**PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ**

**FACULTAD DE CIENCIAS E INGENIERÍA**


# IMPLEMENTACIÓN DE UN *E-COMMERCE* QUE INCORPORE EL USO DE LA TECNOLOGÍA *BLOCKCHAIN* Y ALGORITMOS DE DETECCIÓN DE FRAUDE COMO MEDIO PARA MEJORAR LA SEGURIDAD Y LA INTEGRIDAD DE LAS TRANSACCIONES

**Tesis para obtener el título profesional de Ingeniero Informático**

**Autor:**

**Henry Javier Pebe Reyes**

**Asesor:**

**Luis Alberto Flores Garcia**

Lima, Mayo, 2025

Informe de Similitud

Yo, Luis Alberto Flores Garcia, docente de la Facultad de Ciencias e Ingeniería de la Pontificia Universidad Católica del Perú, asesor(a) de la tesis/el trabajo de investigación titulado: Implementación de un ecommerce que incorpore el uso de la tecnología blockchain y algoritmos de detección de fraude como medio para mejorar la seguridad y la integridad de las transacciones, del autor Henry Javier Pebe Reyes dejo constancia de lo siguiente:

- El mencionado documento tiene un índice de puntuación de similitud de 20 %. Así lo consigna el reporte de similitud emitido por el software Turnitin el 23/04/2025.
- He revisado con detalle dicho reporte y la Tesis o Trabajo de Suficiencia Profesional, y no se advierte indicios de plagio.
- Las citas a otros autores y sus respectivas referencias cumplen con las pautas académicas.

San Miguel 23 de abril de 2025

| Apellidos y nombres del asesor / de la asesora:<br>Flores García Luis Alberto | |
|---|---|
| DNI:<br>10772024 | Firma<br>  |
| ORCID:<br>https://orcid.org/0000-0002-1359-283X | |

# Resumen

El crecimiento acelerado del comercio electrónico en el Perú ha venido acompañado de desafíos significativos en seguridad, integridad y confianza en las transacciones digitales. Estas deficiencias han derivado en brechas de seguridad, pérdidas económicas y disminución de la confianza de los usuarios. En respuesta a esta problemática, la presente investigación propone el diseño, implementación y evaluación de un sistema de comercio electrónico que integra la tecnología *blockchain* y un algoritmo de detección de fraudes.

El sistema desarrollado utiliza contratos inteligentes en *blockchain* para garantizar la integridad de los datos transaccionales y emplea un algoritmo criptográfico para proteger la información sensible de los usuarios. Adicionalmente, se diseñó un algoritmo de detección de fraudes capaz de analizar datos en tiempo real e históricos, identificando y aprendiendo en base a los patrones sospechosos y fortaleciendo la seguridad del sistema. Entre las funcionalidades clave se incluye una interfaz gráfica intuitiva, un módulo de chat directo entre compradores y vendedores, y la integración de una pasarela de pago segura.

Los resultados demuestran que las soluciones propuestas no solo reducen significativamente las vulnerabilidades del sistema, sino que también optimizan la confianza de los usuarios, disminuyen los costos asociados al fraude y sientan las bases para un comercio electrónico más seguro y confiable en el Perú. Esta investigación se destaca por ser un aporte innovador en el ámbito de la seguridad digital en el *e-commerce*, mostrando el potencial transformador de la tecnología *blockchain* y los algoritmos de aprendizaje automático.

# Tema FCI

**PARA OPTAR:** Título profesional de Ingeniero Informático

**TEMA:** Implementación de un *e-commerce* que incorpore el uso de la tecnología *blockchain* y algoritmos de detección de fraude como medio para mejorar la seguridad y la integridad de las transacciones

**ÁREA:** Sistemas de Información

**ASESOR:** Luis Alberto Flores Garcia

**ALUMNO(S)**: Henry Javier Pebe Reyes – 20191425

**FECHA:** 03/08/2024

**MÁXIMO:** 135 páginas

Descripción y Objetivos:

La seguridad en el comercio electrónico ha evolucionado como una de las principales preocupaciones para empresas y usuarios debido a las crecientes amenazas digitales. Sin embargo, a pesar de los avances tecnológicos, muchas plataformas de comercio electrónico siguen enfrentando problemas relacionados con la seguridad de la información y la protección de datos personales. La falta de medidas adecuadas de seguridad y la debilidad en los sistemas de autenticación son algunos de los factores que contribuyen a estas vulnerabilidades. La introducción de tecnologías avanzadas como *blockchain* y algoritmos de detección de fraude promete abordar estos desafíos, pero también requiere una implementación cuidadosa y bien evaluada para evitar posibles riesgos. La implementación de un sistema de *e-commerce* que incorpore *blockchain* y algoritmos de detección de fraude tiene el potencial de mejorar significativamente la

seguridad y la integridad de las transacciones. *Blockchain* ofrece una solución robusta para la transparencia y la integridad de los datos, mientras que los algoritmos de detección de fraude pueden identificar y prevenir actividades fraudulentas en tiempo real. Para abordar estos problemas, el presente proyecto de tesis se enfoca en el diseño, implementación y evaluación de un sistema de comercio electrónico basado en tecnología *blockchain* y algoritmos de detección de fraude. Este proyecto no solo busca mejorar la seguridad y la integridad de las transacciones, sino también establecer un modelo replicable que pueda ser adoptado por otras organizaciones para fortalecer sus sistemas de comercio electrónico. La combinación de *blockchain* y algoritmos de detección de fraude ofrece una solución innovadora y efectiva para los desafíos actuales del *e-commerce*, garantizando la confianza y la protección de los usuarios. Este sistema está destinado a garantizar la seguridad y la integridad de las transacciones, restaurando así la confianza de los clientes y mejorando la protección de los datos personales. Dada la problemática planteada y la justificación del caso, se procede a indicar a continuación los propósitos concretos de este proyecto de tesis.

Objetivos específicos:

1. Implementar componentes para el sistema de información, con la finalidad de asegurar el almacenamiento e integridad de los datos.
2. Implementar las funcionalidades transaccionales necesarias en el sistema de información para facilitar operaciones eficientes y seguras.
3. Diseñar, desarrollar e integrar un algoritmo de detección de fraudes que pueda analizar datos de transacciones históricas y en tiempo real, identificando patrones y comportamientos sospechosos en el sistema de comercio electrónico basado en

*blockchain*, reduciendo los problemas relacionados con la seguridad e integridad de las transacciones.

**Tabla de Contenido**

**Índice de tablas**

# Capítulo 1. Generalidades

## 1.1 Problemática

### 1.1.1 Árbol de problemas

Un árbol de problemas es una herramienta visual que se utiliza para analizar y comprender una situación problemática de manera detallada. Permite descomponer un problema complejo en partes más pequeñas y comprensibles. Cada rama del árbol representa un aspecto específico del problema, lo que facilita la identificación de las causas principales y sus efectos. Al visualizar el problema de esta manera, se pueden identificar soluciones más efectivas y centradas (García, J., 2009).

En la tabla 1, se presenta una tabla donde se podrá visualizar el árbol de problemas para el presente proyecto.

- **Tabla 1: Árbol de problemas**

| | | | | |
|---|---|---|---|---|
| **Efectos** | • Brechas de seguridad que pueden llevar a la exposición de datos sensibles<br>• Pérdida de confianza de los usuarios y daño a la reputación de la empresa. | • Pérdida financiera para las empresas y consumidores afectados.<br>• Amenazas por el aumento de movimientos fraudulentos | • Interrupción del servicio que puede resultar en pérdidas de ingresos.<br>• Daño a la reputación de la empresa y pérdida de usuarios. | • Posible acceso no autorizado a información confidencial de los usuarios.<br>• Deficiencia de transparencia en la gestión de intermediarios. |
| **Problema central** | Deficiencia de seguridad e integridad en los sistemas de información dentro del comercio electrónico | | | |
| **Causas** | Falta de medidas adecuadas de protección de datos personales | Débil autenticación y protección de credenciales | Deficiencias en la seguridad de las transacciones | Presencia de intermediarios vulnerables |

Nota: Elaboración propia

### 1.1.2 Descripción

La industria del comercio electrónico en el Perú experimentó un impresionante crecimiento del 55% en el año 2021, lo que marcó un hito en el aumento de empresas que se aventuraron en este próspero mercado. Este fenómeno se debe en gran medida a la transformación del comercio electrónico en una herramienta indispensable para empresas de todos los tamaños en el Perú (CEPLAN, 2023). Las ventas de comercio electrónico en el Perú alcanzaron un aumento del 55% respecto al 2020 y se proyecta que esta seguirá creciendo un 53% para el siguiente año (Americas Market Intelligence, 2022). Por lo tanto, El aumento del comercio electrónico en Perú ha sido notable en años recientes. Cada vez hay más empresas que buscan mejorar el alcance, la cobertura de sus ventas y obtener nuevos clientes a través de internet.

Actualmente, existen diversas medidas de seguridad cibernética que ayudan a mitigar los riesgos asociados a ataques como el *ransomware* y otras amenazas digitales. Entre las prácticas más recomendadas se encuentran el uso de un antivirus confiable y actualizado, la instalación de *firewalls* para detectar comportamientos sospechosos, la realización frecuente de copias de seguridad, la verificación del origen de los correos electrónicos antes de abrir enlaces o descargar archivos, y la activación de actualizaciones automáticas del sistema operativo. Asimismo, se aconseja desconfiar de mensajes con ofertas exageradas o que generen un sentido de urgencia, ya que suelen ser tácticas comunes de los atacantes (Thomson Reuters, 2023). Asimismo, se enfatiza la importancia de tomar precauciones al conectarse a redes Wi-Fi públicas y de evitar hacer clic en enlaces o descargar archivos adjuntos de fuentes desconocidas (Bank of America, 2022).

Sin embargo, el ecommerce en el Perú se enfrenta a desafíos significativos en términos de seguridad, integridad y confianza de los usuarios. Estos desafíos específicos, como la deficiencia de seguridad en las transacciones y la deficiencia de confianza del usuario debido a problemas de autenticidad y protección de datos personales, están directamente relacionados con la deficiencia de seguridad e integridad en los sistemas de información dentro del comercio electrónico en el país. Esta carencia de seguridad e integridad en los sistemas de información actúa como un problema central para el desarrollo continuo y sostenible de la industria del comercio electrónico en el Perú (Castillo Telles, Arroyo García, 2017).

A continuación, se describe cada una de estas causas específicas:

- Deficiencia de protección de datos personales: Surgen desafíos significativos en el ámbito de la recopilación, almacenamiento y análisis de datos, lo que a su vez facilita la aparición de brechas de seguridad, exponiendo la privacidad de datos personales. Estos desafíos no solo se limitan a la gestión de datos, sino que también afectan la calidad de la información y su capacidad de ser rastreada, lo que tiene un impacto directo en la protección y la seguridad de los datos en cuestión (Treiblmaier & Sillaber, 2021). Como consecuencia, se puede erosionar la confianza de los usuarios y dañar la reputación de la empresa debido a una inadecuada gestión de la protección de datos.

- Débil autenticación y protección de credenciales: A pesar de que existen soluciones basadas en la criptografía para abordar estos desafíos, su implementación adecuada se ha visto obstaculizada debido al aumento en las prácticas fraudulentas que abarcan diversas modalidades, las cuales pueden afectar la integridad de los usuarios debido a que no se tiene una buena identificación de la autenticación y de las credenciales de los usuarios. Entre estas actividades fraudulentas, se tiene la apropiación de cuentas, que implica la obtención no autorizada de las credenciales de un usuario; el robo de identidad, que conlleva el uso indebido de la información personal de un individuo para llevar a cabo compras no autorizadas; el fraude silencioso, que busca evadir la detección mediante estrategias maliciosas; y el fraude de devolución de cargo, que consiste en solicitar un reembolso después de recibir un producto o servicio. Es importante destacar que la amenaza del incremento de estos tipos de fraudes puede tener repercusiones financieras significativas tanto para los consumidores como para los vendedores. Además, socavan la confianza general en el comercio electrónico como canal seguro para la compra de productos y servicios (Pranto et al., 2022).

- Inseguridad en las transacciones: Diversos tipos de ataques representan una amenaza constante para la integridad de las transacciones, debilitando su calidad y eficiencia. Entre estos, destacan los ataques de servicio, los ataques DDoS, las inyecciones SQL, el secuestro del flujo del cliente, y otros similares. Estos incidentes pueden tener un impacto negativo en las solicitudes realizadas, los procesos de pago y la recepción de bienes o servicios debido a que pueden provocar interrupciones en los servicios, comprometiendo la fluidez y la seguridad de las operaciones en el *e-commerce* (Pleskach et al., 2022). Como resultado adicional, se pueden experimentar tanto pérdidas económicas como daños en la reputación de la empresa, así como una disminución en la fidelidad de los usuarios.

- Por otro lado, aunque los intermediarios simplifican las transacciones, la falta parcial de un trato directo con el vendedor puede disminuir la confianza del cliente y dificultar la fidelización (Beetrack, 2020). Los intermediarios necesitan acceder a información sobre las transacciones, lo que puede incluir datos personales y financieros de los usuarios, dejando la posibilidad del acceso a datos sensibles y aumentar el riesgo de exposición de datos sensibles en caso de una violación de seguridad por la deficiencia de transparencia en la gestión de los intermediarios, por lo tanto, es necesario medidas adecuadas de seguridad ante esta situación (Safety Net Project, 2022). Los intermediarios pueden influir en la estructura de costos y operaciones de las empresas. Por ejemplo, pueden financiar las ventas a los clientes y pagar a los fabricantes antes de que los productos se vendan realmente (Sage Advice, 2023). Aunque esto puede ser beneficioso, también puede resultar en una pérdida de autonomía y flexibilidad para las empresas en la gestión de su propia información y operaciones; incluso, puede generar una carencia de transparencia en la gestión de intermediarios.

En resumen, el crecimiento extraordinario de la industria del comercio electrónico en el Perú ha sido innegable. Sin embargo, este auge se ha visto perjudicado por el problema central que es la deficiencia de seguridad e integridad en los sistemas de información, que abarca desafíos significativos relacionados con la seguridad, la integridad y la confianza en el comercio electrónico.

La deficiencia de protección adecuada de datos personales ha llevado a brechas de seguridad, exponiendo datos sensibles y socavando la confianza de los usuarios (Treiblmaier & Sillaber, 2021). La debilidad en la autenticación y protección de credenciales ha resultado en la pérdida de la confidencialidad de los usuarios y ha permitido el aumento de movimientos fraudulentos (Pleskach et al., 2022).

La inseguridad en las transacciones ha causado pérdidas financieras tanto para las empresas como para los consumidores, junto con una interrupción del servicio que ha llevado a pérdidas de ingresos y daños en la reputación de las empresas. Además, la presencia de intermediarios vulnerables ha exacerbado estos problemas al comprometer la transparencia en la gestión de las transacciones, lo que ha llevado a posibles accesos no autorizados a información confidencial de los usuarios (Pleskach et al., 2022).

A pesar de la presencia de herramientas de ciberseguridad y la participación de intermediarios para aumentar el alcance, la deficiencia de seguridad en la gestión de datos sensibles y los riesgos asociados han generado una brecha importante en la confianza del cliente. Por lo tanto, este desajuste entre el crecimiento aparentemente exitoso del comercio electrónico y la falta parcial de integridad y seguridad en los sistemas de información subraya la urgencia de abordar de manera integral estos desafíos para garantizar un desarrollo continuo y sostenible de la industria del comercio electrónico en el Perú.

### 1.1.3 Problema elegido

Basándonos en lo presentado en la subsección previa, podemos deducir que la protección de la información en los sistemas de comercio electrónico tiene fallos que aumentan la posibilidad de operaciones fraudulentas, robo de identidad, ataques cibernéticos y otras acciones negativas. Estas deficiencias a su vez resultan en una disminución de la protección e integridad de los datos de los usuarios, lo que a su vez conduce a la pérdida de confianza de los usuarios en la implementación del sistema de información. Este problema se agrava debido a la deficiencia de medidas preventivas y correctivas eficaces para abordar estos inconvenientes en los sistemas de comercio electrónico. Precisamente, el objetivo de este proyecto de fin de carrera es abordar esta problemática y proponer soluciones al respecto.

## 1.2 Objetivos

### 1.2.1 Objetivo general

Diseñar, implementar y evaluar un sistema de comercio electrónico que integre la tecnología *blockchain* para garantizar la seguridad e integridad de las transacciones y un algoritmo de detección de fraude para identificar y prevenir movimientos fraudulentos. Esto se hace con el propósito de reducir las vulnerabilidades que incrementan la probabilidad de movimientos fraudulentos, robo de identidad, ataques cibernéticos y otras acciones negativas. El objetivo es potenciar la salvaguarda e integridad de la información en las transacciones y restaurar la confianza de los clientes en la implementación de estos mismo dentro del sistema, abordando así la problemática identificada previamente en cuanto a las deficiencias en la seguridad de la información en los sistemas de comercio electrónico.

### 1.2.2 Objetivos específicos

- O1: Implementar componentes para el sistema de información, con la finalidad de asegurar el almacenamiento e integridad de los datos.
- O2: Implementar las funcionalidades transaccionales necesarias en el sistema de información para facilitar operaciones eficientes y seguras.
- O3: Diseñar, desarrollar e integrar un algoritmo de detección de fraudes que pueda analizar datos de transacciones históricas y en tiempo real, identificando patrones y comportamientos sospechosos en el sistema de comercio electrónico basado en *blockchain*, reduciendo los problemas relacionados con la seguridad e integridad de las transacciones.

### 1.2.3 Resultados esperados

- O1: Implementar componentes para el sistema de información, con la finalidad de asegurar el almacenamiento e integridad de los datos.
    - R1: Documentación de requerimientos y prototipo de arquitectura del sistema de información.
    - R2: Componente del sistema de información que usa *Smart Contracts* para el almacenamiento de las transacciones en *blockchain* con componentes como el registro de transacciones en la cadena de bloques, a fin de garantizar la integridad de los datos sensibles.
    - R3: Implementación de un algoritmo criptográfico para asegurar el almacenamiento de los datos privados del usuario.
- O2: Implementar las funcionalidades transaccionales necesarias en el sistema de información para facilitar operaciones eficientes y seguras.

- R4: Documentación de requerimientos funcionales y no funcionales del objetivo, y prototipo de la interfaz gráfica del sistema de información.
- R5: Implementación del sistema de información incluyendo la interfaz gráfica y las funcionalidades que la engloba.
- R6: Funcionalidad de chat para la interacción directa entre compradores y vendedores.
- R7: Integración de una pasarela de pago como sistema seguro que proteja la información financiera del comprador y ofrezca opciones de pago confiables, como tarjetas de crédito, billeteras digitales o sistemas de pago en línea.

- O3: Diseñar, desarrollar e integrar un algoritmo de detección de fraudes que pueda analizar datos de transacciones históricas y en tiempo real, identificando patrones y comportamientos sospechosos en el sistema de comercio electrónico basado en *blockchain*, reduciendo los problemas relacionados con la integridad de las transacciones.
  - R8: Especificación de requerimientos funcionales y no funcionales.
  - R9: Recolección y procesamiento de datos de transacciones históricas y en tiempo real para la implementación de un almacenamiento y gestionamiento de medianas cantidades de datos.
  - R10: Implementación del algoritmo de detección de fraudes capaz de analizar tanto datos de transacciones históricas como información en tiempo real. Este sistema estará diseñado para identificar patrones y comportamientos sospechosos, tales como actividades inusuales,

volúmenes extraordinarios de transacciones que puedan indicar actividad fraudulenta

- R11: Integración del algoritmo de detección de fraudes dentro del sistema de información para mejorar la seguridad de las transacciones en el e-commerce.

### 1.2.4 Mapeo de objetivos, resultados y verificación

En la tabla 2, se mostrará el mapeo de los resultados y las verificaciones de cada objetivo planteado para esta investigación.

■ **Tabla 2: Mapeo de los resultados y verificación de cada objetivo**

| **Objetivo 1:** Implementar componentes para el sistema de información, con la finalidad de asegurar el almacenamiento e integridad de los datos. | | |
|---|---|---|
| **Resultado** | **Medio de verificación** | **Indicador objetivamente verificable** |
| R1: Documentación de requerimientos y prototipo de arquitectura del software. | -Documento donde se presentan los requisitos funcionales y no funcionales del sistema de información.<br><br>-Documento del prototipo de la arquitectura de software incluyendo la vista funcional, lógica y componentes. | -Revisión y aprobación del documento de especificación de requerimientos por parte del especialista de *blockchain*, considerando una tasa del 100% de aprobación.<br><br>-Revisión y validación del documento de prototipo de la arquitectura de software por parte de un especialista en *blockchain* y en arquitectura de software, considerando una tasa del 100% de aprobación. |
| R2: Componente del sistema de información que usa *Smart Contracts* para el almacenamiento de las transacciones en *blockchain*, a | -Código fuente del componente del sistema de información.<br><br>-Plan de pruebas del | -Pruebas exitosas del almacenamiento y lectura de los datos de las transacciones realizadas en el sistema. |

| | | |
|---|---|---|
| fin de garantizar la integridad de los datos sensibles. | componente del sistema de información. | |
| R3: Implementación de un algoritmo criptográfico para asegurar el almacenamiento de los datos privados del usuario. | -Código fuente de los algoritmos criptográficos.<br>-Plan de pruebas de los algoritmos criptográficos. | -Pruebas exitosas de funcionamiento del algoritmo criptográfico en el sistema por el autor de la tesis. |
| **Objetivo 2:** Implementar las funcionalidades transaccionales necesarias en el sistema de información para facilitar operaciones eficientes y seguras. | | |
| **Resultado** | **Medio de verificación** | **Indicador objetivamente verificable** |
| R4: Documentación de requerimientos y prototipo de la interfaz gráfica del sistema de información. | -Documento actualizado donde se tiene los requisitos funcionales y no funcionales del sistema de información con las modificaciones.<br><br>-Documento que incluye el prototipo del sistema de información y sus módulos. | -Revisión y aprobación de la especificación de requerimientos por parte del especialista de *e-commerce*, considerando una tasa del 100% de aprobación.<br><br>-Revisión y confirmación del documento de prototipo de la interfaz gráfica por parte de un especialista en *e-commerce*, considerando una tasa del 100% de aprobación. |
| R5: Implementación del sistema de información incluyendo la interfaz gráfica y las funcionalidades que la engloba. | -Código fuente del sistema de información.<br><br>-Plan de pruebas de funcionalidad del software. | -Pruebas de funcionalidad realizadas por el tesista y revisadas por un especialista de *e-commerce* con una tasa del 100% de aprobación. |
| R6: Funcionalidad de chat para la interacción directa entre compradores y vendedores. | -Código fuente de la funcionalidad de interacción directa del sistema de información.<br><br>-Plan de pruebas de la | -Pruebas de la funcionalidad de la interacción directa del comprador y el vendedor, el cual deberá ser verificada por el especialista del *e-commerce* y de tener un nivel de aprobación con una tasa de éxito del 90%. |

| | | |
|---|---|---|
| | funcionalidad de interacción directa del sistema de información. | |
| R7: Integración de una pasarela de pago como sistema seguro que proteja la información financiera del comprador y ofrezca opciones de pago confiables, como tarjetas de crédito, billeteras digitales o sistemas de pago en línea. | -Código fuente del módulo.<br><br>-Plan de pruebas del módulo. | -Pruebas de funcionamiento del sistema de pago, seguridad de la transmisión de datos y gestión de errores de pago, el cual deberá tener un nivel de aprobación de un especialista de *e-commerce* en un 90%. |
| **Objetivo 3:** Diseñar, desarrollar e integrar un algoritmo de detección de fraudes que pueda analizar datos de transacciones históricas y en tiempo real, identificando patrones y comportamientos sospechosos en el sistema de comercio electrónico basado en *blockchain*, reduciendo los problemas relacionados con la integridad de las transacciones. | | |
| **Resultado** | **Medio de verificación** | **Indicador objetivamente verificable** |
| R8: Especificación de requerimientos funcionales y no funcionales del algoritmo de detección de fraude. | Documento actualizado donde se tiene los requisitos funcionales y no funcionales del algoritmo de detección. | Revisión y validación del documento de especificación de requerimientos del algoritmo de detección por el especialista de machine learning, considerando una tasa del 100% de aprobación. |
| R9: Recolección y procesamiento de datos de transacciones históricas y en tiempo real para la implementación de un almacenamiento y gestionamiento de medianas cantidades de datos. | -Documentación sobre los registros detallados del proceso de recolección y procesamiento de datos. | -Revisión y validación de la documentación sobre la recolección y procesamiento de datos por parte de un especialista en análisis de datos, considerando una tasa del 98% de aprobación. |
| R10: Implementación del algoritmo de detección de | -Documentación sobre los posibles algoritmos de | -Pruebas del algoritmo de detección utilizando un conjunto de datos históricos |

| | | |
|---|---|---|
| fraudes capaz de analizar tanto datos de transacciones históricas como información en tiempo real. Este sistema estará diseñado para identificar patrones y comportamientos sospechosos, tales como actividades inusuales, volúmenes extraordinarios de transacciones que puedan indicar actividad fraudulenta | machine learning a implementar.<br><br>-Código fuente del algoritmo de detección de fraudes.<br><br>-Documentación sobre las verificaciones de la funcionalidad del algoritmo de detección. | generados específicamente para este propósito, revisada por un especialista de *machine learning*, considerando una tasa de éxito del 90%.<br><br>-Pruebas del algoritmo en tiempo real bajo diversas condiciones y escenarios donde se ponga a prueba los patrones y comportamientos sospechosos, revisadas por un especialista de machine learning, considerando una tasa de éxito del 90%. |
| R11: Integración del algoritmo de detección de fraudes dentro del sistema de información para mejorar la seguridad de las transacciones en el *e-commerce*. | -Código fuente del algoritmo integrado en el sistema de información.<br><br>-Plan de pruebas del algoritmo de detección de fraude en el sistema. | -Pruebas de funcionalidad, rendimiento y seguridad después de la integración, revisado por un especialista de machine learning considerando una tasa de éxito del 90%.<br><br>-Evaluación del nivel de precisión del algoritmo al identificar patrones y comportamientos sospechosos después de la integración, revisado por un especialista de machine learning considerando una tasa de éxito del 90%. |

Nota: Elaboración propia

## 1.3 Herramientas y Métodos

En esta sección, se proporcionarán detalles sobre cada herramienta, método y proceso que se puso en marcha para alcanzar los objetivos concretos.

### 1.3.1 Resumen de las herramientas

En la tabla 3, se muestran las herramientas, como también los métodos y procedimientos para cada uno de los resultados establecidos para esta investigación.

■ **Tabla 3: Herramientas, métodos y procedimientos de los resultados**

| **Resultado** | **Herramienta** | **Método y procedimiento** |
|---|---|---|
| R1: Documentación de requerimientos y prototipo de arquitectura del sistema de información. | Microsoft Excel, Microsoft Word | -UML |
| R2: Componente del sistema de información que usa *Smart Contracts* para el almacenamiento de las transacciones en *blockchain*, a fin de garantizar la integridad de los datos sensibles. | -Plataforma *blockchain*: Ethereum, Solidity, Ganache.<br><br>-Herramientas de desarrollo y pruebas: Truffle.<br><br>-Vista de Front-end: Web3.js, Javascript, React js, Solidity<br><br>-Vista de Back end: .Net, Sql<br><br>-Versiones: Github.<br><br>-Diagramas: Lucidchart | -Ciclo de desarrollo iterativo<br><br>-UML |
| R3: Implementación de un algoritmo criptográfico para asegurar el almacenamiento de los datos privados del usuario. | -Vista de Front-end: Javascript, React js.<br><br>-Vista de Back-end: MySQL y .Net (Bibliotecas de encriptación)<br><br>-Versiones: Github.<br><br>-Diagramas: Lucidchart<br><br>-Interfaz: Figma | -Ciclo de desarrollo iterativo |

| | | |
|---|---|---|
| R4: Documentación de requerimientos funcionales y no funcionales del objetivo, y prototipo de la interfaz gráfica del sistema de información. | Microsoft Excel, Microsoft Word<br><br>-Interfaz: Figma<br><br>Diagramas: Lucidchart | -Ciclo de desarrollo iterativo<br><br>-UML |
| R5: Implementación del sistema de información incluyendo la interfaz gráfica y las funcionalidades que la engloba. | -Vista de Front-end: Java, Node.js<br><br>-Vista de Back-end: .Net<br><br>-Versiones: Github.<br><br>-Diagramas: Lucidchart<br><br>-Interfaz: Figma | -Ciclo de desarrollo iterativo |
| R6: Funcionalidad de chat para la interacción directa entre compradores y vendedores. | -Plataformas de Desarrollo Web: React.js, Node.js.<br><br>-Lenguajes de Programación: Java, Javascript.<br><br>-Herramientas de Bases de Datos: MySQL | -Ciclo de desarrollo iterativo |
| R7: Integración de una pasarela de pago como sistema seguro que proteja la información financiera del comprador y ofrezca opciones de pago confiables, como tarjetas de crédito, billeteras digitales o sistemas de pago en línea. | -Pasarelas de Pago: Stripe<br><br>-BackEnd: .Net (Uso de la biblioteca Guid)<br><br>-Versiones: Github.<br><br>-Diagramas: Lucidchart<br><br>-Interfaz: Figma | -Ciclo de desarrollo iterativo |

| | | |
|---|---|---|
| R8: Especificación de requerimientos funcionales y no funcionales. | Microsoft Excel, Microsoft Word | -Ciclo de desarrollo iterativo |
| R9: Recolección y procesamiento de datos de transacciones históricas y en tiempo real para la implementación de un almacenamiento y gestionamiento de medianas cantidades de datos. | Microsoft Excel<br><br>Python | -Ciclo de desarrollo iterativo |
| R10: Selección, análisis y diseño del algoritmo de detección de fraudes capaz de analizar tanto datos de transacciones históricas como información en tiempo real. Este sistema estará diseñado para identificar patrones y comportamientos sospechosos, tales como actividades inusuales, volúmenes extraordinarios de transacciones que pueda indicar actividad fraudulenta | -Lenguajes de Programación: Java, Javascript, Node.js, Python<br>-Bibliotecas de Aprendizaje Automático: TensorFlow.js<br><br>-Plataformas de *Blockchain*: Ethereum, Ganache.<br><br>-Herramientas Específicas para *Blockchain*: Web3.js<br><br>-Versiones: Github.<br><br>-Diagramas: Lucidchart<br><br>-Interfaz: Figma | -Ciclo de desarrollo iterativo |
| R11: Integración del algoritmo de detección de fraudes dentro del sistema de información para mejorar la seguridad de las transacciones en el *e-commerce*. | Python<br><br>-Bibliotecas de Aprendizaje Automático: TensorFlow.js<br><br>-Herramientas de | -Ciclo de desarrollo iterativo |

| | | |
|---|---|---|
| | procesamiento en tiempo real: Apache Kafka<br><br>-Herramientas de Bases de Datos: MySQL<br><br>-Versiones: Github.<br><br>-Diagramas: Lucidchart | |

Nota: Elaboración propia

### 1.3.2 Herramientas

A continuación, se detallan las herramientas utilizadas para alcanzar los resultados esperados en este proyecto.

#### *1.3.2.1 Blockchain*

La tecnología *blockchain* se define como una nueva tecnología basada en hash que está en la base de las plataformas para el comercio y la ejecución de contratos inteligentes, además, es un libro de contabilidad distribuido que permite transacciones sin necesidad de intermediarios (Sullivan & Di Pierro, n.d.).

Entre sus innumerables ventajas se destacan la seguridad, la transparencia, la eficiencia y la eliminación de intermediarios (IBM, n.d.). Además, esta tecnología permite que todas las transacciones sean visibles para todos los participantes de la red y puedan verificar su autenticidad (IBM, n.d.). La tecnología *blockchain* ofrece una robusta capacidad de resistencia a los errores (Habib et al., 2022). Al ser utilizada como un libro de contabilidad abierto, elimina la necesidad de intermediarios para validar o liquidar transacciones, ya que los usuarios pueden observar todo lo que ocurre en una

plataforma de código abierto (Habib et al., 2022). Además, al prescindir de intermediarios, las empresas pueden ahorrar tiempo, dinero y recursos, al tiempo que mejoran la eficiencia de sus operaciones (IBM, n.d.).

Las características de esta tecnología serán importantes para la seguridad tanto de la información sensible, como también la información de las transacciones. Asimismo, se implementará para la integración de diversos componentes y herramientas.

#### *1.3.2.2* Figma

Figma es una herramienta de diseño de interfaz colaborativa que se aloja en la web. Se puede crear, probar y diseñar pantallas de sitios web, aplicaciones móviles y cualquier otra interfaz gráfica interactiva (Centro de Estudios de Innovación, n.d.). En el proyecto, se ha optado por utilizar Figma para la creación de los prototipos de interfaz. Asimismo, se busca una visualización más clara y comprensible de los requisitos del proyecto, por lo que Figma permite crear interfaces detalladas y proporciona una plataforma colaborativa que facilita la comprensión y validación de los requisitos por parte de todos los *stakeholders* involucrados.

#### *1.3.2.3* Criptografía

La criptografía es una rama de las matemáticas, que, al aplicarse a mensajes digitales, proporcionan las herramientas idóneas para solucionar los problemas de la confiabilidad y la autenticidad (Mendívil, I., 1997). La criptografía se emplea en diferentes ámbitos, el comercio electrónico, la seguridad informática, la defensa y la inteligencia ya que permite cifrar y descifrar la información (Universidad VIU., 2021). El cifrado consiste en

transformar la información original en un formato ilegible, mientras que el descifrado consiste en volver a transformar la información cifrada en su formato original (Universidad VIU., 2021).

La criptografía se utilizará para cifrar las transacciones, protegiendo así los datos sensibles, como la información de pago y los detalles del cliente.

#### *1.3.2.4* Ethereum

Ethereum representa una plataforma descentralizada impulsada por tecnología *blockchain*, con la ambición de establecerse como un Internet descentralizado y una tienda de aplicaciones completamente distribuida. En esencia, Ethereum es una red global de computadoras que operan conforme a un conjunto de reglas definidas, denominadas el protocolo Ethereum. Esta red no solo sirve como una infraestructura digital, sino que también se erige como un núcleo vital para diversas comunidades y aplicaciones (Ethereum, 2023).

Esta herramienta se utilizará para crear *Smart Contracts*, así como la implementación de características de la tecnología *blockchain* en transacciones, lo que garantiza un registro público y transparente de todas las operaciones realizadas.

#### *1.3.2.5* Solidity

Solidity destaca como un lenguaje de programación orientado a objetos diseñado específicamente para implementar contratos inteligentes en diversas plataformas *blockchain*, con un enfoque especial en Ethereum (IEBSchool, 2023). Solidity es un lenguaje versátil y seguro, ya que incluye mecanismos como controles de acceso, gestión de excepciones y modificadores que

permiten verificar condiciones antes de ejecutar funciones, lo que fortalece la protección de los contratos inteligentes (IONOS, 2023). Además, su compatibilidad con la Ethereum Virtual Machine (EVM) y su sintaxis similar a lenguajes como JavaScript y C++ facilitan el desarrollo de aplicaciones descentralizadas complejas (IONOS, 2023)

Dado que se ha seleccionado Ethereum como la herramienta para implementar la tecnología *blockchain* en el proyecto, es imprescindible utilizar Solidity para alcanzar nuestros objetivos en el desarrollo del sistema de información.

#### *1.3.2.6* Truffle

Truffle es una suite completa de herramientas diseñada específicamente para el desarrollo de contratos inteligentes en la plataforma Ethereum. Esta herramienta es fundamental en el proceso de desarrollo debido a su capacidad para proporcionar un entorno de desarrollo robusto, un marco de pruebas integral y una canalización de activos dedicada para Ethereum, lo que simplifica significativamente la creación de contratos inteligentes (Kaleido, 2023).

Ofrece una consola interactiva, una herramienta de compilación eficiente y una herramienta de migración que agiliza el proceso de desarrollo en Ethereum. Además, Truffle incorpora un marco de pruebas integrado que permite a los desarrolladores escribir y ejecutar pruebas automatizadas para validar la funcionalidad de sus contratos inteligentes (Kaleido, 2023).

Asimismo, Truffle también incluye Ganache, que se utiliza específicamente para pruebas y desarrollo (Truffle Suite, 2023).

Se utilizará Truffle para llevar a cabo la implementación eficaz de los contratos inteligentes, asegurando una integración fluida con las herramientas de Ethereum y Solidity.

#### *1.3.2.7* Ganache

Ganache es una herramienta fundamental para desarrolladores y entusiastas de Ethereum, ya que posibilita el despliegue de cadenas de bloques localmente. Esta aplicación emula el comportamiento de la cadena de bloques original de Ethereum, permitiendo la personalización de diversos parámetros para adaptarse a las necesidades específicas del usuario. Además de su capacidad para simular la red *blockchain*, Ganache ofrece un seguimiento detallado de los bloques generados, las transacciones realizadas, los contratos inteligentes desplegados y otros eventos relevantes en la red (Taibo Escarramán, A., 2022).

En el contexto de la investigación presente, la implementación de Ganache proporcionará una base sólida para simular el entorno de *blockchain* localmente, lo que simplificará significativamente el desarrollo y pruebas del sistema de información en estudio.

#### *1.3.2.8* Python

Es un lenguaje de programación de alto nivel, *general-purpose* y orientado a objetos, que se utiliza en una amplia variedad de aplicaciones, incluyendo el desarrollo de software, el *machine learning*, la inteligencia artificial, la seguridad informática, entre otros (Amazon Web Services, n.d.). En el desarrollo de este proyecto, se emplea Python como herramienta para llevar a cabo la recolección y procesamiento de datos, así como para la

investigación de posibles algoritmos de *machine learning* junto a la fase de entrenamiento de los modelos debido a su sencillez y eficiencia para la creación de código fuente de la inteligencia artificial.

#### *1.3.2.9* JavaScript

JavaScript es un lenguaje de programación esencial empleado por los desarrolladores para crear páginas web interactivas. Las funciones dinámicas de JavaScript transforman la experiencia del usuario en un sitio web. Este lenguaje permite a los navegadores responder a las interacciones del usuario, modificando la disposición del contenido en tiempo real. Al utilizar JavaScript, se logra una experiencia del usuario más atractiva y fluida, lo que se traduce en un rendimiento superior al implementarlo en el diseño del *front-end* en este proyecto del sistema de información (Amazon Web Services, 2023). Se ha optado por JavaScript en el *front-end* debido a su estructura familiar, basada en la experiencia adquirida en proyectos universitarios anteriores. Esta elección brinda la posibilidad de desarrollar de manera dinámica gracias a su amplia variedad de bibliotecas disponibles.

#### *1.3.2.10* Web3.js

Web3.js es una biblioteca de JavaScript que ofrece APIs esenciales para conectarse y comunicarse con los nodos de la red Ethereum. Considerada una biblioteca importante para interactuar con la *blockchain* de Ethereum, esta es fundamental en el desarrollo de aplicaciones descentralizadas en esta plataforma innovadora. Web3.js no solo facilita la creación de interfaces de usuario, sino también la interacción sin problemas con contratos inteligentes y otros elementos clave de Ethereum (McCubbin,

G., 2023).

Debido a su buena comunicación con los nodos de la red Ethereum, Web3.js se convierte en una herramienta altamente efectiva, ya que ofrece una integración sin problemas entre el código JavaScript y la plataforma Ethereum, lo que la hace sumamente rentable.

#### *1.3.2.11* **React js**

React.js es una fuente de código abierto de JavaScript y basada en componentes (React, 2023). Para este proyecto, se optará por usar React para el diseño del *front-end* debido a sus capacidades para crear interfaces de usuario rápidas y dinámicas. Esta herramienta proporciona la ventaja de construir componentes HTML reutilizables y anidados de manera sencilla y eficiente (React, 2023).

Gracias al dominio previo de la biblioteca React.js obtenido en proyectos universitarios anteriores, su aplicación en el desarrollo del sistema de información se realizará de forma sencilla y eficiente. Además, se requieren componentes dinámicos para llevar a cabo este desarrollo de manera efectiva.

#### *1.3.2.12* **.Net**

.NET es una plataforma para desarrolladores de código abierto, multiplataforma y gratuita diseñada para compilar muchos tipos de aplicaciones diferentes. Puede ejecutar programas escritos en varios lenguajes, siendo C# el más popular. La plataforma .NET se ha diseñado para ofrecer productividad, rendimiento, seguridad y confiabilidad. La adaptabilidad entre dominios de programación (nube, cliente, juegos) está

habilitada con implementaciones especializadas del modelo de programación de uso general (Microsoft, 2024).

Para el presente proyecto, se busca aprovechar el rendimiento y adaptabilidad que propone .Net para el ámbito de *Back-end*, así como también aprovechar los conocimientos previos que presenta el tesista para su implementación.

#### *1.3.2.13* Github

GitHub es una plataforma basada en la nube diseñada para el desarrollo de software y la gestión de versiones utilizando Git. Esta herramienta es esencial para los desarrolladores, ya que les permite almacenar, administrar y colaborar en su código de manera eficiente. Al proporcionar un sólido sistema de control de versiones, GitHub facilita el seguimiento y la colaboración en proyectos, lo que garantiza una coordinación efectiva entre los miembros del equipo. Esta funcionalidad es esencial para cualquier proyecto de desarrollo de software, permitiendo una colaboración fluida y el mantenimiento eficiente del código base (TechTarget, 2023).

Al tener experiencia en el uso de esta plataforma, resulta sencillo su implementación para almacenar el progreso de los códigos fuente del proyecto.

#### *1.3.2.14* Lucidchart

Lucidchart es una aplicación de diagramación basada en la nube que permite a los usuarios colaborar visualmente en la creación, revisión y compartición de gráficos y diagramas para mejorar procesos, sistemas y

estructuras organizacionales (Lucidchart, n.d.). Se usará esta herramienta debido a que permite visualizar los flujos de los módulos y componentes del sistema de mejor manera.

#### *1.3.2.15* Apache Kafka

Apache Kafka es una plataforma de procesamiento de eventos y almacenamiento distribuido de datos en tiempo real de código abierto, desarrollada por la *Apache Software Foundation* y escrita en Java y Scala, pero también está diseñada para JavaScript. Se destaca como un sistema de almacenamiento distribuido que permite a los usuarios manejar volúmenes masivos de datos en tiempo real. La alta escalabilidad y baja latencia de Kafka garantizan que los usuarios puedan procesar y analizar datos en tiempo real de manera efectiva y eficiente (Amazon Web Services, 2023).

Para el presente proyecto, se necesitará de integraciones de módulos de diferentes aspectos de la operación, como procesamiento de pagos, por lo que Apache Kafka actúa como un intermediario de datos en tiempo real, permitiendo la integración sin problemas entre estos componentes. Además, facilita el flujo continuo de datos en tiempo real, lo que significa que se puede transmitir información relevante sobre las transacciones del *e-commerce* de manera instantánea.

#### *1.3.2.16* Node.js

Node.js es un ambiente de ejecución de JavaScript de código abierto y multiplataforma, popular para muchos tipos de proyectos. Una aplicación Node.js se ejecuta en un único proceso, evitando crear nuevos hilos para cada

solicitud. Utiliza primitivas de E/S asíncronas en su biblioteca estándar para evitar que el código se bloquee, y generalmente las bibliotecas en Node.js están escritas con arquetipos sin bloqueo. Además, los programadores frontend que redactan JavaScript para el navegador también tienen la posibilidad de redactar el código en el lado del servidor sin necesidad de aprender otro lenguaje (Node.js, 2022). En el contexto de la presente investigación, la implementación de Node.js será fundamental para ejecutar una variedad de proyectos cruciales relacionados tanto con Ethereum como con JavaScript.

#### *1.3.2.17* **MySQL**

MySQL es la base de datos de código abierto más popular del mercado, incluye numerosas funciones desarrolladas en estrecha colaboración con los usuarios durante más de 25 años. Por lo tanto, la gran mayoría de aplicaciones o lenguajes de programación son compatibles con MySQL Database (Oracle Corporation, 2023). La robusta arquitectura del *back-end* se convierte en un componente importante para el almacenamiento de datos en este proyecto específico. Su flexibilidad y confiabilidad hacen de MySQL una elección clave para gestionar datos de forma eficiente y escalable en este desarrollo.

#### *1.3.2.18* **TensorFlow.js**

TensorFlow.js es una potente biblioteca de JavaScript diseñada para el aprendizaje automático tanto en navegadores web como en Node.js. Con esta herramienta, es posible desarrollar modelos de aprendizaje automático directamente en JavaScript y utilizarlos sin problemas en el navegador o en

entornos Node.js. Una de las características destacadas de TensorFlow.js es su capacidad para permitir a los desarrolladores crear y entrenar modelos de aprendizaje automático de forma local en el navegador, eliminando así la necesidad de enviar datos a un servidor externo para su procesamiento. Además, la biblioteca proporciona una variedad de modelos pre-entrenados que pueden aplicarse a tareas comunes de aprendizaje automático, como la clasificación de imágenes y el procesamiento del lenguaje natural, lo que simplifica significativamente el proceso de desarrollo (TensorFlow, 2023).

Se utilizará TensorFlow.js, en este proyecto, para implementar algoritmos de aprendizaje automático que analicen los patrones de comportamiento de los usuarios en tiempo real y modelos predictivos que ayuden a prever posibles actividades fraudulentas antes de que ocurran.

#### *1.3.2.19* **Stripe**

Stripe es una plataforma líder en procesamiento de pagos en línea, permitiendo a empresas y autónomos gestionar pagos en Internet y realizar transferencias a nivel global (Stripe, 2023). Esta herramienta brinda una forma segura y sencilla para que los comerciantes acepten pagos en línea. Además de facilitar transacciones seguras, Stripe ofrece una amplia gama de herramientas diseñadas para asistir a las compañías en la lucha contra el fraude, emitir facturas, generar tarjetas virtuales y físicas, reducir fricciones en el proceso de compra y administrar las finanzas corporativas. Stripe es una plataforma de pagos en línea ampliamente utilizada en todo el mundo, compatible con múltiples monedas y canales, incluyendo sitios web, aplicaciones móviles y plataformas de comercio electrónico y también

proporciona opciones de financiación y simplifica la administración de gastos empresariales (Stripe, 2023).

Se utilizará Stripe, en el presente proyecto, para aceptar pagos con tarjeta de crédito y débito de los clientes de manera segura, protegiendo así la información financiera sensible de los usuarios durante las transacciones.

#### *1.3.2.20* Algoritmo de Detección de Fraude

Un algoritmo de detección de fraude es un conjunto de reglas y técnicas matemáticas que se utilizan para identificar patrones sospechosos en grandes conjuntos de datos y detectar posibles fraudes (SEON, 2018). Los algoritmos de detección de fraude son importantes porque permiten a las empresas identificar anomalías en tiempo real y prevenir actividades maliciosas que podrían comprometer tanto la seguridad financiera como la confianza del cliente. En particular, el uso de técnicas de machine learning se ha consolidado como una estrategia eficaz, ya que permite analizar grandes volúmenes de datos, detectar patrones atípicos y adaptarse a nuevas tácticas de fraude, reduciendo el riesgo de pérdidas económicas y mejorando la experiencia del usuario (Stripe, 2023).

Los algoritmos de detección de fraudes se aplican para identificar en tiempo real transacciones sospechosas en el entorno digital, clasificándolas como legítimas, sospechosas o fraudulentas. Estos algoritmos pueden aprender de experiencias previas y tomar predicciones en tiempo real. De esta manera, pueden comprender cómo se llevan a cabo las actividades fraudulentas en el ámbito cibernético (Akhilomen, 2013).

#### *1.3.2.21* Detección de Anomalías

La detección de anomalías es una técnica que se utiliza para identificar valores atípicos o desviaciones inesperadas en un conjunto de datos (Amazon Web Services, 2023). Se utiliza esta técnica para alertar sobre cambios inesperados en los datos y proteger el sistema en tiempo real frente a instancias que podrían provocar pérdidas financieras significativas, violaciones de datos y otros eventos perjudiciales (Amazon Web Services, 2023).

Esta técnica será empleada para dar apoyo al algoritmo de detección de fraudes, ya que tiene la capacidad de identificar patrones inusuales o comportamientos atípicos en los datos de las transacciones en tiempo real.

#### *1.3.2.22* Registro de eventos

El registro de eventos es una importante herramienta empleada para capturar y preservar datos relativos a eventos críticos tanto de software como de hardware. Estos eventos pueden originarse en diversas fuentes y se consolidan en un único repositorio conocido como "registro de eventos". Además, este sistema establece un enfoque estandarizado y centralizado que permite que las aplicaciones se registren y puedan ser posteriormente analizadas a través de estos eventos (Microsoft Learn, 2021).

Se implementará el Registro de Eventos para documentar de manera inmutable todas las transacciones llevadas a cabo en el *e-commerce*. Esta práctica garantizará la transparencia, fortaleciendo así la integridad de los datos y fomentando la confianza del cliente en el sistema de información.

### 1.3.3 Métodos

A continuación, se detallan los métodos utilizados para alcanzar los resultados esperados en este proyecto.

#### 1.3.3.1 PMBOK Guide (Project Management Body of Knowledge)

El PMBOK 7 desarrollado por el *Project Management Institute* (PMI), se destaca en cómo enfocar los proyectos para dotarlos de valor, cómo una guía de buenas prácticas y estándar reconocido internacionalmente en el campo de la gestión de proyectos, proporcionando un conjunto detallado de prácticas y conocimientos para la gestión de proyectos, buscando ser más universales y adaptados a las necesidades de los proyectos (*IEBS Business School*, 2024).

En su estructura, el PMBOK Guide identifica cinco grupos clave de procesos, conocidos como Grupos de Procesos de la Dirección de Proyectos. Cada uno de estos grupos reúne una serie específica de procesos que son fundamentales para el éxito en la ejecución de proyectos (*Project Management Institute*, 2021).

- **Grupo de Procesos de Inicio:** son aquellos procesos realizados para definir un nuevo proyecto o una nueva fase de un proyecto existente al buscar y obtener la autorización para iniciar el proyecto o fase. Para este proyecto se solicitó la aprobación del docente del curso, del asesor de tesis y del comité de tesis.
- **Grupo de Procesos de Planificación:** son procesos requeridos para establecer el alcance del proyecto, refinar los objetivos y definir el

curso de acción requerido para alcanzar los objetivos propuestos del proyecto. En este proyecto, se tuvo el Entregable 1.1, el cual está como anexo 1 en el presente documento, para poder establecer las planificaciones correspondientes.

- **Grupo de Procesos de Ejecución:** son procesos realizados para completar el trabajo definido en el plan del proyecto.
- **Grupo de Procesos de Monitoreo y Control:** son procesos requeridos para rastrear, revisar y regular el progreso y el desempeño del proyecto. En este presente proyecto, se tuvo el monitoreo mediante la supervisión del asesor y profesores del curso.
- **Grupo de Procesos de Cierre de fase o de proyecto:** son procesos realizados para finalizar todas las actividades a través de todos los Grupos de Procesos, a fin de cerrar formalmente el proyecto o fase. Para esta fase final se recopila y entrega toda la documentación necesaria al momento de la exposición de la tesis.

#### 1.3.3.2 Ciclo de desarrollo iterativo

En este proyecto, se adoptó el ciclo de desarrollo iterativo para fraccionar los progresos del proyecto en entregas más manejables. Para cada una de estas entregas, se llevó a cabo un proceso correspondiente que incluyó la planificación, el diseño, la implementación y las pruebas, todo dentro de un marco de tiempo predeterminado según el cronograma establecido en el plan de proyecto. Además, al concluir cada iteración, se presentó el avance del documento correspondiente para su revisión y validación por parte de

expertos, incluyendo el asesor de la tesis. Estas validaciones garantizan la calidad y la adecuación de los resultados obtenidos antes de avanzar a la siguiente fase del proyecto.

#### 1.3.3.3 UML (Unified Modeling Language)

El Lenguaje Unificado de Modelado (UML) fue creado para forjar un lenguaje de modelado visual común y semántica y sintácticamente rico para la arquitectura, el diseño y la implementación de sistemas de software complejos, tanto en estructura como en comportamiento. Los diagramas UML representan los límites, la estructura y el comportamiento del sistema y de los objetos que contiene. Aunque UML no es un lenguaje de programación, existen herramientas que permiten generar código en diversos lenguajes a partir de sus diagramas. UML está estrechamente relacionado con el análisis y diseño orientados a objetos (Lucidchart, 2023). En el contexto de este proyecto de Tesis, UML se emplea para crear diagramas específicos de estructura y diseño, facilitando una comprensión clara y concisa de la planificación y la arquitectura del sistema de información propuesto.

# Capítulo 2. Marco Legal/Regulatorio/Conceptual/otros

En este capítulo, se aborda y presenta el marco conceptual, los conceptos relevantes y los ejemplos ilustrativos que conforman el fundamento teórico de la investigación sobre la implementación de un *e-commerce* basado en tecnología *blockchain* y algoritmos de detección de fraude. A través de esta estructura, se pretende ofrecer una base sólida para comprender de manera correcta los términos usados en esta investigación.

## 2.1 Definiciones

### 2.1.1 *E-commerce* (Comercio Electrónico)

El comercio electrónico, conocido como *e-commerce*, abarca la compra y venta de bienes y servicios a través de Internet, y prácticamente cualquier producto o servicio imaginable está disponible mediante este tipo de transacciones (Investopedia, 2023). El comercio electrónico implica el uso de transacciones electrónicas, como pagos en línea y firmas digitales, para facilitar las transacciones comerciales (Jain, Malviya, Arya, 2021).

Una de las principales ventajas del comercio electrónico es su capacidad para ampliar el alcance del negocio a nivel global. A diferencia de una tienda física, una plataforma de e-commerce permite ofrecer productos o servicios a clientes ubicados en distintas regiones del mundo, sin las limitaciones geográficas tradicionales. Esta expansión del mercado brinda mayores oportunidades de crecimiento, ya que el negocio puede operar las 24 horas del día y llegar a públicos más amplios, aprovechando herramientas digitales para posicionarse en nuevos nichos y competir en entornos internacionales (Instituto Europeo de Posgrado, n.d.).

Además, el *e-commerce* ofrece la ventaja significativa de reducir drásticamente los costos operativos para las empresas. Al eliminar la necesidad de mantener una tienda

física, se evitan gastos relacionados con alquileres, personal y costos operativos fijos (Bayona, S., y Estrada, R., 2020).

Ciertamente, muchas empresas de renombre han adoptado exitosamente el comercio electrónico como parte fundamental de su estrategia de ventas y servicios. Ejemplos notables a nivel global incluyen a Amazon, Alibaba, MercadoLibre y Walmart (Seeking Alpha, 2022, Lustig, N., 2018). Además, en el contexto peruano, empresas como Wong, Inkafarma, BCP, Alicorp y Molitalia también han implementado esta tendencia, aprovechando las oportunidades que ofrece el comercio electrónico (Méndez Pérez, n.d.).

### 2.1.2 Seguridad de Información

La seguridad de la información es el conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información. La seguridad de la información es importante para las empresas y organizaciones, ya que busca mantener los tres pilares de la seguridad de información: confidencialidad, la disponibilidad e integridad de los datos (Microsoft, n.d.). En el contexto de la implementación de un e-commerce, la seguridad de la información es fundamental para garantizar la integridad y la privacidad de los datos de los clientes y de la empresa. Para ello, es indispensable adoptar medidas como el uso de certificados SSL/TLS, autenticación multifactor, plataformas de pago con estándares PCI-DSS, y software actualizado, lo que contribuye a proteger los datos sensibles durante las transacciones y fortalece la confianza del consumidor en los entornos digitales (Conekta, 2023).

### 2.1.3 Privacidad de Datos Personales

La privacidad de los datos personales se define como la capacidad de los individuos de controlar la recopilación, el uso y la difusión de su información

personal. La preocupación por este tema surge cuando los usuarios sienten que su información personal se recopila, utiliza o divulga sin su conocimiento o consentimiento, por lo tanto, se destaca la importancia de la privacidad de la información personal para mantener la confianza entre individuos y organizaciones (Milberg et al., 1995). En el contexto del comercio electrónico, esta confianza se refuerza mediante políticas claras sobre el uso de los datos, las cuales establecen que el tratamiento de los datos personales debe realizarse con el consentimiento expreso del usuario, con finalidades específicas y respetando su derecho a acceder, rectificar, cancelar u oponerse al uso de su información (CAPECE, 2023).

### 2.1.4 Transparencia en las transacciones

En el contexto de la tecnología *blockchain*, la transparencia adquiere una dimensión específica, refiriéndose a la capacidad de los participantes del mercado para visualizar y verificar las transacciones registradas en la cadena de bloques. Este nivel de transparencia se materializa debido a que la información se replica entre todos los usuarios y se verifica de manera consensuada (PwC., 2021).

### 2.1.5 Intermediarios en transacciones

Los intermediarios en transacciones son entidades o individuos que actúan como puente entre dos partes que desean realizar una transacción. Su función principal es facilitar el proceso de compra y venta, asegurando que ambas partes cumplan con sus respectivas obligaciones. Los intermediarios pueden ofrecer una variedad de servicios, tales como asesoramiento, negociación, mediación, y garantizar la seguridad y legitimidad de la transacción. Los intermediarios en transacciones son importantes porque permiten a los distintos participantes del mercado realizar transacciones de manera más eficiente y efectiva (Economipedia, 2016).

### 2.1.6 Ley de Protección de Datos Personales

La Ley N° 29733 tiene como objetivo principal garantizar la privacidad y protección de los datos personales de los ciudadanos peruanos. Además, se presentan medidas de protección como el consentimiento, es decir, las empresas y organizaciones obtengan el consentimiento de las personas antes de recopilar, almacenar o utilizar sus datos personales. Asimismo, se implementan principios de protección para el tratamiento de datos personales, incluyendo la finalidad, proporcionalidad, calidad, seguridad, confidencialidad y consentimiento (Gobierno del Perú, 2011). Por lo tanto, es un marco normativo que los sistemas de información dentro del *e-commerce* deben priorizar.

### 2.1.7 Ley de Protección al Consumidor en el Perú

La Ley N° 29571 tiene como objetivo principal proteger los derechos e intereses de los consumidores y regular las relaciones entre consumidores y proveedores de bienes y servicios. Además, se consideran los Derechos Básicos del Consumidor, incluyendo el derecho a la información, el derecho a la elección, el derecho a la seguridad, el derecho a la protección contra publicidad engañosa o abusiva, y el derecho a la reparación o compensación por productos o servicios defectuosos. También, se prohíbe prácticas comerciales desleales o abusivas, como la publicidad engañosa, la venta atada, el sobreendeudamiento y la discriminación injusta. Asimismo, se establece la responsabilidad de los proveedores por productos o servicios defectuosos y les obliga a ofrecer información precisa y completa sobre los productos o servicios que ofrecen (Presidente La República, E. de., n.d.).

### 2.1.8 Ley Complementaria de la Ley de Protección al Consumidor en Materia de Servicios Financieros

La Ley Nº 28587 es una normativa en el Perú que tiene como objetivo proteger a los consumidores en el ámbito de los servicios financieros. Establece que las empresas deben brindar información clara, precisa y oportuna sobre los productos y servicios financieros que ofrecen, así como sobre las condiciones y costos asociados a los mismos. Asimismo, establece que las empresas deben informar a los usuarios sobre sus derechos y obligaciones en relación con los productos y servicios financieros (Congreso del Perú, 2005).

### 2.1.9 Acceso no autorizado

El acceso no autorizado es el intento o logro de ingresar a un sistema, red, aplicación o base de datos sin el permiso del propietario legítimo. Este tipo de

intrusión busca vulnerar la confidencialidad, integridad o disponibilidad de la información, aprovechando fallas técnicas, errores humanos o mecanismos de seguridad débiles. Puede llevarse a cabo mediante técnicas como phishing, malware, fuerza bruta o la explotación de vulnerabilidades. Las consecuencias incluyen robo de datos, daños reputacionales y pérdidas económicas, por lo que su prevención requiere contraseñas fuertes, autenticación multifactor, actualizaciones constantes y educación en ciberseguridad. (VPN Unlimited, n.d.)

### 2.1.10 Integridad de la información

La integridad de la información en un sistema de información se refiere a asegurar la exactitud y fiabilidad de los datos almacenados. Este aspecto es fundamental para la seguridad de la información, junto con la confidencialidad y la disponibilidad (ESGinnova Group, 2018).

### 2.1.11 Intermediarios vulnerables

Los intermediarios vulnerables en el comercio electrónico son aquellos individuos o entidades que presentan una mayor susceptibilidad a sufrir o provocar problemas o riesgos durante el proceso de compra y venta de bienes y servicios en línea (Moreno Sánchez, J., 2021).

### 2.1.12 Autenticación débil

La autenticación débil en un sistema de información se refiere al uso de mecanismos poco seguros para verificar la identidad de un usuario, lo que expone al sistema a riesgos significativos de acceso no autorizado. El ejemplo más común de autenticación débil es el uso exclusivo de nombres de usuario y contraseñas, especialmente cuando estas contraseñas son fáciles de adivinar (como “123456” o

“contraseña”), se reutilizan en múltiples servicios o no se almacenan adecuadamente (Auth0, 2025).

### 2.1.13 Brecha de seguridad

Una brecha de seguridad en un sistema de información es un incidente que facilita el acceso no autorizado a datos informáticos, aplicaciones, redes o dispositivos, lo que puede desembocar en la exposición, robo o manipulación de información confidencial o sensible (Kaspersky, n.d.).

### 2.1.14 Daño reputacional

El daño reputacional se refiere al impacto negativo en la percepción que el público tiene de una organización, ya sea por sus acciones o inacciones. Este deterioro puede acarrear consecuencias significativas para la empresa, como la disminución de la lealtad y confianza de los clientes, la caída en las ventas e incluso acciones legales. Ocurre cuando la reputación de una empresa se ve afectada por una percepción negativa del público en general (Cortés, N., 2023).

# Capítulo 3. Estado del Arte

## 3.1 Introducción

El propósito de este capítulo es realizar un análisis detallado de las tecnologías pertinentes y sus características a través de una investigación basada en preguntas de revisión. Este análisis se llevará a cabo utilizando una estrategia de revisión, un formulario de extracción y criterios de inclusión y exclusión. El objetivo final es obtener respuestas a las preguntas planteadas en la revisión, con el fin de establecer una base sólida para el desarrollo del proyecto de investigación.

## 3.2 Objetivos de revisión

Por un lado, a través de la revisión teórica, se analiza críticamente las fuentes de información existentes con la finalidad de obtener bases conceptuales y teóricas para la investigación, asimismo, se identifican similitudes y diferencias entre las investigaciones previas y ayudan a establecer las bases teóricas para el tema de investigación actual (Universidad Autónoma de Barcelona, 2020, p. 3,4). Para este documento, se utilizó una revisión sistemática, siguiendo un enfoque similar al de Kitchenham (Kitchenham, 2004, p. 1,2), para recopilar y analizar la información existente sobre los conceptos de la tecnología de *blockchain*, incluyendo definiciones, tipos, funcionalidades y formas de implementación. Esto proporciona una base de investigación fidedigna y rigurosa.

Por otra parte, a través de una revisión empírica, es posible adquirir pruebas concretas y verificables relacionadas con el tema de investigación en cuestión (Lifeder, 2022). En este sentido, la implementación de esta metodología se convierte en un recurso importante, ya que tiene como objetivo proponer la aplicación conjunta de la tecnología *blockchain* y un algoritmo de detección. Este planteamiento pretende

fortalecer la seguridad de los sistemas de información en el contexto del comercio electrónico, sustentándose en conclusiones y teorías debidamente formuladas.

## 3.3 Preguntas de revisión

Con el objetivo de adquirir información relevante para el tema de investigación, se llevarán a cabo preguntas de revisión.

- P1: ¿Cuáles son los desafíos y vulnerabilidades más comunes en términos de seguridad de información que los sistemas de comercio electrónico suelen enfrentar en la actualidad?
- P2: ¿Cuáles son las medidas de seguridad de información que están siendo actualmente empleadas en los sistemas de información orientados al comercio electrónico?
- P3: ¿Cómo contribuye la tecnología *blockchain* a mejorar la seguridad de la información durante las transacciones y cuáles son las características específicas que esta tecnología aporta a estas medidas de seguridad?
- P4: ¿Cuáles serían los beneficios de incorporar la tecnología *blockchain* en el fortalecimiento de la seguridad de las transacciones en el ámbito del comercio electrónico?

## 3.4 Estrategia de revisión

Con el propósito de identificar las palabras clave relacionadas con sistemas de información que refuercen la seguridad y la integridad de las transacciones en el contexto del comercio electrónico, se empleó el enfoque PICOC, el cual es ampliamente utilizado en la investigación para formular preguntas clínicas y estructurar la búsqueda bibliográfica. Asimismo, este método, que asiste en la adquisición y resolución de información relevante, se basa en los criterios de población, intervención, comparación, resultado y contexto (TutFG, n.d.). En la tabla 4, se busca obtener la cadena de búsqueda que puedan resolver las preguntas establecidas.

- **Tabla 4: Criterios de PICOC 1**

| Criterios | Descripción |
|---|---|
| Población | Sistema de información o Sistemas electrónicos de información o producto de software |
| Intervención | Seguridad de la información |
| Comparación | No aplica debido a que no se busca tener una comparación, sino una mejora. |
| Salida | Efectividad de las medidas de seguridad de la información |
| Contexto | Comercio electrónico |

Nota: Elaboración propia.

A continuación, en la tabla 5, se presentará el método PICOC con las palabras en inglés, las cuales serán de apoyo para el desarrollo de la cadena de búsqueda de la tabla anterior.

- **Tabla 5: Criterios de PICOC 1 (Formato en inglés)**

| Criterios | Descripción |
|---|---|
| Población | *Information system, electronic information systems, Product software* |
| Intervención | *Information security* |
| Comparación | No aplica. |
| Salida | *Effectiveness of information security measures.* |
| Contexto | *E-commerce* |

Nota: Elaboración propia.

Además, dado que los resultados derivados del criterio PICOC previo no aborda en la totalidad las interrogantes planteadas, se optó por elaborar una tabla adicional que permitiera dar cabida a la resolución completa de dichas preguntas. En la tabla 6, se expone la aplicación del segundo criterio del enfoque PICOC.

- **Tabla 6: Criterios de PICOC 2**

| Criterios | Descripción |
|---|---|
| Población | Sistema de información o producto de software o software |
| Intervención | Tecnología *blockchain* o algoritmo de detección |
| Comparación | No aplica. |
| Salida | Reducción de fraude o protección de datos personales o integridad transaccional |
| Contexto | Comercio electrónico |

Nota: Elaboración propia.

En la tabla 7, se muestra el procedimiento PICOC, acompañado de las palabras en inglés empleadas para la elaboración de la cadena de búsqueda de la tabla previa.

- **Tabla 7: Criterios de PICOC 2 (Formato en inglés)**

| Criterios | Descripción |
|---|---|
| Población | *Information system, Product software* |
| Intervención | *blockchain technology, detection algorithm* |
| Comparación | No aplica debido a que no se busca tener una comparación, sino una mejora. |
| Salida | *Reduction of fraud or protection of personal* |

| | |
|---|---|
| | *data or transactional integrity* |
| Contexto | *E-commerce* |

Nota: Elaboración propia.

### 3.4.1 Motores de búsqueda a usar

Con el propósito de llevar a cabo la exploración de la literatura, la parte integral de la revisión sistemática, y de abordar las interrogantes planteadas en este documento, se emplearon dos fuentes de datos tecnológicas de gran relevancia como las principales fuentes de información para esta investigación: Scopus y ScienceDirect.

### 3.4.2 Cadenas de búsqueda a usar

En esta sección, dentro de la tabla 8, se crearon las cadenas de búsqueda mediante la combinación de términos que fueran sinónimos o pertenecieran a la misma categoría, utilizando el operador "*OR*", y para conectar las distintas categorías se empleó el operador "*AND*".

- **Tabla 8: Cadenas de búsquedas**

| ID | Construcción | Cadenas generales básicas de búsqueda | Cantidad de estudios primarios seleccionados |
|---|---|---|---|
| 1 | *(P AND I)* | *("Information system" OR "Electronic information systems" OR "product software" OR "software") AND* | 3 |

| | | | |
|---|---|---|---|
| | | *(("Information security" OR "Effectiveness of information security measures") AND ("e-commerce"))* | |
| 2 | *(P AND I)* | *(“Information system” OR “Product software”) AND ((“blockchain technology” OR “detection algorithm”) AND ((“Reduction of fraud” OR “Protection of personal data” OR “transactional integrity”) OR "e-commerce"))* | 7 |

Nota: Elaboración propia

Es fundamental destacar que al realizar una búsqueda en Scopus, se debe introducir los términos clave en la sección denominada "*Search documents*". En el caso de ScienceDirect, es necesario ingresar los términos en el campo designado como "*Find articles with these terms*".

Para cada una de las bases de datos mencionadas anteriormente, se colocaron las siguientes cadenas de búsqueda presentadas en la tabla 9.

- **Tabla 9: Cadenas de búsquedas para cada base de datos**

| Base de datos | Cadena de búsqueda | Apartado de búsqueda |
|---|---|---|

| | | |
|---|---|---|
| Scopus | *TITLE (("Information system" OR "Electronic information systems" OR "product software" OR “software”) AND (("Information security" OR "Effectiveness of information security measures") AND ("e-commerce")))* | *Search Documents* |
| ScienceDirect | *TITLE = ((“Information system” OR “Product software”) AND ((“blockchain technology” OR “detection algorithm”) AND ((“Reduction of fraud” OR “Protection of personal data” OR “transactional integrity”) OR "e-commerce")))* | *Find articles with these terms* |

Nota: Elaboración propia

Posteriormente, se realizó la búsqueda con la cadena dentro de las bases de datos y se obtuvieron los siguientes resultados en la tabla 10.

- **Tabla 10: Cantidad de documentos por motor de búsqueda**

| Motor de búsqueda | Cantidad de documentos de la cadena 1 | Cantidad de documentos de la cadena 2 |
|---|---|---|
| Scopus | 24 | 13 |
| ScienceDirect | 72 | 59 |
| **Total** | 96 | 72 |

Nota: Elaboración propia

## 3.5 Formulario de extracción

En esta parte y dentro de la tabla 11, se exhibirá el formato de extracción diseñado para responder las interrogantes establecidas en el segundo apartado del presente documento sobre la revisión sistemática, fundamentado en los documentos identificados.

■ **Tabla 11: Estructura del formulario de extracción**

| Campo | Descripción | Pregunta |
|---|---|---|
| ID | Por ej.: D001 | General |
| Título | Título del documento | General |
| Tipo de documento | Por ej.: Artículo, Revista, Tesis, Informe de investigación, Libro de investigación, Memoria de conferencia, entre otros | General |
| Autor(es) | Nombre del autor o autores | General |
| Año de publicación | Año de publicación del documento | General |
| Motor de búsqueda | Nombre del motor de búsqueda | General |
| Abstract | Resumen descriptivo del documento | General |
| Desafíos en términos de seguridad de información | ¿Cuáles son los desafíos y vulnerabilidades presentes en la seguridad de información que los sistemas de comercio electrónico enfrentan? | P1 |
| Vulnerabilidades en términos de seguridad de información | ¿Cuáles son las vulnerabilidades presentes en la seguridad de información que los sistemas de comercio electrónico enfrentan? | P1 |
| Aspectos de la seguridad de información | ¿Qué medidas de la seguridad de información se | P2 |

| | | |
|---|---|---|
| | pueden extraer? | |
| Uso de la tecnología *blockchain* | ¿Cuál es la funcionalidad y característica de la tecnología *blockchain* en la seguridad de información durante las transacciones? | P3 |
| Beneficios de la tecnología *blockchain* | ¿Cuáles son los beneficios que se muestran en el uso de la tecnología *blockchain*? | P4 |

Nota: Elaboración propia

## 3.6 Criterios de inclusión/Criterios de exclusión

Con la finalidad de poder seleccionar las literaturas de mayor importancia entre los resultados obtenidos en la búsqueda previa con la cadena, se seleccionaron criterios de inclusión y exclusión. Estos criterios ayudan a poder reducir e incluir los documentos más relevantes a revisar para el tema de investigación.

### 3.6.1 Criterio de inclusión

Las características específicas que los documentos deben contener para ser considerados elegibles o adecuados para formar parte de las fuentes relevantes y representativas para el tema de investigación son las siguientes:

- Los documentos deben estar escritos en inglés o en español.
- La fecha de publicación de los documentos debe estar dentro del rango temporal de 2018 a 2023 debido a que se tendrá una información más actualizada sobre la investigación.
- Tener acceso al texto completo del documento sin necesidad de realizar un pago para obtenerla.

- Los documentos deben haber sido citados por más de un artículo, informe o documento de tesis, esto ofrece más seguridad en la selección del estado del arte.
- Los documentos nuevos que carecen de citas deben incluir un *abstract* que contribuya significativamente al tema en cuestión para su consideración.
- Los documentos deben estar dedicados al tema de la seguridad de información o a un sistema de información.
- Los documentos deben estar enfocados en el contexto de *e-commerce*.
- Los documentos deben presentar la implementación de la tecnología *blockchain* dentro de su investigación.
- Se usaron documentos sobre artículos académicos para esta investigación debido a que proporcionan información concisa y precisa.

### 3.6.2 Criterio de exclusión

Con las siguientes características, se busca que los documentos sean de aporte científico confiable que puedan demostrar la validez y confiabilidad de los resultados de esta investigación:

- Los documentos considerados literatura gris, es decir, aquellos que no son fácilmente accesibles a través de los canales de publicación tradicionales, como artículos de revistas académicas o libros y que no necesariamente presentan un autor explícito debido a que no garantizan citaciones formales.
- Los documentos que no estén directamente relacionados con el tema de estudio, es decir, aquellos que no aborden la tecnología *blockchain*, algoritmos de detección y *e-commerce* en su título o *abstract*.

- Los documentos duplicados que generan confusiones o inconsistencia de información.

### 3.7 Estudios Primarios

En esta sección, se presentan los estudios primarios que ofrecerán apoyo en la resolución de las preguntas planteadas. Esta selección se ha elaborado mediante la revisión de los títulos y *abstract*, teniendo en cuenta los criterios de inclusión y exclusión. Para una mejor organización, la información se presentará en la tabla 12:

■ **Tabla 12: Listado de Estudios Primarios identificados**

| ID | Títulos de la publicación | Autor | Citación en formato APA | Año | Fuente |
|---|---|---|---|---|---|
| 1 | *Determinants of consumers' adoption intention for blockchain technology in E-commerce* | Ali Esfahbodi, Gu Pang, Liuhan Peng | *Esfahbodi, A., Pang, G., & Peng, L. (2022). Determinants of consumers' adoption intention for blockchain technology in E-commerce. Journal of Digital Economy, 1(2), 89–101.* | 2022 | ScienceDirect |
| 2 | *The impact of blockchain on e-commerce: A framework for salient research topics* | Horst Treiblmaier, Christian Sillaber | *Treiblmaier, H., & Sillaber, C. (2021). The impact of blockchain on e-commerce: A framework for salient research topics. Electronic Commerce Research and Applications, 48.* | 2021 | ScienceDirect |
| 3 | *Current State and Trends in the Development of* | Valentyna Pleskach, Viktor Krasnoshchok, Mariia Melnyk, Svitlana Klymenko, | *Pleskach, V., Krasnoshchok, V., Melnyk, M., Klymenko, S., & Tumasonis, R. (2022). Current State and Trends in* | 2021 | ScienceDirect |

| | | | | | |
|---|---|---|---|---|---|
| | *E-Commerce Software Protection Systems* | Romanas Tumasonis | *the Development of E-Commerce Software Protection Systems*. | | |
| 4 | *A Blockchain, Smart Contract and Data Mining Based Approach toward the Betterment of ECommerce* | Tahmid Hasan Pranto, Abdulla All Noman, Mustafizur Rahaman, A. K. M. Bahalul Haque, A. K. M. Najmul Islam, Rashedur M. Rahman | *Pranto, T. H., Noman, A. A., Rahaman, M., Haque, A. K. M. B., Islam, A. K. M. N., & Rahman, R. M. (2022). A Blockchain, Smart Contract and Data Mining Based Approach toward the Betterment of E-Commerce. Cybernetics and Systems, 53(5), 443–467.* | 2021 | Scopus |
| 5 | *Blockchain-Based E-Commerce: A Review on Applications and Challenges* | Hamed Taherdoost, Mitra Madanchian | *Taherdoost, H., & Madanchian, M. (2023). Blockchain-Based E-Commerce: A Review on Applications and Challenges. In Electronics (Switzerland) (Vol. 12, Issue 8). MDPI.* | 2022 | Scopus |
| 6 | *A Survey on Blockchain for Information Systems Management and Security* | David Berdik, Safa Otou, Nikolas Schmida, Dylan Porte, Yaser Jararweha | *Berdik, D., Otoum, S., Schmidt, N., Porter, D., & Jararweh, Y. (2021). A Survey on Blockchain for Information Systems Management and Security. Information Processing and Management, 58(1).* | 2021 | ScienceDirect |
| 7 | *Blockchain technology: A survey on applications and* | Bhabendu Kumar Mohana, Debasish Jena, Soumyashree S. | *Mohanta, B. K., Jena, D., Panda, S. S., & Sobhanayak, S. (2019). Blockchain technology: A survey on applications and security* | 2019 | ScienceDirect |

| | | | | | |
|---|---|---|---|---|---|
| | *security privacy Challenges* | Panda, Srichandan Sobhanayak | *privacy Challenges. In Internet of Things (Netherlands) (Vol. 8). Elsevier B.V.* | | |
| 8 | *Using the security triad to assess blockchain technology in public sector applications* | Merrill Warkentin, Craig Orgeron | *Warkentin, M., & Orgeron, C. (2020). Using the security triad to assess blockchain technology in public sector applications. International Journal of Information Management, 52.* | 2020 | ScienceDirect |
| 9 | *Developing an anti-counterfeit system using blockchain technology* | Anthony, Michael Christian Leea, Rafaelle Richel Pearla, Iván Sebastián Edberta, Derwin Suhartonoa | *Anthony, Lee, M. C., Pearl, R. R., Edbert, I. S., & Suhartono, D. (2023). Developing an anti-counterfeit system using blockchain technology. Procedia Computer Science, 216, 86–95.* | 2022 | ScienceDirect |
| 10 | *Fraud detection and prevention in e-commerce: A systematic literature review* | Vinicius Facco Rodrigues, Lucas Micol Policarpo, Diórgenes Eugênio da Silveira, Rodrigo da Rosa Righi, Cristiano André da Costa, Jorge Luis Victória Barbosa, Rodolfo Stoffel Antunes, Rodrigo Scorsatto, Tanuj Arcot | *Rodrigues, V.F., Policarpo, L. M., da Silveira, D. E., da Rosa Righi, R., da Costa, C. A., Barbosa, J. L. V., Antunes, R. S., Scorsatto, R., & Arcot, T. (2022). Fraud detection and prevention in e-commerce: A systematic literature review. Electronic Commerce Research and Applications, 56.* | 2022 | ScienceDirect |

Nota: Elaboración propia

## 3.8 Respuestas de las preguntas

### 3.8.1 Respuesta de la pregunta P1

Pregunta 1: ¿Cuáles son los desafíos y vulnerabilidades más comunes en términos de seguridad de información que los sistemas de comercio electrónico suelen enfrentar en la actualidad?

En la actualidad, se presentan diversos desafíos y vulnerabilidades que los sistemas de información deben de lidiar en función de mejorar su seguridad de información en el contexto del comercio electrónico, los cuales son los siguientes:

- Se tiene la manipulación de datos sin autorización, provocando carencias de transparencia y trazabilidad, lo que perjudica que la información sea verídica y auténtica (Esfahbodi et al., 2022).
- El comercio electrónico enfrenta diversas amenazas relacionadas con el software, las cuales comprometen tanto la seguridad como la confianza en este sistema. Por un lado, se enfrenta a ataques cibernéticos y piratería informática, siendo la información de los usuarios accesible públicamente. Este fenómeno ha llevado a un aumento significativo en estafas, causando pérdidas financieras considerables tanto para compradores como para vendedores (Esfahbodi et al., 2022; Pranto et al., 2022; Rodrigues et al., 2022). Por otro lado, las amenazas incluyen la denegación distribuida de servicios, ataques DDoS, inyecciones SQL, ataques XSS, secuestro del recorrido del usuario y bots corruptos, entre otros desafíos (Pleskach et al., 2022). Además, se han observado comportamientos fraudulentos como la apropiación de cuentas, robo de identidad, fraude silencioso y fraude de devolución de cargo, impactando tanto financieramente a las partes involucradas como socavando la

confianza general en el comercio electrónico (Pranto et al., 2022). El problema se agrava con el aumento de las falsificaciones de productos, usuarios y transacciones, impulsado por el uso compulsivo del internet y la informalidad en la cultura de la sociedad. Esto ha llevado a un incremento en los costos operativos para combatir estas falsificaciones, así como a pérdidas significativas de ventas en el ámbito del comercio electrónico (Anthony et al., 2023). La evolución constante en las estrategias de los ataques cibernéticos también ha sido una preocupación, aumentando el riesgo de vulnerabilidad de los datos sensibles de los usuarios almacenados en los sistemas de información. Estos ataques no solo han comprometido la seguridad, sino que también han dejado registros de pérdidas financieras considerables (Rodrigues et al., 2022).

- Se presenta problemas de protección y seguridad de datos desde el punto de vista del usuario, lo que disminuye la confianza de estos últimos en la utilización de los sistemas de información dentro del comercio electrónico, provocando a su vez una insatisfacción ante la situación actual de la seguridad de información (Treiblmaier & Sillaber, 2021).
- En algunas situaciones, el comercio electrónico tradicional puede estar expuesto a la posibilidad de que se divulguen los datos de los usuarios. Esto también provoca la posibilidad de manipulación de los datos y obtención de grandes cantidades de datos sin autorización, afectando la integridad y veracidad de la información almacenada (Taherdoost & Madanchian, 2023). Incluso, se pueden presentar pérdidas de datos o interrupciones del servidor dentro del sistema de información del comercio electrónico, lo que perjudica

las operaciones de la empresa al no presentar una tolerancia a fallos (Berdik et al., 2021).

- Se presenta poca eficiencia en las operaciones, costos y velocidad al implementar un sistema de información dentro del comercio electrónico (Taherdoost & Madanchian, 2023).
- En el historial de datos, existe un desequilibrio notable, con un predominio de transacciones legítimas sobre las fraudulentas (algunas de estas últimas se encuentran ocultas). Esta disparidad plantea un desafío significativo en el mejoramiento de la seguridad de la información (Rodrigues et al., 2022).

### 3.8.2 Respuesta de la pregunta P2

Pregunta 2: ¿Cuáles son las medidas de seguridad de información que están siendo actualmente empleadas en los sistemas de información orientados al comercio electrónico?

En la actualidad, se han establecido medidas de seguridad de la información destinadas a hacer frente a las amenazas y riesgos que podrían comprometer la integridad de los sistemas de información utilizados en el comercio electrónico.

Una de las medidas consiste en la implementación de un robusto sistema de protección contra accesos no autorizados, que se logra mediante la utilización de firmas electrónicas cualificadas. Además, se lleva a cabo un riguroso seguimiento y control para garantizar el cumplimiento de los requisitos de seguridad de la información en las infraestructuras digitales que respaldan el comercio electrónico (Pleskach et al., 2022).

Para fortalecer aún más la seguridad e integridad de los sistemas de información, se implementan herramientas antivirus y sistemas de prevención de intrusiones. Estos

sistemas tienen como objetivo prevenir la entrada de *malware* y el acceso no autorizado a la información. Asimismo, se incorpora una herramienta de registro de eventos y detección de incidentes cibernéticos para mejorar la transparencia y la capacidad de respuesta, lo que asegura la continuidad y una rápida recuperación de las actividades (Pleskach et al., 2022).

En el ámbito del fortalecimiento de la detección de fraudes, se utiliza la creación de reglas a partir de extensos conjuntos de datos, un enfoque efectivo para abordar los desafíos relacionados con las transacciones fraudulentas en el comercio electrónico (Pranto et al., 2022). Paralelamente, se implementa la detección de reseñas falsas y difamaciones deliberadas como parte de un sistema de evaluación de la reputación de los vendedores (Pranto et al., 2022).

Adicionalmente, se realiza la recopilación, almacenamiento, organización y manipulación de información geográfica, que incluye las coordenadas de latitud y longitud de las transacciones, con el objetivo de garantizar una comunicación segura de la información. También se desarrollan esquemas de identificación y autenticación para verificar la identidad de los usuarios involucrados, y se utiliza para transmitir información a las partes relevantes (Berdik et al., 2021).

Además, se utiliza software de aplicación de bases de datos debido a su amplia capacidad de almacenamiento, capacidades de registro y rapidez en la recuperación de datos a través de consultas de búsqueda. Esto se hace con el propósito de administrar, facilitar el acceso y recuperar datos de manera eficiente, permitiendo así un control y monitoreo efectivo de los procedimientos que implican la entrega de datos (Berdik et al., 2021).

En adición, se han adoptado medidas altamente especializadas para minimizar o eliminar riesgos en el comercio electrónico. Por ejemplo, se aplican estrategias basadas en el aprendizaje automático, que involucran el análisis de patrones a través de métodos de clasificación dentro del sistema de información con el fin de prever posibles comportamientos fraudulentos (Rodrigues et al., 2022). Esta labor se apoya en algoritmos de clasificación, como los bosques aleatorios, la regresión logística y las redes neuronales artificiales, empleados para detectar y prevenir operaciones fraudulentas en el contexto del comercio electrónico (Rodrigues et al., 2022).

Asimismo, se recurre a técnicas de detección de anomalías no supervisadas para analizar el comportamiento de los usuarios en el comercio electrónico. Estas técnicas, combinadas con un análisis exhaustivo de datos, permiten identificar transacciones fraudulentas (Rodrigues et al., 2022).

Por último, se ha mejorado la capacidad de los sitios web para capturar y rastrear en tiempo real el comportamiento de los usuarios. Esto posibilita un análisis detallado del comercio electrónico incluso antes de que el usuario realice una transacción, con el propósito de que los sistemas puedan prevenir el fraude de manera anticipada a lo largo de todo el proceso (Rodrigues et al., 2022).

### 3.8.3 Respuesta de la pregunta P3

Pregunta 3: ¿Cómo contribuye la tecnología *blockchain* a mejorar la seguridad de la información durante las transacciones y cuáles son las características específicas que esta tecnología aporta a estas medidas de seguridad?

La tecnología *blockchain* engloba una serie de funcionalidades que se pueden integrar para fortalecer las medidas de seguridad en las transacciones y el manejo de información.

En un enfoque inicial, con el uso de la tecnología *blockchain*, se proporciona una mejor trazabilidad al permitir el registro y consulta de la información almacenada en tiempo real, estableciendo una base de datos inalterable y a salvo de manipulaciones (Esfahbodi et al., 2022).

Junto a este enfoque, la tecnología *blockchain*, en conjunto con la criptografía, se utiliza para validar y encadenar transacciones, las cuales son posteriormente registradas y están disponibles públicamente sin posibilidad de modificación sin autorización. Esta combinación garantiza la accesibilidad de la información al tiempo que proporciona una sólida protección para los datos sensibles, asegurando su integridad y validez en todo momento (Warkentin & Orgeron, 2020).

Del mismo modo, la tecnología *blockchain* permite que los datos de las transacciones puedan ser rastreadas hasta la fuente, a través de la estructura de cadena, al mismo tiempo que disminuye la capacidad de terceros de poder recopilar información de los usuarios, brindando así una salvaguarda significativa para la privacidad en línea. En otras palabras, facilita a los usuarios utilizar y compartir su información de manera confiable y segura (Esfahbodi et al., 2022).

Además de actuar como una red de intercambio para mover transacciones, valor y activos sin la intervención de intermediarios, impulsando de esta manera la transparencia y validación de las transacciones en el comercio electrónico (Treiblmaier & Sillaber, 2021), la tecnología *blockchain* también garantiza un entorno altamente seguro ante cualquier tipo de manipulación, esto mediante la autorización para el acceso y modificación de la información almacenada (Pranto et al., 2022).

De manera paralela, habilita la transmisión y lectura de registros de transacciones, sin la posibilidad de una alteración, de esta manera, se asegura el almacenamiento,

recopilación y compartición de la información de forma auténtica (Mohanta et al., 2019).

Respecto al tema del almacenamiento de datos, la tecnología *blockchain* permite almacenar todas las transacciones y datos mediante un cifrado sólido, registrándose con una identificación única (Anthony et al., 2023).

Una faceta adicional relevante es que la tecnología *blockchain* ofrece la capacidad de generar registros seguros y transparentes, como también la capacidad de verificar la legitimidad de las operaciones (Taherdoost & Madanchian, 2023).

Asimismo, mediante la aplicación de un algoritmo, es posible identificar tanto las secuencias temporales de las entradas de los usuarios como los conjuntos de transacciones (Taherdoost & Madanchian, 2023).

Por último, posibilita la distribución descentralizada de información a otras entidades, asegurando la seguridad y la integridad de los datos al impedir la alteración de las transacciones históricas dentro de la base de datos (Berdik et al., 2021).

### 3.8.4 Respuesta de la pregunta P4

Pregunta 4: ¿Cuáles serían los beneficios de incorporar la tecnología *blockchain* en el fortalecimiento de la seguridad de las transacciones en el ámbito del comercio electrónico?

Al integrar la tecnología *blockchain* en el sistema de información con el objetivo de reforzar la seguridad de las transacciones en el ámbito del comercio electrónico, se pueden destacar una serie de beneficios que se describirán a continuación.

En primer lugar, la tecnología *blockchain* proporciona una base de datos compartida, la cual se distingue de la tradicional principalmente debido a su inalterabilidad de

datos, transparencia en el registro de transacciones y la capacidad de rastreo hasta la fuente. Esto otorga a los usuarios tener la confianza para registrar y acceder a la información de forma precisa y oportuna (Esfahbodi et al., 2022).

Esta inmutabilidad de los datos dentro del sistema, que incluye la tecnología *blockchain*, contribuye a mejorar la seguridad, que en la actualidad se ve constantemente amenazada por ataques cibernéticos (Taherdoost & Madanchian, 2023). Adicionalmente a esto, se mejora la integridad mediante la protección de la validez de los datos contra cambios no deseados (Warkentin & Orgeron, 2020).

Además, al asegurar la transparencia en el registro de las transacciones, se logra el beneficio adicional de reducir las amenazas a la seguridad, como el fraude y el acceso no autorizado a la información (Treiblmaier & Sillaber, 2021). Complementariamente, la tecnología *blockchain* incorpora una estructura que dificulta extraordinariamente la creación de registros fraudulentos dentro de la base de datos. Esto, en última instancia, proporciona una experiencia de usuario coherente y auténtica (Berdik et al., 2021).

Por último, la ventaja de la capacidad de la trazabilidad facilita el intercambio de datos tanto dentro como fuera de la organización, reduciendo el riesgo y los costes asociados (Pranto et al., 2022). Incluso, se mejora la confidencialidad al tener una protección de los datos contra el acceso no autorizado (Warkentin & Orgeron, 2020).

Adicionalmente, al tratarse de una base de datos compartida, los nodos pueden acceder a la información en cualquier momento y lugar en tiempo real, lo que simplifica enormemente la adquisición y flexibilidad de los datos (Esfahbodi et al., 2022).

Es esencial tener en cuenta que cada transacción en tecnología *blockchain* conlleva un costo que puede variar según la red y el tipo de transacción. A pesar de esto, en comparación con las tecnologías tradicionales, el uso de *blockchain* implica costos más bajos y ofrece ventajas significativas (Longo et al., 2020).

Por un lado, la adopción de la tecnología *blockchain* en sistemas de información ofrece oportunidades significativas para mejorar la eficiencia y reducir los costos asociados con la búsqueda y recuperación de datos (Esfahbodi et al., 2022). La capacidad de verificar y auditar fácilmente las transacciones en una cadena de bloques puede mejorar la confiabilidad de los datos y reducir los errores, lo que a su vez puede aumentar la eficiencia operativa (Esfahbodi et al., 2022).

De igual importancia, la implementación de la tecnología *blockchain* conlleva una reducción general de costos, ya sean de tipo temporal, de esfuerzo o financieros, lo que a su vez impulsa la interoperabilidad y eficiencia del sistema de información (Berdik et al., 2021).

De manera similar, la tecnología *blockchain* tiene la capacidad de suprimir la necesidad de terceros que ejerzan control centralizado, introduciendo en su lugar nuevos sistemas de seguridad. Este propósito es el de prevenir posibles manipulaciones maliciosas de los datos, lo que a su vez conduce a un fortalecimiento de la seguridad y la integridad en las transacciones (Esfahbodi et al., 2022). Del mismo modo, al no tener intermediarios durante las transacciones, se tendrían procesos más eficientes en cuanto a tiempo, autenticidad y calidad (Pranto et al., 2022).

## 3.9 Conclusiones

En este capítulo, se ha explorado en detalle las medidas y las tecnologías relacionadas con la seguridad de la información en el contexto del comercio electrónico y hemos analizado sus características, beneficios y desafíos. A través de una revisión teórica y empírica, se ha identificado las medidas de seguridad actuales en sistemas de información de comercio electrónico y se ha explorado cómo la tecnología *blockchain* se integra en estas medidas.

Se ha descubierto que los sistemas de información de comercio electrónico enfrentan una serie de desafíos y vulnerabilidades, incluyendo la manipulación de datos, ataques cibernéticos, protección de datos personales, fraudes y falsificaciones. Para abordar estos problemas, se emplean medidas de seguridad como protección contra accesos no autorizados, sistemas antivirus, detección de fraudes, registro de eventos y detección de intrusiones, incluyendo la implementación de algoritmos de clasificación o de técnicas de detección de anomalías.

La tecnología *blockchain* emerge como una solución prometedora para fortalecer la seguridad de las transacciones en el comercio electrónico. Sus características específicas, como la inmutabilidad de datos, transparencia, trazabilidad y resistencia a la manipulación aportan beneficios significativos. Estos beneficios incluyen una mayor confianza en la autenticidad de los datos, reducción de riesgos de fraude, mejora en la integridad de la información y la característica para compartir información de forma segura. Incluso, la implementación de la tecnología *blockchain* también conlleva ventajas en términos de eficiencia y reducción de costos, al eliminar intermediarios y simplificar la gestión de datos.

En conclusión, la integración entre la aplicación de esta tecnología y las actuales medidas de seguridad de la información, incluyendo principalmente los algoritmos previamente mencionados en este capítulo, fortalecería de manera significativa la seguridad en el ámbito del comercio electrónico. Esto establecería una base sólida que garantiza transacciones en línea seguras y confiables.

# Capítulo 4. Implementación de componentes para asegurar almacenamiento e integridad de datos

## 4.1 Documentación de requerimientos y prototipo de arquitectura del software (Resultado 1).

Con el fin de comprender las funcionalidades del sistema de información que emplea la tecnología *blockchain* para el almacenamiento de las transacciones, se ha elaborado un documento que detalla y explica tanto los requisitos funcionales como los no funcionales. Estos requerimientos fueron inicialmente elaborados por el tesista y posteriormente revisados, analizados y comentados por los especialistas correspondientes, quienes realizaron las observaciones necesarias para su mejora. Para simplificar la presentación de los documentos adjuntos, todos los requisitos funcionales y no funcionales de cada objetivo se han recopilado en un único archivo de Excel, que se tiene adjunto en el Anexo C.

En la tabla 13, se presentan los requisitos funcionales específicos del resultado 1.

- **Tabla 13: Requerimientos funcionales del resultado 1**

| Identificador | Descripción |
|---|---|
| RF001 | El sistema permitirá utilizar la tecnología *blockchain* para el almacenamiento de la información de las transacciones, a fin de establecer inmutabilidad para estos datos y garantizar su recuperación en caso de necesidad. |
| RF002 | El sistema permitirá integrar la tecnología *blockchain* dentro del sistema de información desde FrontEnd |
| RF003 | El sistema permitirá aplicar autenticación de contraseña estándar para las cuentas de usuario, asegurando la protección y confidencialidad de las credenciales de inicio de sesión. Esto se llevará a cabo mediante la implementación de mecanismos de encriptación utilizando bibliotecas de .NET para garantizar la seguridad de la contraseña del usuario. Durante el proceso de registro y autenticación, las contraseñas se encriptarán antes de almacenarse en la base de datos. |
| RF004 | El sistema permitirá un proceso de registro de usuarios que incluirá una |

| | |
|---|---|
| | verificación básica para garantizar la autenticidad de las cuentas creadas. |
| RF005 | El sistema permitirá agregar la opción de restablecer la contraseña en caso de olvido, lo que mejorará significativamente la experiencia del usuario al proporcionar una solución conveniente y segura para recuperar el acceso a sus cuentas. Cuando un usuario olvide su contraseña, podrá utilizar la función de restablecimiento de contraseña para recibir la contraseña por correo electrónico. |
| RF006 | El sistema permitirá a los usuarios gestionar sus preferencias de privacidad mediante la gestión del contenido de sus datos personales, brindándoles un mayor control sobre cómo se utilizan y comparten sus datos dentro del sistema. |
| RF007 | El sistema permitirá a los usuarios utilizar su correo electrónico como método de verificación de dos pasos para acceder al sistema de información, proporcionando una capa adicional de seguridad. Cuando un usuario intente iniciar sesión en su cuenta, después de ingresar su nombre de usuario y contraseña correctamente, el sistema enviará automáticamente un token de verificación único al correo electrónico asociado con la cuenta del usuario. Una vez que el usuario reciba el token en su correo electrónico, deberá ingresar este código en el sistema para completar el proceso de verificación de dos pasos y obtener acceso a su cuenta. |
| RF008 | El sistema deberá registrar de manera transparente todas las operaciones realizadas sobre los datos, incluyendo modificaciones. Este registro de auditoría contendrá un seguimiento detallado de cada acción realizada en el sistema, incluyendo la fecha y hora de la operación, la identidad del usuario que la llevó a cabo y una descripción del cambio. |

Nota: Elaboración propia

Además, como parte del proceso de verificación, se han llevado a cabo reuniones con mi asesor de tesis, un especialista en comercio electrónico y otro en seguridad de la información, específicamente en relación con fraudes. Con el propósito de respaldar estas reuniones, adjunto en los Anexos D y E las actas correspondientes, donde se incluyen observaciones sobre el documento. Asimismo, el acta de validación de los requerimientos de este resultado se encuentra en el Anexo T.

Por otro lado, el documento del Prototipo de Arquitectura de Software tiene como objetivo ofrecer una visión funcional, lógica y de componentes del sistema de información. Este documento, que se adjunta en el Anexo F, también incluye las

verificaciones realizadas por expertos en el campo, cuyas actas de validación se encuentran en el Anexo G.

Con el fin de mostrar una vista referencial, se mostrará la vista de componentes junto a su diseño en la imagen 1 y 2 respectivamente debido a que es la parte más crucial para la investigación y la que proporciona un mayor detalle de las herramientas a utilizar en el sistema de información.

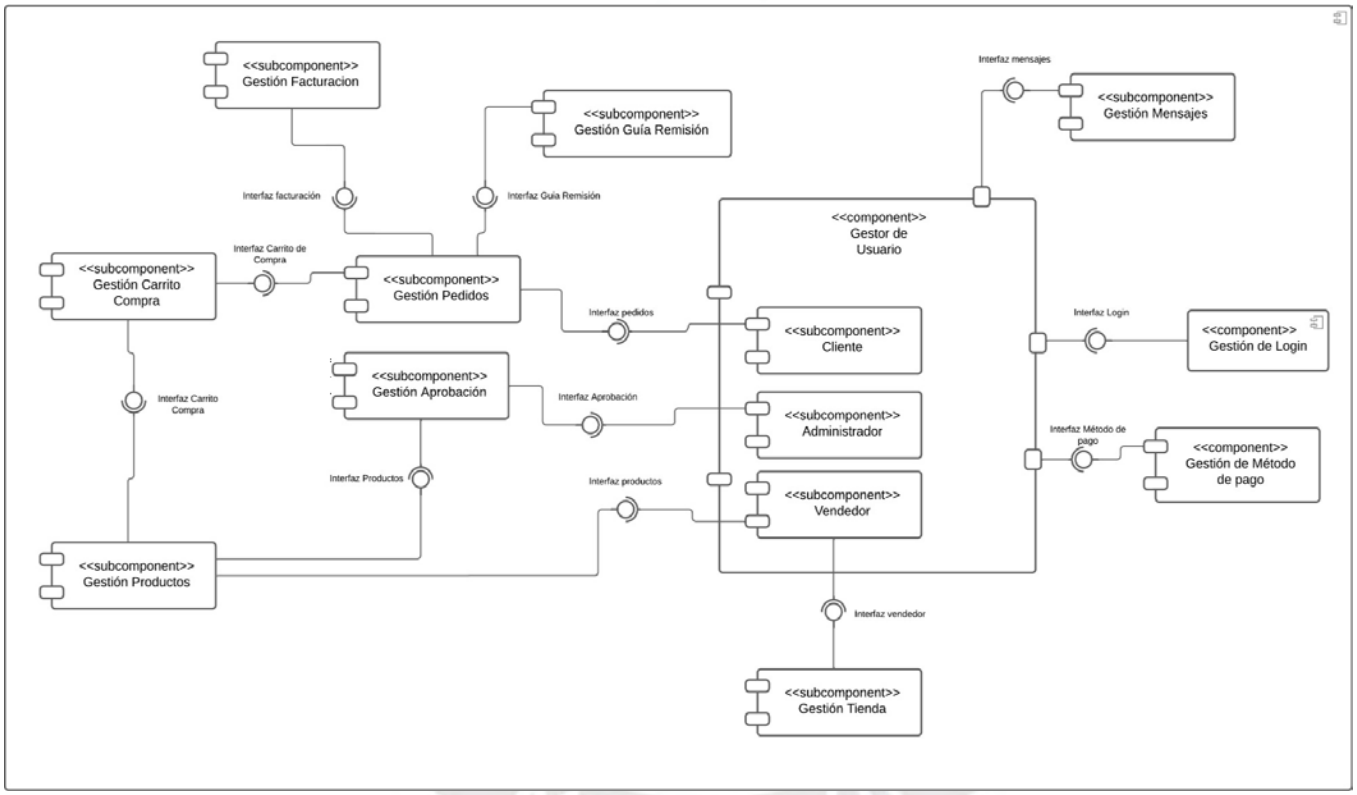


Imagen 1: Diagrama de componentes

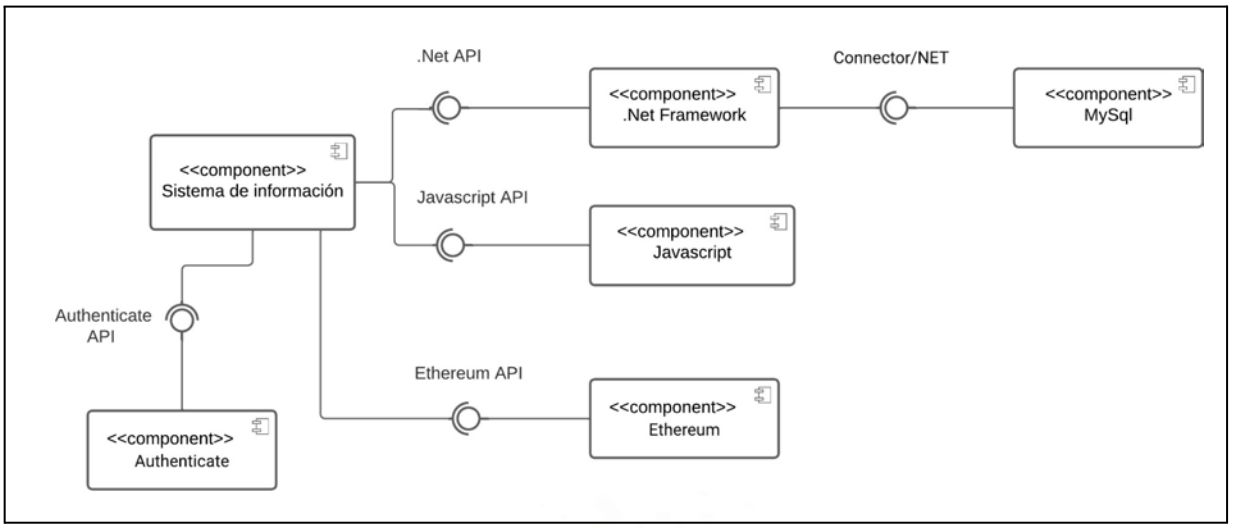


Imagen 2: Diseño de componentes

## 4.2 Componente del sistema de información que usa Smart Contracts para el almacenamiento de las transacciones (Resultado 2).

Para asegurar un almacenamiento inmutable y transparente de las transacciones, se ha implementado la tecnología *blockchain* utilizando *Smart Contracts*. Para esta tarea, se han empleado herramientas como Solidity, Ganache y Web3.js para su integración en el sistema de información. Este proceso se implementa justo antes de realizarse el procesamiento de pago y se encuentra en la sección de FrontEnd. El código fuente correspondiente se localiza en la carpeta de FrontEnd, más en específico en la ruta "*react-frontend>src>Blockchain>contracts>Ecommerce.sol*", mientras que la implementación e integración se puede observar en los archivos "*react-frontend>src>js>Comprador>MetodoPago.js*" y "*react-frontend>src>js>Comprador>StripePaymentForm.js*". En estos últimos archivos mencionados, la función que invoca a los Smart Contracts es "*createAndVerifyTransaction*". Toda esta información está documentada en el código fuente del sistema de información, en el Anexo K.

El documento de la funcionalidad del componente se encuentra en el Anexo P, donde se visualiza los detalles de este.

### 4.3 Implementación de un algoritmo criptográfico (Resultado 3).

Para reforzar la seguridad de los usuarios en el sistema de información, se han integrado bibliotecas de criptografía de .NET para proteger las contraseñas almacenadas. En este enfoque criptográfico, se ha establecido una clave única que se guarda en la base de datos, permaneciendo oculta hasta que sea necesaria para cifrar o descifrar los datos. Este método asegura un almacenamiento robusto mediante una criptografía, ayudando a tener una mejor seguridad e integridad al momento de realizar el inicio de sesión mediante este algoritmo criptográfico. El código fuente de esta implementación está situado en la carpeta "BackEnd>Controllers". Se pueden encontrar más detalles sobre este código en el Anexo K. Además, se tiene un documento detallado sobre la funcionalidad del algoritmo criptográfico empleado en esta investigación dentro del Anexo Q. Este documento proporciona una descripción del diseño y el funcionamiento interno del algoritmo, demostrando su lógica y su efectividad.

# Capítulo 5. Funcionalidades transaccionales para operaciones seguras y eficientes

## 5.1 Documentación de requerimientos y prototipo de la interfaz gráfica del sistema de información (Resultado 4).

El documento que contiene los requerimientos funcionales y no funcionales está disponible en el Anexo C, tal como se detalla en el Capítulo 4, con el objetivo de integrar la información en un único documento y las actas de reuniones con el especialista sobre los temas están adjuntados en el Anexo D. Estos requerimientos fueron inicialmente elaborados por el tesista y posteriormente revisados, analizados y comentados por los especialistas correspondientes, quienes realizaron las observaciones necesarias para su mejora.

Se muestra una lista de los módulos principales de funcionalidades dentro del sistema en la tabla 14, con el fin de ofrecer una vista de referencia de los requisitos funcionales.

- **Tabla 14: Lista de módulos del requerimiento funcional del resultado 4**

| Módulo | Descripción |
|---|---|
| Gestión de Roles y Permisos | Este módulo se encarga de definir y gestionar los roles de usuario, así como los permisos y funcionalidades asociadas a cada rol. |
| Gestión de Pedidos | Este módulo maneja todas las operaciones relacionadas con la gestión de pedidos, incluyendo la visualización, filtrado y gestión de pedidos realizados en la plataforma. |
| Gestión de Inventario | Este módulo permite a los vendedores actualizar y monitorear los productos disponibles para la venta, incluyendo la adición, modificación y eliminación de productos en el inventario. |
| Gestión de Tiendas | Este módulo permite a los vendedores actualizar y monitorear los productos disponibles para la venta, incluyendo la adición, modificación y eliminación de productos en el inventario. |
| Gestión de Reclamos | Este módulo permite a los usuarios enviar reclamos sobre pedidos específicos o productos, así como visualizar y gestionar reclamos realizados en la plataforma. |

| | |
|---|---|
| Integración *Blockchain* | Este módulo se encarga de la integración de un *Smart Contract* en una plataforma *blockchain* para registrar transacciones de forma inmutable y transparente. |
| Gestión de Perfiles de Usuario | Este módulo proporciona a los usuarios una experiencia segura y personalizada a través de la funcionalidad del perfil, posibilitando la visualización y modificación de la información del usuario. |
| Verificación de Integridad de Productos | Este módulo implementa mecanismos de verificación de la integridad de los productos vendidos dentro de un pedido, como la trazabilidad y visualización de la información de los pedidos realizados. |
| Recuperación de Cuentas Eliminadas | Este módulo permite recuperar cuentas o tiendas eliminadas, mejorando la experiencia del usuario. |
| Estadísticas de Pedidos | Este módulo proporciona a los usuarios una interfaz para visualizar estadísticas detalladas de los pedidos realizados en la plataforma. |
| Búsqueda y Filtrado de Productos | Este módulo proporciona la capacidad de buscar y filtrar productos por SKU, nombre y tipo de producto para facilitar la navegación. |
| Comunicación entre Compradores y Vendedores | Este módulo facilita la comunicación directa entre compradores y vendedores a través de un sistema de mensajes en la plataforma (chat), permitiendo resolver preguntas o problemas relacionados con la transacción. |
| Gestión de Pagos y Seguridad | Este módulo permite y asegura los pagos de las transacciones a través de una pasarela de pago confiable, incluyendo la capacidad de almacenar la información de las tarjetas de crédito de los usuarios de forma segura mediante un token. |

Nota: Elaboración propia

Además, se proporciona un documento que presenta las pantallas más relevantes del sistema de información. Se consideran tres roles de usuario dentro del *e-commerce* objeto de esta investigación: Administrador, responsable de la gestión de publicaciones de productos y pedidos; Vendedor, vinculado a una tienda y con capacidad para publicar productos y gestionar ventas y ganancias; y Comprador, quien visualiza y compra productos, generando así pedidos. Este documento se encuentra adjunto en el Anexo H. Por otro lado, el Acta de Reunión con el especialista en *E-commerce* se incluye en el Anexo D, donde se registran observaciones y sugerencias para el prototipo de interfaz

final, derivadas de dichas reuniones. Asimismo, el Acta de validación con el especialista en *E-commerce* se encuentra en el Anexo U, donde se encuentran la firma.

A continuación, se presenta una vista referencial sobre algunas pantallas para cada rol importante en las imágenes 3, 4 y 5 dentro del sistema realizadas en Figma:

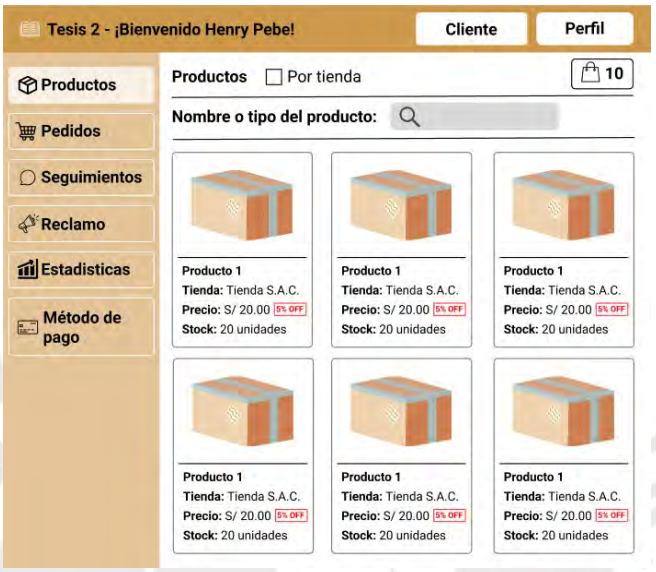


Imagen 3: Vista referencial de las funcionalidades del rol de Cliente en el sistema

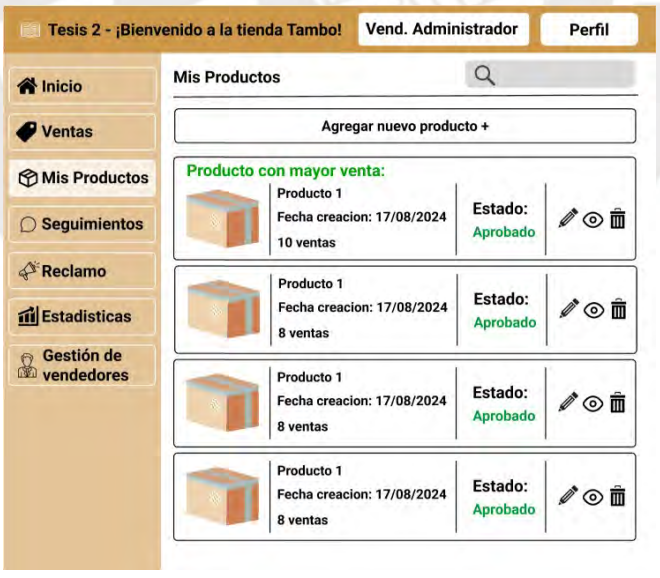


Imagen 4: Vista referencial de las funcionalidades del rol de Vendedor en el sistema

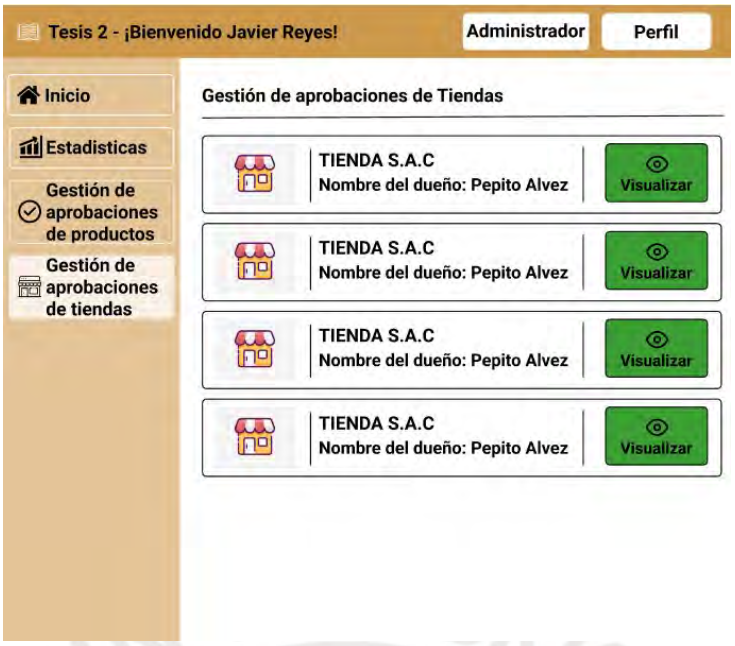


Imagen 5: Vista referencial de las funcionalidades del rol de Administrador en el sistema

## 5.2 Implementación del sistema de información incluyendo la interfaz gráfica y las funcionalidades (Resultado 5).

Para la implementación del sistema de información, se optó por utilizar React.js para el FrontEnd y .Net junto con MySQL para el Backend. Dentro del sistema de información, se tiene las funcionalidades que tiene cada rol del sistema (comprador, vendedor administrador, vendedor asistente y administrador). Además, como se comentó en el capítulo 2, se empleó Solidity, Web3.js y Ganache para las capas de seguridad y almacenamiento de *blockchain*, asegurando así la integridad de los datos sensibles. El código fuente correspondiente se encuentra adjunto en el Anexo K, donde se pueden visualizar tanto las carpetas del Backend como las del FrontEnd, dentro de esta última se encuentra la carpeta "*react-frontend>src>Blockchain*", en el que se encuentra el código fuente del *Smart Contracts*. De igual manera, se cuenta con un documento que detalla y muestra cada funcionalidad relevante para todos los roles considerados en el sistema de información en el Anexo R. Este enfoque tiene como objetivo demostrar la efectividad y el alcance funcional del sistema de manera completa y detallada. Por otro lado, se tiene el

Acta de Validación del documento de las funcionalidades del sistema de información en el Anexo V, firmado por el especialista de *e-commerce.*

## 5.3 Funcionalidad de chat para la interacción directa entre compradores y vendedores (Resultado 6).

En este capítulo, se ha implementado una funcionalidad de chat diseñada para que tanto el comprador como el vendedor puedan interactuar directamente sobre los pedidos que están vinculados entre ellos. Es importante destacar que esta opción puede ser finalizada si así lo solicita el comprador. El propósito principal de este chat es facilitar el intercambio de información o comentarios relacionados con el estado de un pedido entregado.

Es relevante señalar que este chat está destinado exclusivamente para la comunicación entre el comprador y los vendedores asociados a una tienda específica. El código fuente de esta funcionalidad se encuentra dentro del código fuente del sistema de información, en las secciones de "DetalleSeguimiento.js" y "DetalleSeguimientoVendedor.js". Estos archivos están ubicados en la subcarpeta de "FrontEnd>react-frontend>src>js", tanto en la subcarpeta del comprador como en la del vendedor, respectivamente.

El documento de la funcionalidad se encuentra en el Anexo N, donde se visualiza los detalles de este. Asimismo, se tiene el Acta de Validación de las pruebas de funcionamiento del módulo de interacción directa del comprador y el vendedor en el Anexo W.

## 5.4 Integración de una pasarela de pago como sistema seguro (Resultado 7).

Se ha implementado una pasarela de pago usando Stripe, con la finalidad de que tanto los compradores y vendedores guarden sus tarjetas de crédito o débito, asimismo, permitir que el comprador pueda consumir de su tarjeta el monto total del pedido. Con esta

integración, se busca facilitar los pagos. Al momento de realizar un guardado, se obtiene un token que el mismo Stripe proporciona para poder identificar la tarjeta y realizar los pagos posteriores, así como también se guarda los 4 últimos dígitos de la tarjeta y la fecha de caducidad para efectos visuales dentro de la interfaz gráfica.

El documento de la integración se encuentra en el Anexo O, donde se visualiza los detalles del mismo. Asimismo, se tiene el Acta de Validación de las pruebas de funcionamiento del módulo del sistema de pago en el Anexo X.

# Capítulo 6. Diseñar, desarrollar e integrar un algoritmo de detección de fraudes

## 6.1 Especificación de requerimientos funcionales y no funcionales del algoritmo de detección de fraude (Resultado 8).

El documento que incluye los requerimientos funcionales y no funcionales del algoritmo de detección de fraude se encuentra disponible en el Anexo C, conforme se presenta en el Capítulo 4, con la finalidad de consolidar la información en un solo documento. Estos requerimientos fueron inicialmente elaborados por el tesista y posteriormente revisados, analizados y comentados por los especialistas correspondientes, quienes realizaron las observaciones necesarias para su mejora. Además, las actas de reuniones con especialistas del tema están adjuntas tanto en el Anexo D como en el E. Asimismo, se tiene el acta de validación de los requerimientos funcionales del resultado, firmada por el especialista de *machine learning* en el Anexo Y.

En la tabla 15, se tiene una vista preliminar sobre los requerimientos funcionales correspondientes al objetivo 3.

- **Tabla 15: Requerimientos funcionales del resultado 8**

| Identificador | Descripción |
|---|---|
| RF033 | El algoritmo implementado en el sistema permitirá generar alertas en tiempo real cuando se detecten comportamientos anómalos. Cuando se detecte una actividad sospechosa, como una compra que no coincide con el historial de transacciones previas del usuario o que presenta características inusuales, el algoritmo generará una alerta inmediata. |
| RF034 | El diseño del algoritmo se llevará a cabo de manera que permita su adaptabilidad y configurabilidad, lo que garantizará su capacidad para ajustarse a diferentes necesidades y escenarios de uso. Esto incluirá la capacidad de modificar parámetros clave del algoritmo en función de la adquisición de diversos datos y cambios de las circunstancias. |
| RF035 | El algoritmo deberá ser capaz de adaptarse dinámicamente a los |

| | |
|---|---|
| | comportamientos del usuario. Esto se logrará mediante la recepción de datos de los pedidos como parámetros, permitiendo al algoritmo ajustar sus criterios de detección de anomalías según la información más reciente disponible. El algoritmo será diseñado para analizar los datos de los pedidos en tiempo real y utilizar esta información para actualizar y refinar sus modelos de detección de comportamientos anómalos. |
| RF036 | El sistema permitirá notificar a los usuarios sobre transacciones sospechosas mediante un correo alternativo, dando la opción de una confirmación o eliminación del pedido mediante un token que será colocado en el sistema para la confirmación de la transacción y realizar el procesamiento de pago. |

Nota: Elaboración propia

## 6.2 Recolección y procesamiento de datos de transacciones históricas y en tiempo real (Resultado 9).

En este capítulo, se presenta un documento detallando los parámetros considerados en el algoritmo de detección de fraude, el formato de los datos utilizados como entradas para su entrenamiento, así como las consideraciones y reglas antifraude aplicadas para distinguir entre transacciones legítimas y fraudulentas y, además, se tiene tres escenarios diferentes para el entrenamiento del algoritmo, donde cada uno de estos escenarios contiene 5000 datos de transacciones.

Parámetros Considerados:

- **Historial de transacciones**: Identifica desviaciones significativas en el comportamiento del usuario.
- **Número de cuenta**: Detecta cambios repentinos en el método de pago utilizado.
- **Frecuencia y volumen de compra**: Establece patrones normales de actividad para cada usuario.
- **Tipo de producto con mayor valor**: Identifica cambios inusuales en los tipos de productos adquiridos.

- **Dirección de entrega**: Detecta cambios frecuentes o repentinos en la dirección de entrega.

Consideraciones de los Datos:

- Se simula que los usuarios tengan múltiples pedidos a su nombre.
- Se considera una probabilidad del 5% de cambios en los parámetros para reflejar modificaciones poco comunes en la información del usuario.
- La cuenta de usuario está protegida mediante encriptación.

Reglas Antifraude:

- **Cambio de dirección de entrega:** Limita el número de cambios de dirección de entrega a un máximo de 8 por mes.
- **Montos inusuales del pedido:** Detecta pedidos que se desvían significativamente del promedio típico del usuario.
- **Cantidades inusuales en el pedido:** Identifica compras con cantidades de productos inusualmente grandes o pequeñas.
- **Cambios repentinos del método de pago:** Permite un máximo de 5 cambios en los métodos de pago utilizados.

Escenarios para el Entrenamiento del Algoritmo:

- **Escenario I:** Considera incrementos significativos en la cantidad y el precio de los productos, con límites establecidos para los cambios de dirección y método de pago.
- **Escenario II:** Ajusta los parámetros del escenario I para aumentar el alcance del algoritmo.

- **Escenario III:** Incorpora variaciones durante fechas festivas, con ajustes en los volúmenes y montos de transacciones y un mayor número de cambios en las direcciones de entrega.

Estos detalles se encuentran en el documento, el cual a su vez se encuentra adjunto en el Anexo I. Además, se incluyen las actas de las reuniones realizadas con especialistas en *E-commerce* y fraude, las cuales se encuentran anexadas en los Anexos D y E, respectivamente, y ayudaron a la mejora de este. Asimismo, se tiene el acta de validación firmada por el especialista de Seguridad de datos en el Anexo L.

A modo de referencia, a continuación, se muestra la estructura de los datos utilizados para el entrenamiento del algoritmo de detección de fraude en la imagen 6:

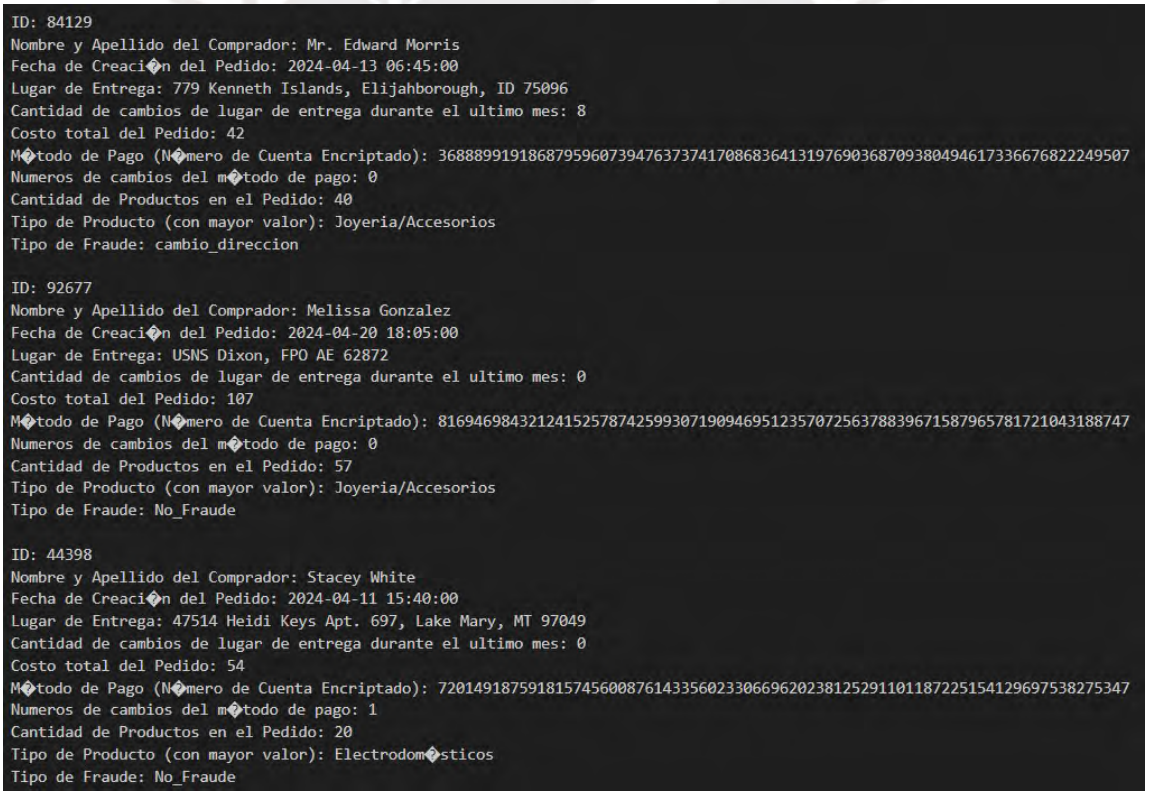


Imagen 6: Estructura de los datos para el entrenamiento del algoritmo

## 6.3 Implementación del algoritmo de detección de fraudes (Resultado 10).

Para la implementación del algoritmo de detección de fraudes, se ha elaborado una documentación que aborda la selección de los algoritmos de machine learning más adecuados para proporcionar un rendimiento óptimo en la detección de fraudes. Esta selección se basa en inputs de datos generados en el capítulo 10 del proyecto. Dicho documento detallado se encuentra adjunto en el Anexo J.

Además, se incluye el código fuente del algoritmo de detección de fraudes. Este algoritmo es capaz de analizar la información de las operaciones efectuadas en el resultado 7 y predecir con un éxito del 90% si un movimiento es fraudulento o legítimo.

Incluso, para la verificación de estos resultados, se ha realizado una documentación en donde se detalla los procesos de verificación de su funcionalidad del algoritmo de detección de fraude, la cual se encuentra en el Anexo M. Asimismo, el acta de validación de esta verificación firmada por el especialista de *Machine Learning* se encuentra en Anexo Z.

## 6.4 Integración del algoritmo de detección de fraudes dentro del sistema de información (Resultado 11).

Para esta integración, se estableció un servidor independiente (con puerto 5000) donde un algoritmo se mantiene activo de manera continua para verificar transacciones y aprender de forma dinámica. El código fuente asociado a la generación de predicciones y al funcionamiento del servidor se encuentra en la carpeta "ArchivosAdicionales", específicamente en los archivos "app.py" y "modelo.py". La integración se encuentra en el FrontEnd, visible en la carpeta "FrontEnd>react-frontend>src>js>Comprador". Dentro de esta estructura, los archivos "MetodoPago.js" y "StripePaymentForm.js" destacan al utilizar la función "AlgoritmoObtener" para comunicarse con el servidor y obtener las

predicciones necesarias del algoritmo. Estos códigos pueden ser visualizados con mayor detalle en el Anexo K. Asimismo, se tiene un documento donde se detalla la prueba de funcionalidad de la integración del algoritmo de detección de fraude en el sistema de información, la cual se tiene en el Anexo S. Además, el acta de validación de estas pruebas de funcionalidad de integración firmadas por el especialista de *Machine Learning* se encuentran en el Anexo AA.

## Capítulo 7. Conclusión de la investigación

La integración de tecnología *blockchain* en el sistema de información se ha revelado como una estrategia para potenciar la seguridad en el comercio electrónico. La inmutable naturaleza de los datos, la transparencia en el registro de transacciones y la capacidad de trazabilidad contribuyen en gran medida a mitigar los riesgos de fraude, salvaguardando la integridad de la información frente a posibles manipulaciones o alteraciones.

Al eliminar intermediarios, la tecnología *blockchain* promueve una relación directa entre compradores y vendedores, simplificando la gestión de datos y permitiendo una verificación eficiente de las transacciones por parte de las partes involucradas. Esta reducción de errores potencia la experiencia del usuario y la eficiencia del sistema de información.

La adopción de una pasarela de pago segura, como Stripe, refuerza este enfoque al proporcionar una plataforma confiable para procesar pagos de manera segura y transparente. Al almacenar una representación en lugar de la información real del usuario, se garantiza una mayor integridad de los datos, mejorando la experiencia del usuario y minimizando riesgos de seguridad.

Por otro lado, el algoritmo de detección de fraude, gracias a su capacidad para analizar datos de forma dinámica y predecir con precisión la legitimidad de las transacciones, ofrece una capa adicional de protección tanto para compradores como para vendedores. Su implementación dentro del sistema de información permite una verificación continua de las transacciones, detectando y previniendo fraudes de manera oportuna, adaptándose constantemente a nuevos tipos de amenazas.

Al fortalecer la seguridad, aumentar la eficiencia y mejorar la experiencia del usuario, este proyecto sienta las bases para un entorno de comercio electrónico más robusto y confiable.

Tanto compradores como vendedores pueden operar con mayor confianza y tranquilidad, cumpliendo así con los objetivos establecidos y generando los resultados esperados.

A partir de los resultados obtenidos en este proyecto, se abren diversas líneas de trabajo futuro. Una de ellas es el despliegue del sistema en un entorno real, utilizando una blockchain pública completamente operativa y múltiples nodos para asegurar la descentralización y resiliencia del sistema.

Asimismo, se propone mejorar el algoritmo de detección de fraude mediante el entrenamiento con una base de datos más amplia y diversa, incorporando técnicas de aprendizaje automático más avanzadas que permitan reconocer nuevos patrones de fraude de manera autónoma.

Otra línea relevante es la adaptación del sistema a diferentes tipos de e-commerce, permitiendo su personalización según la naturaleza del negocio. Finalmente, se plantea la posibilidad de integrar otras tecnologías emergentes para fortalecer aún más la seguridad y confianza del sistema.

**Referencias**

Akhilomen, J. (2013). Data mining application for cyber credit-card fraud detection system. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 7987 LNAI*, 218–228. https://doi.org/10.1007/978-3-642-39736-3_17

Amazon Web Services. (2023). *¿Qué es Java? Explicación del lenguaje de programación Java - AWS.* https://aws.amazon.com/es/what-is/java/ (Consultado el 17 de octubre del 2023)

Amazon Web Services. (2023). *¿Qué es JavaScript? Explicación de JavaScript (JS) - AWS.* Recuperado de https://aws.amazon.com/es/what-is/javascript/ (Consultado el 17 de octubre del 2023)

Amazon Web Services. (2023). *What is Kafka? Managed Kafka - Amazon Managed Streaming for Apache Kafka (MSK) - AWS.* Recuperado de https://aws.amazon.com/es/msk/what-is-kafka/ (Consultado el 17 de octubre del 2023)

Amazon Web Services. (2023). *¿Qué es la detección de anomalías? - Explicación de la detección de anomalías en machine learning - AWS.* Recuperado de *https://aws.amazon.com/es/what-is/anomaly-detection/* (consultado el 11 de setiembre del 2023)

Americas Market Intelligence. (2022). Peru E-Commerce Market Data. Recuperado de https://americasmi.com/insights/peru-ecommerce-market-data/ (consultado el 17 de setiembre del 2023)

Auth0. (n.d.). ¿Qué es la autenticación? Introducción a IAM. Recuperado de https://auth0.com/es/intro-to-iam/what-is-authentication (consultado el 7 de abril del 2025)

AWS. (2023). *AWS | Lambda - Gestión de recursos informáticos*. Recuperado de https://aws.amazon.com/es/lambda/ (Consultado el 17 de octubre del 2023)

Anthony, Lee, M. C., Pearl, R. R., Edbert, I. S., & Suhartono, D. (2023). Developing an anti-counterfeit system using *blockchain* technology. Procedia Computer Science, 216, 86–95. https://doi.org/10.1016/j.procs.2022.12.114

Bank of America. (2022). *Fraud Protection, Prevention & Cyber Security Solutions*. Recuperado de https://business.bofa.com/en-us/content/fraud-prevention-and-cyber-security-solutions.html (consultado el 17 de setiembre del 2023)

Bayona, S., y Estrada, R. (2020). *Factores Críticos para la Adopción del Comercio Electrónico en Pymes de Turismo*. Recuperado de https://www.proquest.com/openview/8a793cf044392188fe43a595bcf6573d/%201?pq-origsite=gscholar&cbl=1006393

Beetrack. (2020). *Comercio electrónico: ventajas, desventajas y tipos*. Recuperado de https://www.beetrack.com/es/blog/comercio-electronico-ventajas (consultado el 21 de setiembre del 2023)

Berdik, D., Otoum, S., Schmidt, N., Porter, D., & Jararweh, Y. (2021). A Survey on *Blockchain* for Information Systems Management and Security. Information Processing and Management, 58(1). https://doi.org/10.1016/j.ipm.2020.102397

Cámara Peruana de Comercio Electrónico (CAPECE). (n.d.). Política de privacidad y protección de datos personales. Recuperado de https://capece.org.pe/politica-de-privacidad/ (consultado el 7 de abril del 2025)

CEI Centro de Estudios de Innovación. (n.d.). *¿Qué es figma? | La mejor herramienta de prototipado web*. Recuperado de https://cei.es/que-es-figma/ (Consultado el 30 de octubre del 2023)

Conekta. (2023). Seguridad en el comercio electrónico: cómo proteger tu negocio y los datos de tus clientes. Recuperado de https://www.conekta.com/blog/seguridad-comercio-electronico (consultado el 7 de abril del 2025)

Congreso del Perú. (2005). *Ley complementaria a la Ley de protección al consumidor en materia de servicios financieros LEY Nº 28587. Congreso del Perú.* https://www.leyes.congreso.gob.pe/Documentos/Leyes/28587.pdf

Cortés, N. (2023). *¿Qué es el daño reputacional, cómo sucede y cómo prevenir una crisis? LinkedIn.* Recuperado de https://www.linkedin.com/pulse/qu%C3%A9-es-el-da%C3%B1o-reputacional-c%C3%B3mo-sucede-y-prevenir-una-nicol%C3%A1s-cort%C3%A9s/?originalSubdomain=es (Consultado el 27 de enero del 2024)

De Negocios, F., Lucía Castillo Telles Daniel Antonio Arroyo García, A., & Laura Cuya, M. (n.d.). *UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS MODELO DE NEGOCIO B2C, TOMANDO COMO REFERENCIA AL PAÍS DE CHILE TRABAJO DE SUFICIENCIA PROFESIONAL Presentado por los Bachilleres*. Recuperado de https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/621424/TSP__Retos+y+estrategias+del+comercio+electro%20nico+peruano,+B2C.pdf?sequence=2

Dolader, C., Joan, R., Roig, B., Luís, J., & Tapia, M. (n.d.). *LA BLOCKCHAIN: FUNDAMENTOS, APLICACIONES Y RELACIÓN CON OTRAS TECNOLOGÍAS DISRUPTIVAS*.

Economipedia. (2016). *Intermediarios financieros - Definición, qué es y concepto*. Recuperado de *https://economipedia.com/definiciones/intermediarios-financieros.html* (consultado el 11 de setiembre del 2023)

Esfahbodi, A., Pang, G., & Peng, L. (2022). Determinants of consumers' adoption intention for blockchain technology in *E-commerce*. *Journal of Digital Economy*, *1*(2), 89–101.

ESGinnova Group. (2018). *Los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad*. Recuperado de https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/ (Consultado el 27 de enero del 2024)

https://doi.org/10.1016/j.jdec.2022.11.001

Ethereum (2023). *¿Qué es Ethereum?* Recuperado de https://ethereum.org/es/what-is-ethereum/ (Consultado el 17 de octubre del 2023)

García, J. (2009). *Análisis de problemas y toma de decisiones.* México D.F.: Pearson Educación. Recuperado de https://laedu.digital/2020/07/29/analisis-de-problemas-y-toma-de-decisiones/ (Consultado el 1 de octubre del 2023)

Gobierno del Perú. (2011). *Ley N° 29733 - Ley de Protección de Datos Personales. Gobierno del Perú.* https://cdn.www.gob.pe/uploads/document/file/272360/Ley%20N%C2%BA%2029733.pdf.pdf?v=1618338779

Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., & Ishfaq, M. (2022). Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing. In *Future Internet* (Vol. 14, Issue 11). MDPI. https://doi.org/10.3390/fi14110341

IBM. (n.d.). *Benefits of blockchain.* Recuperado de *https://www.ibm.com/es-es/topics/benefits-of-blockchain* (consultado el 11 de setiembre del 2023)

IBM. (n.d.). *¿Qué es la tecnología blockchain? - IBM Blockchain*. Recuperado de *https://www.ibm.com/es-es/topics/blockchain* (consultado el 11 de setiembre del 2023)

IBM. (2021). *Unified Modeling Language (UML) model*. Recuperado de https://www.ibm.com/docs/es/iis/11.5?topic=types-unified-modeling-language-uml-model (Consultado el 17 de octubre del 2023)

IEBS Business School. (2024). *Qué es PMBOK y cómo usarlo en gestión de proyectos*. Recuperado de https://www.iebschool.com/blog/que-es-pmbok-y-como-usarlo-en-gestion-de-proyectos-agile-scrum/ (Consultado el 27 de enero del 2024)

IEBSchool (2023). *Solidity: El lenguaje de programación de Ethereum*. Recuperado de https://www.iebschool.com/blog/solidity-lenguaje-programacion-ethereum-tecnologia/ (Consultado el 17 de octubre del 2023)

IONOS. (2023). ¿Qué es Solidity?. Recuperado de https://www.ionos.com/es-us/digitalguide/paginas-web/desarrollo-web/solidity/ (consultado el 7 de abril del 2025)

Instituto Europeo de Posgrado (IEP). (n.d.). ¿Cuáles son las ventajas del comercio electrónico?. Recuperado de https://iep.edu.es/ventajas-comercio-electronico/ (consultado el 7 de abril del 2025)

Investopedia. (2023). *E-commerce Defined: Types, History and Examples.* *https://www.investopedia.com/terms/e/ecommerce.asp* (consultado el 11 de setiembre del 2023)

Jain, V., Malviya, B., & Arya, S. (2021). *An overview of electronic commerce (e-commerce).* https://doi.org/10.47750/cibg.2021.27.03.090

Kaleido (2023). *Truffle: Blockchain and Smart Contract Tools*. Recuperado de https://www.kaleido.io/blockchain-platform/truffle Consultado el 17 de octubre del 2023)

Kaspersky (n.d.). *¿Qué es una brecha de seguridad?* Recuperado de https://www.kaspersky.es/resource-center/threats/what-is-a-security-breach (Consultado el 27 de enero del 2024)

Kitchenham, B. (2004). *Procedures for Performing Systematic Reviews*. https://romisatriawahono.net/lecture/rm/survey/research%20methodology/Kitchenham%20-%20Systematic%20Review%20Process%20Research%20-%202013.pdf (consultado el 18 de agosto del 2023)

Lucidchart. (2023). What is Unified Modeling Language https://www.lucidchart.com/pages/tutorial/uml (Consultado el 17 de octubre del 2023)

Lustig, N. (2018). *How MercadoLibre Dominates Latin America's E-commerce Industry*. *Nathan Lustig.* Recuperado de https://www.nathanlustig.com/how-mercadolibre-dominates-latin-americas-e-commerce-industry/ (consultado el 18 de setiembre del 2023)

Longo, F., Nicoletti, L., & Padovano, A. (2020). Estimating the Impact of Blockchain Adoption in the Food Processing Industry and Supply Chain. *International Journal of Food Engineering*, *16*(5–6). https://doi.org/10.1515/ijfe-2019-0109

Lifeder. (n.d.). *Investigación empírica*. Recuperado de https://www.lifeder.com/investigacion-empirica/ (consultado el 18 de agosto del 2023)

McCubbin, G. (2023). *Intro to Web3.js · Ethereum Blockchain Developer Crash Course. Dapp University*. Recuperado de https://www.dappuniversity.com/articles/web3-js-intro (Consultado el 17 de octubre del 2023)

Méndez Pérez, J. (n.d.). *Ie-P INFORME e-PAÍS Editado por ICEX España Exportación e Inversiones*. https://www.icex.es/content/dam/es/icex/oficinas/065/documentos/2022/02/documentos-anexos/DOC2022900785_2.pdf

Mendívil, I. (1997). *El ABC de los Documentos Electrónicos Seguros.* http://www.tierradelazaro.com/wp-content/uploads/2015/11/abc.pdf

Microsoft. (n.d.). *Microsoft Word: software de procesamiento de textos | Microsoft 365*. Recuperado de https://www.microsoft.com/es-es/microsoft-365/word (Consultado el 30 de octubre del 2023)

Microsoft. (2024). *¿Qué es .NET? Una plataforma para desarrolladores de código abierto*. Recuperado de https://dotnet.microsoft.com/es-es/learn/dotnet/what-is-dotnet (Consultado el 20 de marzo del 2024)

Microsoft. (n.d.). *¿Qué es seguridad de la información (Infosec)?* Recuperado de *https://www.microsoft.com/es-mx/security/business/security-101/what-is-information-security-infosec* (consultado el 11 de setiembre del 2023)

Microsoft Learn. (2021). *Event Logging (Event Logging) - Win32 apps | Microsoft Learn*. Recuperado de *https://learn.microsoft.com/en-us/windows/win32/eventlog/event-logging* (consultado el 11 de setiembre del 2023)

Milberg, S. J., Burke, S. J., Jeff Smith, H., & Kallman, E. A. (1995). *Personal Information and Regulatory Approaches* (Vol. 38, Issue 12).

Mohanta, B. K., Jena, D., Panda, S. S., & Sobhanayak, S. (2019). Blockchain technology: A survey on applications and security privacy Challenges. In Internet of Things (Netherlands) (Vol. 8). Elsevier B.V. https://doi.org/10.1016/j.iot.2019.100107

Moreno Sánchez, J. (2021). *Vulnerabilidades orientadas a clientes de e-commerce y su raíz de la pandemia COVID-19*. Recuperado de https://repository.libertadores.edu.co/bitstream/handle/11371/4909/Moreno_Sanchez_2021.pdf?isAllowed=y&sequence=1 (Consultado el 27 de enero del 2024)

Node.js (2022). Introducción a Node.js. Recuperado de https://nodejs.org/en/learn/getting-started/introduction-to-nodejs (Consultado el 19 de febrero del 2024)

Normas APA. (n.d.). Estado del arte. Recuperado de https://normasapa.in/estado-del-arte/ (consultado el 18 de agosto del 2023)

Observatorio Nacional de Prospectiva: CEPLAN. (2023). *Comercio electrónico en el Perú: Evolución, situación actual y perspectivas*. https://observatorio.ceplan.gob.pe/ficha/t68

Oracle Corporation. (2023). *¿Qué es MySQL?* https://www.oracle.com/pe/mysql/what-is-mysql/ (Consultado el 17 de octubre del 2023)

Pleskach, V., Krasnoshchok, V., Melnyk, M., Klymenko, S., & Tumasonis, R. (2022). Current State and Trends in the Development of E-Commerce Software Protection Systems. https://marketer.ua/e-commerce-worldwide-

Pranto, T. H., Noman, A. A., Rahaman, M., Haque, A. K. M. B., Islam, A. K. M. N., & Rahman, R. M. (2022). A Blockchain, Smart Contract and Data Mining Based Approach toward the Betterment of E-Commerce. Cybernetics and Systems, 53(5), 443–467. https://doi.org/10.1080/01969722.2021.2018545

Presidente La República, E. de. (n.d.). *LEY Nº 29571.-Código de protección y defensa del consumidor LEY Nº 29571*.

Project Management Institute (PMI). (2021). exclamation A Guide to the Project Management Body of Knowledge (PMBOK Guide) - Seventh Edition. Newtown Square, PA: PMI. https://www.pmi.org/pmbok-guide-standards/foundational/pmbok

PwC. (2021). *Blockchain: brindando confianza y transparencia*. Recuperado de *https://www.pwc.com/ia/es/publicaciones/perspectivas-pwc/Blockchain-brindando-confianza-y-transparencia.html* (consultado el 11 de setiembre del 2023)

React (2023). *Describir la UI – React*. Recuperado de https://es.react.dev/learn/describing-the-ui/ (Consultado el 17 de octubre del 2023)

Rodrigues, V. F., Policarpo, L. M., da Silveira, D. E., da Rosa Righi, R., da Costa, C. A., Barbosa, J. L. V., Antunes, R. S., Scorsatto, R., & Arcot, T. (2022). Fraud detection and prevention in e-commerce: A systematic literature review. Electronic Commerce Research and Applications, 56. https://doi.org/10.1016/j.elerap.2022.101207

Rojas, A., & Rodrigo, L. (n.d.). *UNIVERSIDAD TECNICA FEDERICO SANTA MARIA Peumo Repositorio Digital USM*

Sabatés1, L. A., & Roca2, J. S. (n.d.). *La revisión de la literatura científica: Pautas, procedimientos y criterios de calidad.* Recuperado de https://ddd.uab.cat/pub/recdoc/2020/222109/revliltcie_a2020.pdf (consultado el 18 de agosto del 2023)

Safety Net Project. (2022). *Intermediarios de datos*. Recuperado de https://www.techsafety.org/intermediarios-de-datos (consultado el 21 de setiembre del 2023)

Sage Advice. (2023). *Distribución: Qué papel ejercen los intermediarios*. Recuperado de

https://www.sage.com/es-es/blog/que-papel-ejercen-los-intermediarios-en-la-distribucion/ (consultado el 21 de setiembre del 2023)

Sánchez, J. A. (2016). *La Publicidad Engañosa en el Comercio Electrónico*. https://repository.usta.edu.co/handle/11634/1026

Seeking Alpha. (2022). *MercadoLibre Better E-Commerce Story Than Amazon*. Recuperado de https://seekingalpha.com/article/4538988-mercado-libre-better-e-commerce-story-than-amazon (consultado el 18 de setiembre del 2023)

SEON. (2018). *Machine Learning para detectar fraude*. Recuperado de *https://seon.io/es/recursos/machine-learning-para-detectar-fraude/* (consultado el 11 de setiembre del 2023)

Stripe. (2023). *Stripe | Plataforma de procesamiento de pagos por Internet*. Recuperado de https://stripe.com/es-us (Consultado el 17 de octubre del 2023)

Stripe. (2023). Cómo funciona el machine learning para detectar y prevenir el fraude en pagos. Recuperado de https://stripe.com/es/resources/more/how-machine-learning-works-for-payment-fraud-detection-and-prevention (consultado el 7 de abril del 2025)

Sullivan, F., & di Pierro, M. (n.d.). *SECTION TITLE COMPUTING PRESCRIPTIONS What Is the Blockchain?* www.computer.org/cise

Taherdoost, H., & Madanchian, M. (2023). Blockchain-Based E-Commerce: A Review on Applications and Challenges. In Electronics (Switzerland) (Vol. 12, Issue 8). MDPI. https://doi.org/10.3390/electronics12081889

Taibo Escarramán, A. (2022). *Seguridad en la Blockchain de Ethereum: explotación y mitigación de vulnerabilidades modernas en Smart Contracts*. Recuperado de https://oa.upm.es/70503/1/TFG_ALEJANDRO_TAIBO_ESCARRAMAN.pdf (Consultado el 19 de febrero del 2024)

TechTarget. (2023). *What Is GitHub? | Definition from TechTarget*. Recuperado de https://www.techtarget.com/searchitoperations/definition/GitHub (Consultado el 17 de octubre del 2023)

TensorFlow. (2023). *TensorFlow.js | Aprendizaje automático para desarrolladores de JavaScript*. Recuperado de https://www.tensorflow.org/js?hl=es-419 (Consultado el 17 de octubre del 2023)

Thomson Reuters. (2023). Ciberseguridad: riesgos y medidas para proteger tus datos. Recuperado de https://www.thomsonreutersmexico.com/es-mx/soluciones-fiscales/blog-fiscal/ciberseguridad-riesgos-y-medidas-para-proteger-tus-datos (consultado el 7 de abril del 2025)

Treiblmaier, H., & Sillaber, C. (2021). The impact of blockchain on e-commerce: A framework for salient research topics. Electronic Commerce Research and Applications, 48. https://doi.org/10.1016/j.elerap.2021.101054

Truffle Suite (2023). *Home*. Recuperado de https://trufflesuite.com (Consultado el 17 de octubre del 2023)

TutFG. (n.d.). *Todo lo que debes saber sobre las preguntas PICO + Ejemplos*. Recuperado de https://tutfg.es/preguntas-pico/ (Consultado el 27 de enero del 2024)

Universidad VIU. (2021). *Qué es la criptografía y cuáles son sus usos*. Recuperado de *https://www.universidadviu.com/es/actualidad/nuestros-expertos/que-es-la-criptografia-y-cuales-son-sus-usos* (consultado el 11 de setiembre del 2023)

VPN Unlimited. (n.d.). Acceso no autorizado. Recuperado de https://www.vpnunlimited.com/es/help/cybersecurity/unauthorized-access (consultado el 7 de abril del 2025)

Warkentin, M., & Orgeron, C. (2020). Using the security triad to assess blockchain technology in public sector applications. *International Journal of Information Management*, *52*. https://doi.org/10.1016/j.ijinfomgt.2020.102090

# Anexo

## Anexo A: Plan de proyecto

### Justificación

El proyecto en cuestión surge como respuesta a las deficiencias presentes en la seguridad de los sistemas de información en el ámbito del comercio electrónico. La creciente necesidad de abordar estas vulnerabilidades ha llevado a la concepción de esta iniciativa, que se propone no solo solucionar los problemas existentes, sino también elevar las expectativas en cuanto a seguridad y confiabilidad.

La pieza central de este proyecto es la implementación de la tecnología blockchain, junto con un algoritmo de detección de fraude. Esta combinación de tecnologías se presenta como una solución innovadora contra las brechas de seguridad presentes en la actualidad en el *e-commerce*. La tecnología blockchain no solo garantizará la inmutabilidad de los datos, sino que también proporcionará una seguridad incomparable. La autenticación y verificación de las transacciones en tiempo real serán posibles gracias a la criptografía y los *smart contracts*, asegurando así la fiabilidad de cada paso en el proceso de compra y venta. Además, el sistema realizará análisis minuciosos de datos históricos y en tiempo real para identificar patrones y comportamientos sospechosos, permitiendo así transacciones directas y seguras entre compradores y vendedores.

Este proyecto presentará control eficiente, así como también, capas de seguridad para la información relevante del comercio electrónico. La integridad de los

datos estará garantizada, previniendo cualquier manipulación o exposición no autorizada. Además, la eficiencia en la gestión de la información se verá significativamente mejorada gracias a los módulos y algoritmos implementados, lo que impactará positivamente la experiencia del usuario al proporcionar un entorno más seguro para las transacciones. También se enfocará en la trazabilidad de las transacciones, utilizando la identificación y análisis de patrones de usuario para prevenir cualquier movimiento fraudulento antes de que ocurra.

Este proyecto enfocado en la seguridad del comercio electrónico no solo protegerá los datos y las transacciones, sino que también revitalizará la confianza de los usuarios y las empresas. Al prevenir de manera proactiva actividades fraudulentas y garantizar transacciones seguras y legítimas, se establecerá un estándar más alto para la integridad en el comercio electrónico. Finalmente, este proyecto establece las bases para un ecosistema de comercio electrónico más confiable y seguro para todos los involucrados.

**Viabilidad**

Durante el transcurso de mi trayectoria académica, se han consolidado en mí conocimientos y experiencia en el ámbito de la programación web, incluyendo lenguajes como JavaScript, Java y React js. Además, he trabajado con herramientas de backend como MySQL y plataformas de control de versiones como GitHub.

En relación con la tecnología blockchain, a pesar de no poseer un conocimiento profundo en Ethereum, Solidity y Truffle, existen recursos como Web3.js que

facilitan la creación de APIs utilizando JavaScript. La abundancia de documentación disponible también contribuye significativamente a reducir la dificultad en el proceso de aprendizaje sobre los temas antes mencionado como también para los temas de criptografía y *machine learning*. Lo mismo ocurre con las demás herramientas mencionadas: la disponibilidad de documentación detallada facilita el aprendizaje y permite aprovechar al máximo estas tecnologías.

En cuanto al aspecto temporal, se establecerá un cronograma detallado que abarque todas las fases del proyecto, desde la fase inicial de la investigación hasta la implementación y las pruebas. Este cronograma incluirá estimaciones precisas del tiempo necesario para aprender y aplicar las tecnologías específicas requeridas.

En lo que respecta a la viabilidad económica, se considerarán los costos asociados con la adquisición de recursos adicionales, como la infraestructura del servidor vinculado a la implementación del *e-commerce*. Asimismo, se buscarán recursos gratuitos, como tutoriales y cursos en línea, que faciliten la adquisición de conocimientos sobre las herramientas necesarias, contribuyendo así a reducir los costos asociados con la formación y la implementación del proyecto.

**Alcance**

El proyecto tiene como propósito fundamental mejorar la seguridad y confiabilidad en las transacciones dentro del comercio electrónico a través de la implementación de un sistema de información basado en la tecnología blockchain y algoritmos de detección de fraude.

En este proyecto, se abordarán diversos tipos de transacciones, como las compras en línea y las transferencias de fondos entre compradores y vendedores. Los ataques considerados en función de la problemática incluyen la suplantación de identidad, movimientos fraudulentos, ataques cibernéticos y la manipulación y exposición de datos sensibles.

Acerca de la implementación del proyecto, se tiene la simulación de una red blockchain en un entorno local, elegido por su facilidad de uso y bajo consumo de recursos. Las transacciones simuladas se generarán internamente utilizando un conjunto de herramientas y algoritmos diseñados para replicar el comportamiento real de una red blockchain. Además, se integrarán datos históricos de transacciones simuladas para mejorar la representatividad del entorno de prueba. Estos datos históricos se basarán en patrones y características de transacciones reales, adaptados para su uso en la simulación. Asimismo, se incluirán datos de prueba específicamente diseñados para entrenar y evaluar el algoritmo de detección de fraude, los cuales se generarán de manera controlada para garantizar la eficacia del modelo.

Desde una perspectiva técnica, se emplearán nodos distribuidos para simular la descentralización y se configurarán parámetros de seguridad y cifrado siguiendo las mejores prácticas y las leyes de protección al consumidor.

Es importante señalar que el proyecto no incluirá la consideración de ataques específicos, como los de fuerza bruta, que quedan fuera del alcance. Asimismo, no se abordará exhaustivamente la evaluación del consumo energético asociado con la implementación de la tecnología blockchain ni se realizará un análisis

completo de todos los aspectos legales y regulatorios, centrándose únicamente en cumplir con los estándares de seguridad establecidos.

Dentro del alcance del proyecto, se contempla la participación de un especialista, quien colaborará en la evaluación de documentaciones, las pruebas de aceptación del prototipo (tanto de la interfaz gráfica como de la arquitectura), y también participará en las pruebas de resistencia de ataques sobre las credenciales de usuario y en las pruebas de seguridad sobre el sistema de pago. Su función incluirá asegurar la seguridad en la transmisión de datos, gestionar errores de pagos y revisar tanto la recolección como el procesamiento de datos, así como la selección del algoritmo de *machine learning*.

Finalmente, para lograr este propósito ambicioso, dentro del alcance se llevarán a cabo una serie de actividades esenciales y estratégicas:

- **Implementación de una Red Blockchain para el Comercio Electrónico Descentralizado:** Se creará una red blockchain segura para respaldar un sistema de comercio electrónico descentralizado. Esta tecnología permitirá la creación de un libro de contabilidad inmutable y transparente. Cada transacción se registrará en bloques de datos cifrados, asegurando así la integridad de la información y eliminando cualquier posibilidad de manipulación. Esta transparencia promueve la confianza en todas las transacciones realizadas en la plataforma.
- **Módulo de Seguridad y Almacenamiento de Datos Sensibles:** Se implementará un módulo de seguridad avanzado para almacenar información sensible de los usuarios en bloques cifrados. Este enfoque

garantiza la privacidad y protección contra accesos no autorizados, lo que es fundamental para cualquier sistema que maneje datos sensibles.

- **Autenticación y Verificación en Tiempo Real:** Se desarrollará un módulo de autenticación y verificación de transacciones en tiempo real utilizando *Smart Contracts* y criptográficas avanzadas. Esto no solo garantiza la confiabilidad de las transacciones, sino que también protege las credenciales e identidades de los usuarios, creando así un ambiente seguro y confiable para el comercio electrónico.
- **Implementación de Algoritmos de Análisis Predictivo:** Se integrarán algoritmos de análisis predictivo que monitorearán las transacciones y los comportamientos de los usuarios en tiempo real. Estos algoritmos identificarán patrones y comportamientos sospechosos, permitiendo la detección temprana de actividades fraudulentas y mejorando la capacidad del sistema para responder de manera proactiva a posibles amenazas.
- **Desarrollo de Funcionalidades Interactivas:** Se desarrollarán funcionalidades que faciliten la interacción directa entre vendedores y consumidores, promoviendo así un entorno de comercio electrónico dinámico y eficiente.
- **Integración de Módulos para Mejorar la Experiencia del Usuario:** Se integrarán módulos esenciales para mejorar la experiencia del usuario, incluyendo un sistema de pago seguro que ofrecerá opciones confiables y convenientes. Además, se implementará un proceso de verificación de identidades en tiempo real para garantizar la autenticidad de las

transacciones. También se establecerá un sistema de retroalimentación y calificaciones que permitirá a los usuarios dejar comentarios sobre sus experiencias, fomentando así la transparencia y la confianza en la plataforma.

- **Establecimiento de Sistemas de Monitoreo Continuo y Evaluaciones Periódicas:** Se establecerán sistemas de monitoreo continuo en tiempo real para supervisar la eficiencia de las transacciones y abordar cualquier problema de inmediato. Además, se realizan evaluaciones periódicas para medir la eficacia del sistema en la detección y prevención de fraudes, así como para evaluar el nivel de confianza del usuario. Estos procesos de evaluación serán fundamentales para identificar áreas de mejora y garantizar que el sistema esté siempre alineado con las expectativas y requerimientos de los usuarios.

Todas estas actividades se llevarán a cabo utilizando las herramientas y procedimientos detallados en el apartado 1.3 del documento, asegurando así la eficiencia y el rendimiento óptimo del sistema. Con esta implementación integral y cuidadosamente diseñada, el proyecto se posicionará como un referente en la seguridad y confiabilidad en el comercio electrónico, ofreciendo a los usuarios una experiencia sin preocupaciones y altamente segura.

**Limitaciones**

Se procederá a detallar las restricciones que incluye este proyecto:

- Para asegurar la validez de los resultados del proyecto, es importante contar con la participación de al menos un experto. Sin embargo, una

limitación potencial radica en la disponibilidad de dicho experto para gestionar los resultados obtenidos.

- Las evaluaciones de cada módulo, junto con las evaluaciones integrales, se llevan a cabo en ambientes locales que representan una red de blockchain. La razón detrás de que se tiene una limitación de los costos adicionales que surgirían al implementarlas en otro entorno, donde sería necesario incurrir en gastos monetarios.
- Dentro de sus limitaciones, se reconoce que las pruebas se llevarán a cabo en un entorno simulado, lo que podría no reflejar todas las complejidades del entorno de producción real.
- La representatividad de los datos históricos estará sujeta a la disponibilidad de información, y la investigación se centrará en un contexto de comercio electrónico genérico, sin abordar las particularidades de diferentes industrias o modelos comerciales más complejos.
- Se destaca que la eficacia de los algoritmos de análisis predictivo dependerá de la cantidad y calidad de los datos disponibles para el entrenamiento, lo que podría afectar la capacidad del sistema para identificar patrones de comportamiento fraudulentos.

**Riesgos**

**A. Identificación de riesgos del proyecto**

Los riesgos fueron identificados mediante un análisis exhaustivo del contexto actual del proyecto. Como resultado de este análisis, se presenta

en la tabla 16, la matriz de riesgos que evalúa tanto la probabilidad como el impacto para determinar la severidad del riesgo, clasificándose como bajo, moderado o alto.

- **Tabla 16: Matriz de riesgos**

| **Impacto\Probabilidad** | Baja | Medio | Alta |
|---|---|---|---|
| Alto | Media | Alta | Alta |
| Medio | Baja | Media | Alta |
| Baja | Baja | Baja | Media |

Nota: Elaboración propia

**B. Riesgos identificados**

A continuación, se presenta un listado de riesgos acompañado de sus evaluaciones de probabilidad, impacto, severidad, así como los planes de mitigación y contingencia asociados en la tabla 17. Con base en los resultados obtenidos y en la matriz de riesgos previamente presentada, podremos determinar si un riesgo se clasifica como alto o bajo.

■ **Tabla 17: Listado de Riesgos**

| N° | Descripción del Riesgo | Causa | Probabilidad | Impacto | Severidad | Plan de Mitigación | Plan de Contingencia |
|---|---|---|---|---|---|---|---|
| 1 | Pérdida del avance | Falla del sistema operativo o problemas de conexión | Media | Alta | Alta | Guardar constantemente los avances en el repositorio GitHub y tener una copia de seguridad en otra computadora. | Utilizar tiempo extra para rehacer el avance de forma más rápida. |
| 2 | Presencia de una enfermedad por parte del autor de la tesis | Problemas de salud tanto física como mental. | Media | Alta | Alta | El autor debe mantener un cuidado de la salud, gestionando el estrés u otras enfermedades mediante un seguimiento médico. | Mantener comunicación con la institución mediante registros detallados sobre la situación médica. |
| 3 | Riesgo de resistencia cultural y organizativa | Falta de comprensión o aceptación inicial de los beneficios y cambios asociados | Media | Alta | Alta | Realizar demostraciones prácticas y casos de uso para ilustrar cómo la implementación de blockchain y algoritmos de detección de fraude simplificará procesos | Incorporar un ciclo continuo de adaptación basado en la retroalimentación recibida. |
| 4 | Acceso a datos | Limitaciones al | Alta | Media | Alta | Buscar y evaluar diversas | Desarrollar modelos de |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | históricos de transacciones | obtener esta clase de datos importantes para el algoritmo de detección de fraude | | | | fuentes de datos disponibles, incluidas bases de datos públicas para garantizar un acceso adecuado a los datos históricos necesarios | simulación que generen datos sintéticos que imitan patrones de transacciones reales para el entrenamiento y evaluación del algoritmo de detección de fraude. |
| 5 | Retrasos en los entregables debido a problemas técnicos | Falla de internet. | Media | Alta | Alta | Realizar pruebas exhaustivas para evitar los problemas técnicos. | Realizar procedimientos alternativos para poder realizar la entrega. |
| 6 | Estimación equivocada de los tiempos para cada tarea | No se tomó en cuenta el tiempo necesario para cada tarea. | Baja | Alta | Media | Revisar y ajustar regularmente las estimaciones a medida que avanza el proyecto. | Reevaluar y priorizar las tareas del proyecto en función del impacto en los objetivos finales. |
| 7 | Demora en la ejecución de tareas que puede | Estimación inadecuada de costos y esfuerzos | Baja | Alta | Media | Realizar una planificación detallada del proyecto, realizando seguimiento y asignación de recursos | Realizar un ajuste en las fechas de entregas y priorizar las tareas críticas. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | ocasionar retrasos en las tareas subsecuentes | | | | | necesarios. | |
| 8 | Retraso del desarrollo debido a las validaciones de expertos | No disponibilidad de los expertos identificados | Baja | Alta | Media | Definir cronogramas claros y realistas para las validaciones de expertos. | Identificar expertos de reserva que puedan realizar la revisión en el plazo determinado. |
| 9 | Riesgo de falsos positivos en la detección de fraude | Identificación errónea de transacciones legítimas como fraudulentas | Baja | Alta | Media | Efectuar un análisis constante y detallado de los modelos de identificación de fraude. | Implementar un proceso de revisión manual para transacciones identificadas como posibles falsos positivos |

Nota: Elaboración propia

## Estructura de descomposición del trabajo (EDT)

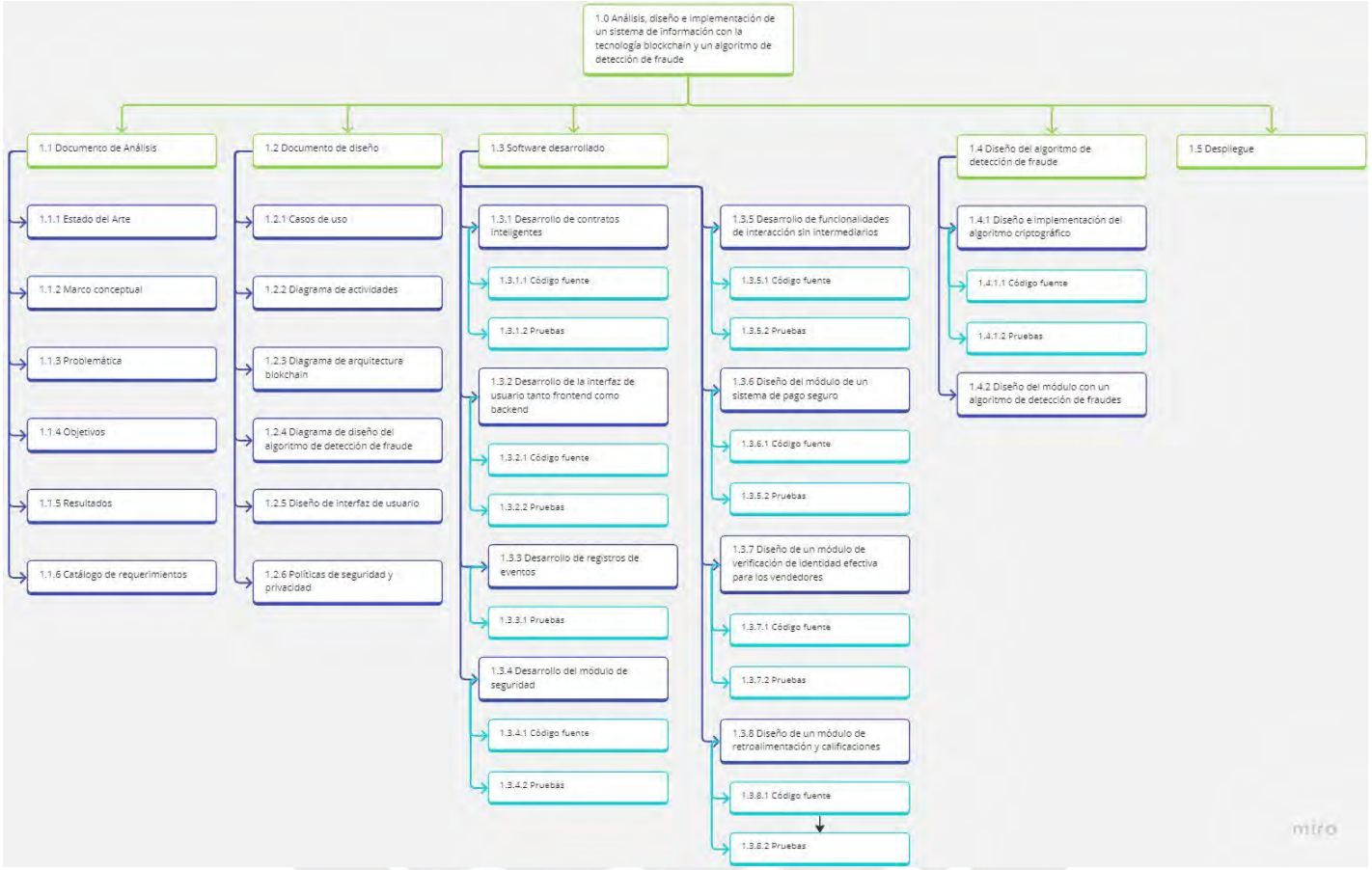


Figura 1. Estructura de descomposición del trabajo para el proyecto.

(Elaboración propia)

## Lista de tareas

| ID | Nombre | Duración estimada (Horas) | Esfuerzo estimado (Horas - persona) |
|---|---|---|---|
| | **Proyecto de Tesis** | **143** | **150** |
| | **1.1. Estado del arte** | **50** | **51** |
| 01 | Explorar en motores de bases de datos. | 24 | 24 |
| 02 | Elaborar el formulario para la recolección de datos | 24 | 24 |

| | | | |
|---|---|---|---|
| 03 | Reunión con el asesor y profesores del curso | 2 | 3 |
| | **1.2. Marco conceptual** | **23** | **23** |
| 04 | Investigación de los conceptos en internet | 18 | 18 |
| 05 | Leer leyes relacionado a la protección | 5 | 5 |
| | **1.3. Problemática** | **29** | **31** |
| 06 | Examinar la problemática en diversos artículos | 18 | 18 |
| 07 | Elaborar árbol de problemas | 4 | 4 |
| 08 | Reunión con el asesor | 2 | 4 |
| 09 | Elaborar la descripción del problema en cuestión | 5 | 5 |
| | **1.4. Objetivos** | **8** | **9** |
| 10 | Establecer el propósito principal del proyecto | 3 | 3 |
| 11 | Establecer los objetivos específicos | 3 | 3 |
| 12 | Reunión con el asesor y profesores del curso | 2 | 3 |
| | **1.5. Resultados** | **11** | **11** |
| 13 | Definir los resultados esperados | 3 | 3 |
| 14 | Crear el mapeo de objetivos, resultados y verificación | 4 | 4 |
| 15 | Definir las herramientas y métodos | 4 | 4 |
| | **1.6. Plan de proyecto** | **22** | **22** |
| 16 | Definir la justificación del proyecto | 2 | 2 |
| 17 | Definir la viabilidad del proyecto | 2 | 2 |
| 18 | Elaborar el alcance del proyecto | 2 | 2 |

| | | | |
|---|---|---|---|
| 19 | Definir las limitaciones del proyecto | 2 | 2 |
| 20 | Desarrollar el plan de manejo de riesgos | 3 | 3 |
| 21 | Elaborar el EDT | 3 | 3 |
| 22 | Elaborar la lista de actividades | 2 | 2 |
| 23 | Desarrollar el cronograma del proyecto | 2 | 2 |
| 24 | Definir recursos del proyecto | 2 | 2 |
| 25 | Definir el coste del proyecto | 2 | 2 |

Nota: Elaboración propia

**Cronograma del proyecto**

| ID | Nombre | Fecha inicio | Fecha fin | Dependencia |
|---|---|---|---|---|
| - - | Proyecto de tesis | 28/08/2023 | | |
| | **1.1. Estado del arte** | **28/08/2023** | **11/09/2023** | |
| 01 | Explorar en motores de bases de datos. | 28/08/2023 | 04/09/2023 | |
| 02 | Elaborar el formulario para la recolección de datos | 04/09/2023 | 11/09/2023 | 01 |
| 03 | Reunión con el asesor y profesores del curso | 11/09/2023 | 11/09/2023 | 02 |
| | **1.2. Marco conceptual** | **11/09/2023** | **18/09/2023** | |
| 04 | Investigación de los conceptos en internet | 11/09/2023 | 15/09/2023 | 02 |
| 05 | Leer leyes relacionado a la protección | 16/09/2023 | 18/09/2023 | 02 |
| | **1.3. Problemática** | **18/09/2023** | **20/09/2023** | |
| 06 | Examinar la problemática en diversos artículos | 18/09/2023 | 18/09/2023 | 03 |
| 07 | Elaborar árbol de | 18/09/2023 | 19/09/2023 | 06 |

| | | | | |
|---|---|---|---|---|
| | problemas | | | |
| 08 | Reunión con el asesor | 20/09/2023 | 20/09/2023 | 07 |
| 09 | Desarrollar la descripción de la problemática | 20/09/2023 | 20/09/2023 | 08 |
| | **1.4. Objetivos** | **22/09/2023** | **02/10/2023** | |
| 10 | Establecer el propósito principal del proyecto | 22/09/2023 | 27/09/2023 | 09 |
| 11 | Establecer los objetivos específicos | 27/09/2023 | 02/10/2023 | 10 |
| 12 | Reunión con el asesor y profesores del curso | 02/10/2023 | 02/10/2023 | 11 |
| | **1.5. Resultados** | **02/10/2023** | **18/10/2023** | |
| 13 | Definir los resultados esperados | 02/10/2023 | 09/10/2023 | 12 |
| 14 | Crear el mapeo de objetivos, resultados y verificación | 09/10/2023 | 13/10/2023 | 13 |
| 15 | Definir las herramientas y métodos | 13/10/2023 | 18/10/2023 | 14 |
| | **1.6. Plan de proyecto** | 18/10/2023 | 15/10/2023 | |
| 16 | Definir la justificación del proyecto | 18/10/2023 | 20/10/2023 | 15 |
| 17 | Definir la viabilidad del proyecto | 20/10/2023 | 21/10/2023 | 16 |
| 18 | Elaborar el alcance del proyecto | 21/10/2023 | 23/10/2023 | 17 |
| 19 | Definir las limitaciones del proyecto | 23/10/2023 | 26/10/2023 | 18 |
| 20 | Desarrollar el plan de manejo de riesgos | 26/10/2023 | 01/11/2023 | 19 |
| 21 | Elaborar el EDT | 01/11/2023 | 04/11/2023 | 20 |
| 22 | Elaborar la lista de actividades | 04/11/2023 | 06/11/2023 | 21 |
| 23 | Desarrollar el cronograma | 06/11/2023 | 10/11/2023 | 22 |

| | | | | |
|---|---|---|---|---|
| | del proyecto | | | |
| 24 | Definir recursos del proyecto | 10/11/2023 | 13/11/2023 | 23 |
| 25 | Definir el coste del proyecto | 13/11/2023 | 15/10/2023 | 24 |

Nota: Elaboración propia

**Recursos del proyecto**

| | **Descripción** | **Cantidad** | **Oportunidad de uso** |
|---|---|---|---|
| **1** | **Involucrados** | | |
| 1.1. | Tesista | 1 | Elaborar el proyecto de tesis |
| 1.2. | Asesor de tesis | 1 | Orientar al tesista en habilidades técnicas. |
| 1.3. | Profesores del curso | 3 | Instruir al tesista sobre los procedimientos de investigación. |
| 1.4. | Jurados de exposición | 2 | Evaluar la exposición del trabajo de tesis. |
| 1.5. | Especialista de *Blockchain* | 1 | Realizar la revisión y validación de los documentos pertinentes. |
| 1.6. | Especialista de *e-commerce* | 1 | Realizar la revisión y validación de los documentos pertinentes. |
| 1.7. | Analista de datos | 1 | Realizar la revisión y validación de los documentos pertinentes. |
| 1.8. | Especialista de *Machine Learning* | 1 | Realizar la revisión y validación de los documentos pertinentes. |
| **2** | **Estándares** | | |
| 2.1. | Normativas jurídicas, procedimientos y técnicas de los sistemas informativos. | - - - | En el proceso de creación del Software. |
| **3** | **Equipamiento** | | |
| 3.1. | Laptop | 1 | Para elaborar la tesis, donde se realizará la documentación y la programación. |
| 3.2. | Energía eléctrica | - - - | Para proporcionar iluminación al tesista. |

| | | | |
|---|---|---|---|
| 3.3. | Servicio de internet | - - - | Para poder establece una conexión a las herramientas que incorporen internet |
| 4 | Herramientas requeridas | | |
| 4.1. | Ethereum | - - - | Para implementar el sistema de información. |
| 4.2. | Solidity | - - - | Para elaborar el contrato inteligente. |
| 4.3. | Truffle | - - - | Para desarrollar el contrato inteligente. |
| 4.4. | Ganache | - - - | Para desarrollar proyectos relacionados a Ethereum. |
| 4.5. | JavaScript | - - - | Para implementar el sistema de información. |
| 4.6. | Web3.js | - - - | Para conectar los nodos de la red Ethereum con las bibliotecas de JavaScript. |
| 4.7. | React js | - - - | Para elaborar el *front-end* del sistema. |
| 4.8. | .Net | - - - | Para desarrollar el *back-end* del sistema. |
| 4.8. | Github | - - - | Administrar las ediciones del proyecto. Además de ser un almacenamiento de copia de seguridad en internet. |
| 4.9. | Lucidchart | - - - | Para elaborar los esquemas de diseño y estudio. |
| 4.10. | Figma | - - - | Para realizar los diagramas de diseño y análisis. |
| 4.11. | Microsoft Word | - - - | Manejo de los requisitos tanto funcionales como no funcionales. |
| 4.12. | Microsoft Excel | - - - | Manejo de los requisitos tanto funcionales como no funcionales. |
| 4.13. | Apache Kafka | - - - | Para gestionar las operaciones de pagos sin intermediarios. |
| 4.14. | Node.js | - - - | Para la ejecución de proyectos de Javascript |
| 4.15. | MySQL | - - - | Para el almacenamiento de datos de manera local y para el desarrollo del back-end. |
| 4.16. | TensorFlow.js | - - - | Para el entrenamiento de modelos de |

| | | | |
|---|---|---|---|
| | | | aprendizaje automático y su interacción con JavaScript. |
| 4.17. | Stripe | - - - | Para el procesamiento de pagos en línea. |
| 4.18. | Algoritmo de Detección de Fraude | - - - | Para detección y prevención de las operaciones fraudulentas usando detección de anomalías. |

Nota: Elaboración propia

**Costeo del proyecto**

| Ítem | Descripción | Unidad | Cantidad |
|---|---|---|---|
| **0.** | **Costo total del proyecto** | | **439** |
| **1.** | **Estudiante o tesista** | | |
| 1.1. | Tesista | Horas | 364 |
| **2.** | **Otros participantes** | | |
| 2.1. | Asesor de Tesis | Horas | 40 |
| 2.2. | Profesor del curso | Horas | 30 |
| 2.3. | Jurados de exposición del curso | Horas | 2 |
| **3** | **Servidores** | | |
| 3.1. | Máquina virtual blockchain Ethereum | - - - | 1 |
| 3.2. | Servidor Ganache para proyectos Ethereum | - - - | 1 |

Nota: Elaboración propia

**Anexo B: Entregable Parcial 1.1 (E1.1) del curso Proyecto de Tesis 1**

20191425_HenryPebe_LuisFlores_E1.1.docx

**Anexo C: Documento de los requerimientos funcionales y no funcionales**

20191425_Henry_Pebe_Luis_Flores_Requerimientos_Funcional_y_No_Funcional.xlsx

**Anexo D: Acta de reunión con el especialista de *E-commerce***

20191425_Henry Pebe_LuisFlores_Acta de Reunion_Ecommerce.pdf

20191425_Henry Pebe_Luis Flores_Acta de Reunion_Ecommerce_2.pdf

**Anexo E: Acta de reunión con el especialista de seguridad de información en términos de fraude**

20191425_Henry Pebe_Luis Flores_Acta de Reunion_Fraude.pdf

20191425_Henry Pebe_Luis Flores_Acta de Reunion_Fraude_2.pdf

**Anexo F: Documento de Arquitectura de Software del sistema**

20191425_Henry Pebe_Luis Flores_Arquitectura de Software.docx

**Anexo G: Acta de validación con el especialista de arquitectura de software**

20191425_Henry Pebe_Luis Flores_Acta validación de la arquitectura de software.pdf

**Anexo H: Documento del Prototipo de la interfaz gráfica del sistema de información**

20191425_Henry Pebe_Luis Flores_Interfaz Gráfica.docx

**Anexo I: Documento de la Recolección y procesamiento de datos de transacción históricas y en tiempo real**

20191425_Henry Pebe_Luis Flores_Recolección y Procesamiento de datos.docx

**Anexo J: Documento de la selección de algoritmos de machine learning y el código fuente del algoritmo de detección de fraude**

20191425_Henry Pebe_Luis Flores_Selección de algoritmos.docx

**Anexo K: Código fuente del sistema de información**

https://github.com/henrypebe/Tesis2.git

**Anexo L: Acta de validación por parte del especialista de Seguridad de datos**

20191425_Henry Pebe_Luis Flores_Acta de validacion_Fraude.pdf

**Anexo M: Documentación sobre las verificaciones de la funcionalidad del algoritmo de detección**

20191425_Henry Pebe_ Luis Flores_Verificacion del Algoritmo de detección de fraude.docx

**Anexo N: Documentación de funcionalidad de la interacción directamente entre comprador y vendedor**

20191425_Henry Pebe_Luis Flores_Prueba de la funcionalidad de la interacción directa.docx

**Anexo O: Documentación de funcionalidad de la integración de la pasarela de pago**

20191425_Henry Pebe_Luis Flores_Prueba de funcionamiento del sistema de pago.docx

**Anexo P: Documentación de funcionalidad del almacenamiento de las transacciones en un Smart Contract**

20191425_Henry Pebe_Luis Flores_Pruebas de almacenamiento en Smart Contract.docx

**Anexo Q: Documentación de funcionalidad del algoritmo criptográfico**

20191425_Henry Pebe_Luis Flores_Pruebas de funcionamiento del algoritmo criptográfico.docx

**Anexo R: Documentación de funcionalidad del sistema de información**

20191425_Henry Pebe_Luis Flores_Pruebas de funcionalidad del sistema de información.docx

**Anexo S: Documentación de la prueba de funcionamiento de la integración del algoritmo de detección de fraude**

20191425_Henry Pebe_Luis Flores_Pruebas de integración del algoritmo de detección de fraude.docx

**Anexo T: Acta de validación de los requerimientos del objetivo 1 por parte del especialista de *Blockchain***

20191425_Henry Pebe_Luis Flores_Validación con Experto_Resultado 1.pdf

**Anexo U: Acta de validación de los requerimientos del objetivo 2 por parte del especialista de *E-commerce***

20191425_Henry Pebe_Luis Flores_Validación con Experto_Resultado 4.pdf

**Anexo V: Acta de validación de las pruebas de funcionalidad del sistema de información por parte del especialista de *E-commerce***

20191425_Henry Pebe_Luis Flores_Validación con Experto_Resultado 5.pdf

**Anexo W: Acta de validación de las pruebas de la funcionalidad de la interacción directa del comprador y el vendedor por parte del especialista de *E-commerce***

20191425_Henry Pebe_Luis Flores_Validación con Experto_Resultado 6.pdf

**Anexo X: Acta de validación de las pruebas de la funcionalidad del módulo de pago por parte del especialista de *E-commerce***

20191425_Henry Pebe_Luis Flores_Validación con Experto_Resultado 7.pdf

**Anexo Y: Acta de validación de los requerimientos del objetivo 3 por parte del especialista de *Machine Learning***

20191425_Henry Pebe_Luis Flores_Validación con Experto_Resultado 8.pdf

**Anexo Z: Acta de validación de las pruebas de la funcionalidad del algoritmo de detección por parte del especialista de *Machine Learning***

20191425_Henry Pebe_Luis Flores_Validación con Experto_Funcionalidad del algoritmo.pdf

**Anexo AA: Acta de validación de las pruebas de funcionalidad, rendimiento y seguridad después de la integración por parte del especialista de *Machine Learning***

20191425_Henry Pebe_Luis Flores_Validación con Experto_Integración del algoritmo.pdf