A white and black text with black text

Description automatically generated with medium confidence

1.1Generalidades

1.2Realidad Problemática

1.3Formulación del Problema

1.4Justificaion del Estudio

1.5Hipótesis (General, Específicos)

1.6Objetivos(General, expeficios)

1.7 Limitantes de la investigacion(Teórico,temporal,espacial)

Capitulo 2

Antecedentes de investigacion

Bases teóricas

Variable dependiente

Variable independiente

Marco Conceptual

## **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)

## **Antecedentes investigativos**

La idea de carritos de compras inteligentes se encuentra en una cantidad considerable de artículos científicos, el cual el término “inteligente” ha abierto un abanico de posibilidades de distintas implementaciones a los carritos de compras actuales (Martinus et al., 2021), de los cuales la gran mayoría se enfoca en la mejora de la experiencia del cliente de los supermercados.

Una investigación creativa realizada por Martinus et al. (2021) es la mejora del carrito de compras tradicional, el cual implica escanear productos con RFID, transmitir datos al servidor y finalizar la compra con un código único en la aplicación, confirmado por el cajero en el aplicativo para actualizar la base de datos (ver Figura 5). Otra investigación realizada por Rajithkumar et al. (2018) modifica un carrito de compra tradicional a uno que incluye la detección de peso a los artículos, el uso de alertas y comunicación con el sistema central para actualizar la base de datos. El desarrollo de un sistema de carrito de compras inteligente que registra los productos y realiza transacciones en línea para la facturación utilizando RFID y ZigBee y el uso de algoritmos fue hecho por Yewatkar et al. (2021). Una investigación científica hecha por Dawkhar et al. (2015) explica cómo se automatiza el proceso de facturación dentro del carrito de compras utilizando tecnología RFID, ofreciendo un soporte teórico y práctico del tema.

**Figura 5**  
*Explicación de un carrito de compras con tecnología RFID*

Diagrama

Descripción generada automáticamente

Nota. Adaptado de “Data Transmission Using RFID System on Smart Shopping Carts for Checkout Process Efficiency in Supermarket at Indonesia” de Martinus, M.S. Wahab, Yudi, & H. Ham, 2021, Procedia Computer Science, 179, p. 905. (https://doi.org/10.1016/j.procs.2021.01.080). CC BY-NC.

Si bien los antecedentes anteriormente mencionados son de hace menos de 10 años y se podría decir que son más relevantes que los de años anteriores, siempre es bueno entender cómo avanzó el tema de carritos inteligentes, una investigación comprende la creación de un carrito de compras inteligente, compuesto por tres componentes principales: comunicación con el servidor, interfaz de usuario y facturación automática, el diseño es para saber cómo acceder a la información en tiempo real, esto fue hecho por Kumar et al. (2013) y otra investigación realizada por Ali & Sonkusare (2013), la cual se enfoca en carritos de compras inteligentes con capacidad para calcular y mostrar automáticamente los precios totales de los productos.

BASES TEORICAS:

(DEFINICION FALTA LA ESTRUCTURA)

DEFINICION DE LAS VARIABLES :

## **Variables**

En este caso, solamente se posee el problema de investigación general, por lo cual se procede a definir la variable independiente y dependiente de la investigación.

## A document with text and numbers Description automatically generated

## A white and blue rectangular table with black text Description automatically generated

## A white rectangular object with black text Description automatically generated

## MARCO CONCEPTUAL

## 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