solo supervisándose por ellos mismos esto aumenta el riesgo de ciberseguridad (Čaušević et al., 2017) por lo que es necesario aumentar la protección de los datos que estos sistemas maneja, adicionalmente hay que tener en consideración que estos sistemas en un inicio fueron diseñados para que exista una rapidez en los procesos sin preocuparse por temas de seguridad (González et al., 2019) por lo que la tesis plantea la hipótesis especifica nula alterna de que con un sistema de ciberseguridad si se asegurará los equipos informáticos del sector salud ante posibles ciberataques.

La seguridad proactiva también es un punto importante ya que en los incidentes de ciberseguridad que ocurren en el sector salud no se toman cómo lecciones aprendidas para algún futuro caso de otro ciberataque (Ebert et al., 2023) por el contrario se debería de tomar estos datos y tenerlos en consideración para nuevos casos y tener mejores procedimientos de respuesta ante incidentes, ya que en la actualidad es necesario que los proceso de respuesta ante incidentes sean flexibles, veloces y de aprendizaje (Naseer et al., 2023) es por ello que la tesis plantea otra hipótesis especifica alterna que con un sistema de ciberseguridad si se realizará un adecuado procedimiento de respuesta ante incidentes de ciberseguridad en empresas del sector salud de Lima.

Teniendo esto en consideración y que lo que se trata de hacer frente es al incremento en los últimos años de ataques de ciberseguridad y el costo que esto conlleva (Gomero y Sanchez, 2024) es que nuestra variable independiente definida es la de un sistema de ciberseguridad, esta variable independiente lo que busca es ver cómo se relaciona con nuestras variables dependientes (Hernández y Mendoza, 2018) por lo que nuestra variable dependiente general es la de Activos con información sensible de los pacientes ante posibles ciberataques en empresas del sector salud de Lima, para poder entender mejor esta relación la podemos ver en la matriz de consistencia el cual se muestra en la tabla 2 donde se ve la relación entre problema, objetivo, hipótesis y las variables.

**Tabla 2** Matriz de consistencia

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Matriz de Consistencia** | | | | |
| **PROBLEMA** | **OBJETIVO** | **HIPÓTESIS** | **VARIABLES** | |
| **DEPENDIENTE** | **INDEPENDIENTE** |
| **Problema General**  No se conoce cómo proteger los activos con información sensible de los pacientes ante posibles ciberataques en empresas del sector salud de Lima. | **Objetivo General**  Proteger los activos con información sensible de los pacientes ante posibles ciberataques en empresas del sector salud de Lima | **Hipótesis General**  Con un sistema de ciberseguridad se protegerá los activos con información sensible de los pacientes ante posibles ciberataques en empresas del sector salud de Lima | Activos con información sensible de los pacientes ante posibles ciberataques en empresas del sector salud de Lima | Sistema de ciberseguridad |
| **Problemas Específicos**  No se conoce cómo asegurar los equipos informáticos del sector salud de Lima. | **Objetivos Específicos**  Asegurar los equipos informáticos del sector salud de Lima. | **Hipótesis Específicas**  Con un sistema de ciberseguridad se asegurará los equipos informáticos del sector salud de Lima ante posibles ciberataques | Equipos informáticos del sector salud de Lima | Sistema de ciberseguridad |
| No se conoce cómo realiza un adecuado procedimiento de respuesta ante incidentes de ciberseguridad en empresas del sector salud de Lima. | Realiza un adecuado procedimiento de respuesta ante incidentes de ciberseguridad en empresas del sector salud de Lima. | Con un sistema de ciberseguridad se realizará un adecuado procedimiento de respuesta ante incidentes de ciberseguridad en empresas del sector salud de Lima | Procedimientos de respuesta ante incidentes de ciberseguridad en empresas del sector salud de Lima | Sistema de ciberseguridad |

*Nota:* Elaboración propia de la relación entre problema, objetivo e hipótesis y sus variables dependientes e independientes

## Antecedentes investigativos

El incremento de los casos de ciberseguridad en los últimos años sumado a la poca relevancia del sector salud en invertir para hacer frente a estos ataques (Dugar, 2021) ha hecho que se generen múltiples artículos de cómo hacer frente a este problema, buscando siempre por objetivo una solución centrada en la privacidad de los pacientes (Javaid et al., 2023).

Uno de estos artículos se plantea un modelo en el cual la información electrónica de los pacientes tenga diversas capas de seguridad de manera que si algún atacante logre interceptar esta información no pueda obtenerla ya que no tiene permisos Zhao et al. (2019), este modelo fue el de registros médicos electrónicos de autoprotección, el cual se muestra en la Figura 6. Este modelo no es tan efectivo teniendo en cuenta que actualmente los datos son compartidos en múltiples dispositivos en tiempo real (Selvaraj y Doraikannan, 2019), por lo que la necesidad de autenticarse en cada equipo que use esta información si bien es efectiva para la seguridad no es muy practica por temas de agilidad.

**Figura 6**Modelo de registros médicos electrónicos de autoprotección

Diagrama

Descripción generada automáticamente

*Nota*: En la figura se muestra cómo es uno de los nodos y cómo es que en base a eventos básicos y conjunciones se logra una decisión para el evento superior. Traducido de Zhao et al. (2019)

Otro artículo que plantea una idea de cómo proteger la información que esta almacenada en los equipos de los pacientes es un artículo de Karuppiah et al, (2019) en este nos menciona que el modelo que la mayoría de los centros médicos utilizan para la transferencia y almacenamiento de datos se le denomina sistema de información médica el cual se muestra en la Figura 7. Además, nos muestra que este es susceptible a que un atacante pueda interceptar los registros médicos que están en tránsito o almacenados en este sistema, esto ya que la mayoría de los sistemas implementados en el sector salud están mal implementados permitiendo una brecha de seguridad aprovechada por el atacante (Salahuddin et al., 2020).

Es por ello que se plantea que en ese sistema de información médica debe haber una capa más de seguridad cómo encriptado de los datos, otro factor de autenticación y un sistema de monitoreo de actividades (Karuppiah et al, 2019). Esta capa de protección permitirá que el sistema tenga mayor integridad de los datos y evitar que el atacante obtenga la información de forma sencilla.

**Figura 7**Caso de ataque al sistema de información medica

Diagrama

Descripción generada automáticamente

*Nota*: En la figura se muestra cómo un atacante obtendría la información de los registros médicos en un sistema convencional de información médica. Traducido de Karuppiah et al, (2019)

# Capítulo II. Marcos Teóricos y conceptuales

## 2.1. Marco teórico

En la última década el aumento de dispositivos que están conectados ha internet y comparten información a crecido de forma astronómica llegando a aproximado de 20 billones en el 2020 y con una proyección de 30 a 50 billones al finales de esta década (Brantly y Brantly, 2020), es por ello que es necesario ser conscientes que a pesar de que estas maquinas han sido mejoradas tecnológicamente y son más poderosas, también son más vulnerables (Roa, 2013) esto debido a que desde un inicio su objetivo era el en hacer más fácil y rápida las operaciones, y no le dieron importancia a la seguridad (Tarikere et al., 2021), es por esto que la seguridad en estos sistemas es más que necesario en la actualidad.

Entre las principales formas de seguridad para los activos dentro de una infraestructura de red esta la segmentación de redes y el control de acceso en las redes (Diogenes et al., 2016) para este control de accesos el dispositivo más común que se usa es el de un corta fuegos el cual se encarga en la capa de red donde se envían los paquetes de según un conjunto de reglas especificar si ingresa la solicitud o descartarlo (Baca, 2016), pero actualmente esta protección no es suficiente y se crearon nuevas maneras de agregar mayor protección a los activos los cuales se detalla en el estado del arte.

**Estado del arte**

### 2.1.2. Defensa en profundidad

Defensa en profundidad es una estrategia de seguridad que no solo se basa en la protección de la red por medio de cortafuegos o segmentación, sino que va más a fondo colocando a los datos de las personas cómo centro y sobre ella agregando capas de seguridad (Ning y Jiang, 2022). Estas capas de seguridad van desde la parte de seguridad de las aplicaciones hasta seguridad en redes de tal manera que si un atacante lograra tener acceso a la red tendría que pasar por múltiples capas antes de tener acceso a los datos de los usuarios.

### 2.1.3. Confianza cero

Confianza cero se basa en el hecho de que siempre los datos se encuentran en peligro es decir que cualquier persona puede ser un posible atacante (Azad et al, 2024), motivo por el cual esta estrategia propone que para poder acceder a los datos debe de estar fundamentado el porque necesita obtener los datos y si necesita actualizar o modificar también es necesario que se sustente (Zhang et al, 2024). Este privilegio mínimo que se logra por lo general es administrado por sistemas donde queda la evidencia de quien tiene acceso a los activos de información.

### 2.1.4. Gestión de identidades y roles

En los últimos años el incremento en el número de aplicaciones ha ido en aumento lo cual a genera que las personas tengan una identidad tanto física y virtual (Liu y Tian, 2023), esta identidad al igual que la física es necesario que sea protegida ya que si alguien lograr tener acceso a las credenciales de nuestra cuenta podría tener acceso a nuestros datos es por ello que otra tendencia en la ciberseguridad es la de gestión de identidades y roles (Agarkar, 2024). Esta estrategia especifica que según tu cargo o rol tienes acceso a ciertos activos, los cuales deben de estar monitoreados constantemente.

### 2.1.5. Sistema de gestión de eventos de seguridad

Sistema de gestión de eventos de seguridad es una solución que se usa para la parte de respuesta ante incidentes, ya que se ha demostrado que en la mayoría de los incidentes de ciberseguridad registrados siempre se vuelven a repetir con patrones similares (Knerler et al., 2022), es por ello que esta solución de sistema de gestión de eventos de seguridad permite que se tenga un registro de eventos anómalos los cuales sirvan de entrada para poder mejorar los procedimientos de seguridad y poder hacer una mejor respuesta ante incidentes de ciberseguridad

## 2.2. Marco conceptual

Para entender mejor la investigación es necesario el desarrollo de un marco conceptual en el cual se explican conceptos fundamentales que se usaran en el desarrollo de la investigación (Bernal, 2010) por lo que esta tesis desarrollará el marco conceptual los siguientes conceptos fundamentales

### 2.2.1. Activo de Información

El activo información es un objeto que es propiedad de una empresa y que cuente con un valor ya sea tangible o no (Baca, 2016). Este valor en conjunto es el que les da un gran valor a los sistemas de información, es por este motivo que en el sector salud la administración de los sistemas de información se centra en el correcto funcionamiento de estos y la protección de estos activos (Wager et al., 2009). Puesto que si no se maneja de manera adecuada puede acabar costándole mucho dinero a la empresa (Jiang et al., 2023) y una mala reputación a futuro.

### 2.2.2. Sistema de información de salud

Es el conjunto de sistemas integrados de prestación de servicios de salud que buscan coordinar de manera adecuada para poder brindar un servicio eficaz y eficiente en el cuidado de la salud de los pacientes (Haux et al., 2004; Salahuddin et al., 2020). El objetivo para el cual fueron diseñados es el de lograr un servicio eficaz y eficiente, pero no mencionan la parte de seguridad es por ello que muchos de estos sistemas presentan múltiples vulnerabilidades por la poca importancia que le dan las empresas del sector salud a la protección de sus datos (Karuppiah et al, 2019) generando que los sistemas funcionen de manera adecuada y con más tecnología, pero sin una buena capa de seguridad.

### 2.2.3. Ataques informáticos

Un ataque informático es un intento por acceder a los activos de información con el objetivo de modificar la confidencialidad, integridad o disponibilidad de estos activos (Baca, 2016) para que se pueda realizar estos ataques los atacantes se aprovechan de las vulnerabilidades existentes en los activos de tal manera que mediante la explotación de esa vulnerabilidad se tiene acceso al activo (Roa, 2013). Por lo que siempre es importante tener actualizados y seguros los equipos para hacer que estos ataques tengan menor cantidad de éxito al intentar explotar las vulnerabilidades.

### 2.2.4. Gestión de vulnerabilidades de ciberseguridad

La gestión de vulnerabilidades de ciberseguridad es un proceso sistemático y necesario que se realiza para la identificación, evaluación y priorización de las vulnerabilidades de ciberseguridad que se identifiquen (Diogenes et al., 2016), esta priorización permitirá que las vulnerabilidades que sean más propensas a ser víctimas de un ataque informático sean las primeras en ser remediadas (Baca, 2016) de tal manera que se logre un rápida respuesta y se mantenga seguro a los activos de información.

## 2.3. Marco sistémico

Para poder abordar el problema de que no se cómo proteger los activos con información sensible de los pacientes ante posibles ciberataques en empresas del sector salud de Lima, es necesario el uso de conceptos de la teoría general de sistemas, pues el ver los sistemas informáticos como piezas aisladas no es la mejor manera ya que la mayoría de los ataques suceden entre sus interacciones (Karuppiah et al, 2019), es por ello que es necesario ver las interacciones y las sinergias de entre estos sistemas ya que dos sistemas por separado al interactuar pueden crear un producto que es mayor a la suma de sus partes (Bertalanffy, 1976; Ossa, 2017).

La sinergia que aumenta con las interacciones, se ve mucho en los sistemas de salud ya que no solo se dan interacción entre sistemas informáticos sino también con sistemas humanos e incluso con sistemas de hospitales externos (McCovery y Matusitz, 2014) este gran numero de interacciones hace que el problema tenga una complejidad muy alta lo cual hace que al generar un cambio este afecte a muchas otras partes (Clarkson et al., 2018) por lo que es necesario una visión holística del problema para poder hacer una solución que afecte a todo el sistema en su totalidad.

Las nuevas tecnologías que están apareciendo en el sector salud permiten mayor flexibilidad entre la interconexión y una gran escalabilidad, pero a su vez aumentan la complejidad ya que aumenta la cantidad de componentes en los sistemas de información de salud (González et al., 2019). Por lo que para hacer frente a esta complejidad es necesario verlo de forma sistémica desde distintos frentes desde el de seguridad de red hasta la seguridad de información de las aplicaciones (Putro et al., 2024). Para lograr ver esto la tesis se apoyará de la teoría general de sistemas para poder entrelazar estas visiones y ver el problema como un todo.

## 2.4. Marco ético

Los datos de los pacientes son uno de los activos más valiosos y sensibles a ataques informáticos en las empresas del sector salud (Brantly y Brantly, 2020). Es por ello que existen normas que como la del Reglamento sanitario internacional, en el cual se especifica que consideraciones se debe de tener al momento de manipular estos datos de los pacientes de manera que estos se hagan con una ética adecuada (Kebede et al., 2024). Estas normas serán respetadas durante todo el proceso de desarrollo de la tesis, de tal manera que se mantenga la integridad y confidencialidad de estos datos.

Otro punto en el cual la ética también es parte es en el caso del almacenamiento de información de los pacientes para futuras investigaciones. El marco de trabajo que vela por una correcta ética en el tratamiento de estos datos es el Marco de gobernanza de la investigación sanitaria el cual se aplica en las instituciones sanitarias de Reino Unido (Sen, 2003; Pourrez et al., 2020). Por lo que podemos notar una gran importancia por parte de los estados y organizaciones a que exista una correcta ética en el tratamiento de estos datos.

Ahora del lado de la ciberseguridad la ética es un punto muy importante ya que constantemente se trabaja con información sensible y muy valiosa, es por ello que los profesionales de ciberseguridad siempre deben de velar por que se respete la confidencialidad, integridad y disponibilidad de los datos (Roa, 2013). Pero también es cierto que al momento de planificar una respuesta frente a un ataque informático la ética no es un punto que muchos toman en cuenta ya que esta en juego su reputación (Shoemaker et al., 2019), a pesar de este dilema existen auditorias que verifican normas de ciberseguridad relacionados a la política nacional en la que se encuentre (Madnick et al., 2023). Para evitar estos dilemas y problemas con auditoria es necesario siempre tener ética y sinceridad con los datos q se manejan a pesar de que esto comprometa la reputación de la empresa.

# Referencias bibliográficas

Agarkar, A. A., Karyakarte, M., Chavhan, G., Patil, M., Talware, R., & Kulkarni, L. (2024). Blockchain aware decentralized identity management and access control system. *Measurement Sensors*, 31(2), 1-10. <https://doi.org/10.1016/j.measen.2024.101032>

Ahmed, I., Hossain, N., Fazio, S., Lezzi, M. & Islam, M. (2024). A decision support model for assessing and prioritization of industry 5.0 cybersecurity challenges. *Sustainable Manufacturing and Service Economics*, 3(9), 1-20. <https://doi.org/10.1016/j.smse.2024.100018>

Angafor, G., Yevseyeva, I. & He, Y. (2020). Game‐based learning: A review of tabletop exercises for cybersecurity incident response training. *Security and Privacy*, *3*(6), 1-19. <https://doi.org/10.1002/spy2.126>

Azad, M., Abdullah, S., Arshad, J., Lallie, H. & Ahmed, Y. (2024). Verify and trust: A multidimensional survey of zero-trust security in the age of IoT. *Internet of Things*, 27(4), 1-7. <https://doi.org/10.1016/j.iot.2024.101227>

Baca, G. (2016). *Introducción a la seguridad informática.* Patria.

Balasamy, K., Krishnaraj, N., Ramprasath, J. & Ramprakash, P. (2022). A secure framework for protecting clinical data in medical IoT environment. *Smart Healthcare System Design,* 3(9), 203-234. <https://doi.org/10.1002/9781119792253.ch9>

Bernal, C. (2010). *Metodología de la investigación administración, economía, humanidades y ciencias sociales* (3rd ed.). Pearson.

Bertalanffy, L. (1976). *Teoría general de los sistemas.* Fondo de Cultura económica.

Bones, E., Hasvold, P., Henriksen, E. & Strandenas, T. (2007). Risk analysis of information security in a mobile instant messaging and presence system for healthcare. *International Journal of Medical Informatics*, *76*(9), 677–687. <https://doi.org/10.1016/j.ijmedinf.2006.06.002>

Brantly, A. & Brantly, N. (2020). Patient-centric cybersecurity. *Journal of Cyber Policy*, *5*(3), 372–391. <https://doi.org/10.1080/23738871.2020.1856902>

Cama, E. (11 de junio del 2020). *El 51% de las compañías en el Perú sostienen que la relación entre ciberseguridad y sus líneas de negocio es inexistente o neutral*. *EY*. <https://www.ey.com/es_pe/news/2020/06/ciberseguridad-lineas-negocio-neutral>

Čaušević, A., Fotouhi, H. & Lundqvist, K. (2017). Data security and privacy in cyber‐physical systems for healthcare. *Security and Privacy in Cyber‐Physical Systems*, 15(10), 305–326. Wiley. <https://doi.org/10.1002/9781119226079.ch15>

Cervera, A. & Goussens, A. (2024). Ciberseguridad y uso de las TIC en el Sector Salud. *Atencion primaria*, *56*(3), 1-7. <https://doi.org/10.1016/j.aprim.2023.102854>

Chen, C., Yang, T., Deng, Y. & Chen, Ch. (2021). A secure Internet of Things medical information sharing and emergency notification system based on nonrepudiation mechanism. *Transactions on Emerging Telecommunications Technologies*, *32*(5), 1-21. <https://doi.org/10.1002/ett.3946>

Clarkson, J., Dean, J., Ward, J., Komashie, A. & Bashford, T. (2018). A systems approach to healthcare: from thinking to ­practice. *Future Healthcare Journal*, 5(3), 151-155. <https://doi.org/10.7861/futurehosp.5-3-151>

Diogenes, Y., Shinder, T. & Shinder, D. (2016). *Microsoft Azure Security Infrastructure*. Microsoft Press.

Domínguez, M., Rodríguez, F., Galeano, J., Calle, J. & Cortés, D. (2024). FLECO: A tool to boost the adoption of holistic cybersecurity management. *Software Impacts*, 19(3), 1-4. <https://doi.org/10.1016/j.simpa.2024.100614>

Dugar, J. (2021). Holistic healthcare cybersecurity. *EDPACS*, *63*(4), 5–7. <https://doi.org/10.1080/07366981.2020.1823614>

Ebert, N., Schaltegger, T., Ambuehl, B., Schöni, L., Zimmermann, V. & Knieps, M. (2023). Learning from safety science: A way forward for studying cybersecurity incidents in organizations. *Computers & Security*, 134(11), 1-12. <https://doi.org/10.1016/j.cose.2023.103435>

Ghafur, S., Grass, E., Jennings, N. & Darzi, A. (2019). The challenges of cybersecurity in health care: the UK National Health Service as a case study. *The Lancet Digital Health*, 1(1), 10–12. <https://doi.org/10.1016/s2589-7500(19)30005-6>

Gomero, R., & Sánchez, D. (2024). Cybersecurity in the support services to occupational physicians in the city of Lima. A pilot study. *Revista Médica Herediana*, 35(1), 38–43. <https://doi.org/10.20453/rmh.v35i1.5298>

González, S., Dormido, S. & Sánchez, J. (2019). LA TEORÍA GENERAL DE SISTEMAS COMO HERRAMIENTA DE INVESTIGACIÓN Y SOLUCIÓN ANTE LA CIBERSEGURIDAD EN SISTEMAS DE AUTOMATIZACIÓN INDUSTRIAL.*Revista internacional de sistemas*, 23(1), 16-18. <https://doi.org/10.7203/ris.23.1.14105>

Handayani, P., Hidayanto, A. & Budi, I. (2018). User acceptance factors of hospital information systems and related technologies: Systematic review. *Informatics for Health & Social Care*, *43*(4), 401–426. <https://doi.org/10.1080/17538157.2017.1353999>

Haux, R., Winter, A., Ammenwerth, E. & Brigl, B. (2004). Strategic Information Management in Hospitals An Introduction to Hospital Information Systems. Springer Science+Business Media.

Hernández, R. & Mendoza, C. (2018). *Metodología de la investigación: las rutas cuantitativas, cualitativas y mixta*. McGraw-Hill.

Hines, W., Montgomery, D., Goldsman, D. & Borror, C. (2005). *Probabilidad y estadística para ingeniería* (4ª ed.)*.* Patria.

Hossain, N., Rahman, S. & Liza, S. (2023). Cyber-susiliency index: A comprehensive resiliency-sustainability-cybersecurity index for healthcare supply chain networks. *Decision Analytics Journal*, *9*(12), 1–17. <https://doi.org/10.1016/j.dajour.2023.100319>

Javaid, M., Haleem, A., Singh, R. & Suman, R. (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cyber Security and Applications*, *1*(2), 1-13. <https://doi.org/10.1016/j.csa.2023.100016>

Jiang, J., Liu, X., Wang, W. & Deveci, M. (2023). Assessing the impact of healthcare service risks on healthcare demand under evolving economic and social structures: An improved GLDS decision making method considering risk attitudes. *Structural Change and Economic Dynamics*, *67*(12), 459–479. <https://doi.org/10.1016/j.strueco.2023.09.002>

Kang, Y. (2023). Development of large-scale farming based on explainable machine learning for a sustainable rural economy: The case of cyber risk analysis to prevent costly data breaches. *Applied Artificial Intelligence: AAI*, *37*(1), 2143-2165. <https://doi.org/10.1080/08839514.2023.2223862>

Karuppiah, M., Obaidat, M., Islam, S. & Vijayakumar, P. (2019). Security analysis on “mutual authentication scheme for multimedia medical information systems”. *Security and Privacy*, *2*(3), 1-7. <https://doi.org/10.1002/spy2.67>

Kaspersky Lab. (2024). Estadísticas sobre las ciberamenazas. Recuperado el 13 de mayo de 2024, de <https://statistics.securelist.com/es/country/peru/ransomware/month>

Kebede, S., DeTora, L., Ekmekci, P., Wassie, T., Baer, C., Addiss, D., Crawley, P. & Bierer, B. (2024). Ethics and global health security. *Modernizing Global Health Security to Prevent, Detect, and Respond*, *1*(4), 19-36. <https://doi.org/10.1016/B978-0-323-90945-7.00018-X>

Kim, J., Park, E., Park, Y., Chun, K. & Wiles, L. (2022). Prosocial rule breaking on health information security at healthcare organisations in South Korea. *Information Systems Journal*, *32*(1), 164-191. <https://doi.org/10.1111/isj.12338>

Kim, L. (2018). Concienciación en materia de ciberseguridad: protección de datos y de pacientes. *Nursing*, *35*(1), 62–64. <https://doi.org/10.1016/j.nursi.2018.02.017>

Knerler, K., Parker I. & Zimmerman, C. (2022). *11 Strategies of a World-Class Cybersecurity Operations Center.* MITRE.

Leszczyna, R. (2019). Standards with cybersecurity controls for smart grid—A systematic analysis. *International Journal of Communication Systems*, *32*(6), 1-20. <https://doi.org/10.1002/dac.3910>

Liu, C. & Tian, Y. (2023). Recognition of digital twin city from the perspective of complex system theory: Lessons from Chinese practice. *Journal of Urban Management*, 12(2), 182–192. <https://doi.org/10.1016/j.jum.2023.04.001>

Madnick, B., Huang, K. & Madnick, S. (2024). The evolution of global cybersecurity norms in the digital age: A longitudinal study of the cybersecurity norm development process. *Information Security Journal a Global Perspective*, *33*(3), 204–225. <https://doi.org/10.1080/19393555.2023.2201482>

Mariano, R. & Núñez, G. (2023). Ciberataques a la logística y la infraestructura crítica en América Latina y el Caribe. *CEPAL.* <https://repositorio.cepal.org/server/api/core/bitstreams/2db8feef-29d6-4981-9741-9ad3154d3789/content>

McCovery, J. & Matusitz, J. (2014). Assessment of collaboration in U.s. health care delivery: A perspective from systems theory. *Social Work in Public Health,* 29(5), 451-461. <https://doi.org/10.1080/19371918.2013.865109>

Mikuletič, S., Vrhovec, S., Skela-Savič, B., & Žvanut, B. (2024). Security and privacy oriented information security culture (ISC): Explaining unauthorized access to healthcare data by nursing employees. *Computers & Security*, 136(1), 1-14. <https://doi.org/10.1016/j.cose.2023.103489>

Mohammed, M., Lakhan, A., Zebari, D., Ghani, M., Marhoon, H., Abdulkareem, K., Nedoma, J. & Martinek, R. (2024). Securing healthcare data in industrial cyber-physical systems using combining deep learning and blockchain technology. *Engineering Applications of Artificial Intelligence*, 129(3), 1-11*.* <https://doi.org/10.1016/j.engappai.2023.107612>

Moreno., M. (2022). *Gestión de incidentes de ciberseguridad*. Ra-Ma.

Naseer, A., Naseer, H., Ahmad, A., Maynard, S. & Siddiqui, A. (2023). Moving towards agile cybersecurity incident response: A case study exploring the enabling role of big data analytics-embedded dynamic capabilities. *Computers & Security*, 135(12), 1-13. <https://doi.org/10.1016/j.cose.2023.103525>

Ning, X. & Jiang, J. (2022). Defense-in-depth against insider attacks in cyber-physical systems. *Internet of Things and Cyber-Physical Systems*, 2(10), 203-211. <https://doi.org/10.1016/j.iotcps.2022.12.001>

Ossa, C. (2017). Teoría General de Sistemas Conceptos y aplicaciones. Universidad Tecnológica de Pereira

Pedchenko, Y., Ivanchenko, Y., Ivanchenko, I., Lozova, I., Jancarczyk, D. & Sawicki, P. (2022). Analysis of modern cloud services to ensure cybersecurity. *Procedia Computer Science*, *207*, 110–117. <https://doi.org/10.1016/j.procs.2022.09.043>

Perumal, A. & Nadar, E. (2020). Architectural framework of a group key management system for enhancing e‐healthcare data security. *Healthcare Technology Letters*, *7*(1), 13-17. <https://doi.org/10.1049/htl.2018.5114>

Pourrez, A., Crespel, E., Djahanchahi, S., Galibert, O. & Cordelier, B. (2020). Ethical positions arising from research on online communities in the health sector. *Health Research Practices in a Digital Context*, *4*(10), 75–92. <https://doi.org/10.1002/9781119779933.ch5>

Presidencia del Consejo de ministros del Perú. (2024). *Reporte sobre entidades que implementaron su equipo de respuestas ante incidentes de seguridad digital*. Recuperado el 22 de abril del 2024 de <https://www.gob.pe/institucion/pcm/informes-publicaciones/2605569-reporte-sobre-entidades-que-implementaron-su-equipo-de-respuestas-ante-incidentes-de-seguridad-digital>

Prümmer, J., Steen, T. & Berg, B. (2024). A systematic review of current cybersecurity training methods. *Computers & Security*, *136*(1), 1-20. <https://doi.org/10.1016/j.cose.2023.103585>

Putro, P., Handri, E. & Sensuse, D. (2024). Information system approaches in cybersecurity. *Procedia Computer Science*, 234(4), 1372–1379. <https://doi.org/10.1016/j.procs.2024.03.135>

Rama, K. & Naganjaneyulu, S. (2024). Designing a block chain based network for the secure exchange of medical data in healthcare systems. *Applied Artificial Intelligence: AAI*, *38*(1), 1-17. <https://doi.org/10.1080/08839514.2024.2318164>

Roa, J. (2013). *Seguridad informática.* McGraw-Hill.

SaberiKamarposhti, M., Ng, K., Chua, F., Abdullah, J., Yadollahi, M., Moradi, M. & Ahmadpour, S. (2024). Post-quantum healthcare: A roadmap for cybersecurity resilience in medical data. *Heliyon*, 10(10), 1-19. <https://doi.org/10.1016/j.heliyon.2024.e31406>

Sabet, C., Lin, J., Zhong, A. & Nguyen, D. (2024). Cybersecurity in the age of digital pandemics: protecting patient data in low-income and middle-income countries. *The Lancet. Global Health*, 12(6), 911–912. <https://doi.org/10.1016/s2214-109x(24)00124-4>

Salahuddin, L., Ismail, Z., Raja Ikram, R. R., Hashim, U. R., Idris, A., Ismail, N. H., Hassan, N. H. & Abdul Rahim, F. (2020). Safe use of hospital information systems: an evaluation model based on a sociotechnical perspective. *Behaviour & Information Technology*, *39*(2), 188–212. <https://doi.org/10.1080/0144929x.2019.1597164>

Sana, L., Nazir, M. M., Iqbal, M., Hussain, L. & Ali, A. (2022). Anomaly detection for cyber internet of things attacks: A systematic review. *Applied Artificial Intelligence: AAI*, *36*(1), 3243-3264. <https://doi.org/10.1080/08839514.2022.2137639>

Selvaraj, P. & Doraikannan, S. (2019). Privacy and security issues on wireless body area and IoT for remote healthcare monitoring. *Intelligent Pervasive Computing Systems for Smarter Healthcare*, 227-253. <https://doi.org/10.1002/9781119439004.ch10>

Sen, B. A. (2003). Research governance: implications for health library and information professionals. *Health Information and Libraries Journal*, 20(1), 3–14. <https://doi.org/10.1046/j.1471-1842.2003.00413.x>

Shoemaker, D., Kohnke, A. & Laidlaw, G. (2019). Ethics and cybersecurity are not mutually exclusive. *EDPACS*, 60(1), 1–10. <https://doi.org/10.1080/07366981.2019.1651516>

Szczepaniuk, H. & Szczepaniuk, E. K. (2023). Cryptographic evidence-based cybersecurity for smart healthcare systems. *Information Sciences*, *649*(11). <https://doi.org/10.1016/j.ins.2023.119633>

Tarikere, S., Donner, I. & Woods, D. (2021). Diagnosing a healthcare cybersecurity crisis: The impact of IoMT advancements and 5G. *Business Horizons*, *64*(6), 799–807. <https://doi.org/10.1016/j.bushor.2021.07.015>

Toussaint, M., Krima, S. & Panetto, H. (2024). Industry 4.0 data security: A cybersecurity frameworks review. *Journal of Industrial Information Integration*, *39*. <https://doi.org/10.1016/j.jii.2024.100604>

Ud, I., Xue, M., Ali, A., Shah, T. & Ilyas, A. (2017). Role of information & communication technology (ICT) and e-governance in health sector of Pakistan: A case study of Peshawar. *Cogent Social Sciences*, 3(1), 1-18. <https://doi.org/10.1080/23311886.2017.1308051>

Wager, K., Lee, F. & Glaser, J. (2009). *Health care information systems: A practical approach for health care management* (3rd ed.). Jossey-Bass.

Wang, W., Di Maio, F. & Zio, E. (2019). Adversarial risk analysis to allocate optimal defense resources for protecting cyber–physical systems from cyber attacks. *Risk Analysis: An Official Publication of the Society for Risk Analysis*, *39*(12), 2766–2785. <https://doi.org/10.1111/risa.13382>

Williams, A. D. (2020). Systems theory principles and complex systems engineering concepts for protection and resilience in critical infrastructure: Lessons from the nuclear sector. *Insight*, 23(2), 14–20. <https://doi.org/10.1002/inst.12293>

Yeole, A. & Kalbande, D. R. (2021). Ensuring security and privacy in IoT for healthcare applications. *Cognitive Engineering for Next Generation Computing*, 299-314. <https://doi.org/10.1002/9781119711308.ch11>

Zarour, M., Alenezi, M., Ansari, M., Pandey, A., Ahmad, M., Agrawal, A., Kumar, R. & Khan, R. A. (2021). Ensuring data integrity of healthcare information in the era of digital health. *Healthcare Technology Letters*, *8*(3), 66-77. <https://doi.org/10.1049/htl2.12008>

Zhan, Y., Ahmad, S., Irshad, M., Al-Razgan, M., Awwad, E., Ali, Y. & Ahmad, A. (2024). Investigating the role of Cybersecurity’s perceived threats in the adoption of health information systems. *Heliyon*, *10*(1). <https://doi.org/10.1016/j.heliyon.2023.e22947>

Zhang, H., Zhang, Z. & Chen, L. (2024). Toward zero trust in 5G industrial internet collaboration systems. *Digital Communications and Networks*, 2(3), 1-9. <https://doi.org/10.1016/j.dcan.2024.03.011>

Zhao, X., Miers, I., Green, M. & Mitrani-Reiser, J. (2019). Modeling the cybersecurity of hospitals in natural and man-made hazards. *Sustainable and Resilient Infrastructure*, *4*(1), 36-49. <https://doi.org/10.1080/23789689.2018.1448666>