

**INGENIERÍA DE SISTEMAS**

**SISTEMA DE ADMINISTRACIÓN DE INVENTARIOS DE INSUMOS PARA LABORATORIO DE ÓPTICA PARA LA MEJORA DEL MANEJO ADMINISTRATIVO**

**Proyecto de Grado para optar al grado de licenciatura en Ingeniería de sistemas**

**Autor: Daniel Santiago Soto Villamil**

**Tutor: Maritza Neysi Paiva Zapana**

**La Paz - Bolivia**

**2024**

**RESUMEN**

**TÍTULO:** SISTEMA DE ADMINISTRACIÓN PARA LA OPTIMIZACIÓN DE INVENTARIOS EN ÓPTICAS CON IMPLEMENTACIÓN DE SEGURIDAD BASADA EN LA ISO 27001 E ISO 27002

AUTOR: DANIEL SANTIAGO SOTO VILLAMIL

PROBLEMÁTICA

Deficiente administración de inventarios y seguridad en los inventarios en ópticas.

OBJETIVO GENERAL

Desarrollar un sistema de administración de inventarios de insumos para laboratorio de óptica para la mejora del manejo administrativo.CONTENIDO

Desarrollo de un sistema de administración de inventarios con implementación de seguridad basada en las normas ISO 27001 e ISO 27002 para ópticas, mediante tecnologías de desarrollo web para el manejo seguro de información sensible, y datos centralizados en un gestor de base de datos.

CARRERA : Ingeniería de Sistemas

PROFESOR GUÍA : Ing. Maritza Paiva Zapana

DESCRIPTORES O TEMAS : Sistema web, React.js Nest.js,

Node.js, PostgreSQL, TypeScript, JavaScript.

PERÍODO DE INVESTIGACIÓN : 2024

EMAIL DE LOS AUTORES : Santiago\_SV@outlook.es

**ÍNDICE**

CAPITULO I

INTRODUCCIÓN

1.1. Antecedentes 1

1.2. Planteamiento Del Problema 4

1.2.1. Identificación Del Problema 6

1.2.2. Problema Central 6

1.2.3. Formulación Del Problema 7

1.3. Objetivos DE LA INVESTIGACION 7

1.3.1. Objetivo General 7

1.3.2. Objetivos Específicos 7

1.3.3. Límite Temporal 8

1.3.4. Límite Geográfico 8

1.4. Justificación 9

1.4.1. Justificación Social 9

1.4.2. Justificación Económica 9

1.5. Tipología Del PROYECTO 10

1.6. MÉTODOS DE INVESTIGACIÓN 11

1.6.1. Enfoque De La Investigación 11

1.6.2. Métodos De Investigación 11

1.6.3. Diseño De La Investigación 12

1.6.4. Tipo De Investigación 12

1.7. Técnicas De Investigación Y Sus Instrumentos 13

1.7.1. Las Entrevistas en Profundidad 13

1.8. Población Y Muestra 14

1.8.1. Población 14

1.8.2. Muestra 14

1.9. Cronograma De GANT 16

CAPITULO II

MARCO TEÓRICO

2.1. Sistema 17

2.2. SISTEMA WEB 17

2.3. HERRAMIENTAS DE DESARROLLO 19

2.3.1. JavaScript 19

2.3.2. TypeScript 21

2.3.3. Node.JS 23

2.3.4. NestJS 24

2.3.5. React 26

2.3.6. TyperORM 27

2.3.7. Material UI 27

2.4. BASE DE DATOS 28

2.4.1. Sistema de Gestión de Bases de Datos 29

2.4.2. SQL 30

2.5. INventario 31

2.5.1. Inventario en la Cadena de Suministro 32

2.5.2. Tipos de Inventario y su Clasificación 33

2.5.2.1. Inventario de ciclo 33

2.5.2.2. Inventario de seguridad 33

Inventario en transito 34

Inventario promocional 34

Inventario de demostración 34

Inventario minorista en bodega 35

Inventario Estacional 35

2.6. ISO 27001 35

2.6.1. Principios Fundamentales de la ISO/IEC 27001 37

2.6.1.1. Contexto de la Organización 37

2.6.1.2. Necesidades y Expectativas de las Partes Interesadas 37

2.6.2. Soporte en el Sistema de Gestión de la Seguridad de la Información (SGSI) 38

2.6.2.1. Recursos Necesarios 38

2.6.2.2. Competencia y Capacitación 39

2.6.2.3. Concienciación del Personal 39

2.6.2.4. Comunicación Efectiva 39

2.6.2.5. Gestión de la Información Documentada 40

2.6.3. Contexto de la Organización 41

2.6.3.1. Comprensión de la Organización y de su Contexto 41

2.6.3.2. Comprensión de las Necesidades de las Partes Interesadas 41

2.6.3.3. Determinación del Alcance del SGSI 42

2.6.3.4. Sistema de Gestión de la Seguridad de la Información 42

2.6.4. Compatibilidad con otras Normas de Sistemas de Gestión 43

**ÍNDICE DE TABLAS**

[Tabla 1 Cronograma de GANT 17](#_Toc183015907)

[Tabla 2 16](#_Toc183015908)

[Tabla 3 19](#_Toc183015909)

[Tabla 4 32](#_Toc183015910)

**ÍNDICE DE FIGURAS**

[**Diagrama de Ishikawa** **¡Error! Marcador no definido.**](#_Toc177572595)

# CAPITULO I

# INTRODUCCIÓN

## Antecedentes

El desarrollo de sistemas de gestión de inventarios ha sido un tema recurrente en el ámbito de la ingeniería de sistemas, dado su impacto directo en la eficiencia técnica y en la optimización de recursos dentro de las organizaciones. Diversos proyectos han abordado esta problemática desde distintas perspectivas, adaptándose a las necesidades específicas de cada sector. La implementación de un sistema centralizado de administración de inventarios, en particular para el sector óptico, representa un desafío técnico y organizacional, que no sólo busca mejorar la eficiencia en la administración de stock, sino también favorecer la seguridad de la información manejada, alineándose con estándares internacionales como ISO 27001 e ISO 27002.

Un primer antecedente relevante es el "Sistema Integrado de Control de Inventario 'ATIPAJ' Compañía Cervecera Boliviana S.A.", desarrollado por Verónica Coarite Tumiri. Este proyecto se centra en la implementación de un sistema de control de inventarios que busca optimizar la gestión de insumos y productos terminados en la empresa cervecera. Se destaca por su enfoque en la integración de diferentes procesos dentro de la empresa, permitiendo una gestión más eficiente y precisa del inventario. La metodología utilizada, basada en la optimización de flujos de trabajo y en la automatización de procesos, proporciona una base sólida para el desarrollo de sistemas similares en otros contextos, como el de las ópticas, donde la precisión en la gestión de inventarios es crucial.

Otro proyecto relevante es el "Sistema para la Gestión de Ventas e Inventario Caso: Importadora Soluciones Médicas Lifemed S.R.L." de Johovana La Fuente Choque. Este sistema fue diseñado para mejorar la gestión de inventarios y ventas en una importadora de soluciones médicas, enfocándose en la trazabilidad y control de productos sensibles. La experiencia obtenida en la gestión de productos de alta rotación y la necesidad de mantener un control estricto de los inventarios puede ser directamente aplicable a la gestión de inventarios en ópticas, donde los productos manejados, como lentes y equipos oftálmicos, también requieren un manejo cuidadoso para evitar pérdidas y optimizar la disponibilidad.

El "Sistema de Control de Inventarios para Laboratorios Crespal S.A. Regional Sucre" desarrollado por Juan Lucio Ramos Paye es otro antecedente que aporta valor a este análisis. Este proyecto aborda la necesidad de un control riguroso de inventarios en un entorno de laboratorio, donde la precisión y la confiabilidad de los datos son fundamentales. La implementación de un sistema que permite un seguimiento detallado de las entradas y salidas de materiales proporciona un marco útil para la gestión de inventarios en ópticas, donde se manejan productos delicados y costosos que deben estar disponibles en el momento justo para satisfacer las necesidades de los clientes.

Por su parte, el proyecto "Sistema de Información de Compras e Inventarios SAMA" de Raúl Francisco Choque Chambilla se centra en la gestión de compras e inventarios en una empresa manufacturera. La implementación de un sistema que no sólo gestiona el inventario, sino que también se integra con los procesos de compras permite una gestión más eficiente y coordinada de los recursos. En el contexto de una óptica, donde la coordinación entre la adquisición de productos y su disponibilidad en inventario es crucial, las lecciones aprendidas de este proyecto son particularmente relevantes.

El "Sistema de Control y Seguimiento de Almacenes para la Corte Departamental Electoral La Paz, Sala Provincias" desarrollado por Virginia Suarez Marin, aborda un contexto completamente diferente, pero con desafíos similares en términos de gestión y seguridad de la información. En este caso, el sistema implementado debía favorecer la integridad y disponibilidad de los materiales almacenados, así como la seguridad en su manejo. La implementación de controles y seguimientos rigurosos en este sistema puede ser adaptada para asegurar que los inventarios en una óptica estén no sólo bien gestionados, sino también protegidos contra accesos no autorizados y manipulaciones indebidas, alineándose con los estándares ISO 27001 e ISO 27002.

El proyecto "Sistema de Entradas y Salidas e Inventario Caso: BOLITAL S.R.L." de Claudia Chiri Honorio, aporta otro ejemplo de cómo la gestión de inventarios puede ser optimizada a través de un sistema automatizado que permita un seguimiento preciso de todos los movimientos de stock. La automatización de estos procesos no sólo mejora la eficiencia técnica, sino que también reduce el riesgo de errores humanos, un aspecto crítico cuando se manejan productos tan específicos como los que se encuentran en una óptica.

Finalmente, el "Software de Gestión y Control de Inventarios Caso: AGADON S.R.L." de Wilmer David Callisaya Apaza, destaca por su enfoque en la implementación de un sistema de gestión de inventarios con una alta dependencia en la tecnología y metodologías ágiles. Este proyecto es especialmente relevante porque integra prácticas de seguridad en la administración de inventarios, utilizando metodologías como Scrum y estándares de calidad como ISO 9126 para asegurar un producto final robusto y seguro. La aplicación de estas metodologías y estándares en el contexto de una óptica permitiría no sólo gestionar los inventarios de manera eficiente, sino también asegurar que la información sea manejada de forma segura y conforme a los requisitos de ISO 27001 e ISO 27002.

La revisión de estos proyectos muestra la importancia de un enfoque integral en la administración de inventarios, que combine la eficiencia técnica con la seguridad de la información. La implementación de un sistema centralizado de administración de inventarios para ópticas, basado en estándares de seguridad internacionales, no sólo mejorará la administración y el control de los productos, sino que también favorecerá la protección de la información, un aspecto cada vez más crítico en el entorno empresarial actual.

## Planteamiento Del Problema

En el contexto actual de las ópticas, la administración de inventarios es un proceso crítico que, si no se administra de manera eficiente, puede generar pérdidas económicas, desabastecimiento de productos y una falta de control sobre el stock disponible. Además, con la creciente digitalización de los procesos comerciales, la seguridad de la información se ha convertido en una prioridad. Sin embargo, muchas ópticas todavía operan con sistemas de administración de inventarios manuales y carecen de medidas de seguridad robustas, lo que las expone a riesgos de vulnerabilidad en la protección de datos.

La implementación de un Sistema de Administración de Inventarios para Ópticas con Optimización y Seguridad Basada en la ISO 27001 e ISO 27002 busca resolver estos desafíos, optimizando la administración del inventario para favorecer la disponibilidad de productos y protegiendo la información sensible conforme a los estándares internacionales de seguridad. El problema radica en el uso de un sistema manual que no administra eficientemente el inventario, sino que también no asegura la integridad y confidencialidad de los datos.

Evidencia de la problemática puede encontrarse en estudios previos que muestran cómo las empresas con sistemas de administración ineficientes experimentan pérdidas significativas de stock, mientras que aquellas que no implementan normativas de seguridad adecuadas enfrentan brechas en la protección de su información (López, 2021). Esto afecta directamente la competitividad de las ópticas, incrementando sus costos operativos y reduciendo su capacidad de responder a la demanda del mercado.

Se espera que el desarrollo de este sistema no solo optimice la operatividad técnica de las ópticas en la administración de inventarios, sino que también brinde una solución robusta para favorecer la seguridad de la información, cumpliendo con las exigencias actuales del mercado en cuanto a eficiencia y protección de datos.

### Identificación Del Problema

El diagrama de Ishikawa se justifica como una herramienta esencial para desglosar y analizar de manera estructurada las causas que contribuyen a la administracion ineficaz de inventarios en ópticas. Al identificar las principales áreas problemáticas, como tecnología, procesos, personal, seguridad, recursos y comunicación, el diagrama facilita una comprensión clara de los factores subyacentes que afectan la eficiencia y seguridad del sistema de inventarios. Esto permite orientar mejor las acciones correctivas y diseñar soluciones que aborden las causas raíz, asegurando una implementación más efectiva de un sistema centralizado y seguro.

Figura 1

Diagrama Ishikawa

Imagen que contiene Diagrama

Descripción generada automáticamente

### Problema Central

La deficiente administración de inventarios y seguridad en las ópticas está afectando tanto la eficiencia operativa como la integridad de la información. Esta situación genera pérdidas económicas, errores en el control de inventarios y aumenta los riesgos asociados a la seguridad de los datos, lo cual puede comprometer tanto la continuidad del negocio como la confianza de los clientes. Se hace necesario optimizar los procesos y mejorar los controles de seguridad para mitigar estos problemas.

### Formulación Del Problema

¿Cuáles son las deficiencias en la administración de inventarios y la seguridad de la información en las ópticas, y cómo afectan estas a la eficiencia técnica y a la protección de datos?

## Objetivos DE LA INVESTIGACIÓN

### Objetivo General

Desarrollar un sistema de administración para la optimización de inventarios en ópticas con implementación de seguridad basada en la ISO 27001 e ISO 27002.

### Objetivos Específicos

* Analizar la trazabilidad en la administración de insumos para laboratorios de óptica, considerando los procesos y flujos de información involucrados.
* Diseñar una base datos para la administración de inventarios que este alineado con las necesidades operativas de las ópticas, permitiendo una mayor comprensión del flujo de información y la protección de datos en los procesos técnicos.
* Desarrollar de los módulos en el sistema de administración de inventarios, enfocándose en la trazabilidad de los productos, para mejorar la eficiencia técnica.
* Proponer la implementación de directrices basadas en las normas ISO 27001 e ISO 27002 en la administración de inventarios en ópticas, con el fin de apoyar el cumplimiento de los estándares internacionales de seguridad y eficiencia.
* Diseñar una base de datos alineada con las características operativas de los laboratorios de óptica, respetando los principios de organización y seguridad de los datos.
* Desarrollar módulos específicos en el sistema de administración de inventarios para gestionar la trazabilidad de los insumos.
* Proponer directrices basadas en las normas ISO 27001 e ISO 27002 en el sistema de administración de insumos para laboratorios de óptica.
* Realizar pruebas de testing para verificar el correcto funcionamiento de los módulos y componentes del sistema.
* Generar reportes automatizados a partir de los datos del sistema, según los requerimientos de los laboratorios de óptica.

## DELIMITACIÓN

### Límite Temporal

La investigación sobre el Sistema de Administración de Inventarios para Ópticas con Implementación de Seguridad Basada en la ISO 27001 e ISO 27002 se llevará a cabo durante el período de octubre hasta enero de 2024. Este intervalo temporal permitirá observar la implementación del sistema en un marco controlado, recopilando datos sobre la optimización de la administración de inventarios y la mejora en la seguridad de la información durante el segundo semestre del año, asegurando que los resultados se obtengan dentro de un tiempo definido y coherente con los objetivos de la investigación.

### Límite Geográfico

La investigación se llevará a cabo en el sector óptico de la ciudad de La Paz, Bolivia, enfocándose en las ópticas que operan dentro de esta área geográfica. Esta delimitación espacial permitirá analizar la implementación del Sistema de Administración de Inventarios con Seguridad Basada en la ISO 27001 e ISO 27002 en un entorno urbano con características comerciales, facilitando la recolección de datos y procurar que los resultados obtenidos sean aplicables y relevantes para las ópticas de esta región.

## Justificación

### Justificación Social

La implementación de un Sistema de Administración de Inventarios para Ópticas con Seguridad Basada en la ISO 27001 e ISO 27002 tiene un impacto social considerable. En primer lugar, optimizar la administración de inventarios en las ópticas puede contribuir a mejorar la estabilidad laboral del personal, al favorecer una planificación más precisa y un control adecuado del stock. Esto no solo evitará situaciones de desabastecimiento o sobreabundancia, sino que también reducirá la presión sobre los empleados, mejorando así el ambiente laboral y fomentando un clima de trabajo más eficiente y organizado. Este impacto positivo en los trabajadores se reflejará en un mejor servicio al cliente, lo que beneficiará a la comunidad en general.

Además, la adopción de estándares internacionales de seguridad en la administración de información sensible servirá como un modelo para otras empresas del sector salud en la región, promoviendo mejores prácticas tanto en el manejo de inventarios como en la protección de datos. Este avance contribuirá a fortalecer la competitividad de las ópticas locales, mientras fomenta la implementación de estándares de calidad que podrían beneficiar tanto a los empleados como a los consumidores, mejorando la seguridad, confianza y eficiencia en el sector óptico de la sociedad.

### Justificación Económica

Desde una perspectiva económica, la implementación de un Sistema de Administración de Inventarios con Seguridad Basada en la ISO 27001 e ISO 27002 en las ópticas de La Paz tiene el potencial de generar importantes beneficios financieros. Al centralizar y optimizar la administración de inventarios, se pueden reducir los costos asociados con el almacenamiento deficiente, las pérdidas por productos faltantes o deteriorados, y los errores en el control del stock. Esto permitirá a las ópticas minimizar el capital inmovilizado en productos que no rotan rápidamente, liberando recursos que podrán destinarse a inversiones más estratégicas, como la adquisición de nueva tecnología o mejoras en el servicio al cliente.

Además, la seguridad mejorada en la protección de los datos mediante la adopción de las normas ISO permitirá evitar posibles pérdidas económicas relacionadas con la vulneración de información. Esto no solo aumentará la confianza del cliente, sino que también fortalecerá la reputación de las ópticas, atrayendo nuevos clientes y asegurando su fidelización a largo plazo. En un mercado altamente competitivo, estas mejoras en la eficiencia y la reducción de costos serán claves para favorecer la sostenibilidad y crecimiento de las ópticas en el mediano y largo plazo.

## Tipología Del PROYECTO

Este proyecto se enmarca en la categoría de proyecto tecnológico, ya que el resultado de la investigación es un Sistema de Administración de Inventarios diseñado específicamente para optimizar la administración de productos en las ópticas, integrando medidas de seguridad basadas en los estándares internacionales ISO 27001 e ISO 27002. El principal objetivo de este sistema es mejorar y automatizar los procesos técnicos de inventario, proporcionando un producto tecnológico que facilitará la vida de los empleados y administradores en las ópticas.

## MÉTODOS DE INVESTIGACIÓN

### Enfoque De La Investigación

El presente proyecto de investigación utilizará un enfoque cualitativo.

Las investigaciones cualitativas suelen producir preguntas antes, durante o después de la recolección y análisis de los datos. La acción indagatoria se mueve de manera dinámica entre los hechos y su interpretación, y resulta un proceso más bien “circular” en el que la secuencia no siempre es la misma, puede variar en cada estudio. (Sampieri, 2018, p. 9)

### Métodos De Investigación

El método de investigación adoptado será inductivo, ya que:

Van de lo particular a lo general. Por ejemplo, en un estudio cualitativo típico, el investigador entrevista a una persona, analiza los datos que obtuvo y saca conclusiones; posteriormente, entrevista a otra persona, analiza esta nueva información y revisa sus resultados y conclusiones; del mismo modo, efectúa y analiza más entrevistas para comprender el fenómeno que estudia. Es decir, procede caso por caso, dato por dato, hasta llegar a una perspectiva más general. (Sampieri, 2018 p. 8)

Lo cual ayudará a la investigación cualitativa que partirá de la observación y el análisis de las experiencias específicas de los empleados y administradores en las ópticas que implementan el Sistema de Administración de Inventarios con Seguridad Basada en la ISO 27001 e ISO 27002. A través de entrevistas y observaciones detalladas, se recopilarán datos empíricos que permitirán generar una comprensión teórica general sobre el impacto del sistema en la eficiencia técnica y la seguridad de la información. Este enfoque facilitará el desarrollo de conclusiones basadas en las experiencias reales dentro del contexto específico de las ópticas.

### Diseño De La Investigación

El diseño de esta investigación será no experimental debido a que:

Podría definirse como la investigación que se realiza sin manipular deliberadamente variables. Es decir, se trata de estudios donde no hacemos variar en forma intencionales variables independientes para ver su efecto sobre otras variables. que hacemos en la investigación no experimental es observar fenómenos tal como se dan en su contexto natural, para después analizarlos. (Sampieri, 2018, p. 205)

Con el fin de analizar cómo la implementación del Sistema de Administración de Inventarios con Seguridad Basada en la ISO 27001 e ISO 27002 influye en la operatividad y la seguridad de la información. Este enfoque permitirá estudiar el impacto del sistema sin intervenir o alterar los procesos naturales de las ópticas, basándose en la recopilación de datos derivados de la observación de situaciones reales.

### Tipo De Investigación

Este estudio será de tipo aplicado y teórico, ya que busca tanto resolver un problema práctico en la administración de inventarios en las ópticas como contribuir al desarrollo teórico en el campo de la seguridad de la información. En su enfoque aplicado, la investigación tendrá como objetivo implementar un Sistema de Administración de Inventarios con Seguridad Basada en la ISO 27001 e ISO 27002, resolviendo un problema concreto de eficiencia técnica y protección de datos en ópticas.

Paralelamente, desde un enfoque teórico, se buscará generar conocimientos que contribuyan a la comprensión de cómo la implementación de estos estándares de seguridad puede ser adaptada y aplicada en el contexto específico de las pequeñas y medianas empresas del sector óptico, aportando así principios generales que podrían ser utilizados en otros ámbitos. (Roberto Hernández Sampieri, 2010)

## Técnicas De Investigación Y Sus Instrumentos

Las técnicas de investigación seleccionadas para este estudio serán

### Las Entrevistas en Profundidad

Debido a que:

“La entrevista cualitativa es más íntima, flexible y abierta. Esta se define como una reunión para intercambiar información entre una persona (el entrevistador) y otra (el entrevistado) u otras (entrevistados).” (Sampieri, 2018, p. 597)

Se llevarán a cabo con empleados clave de las ópticas, permitiendo explorar de manera detallada sus experiencias y percepciones sobre el sistema de administración de inventarios y su impacto en la operatividad y seguridad. Simultáneamente, el investigador realizará observación participante dentro de las ópticas, involucrándose directamente en el entorno para observar de primera mano cómo se manejan los inventarios y cómo interactúan los empleados con el sistema implementado. Los datos recolectados a través de ambas técnicas se analizarán para identificar patrones de comportamiento y temas comunes, proporcionando una visión más profunda del impacto del sistema en el entorno laboral. A partir de estos hallazgos, se evaluarán las mejoras operativas y los desafíos que enfrenta el sistema, con el fin de generar conclusiones que ayuden a optimizar su implementación en el futuro.

## Población Y Muestra

### Población

La población de esta investigación estará compuesta por la óptica “Óptica Visión” de la ciudad de La Paz, Bolivia, que utilizan o están en proceso de implementar un sistema de administración de inventarios y cuentan con 4 sucursales. Esta población incluirá tanto los empleados operativos (como encargados de almacén), los administradores de las ópticas, quienes interactúan directamente con el sistema y tienen conocimiento sobre la administración de inventarios y la seguridad de la información.

### Muestra

La muestra de esta investigación será un subconjunto de esta óptica. Para este estudio, se seleccionarán 2 ópticas, que proporcionen una representación adecuada de la variedad existente en el sector.

Por lo tanto, será una muestra no probabilística como afirma Sampieri (2018):

“Para esta investigación se utiliza las muestras por conveniencia Sampieri (2018) afirman que “estas muestras están formadas por los casos disponibles a los cuales tenemos acceso. Tal fue la situación de Rizzo (2004), quien no pudo ingresar a varias empresas para efectuar entrevistas a profundidad en niveles gerenciales acerca de los factores que conforman el clima organizacional, y entonces decidió entrevistar a compañeros que junto con ella cursaban un posgrado en desarrollo humano y eran directivos de diferentes organizaciones” (p. 433)

Siendo así que, para este estudio, se seleccionarán 2 ópticas, que proporcionen una representación adecuada de la variedad existente en el sector. En cada óptica, se entrevistarán al menos 2 empleados clave (un administrador y un empleado operativo) para obtener diversas perspectivas sobre la implementación del sistema. La selección de la muestra será de muestreopor criterio, que permitirá seleccionar a los participantes más adecuados, como empleados y administradores que interactúan directamente con el Sistema de Administración de Inventarios y que tienen experiencia en la gestión de inventarios.

## Cronograma De GANT

Tabla 1 Cronograma de GANT

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Tiempo en Semanas (Octubre 2024 - Enero 2025)** | | | | | | | | | | | | | | | | |
| **Actividades** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| Elaboración de Marco Teórico |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Elaboración de Diseño Metodológico |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Revisión y Corrección del documento |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Elaboración de la propuesta |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Conclusiones, recomendaciones, bibliografía y anexos |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Revisión y Corrección del documento |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Defensa interna |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Corrección de observaciones y recomendaciones |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Orden de Empaste |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

# CAPITULO II

# MARCO TEÓRICO



## Sistema

Según Sommerville (2011), “un sistema puede entenderse como un conjunto de componentes interrelacionados que trabajan juntos para realizar una función específica o alcanzar un objetivo común". (p. 15).

Este concepto implica que cada elemento dentro del sistema cumple un rol particular, contribuyendo al funcionamiento integral y coherente del conjunto. Además, Sommerville enfatiza que la efectividad de un sistema no radica solo en la capacidad de sus partes individuales, sino en cómo estas están organizadas y en la forma en que interactúan entre sí para lograr el propósito general para el cual fueron diseñadas. Así, un sistema bien estructurado no solo optimiza los recursos disponibles, sino que también mejora la eficiencia y la capacidad de respuesta de una organización frente a las demandas y cambios en su entorno operativo.

## SISTEMA WEB

Según TechTarget (2023) un sistema o aplicación web (o web app) es un programa de aplicación que se almacena en un servidor remoto y se entrega a través de Internet mediante una interfaz de navegador. Por definición, los servicios web también son aplicaciones web, y muchos sitios web, aunque no todos, contienen aplicaciones web.

Los desarrolladores diseñan aplicaciones web para una amplia variedad de usos y usuarios, desde organizaciones hasta individuos, por diversas razones. Las aplicaciones web comúnmente utilizadas pueden incluir correo web, calculadoras en línea o tiendas de comercio electrónico. Aunque algunos usuarios solo pueden acceder a ciertas aplicaciones web mediante un navegador específico, la mayoría están disponibles sin importar el navegador.

Las aplicaciones web no necesitan descargarse, ya que se accede a ellas a través de una red. Los usuarios pueden acceder a una aplicación web mediante un navegador web, como Google Chrome, Mozilla Firefox o Safari.

Para que una aplicación web funcione, necesita un servidor web, un servidor de aplicaciones y una base de datos. Los servidores web gestionan las solicitudes que provienen de un cliente, mientras que el servidor de aplicaciones completa la tarea solicitada. Una base de datos almacena cualquier información necesaria.

Las aplicaciones web suelen tener ciclos de desarrollo cortos y equipos de desarrollo reducidos. La mayoría de los desarrolladores escriben aplicaciones web en JavaScript, HTML5 o CSS. La programación del lado del cliente generalmente utiliza estos lenguajes, que ayudan a construir la parte frontal de la aplicación. La programación del lado del servidor crea los scripts que utilizará la aplicación web. Lenguajes como Python, Java y Ruby se utilizan comúnmente en la programación del lado del servidor.

## HERRAMIENTAS DE DESARROLLO

Las herramientas de desarrollo por definición:

Las herramientas de desarrollo del software (llamadas en ocasiones herramientas de Ingeniería de Software Asistido por Computadora o CASE, por las siglas de Computer-Aided Software Engineering) son programas usados para apoyar las actividades del proceso de la ingeniería de software. En consecuencia, estas herramientas incluyen editores de diseño, diccionarios de datos, compiladores, depuradores (debuggers), herramientas de construcción de sistema, etcétera. (Sommerville, 2011, p. 37)

### JavaScript

JavaScript fue introducido en 1995 como un lenguaje diseñado para agregar interactividad a las páginas web en el navegador Netscape Navigator. Desde entonces, ha sido adoptado por todos los navegadores principales, permitiendo el desarrollo de aplicaciones web modernas que facilitan la interacción directa del usuario sin necesidad de recargar la página constantemente. Como señala Haverbeke (2018), "JavaScript hizo posible una nueva era de aplicaciones web dinámicas, transformando la manera en que los usuarios interactúan con las páginas" (pág. 6).

Es importante destacar que, a pesar de compartir parte del nombre, JavaScript y Java tienen muy poco en común. Según Haverbeke (2018), "el nombre fue una estrategia de marketing para aprovechar la popularidad que Java tenía en ese momento, lo que dejó a JavaScript con un nombre que no refleja su verdadera naturaleza" (pág. 6). A medida que fue adoptado fuera de Netscape, surgió la necesidad de estandarizarlo, dando lugar al Estándar ECMAScript, desarrollado por Ecma International, que unificó las implementaciones del lenguaje. Aunque JavaScript y ECMAScript suelen utilizarse indistintamente, ambos términos representan el mismo lenguaje bajo diferentes contextos.

El diseño inicial de JavaScript era extremadamente permisivo, lo que lo hacía accesible para principiantes, pero también dificultaba la detección de errores.

Haverbeke (2018) comentó lo siguiente:

El lenguaje aceptaba casi cualquier cosa que escribiera, pero la interpretaba de una manera que era completamente diferente de lo que quería decir. Por supuesto, esto tenía mucho que ver con el hecho de que no tenía idea de lo que estaba haciendo, pero hay un problema real aquí: JavaScript es ridículamente liberal en lo que permite. (pág. 7).

Sin embargo, esta flexibilidad también permitió la implementación de técnicas avanzadas que serían imposibles en lenguajes más rígidos. Con el tiempo, los desarrolladores aprendieron a apreciar estas características.

JavaScript ha evolucionado significativamente desde su creación. Entre 2000 y 2010, ECMAScript versión 3 fue ampliamente compatible, estableciendo las bases del dominio de JavaScript en la web. Según Haverbeke (2018), "la ambiciosa versión 4, que planeaba mejoras radicales, fue abandonada en 2008 debido a su complejidad, lo que dio lugar a una versión 5 más práctica y accesible en 2009" (pág. 7). La versión ECMAScript 6, lanzada en 2015, incluyó varias de las innovaciones planificadas para la versión 4 y marcó el inicio de actualizaciones anuales para el lenguaje.

La evolución constante del lenguaje requiere que los navegadores y otros entornos se actualicen regularmente para soportar las nuevas características. Como menciona Haverbeke (2018), "los diseñadores de lenguajes tienen cuidado de no realizar cambios que puedan romper programas existentes, asegurando la compatibilidad hacia atrás en nuevos navegadores" (pág. 8). Esta compatibilidad garantiza que las aplicaciones más antiguas puedan seguir funcionando, incluso con las versiones más recientes del lenguaje.

JavaScript también se ha expandido más allá de los navegadores web. Algunas bases de datos, como MongoDB y CouchDB, utilizan JavaScript como lenguaje de scripting y consulta, mientras que plataformas como Node.js proporcionan un entorno para programar en JavaScript fuera del navegador. Este uso en diversas plataformas lo ha convertido en un lenguaje versátil y esencial para el desarrollo moderno, tanto en el frontend como en el backend (Haverbeke, 2018, p. 7).

### TypeScript

TypeScript se ha convertido en uno de los lenguajes de programación con mayor auge en los últimos años. En el informe anual de GitHub, TypeScript ocupa la cuarta posición entre los lenguajes más utilizados, después de JavaScript, Python y Java, lo que resalta su relevancia y adopción en el desarrollo moderno. Según Stack Overflow, TypeScript es también el segundo lenguaje más apreciado por los desarrolladores, después de Rust, una posición que evidencia su gran aceptación en la comunidad de programación (Talaminos, 2022, pp. 9-10)

Este lenguaje ha logrado posicionarse de manera destacada dentro del ecosistema de JavaScript. Como señala el informe "State of JavaScript" (2021), en una encuesta que involucró a más de 23,000 programadores de 137 países, TypeScript fue galardonado como la tecnología más adoptada dentro de la comunidad de JavaScript, lo que refleja su influencia y uso cada vez mayor. Según State of JavaScript (2021), "TypeScript recibió el premio a la tecnología más adoptada", lo que confirma la popularidad del lenguaje a nivel global (pp. 9-10).

TypeScript no solo ha sido adoptado por proyectos de software importantes, sino también por empresas de renombre mundial. Herramientas y plataformas como Angular, Vue, Jest, Ionic y Visual Studio Code han incluido TypeScript en su desarrollo, y compañías como Google, Airbnb, PayPal y Slack lo han implementado en sus sistemas para aprovechar sus capacidades en aplicaciones empresariales de gran escala. Este creciente uso es prueba de la versatilidad y robustez que TypeScript ofrece en la programación, especialmente cuando se buscan aplicaciones escalables y seguras (Talaminos, 2022, p. 10)

A su vez, la comunidad de TypeScript experimenta un crecimiento constante, proporcionando una base sólida para los desarrolladores. Cada vez hay una mayor cantidad de documentación en línea y repositorios de GitHub con recursos y bibliotecas específicas, que facilitan la integración del lenguaje en diversos proyectos. Esta disponibilidad de recursos es clave para el aprendizaje y adopción de TypeScript en entornos profesionales y educativos. Según Talaminos, (2022), "la comunidad de TypeScript crece constantemente y cada vez existe mayor cantidad de documentación en la red e incluso repositorios de GitHub muy completos con multitud de recursos relacionados con el lenguaje" (p. 10).

Frente al tema, "TypeScript extiende las funcionalidades de JavaScript, proporcionando características avanzadas como genéricos y decoradores" (Talaminos, 2022, p. 11). Este diseño le permite a TypeScript aumentar la seguridad y el control en el desarrollo de aplicaciones. Además, al ser un superconjunto de JavaScript, TypeScript permite a los desarrolladores beneficiarse de todas las características de JavaScript, pero con ventajas adicionales en la depuración y mantenimiento del código. Como sugieren estos aspectos, el dominio de TypeScript resulta valioso para aquellos que buscan mejorar la calidad y eficiencia de sus proyectos web (Talaminos, 2022, 11).

### Node.JS

Node.js representa una evolución significativa en el uso de JavaScript al permitir que funcione en el lado del servidor. Su arquitectura asincrónica ofrece una ventaja importante al ejecutar múltiples solicitudes sin bloquearse, mejorando la eficiencia y velocidad en comparación con tecnologías de servidor tradicionales. Según López (2021) "lo que se pretende con llevar JavaScript y su asincronía al lado del servidor es tener una asincronía real en el lado del servidor" (p. 15). Esta asincronía permite que una máquina servidora gestione múltiples solicitudes de forma simultánea, esperando las respuestas de otros servidores sin que esto afecte el rendimiento general del sistema.

Node.js, además, emplea el motor de JavaScript para ejecutar estas tareas, lo que lo convierte en una tecnología rápida y eficiente. A diferencia de lenguajes como PHP o Java, que requieren de un servidor web (como Apache o Tomcat) para gestionar peticiones, Node.js opera de manera autónoma, evitando así la necesidad de configuraciones adicionales. Como explican López (2021), "lo mejor de todo, [Node.js] no necesita de servidor Web, ni Apache, ni Tomcat, ni IIS, ni NGinx ni ningún otro" (p. 15). Esta característica es especialmente beneficiosa en aplicaciones de tiempo real, como chats y juegos en línea, donde el tiempo de respuesta es crucial para la experiencia del usuario. Por último, Node.js destaca en la gestión de operaciones concurrentes gracias a su diseño no bloqueante, lo que permite una mejor respuesta en aplicaciones con altos volúmenes de tráfico, adaptándose así a las necesidades de las aplicaciones web modernas (López, 2021, p. 16).

### NestJS

Nest.js es uno de los frameworks de Node.js de más rápido crecimiento para construir aplicaciones backend eficientes, escalables y de nivel empresarial. Este framework, que se basa en el moderno JavaScript y TypeScript, permite desarrollar aplicaciones altamente comprobables y mantenibles, lo que lo convierte en una opción popular entre los desarrolladores que buscan estructura y organización en sus proyectos. Con más de 46,6k estrellas y 5,4k bifurcaciones en GitHub, y un promedio de 700,000 descargas semanales, Nest.js se destaca como un recurso confiable para la construcción de backend con Node.js. Según su documentación, este framework se ha diseñado para aprovechar las capacidades de TypeScript, el cual agrega tipado estático y mejora la calidad del código, además de ser compatible con otros patrones de diseño arquitectónicos como MVC (Modelo-Vista-Controlador), lo cual facilita la estructuración de aplicaciones complejas (kinsta, 2022, párr. 1).

Nest.js es especialmente útil en proyectos que requieren alta escalabilidad y sostenibilidad a largo plazo, y es frecuentemente adoptado por empresas que buscan una plataforma robusta para sus servicios en producción. Entre sus características distintivas, Nest.js destaca por su enfoque modular, lo que permite dividir el proyecto en módulos individuales, facilitando su mantenimiento y prueba en equipos de trabajo grandes. Esta estructura modular es una de las razones por las que se ha convertido en la elección preferida para el desarrollo de APIs, microservicios y aplicaciones de gran escala en la industria. Empresas de renombre como Adidas, Decathlon y Capgemini utilizan Nest.js para sus aplicaciones backend, lo que resalta su capacidad para manejar exigencias empresariales (kinsta, 2022, párr 2).

### React

React es una de las librerías de JavaScript más populares para el desarrollo de aplicaciones web y móviles, destacándose por su capacidad para crear interfaces de usuario (UI) a través de componentes reutilizables. Creada por Facebook, esta biblioteca permite a los desarrolladores construir aplicaciones que responden rápidamente a los cambios de datos sin recargar la ppina, lo cual mejora la experiencia del usuario. React contiene una colección de fragmentos de código JavaScript reutilizables utilizados para crear interfaces de usuario (UI) llamadas componentes (Deyimar, 2023, párr. 2). Es importante destacar que React no es un framework completo, sino que está diseñado específicamente para gestionar la capa de vista de una aplicación, permitiendo la integración con otras herramientas o frameworks como Angular y Vue en caso de requerir funcionalidades más avanzadas.

React opera mediante un sistema de componentes, donde cada parte de la UI es un bloque independiente que se puede combinar con otros componentes, lo que permite reutilización y mantenibilidad en proyectos de gran escala (Deyimar, 2023, párr. 3). Su popularidad en el desarrollo front-end se debe, entre otras cosas, al DOM virtual, una representación ligera del DOM real que optimiza la velocidad de renderizado y mejora el rendimiento de la aplicación.

Según Deyimar (2023):

Esto convierte a React en una alternativa ideal para desarrollar aplicaciones de una sola página (SPA) y aplicaciones móviles a través de su versión móvil, React Native, la cual comparte principios y sintaxis con ReactJS pero se enfoca en plataformas móviles (párr. 4).

### TyperORM

TypeORM es una biblioteca de mapeo objeto-relacional (ORM) diseñada para operar en múltiples entornos, incluyendo Node.js, React Native, Ionic, Electron y otros, ofreciendo soporte para TypeScript y JavaScript (ES2021). Esta herramienta tiene como objetivo facilitar el desarrollo de aplicaciones que utilicen bases de datos, desde proyectos pequeños con pocas tablas hasta aplicaciones empresariales de gran escala que requieren múltiples bases de datos. Según su documentación, "TypeORM es un ORM que puede ejecutarse en NodeJS, Browser, Cordova, PhoneGap, Ionic, React Native, NativeScript, Expo y Electron" (typeorm, 2023, párr. 1). Su versatilidad lo convierte en una excelente opción para desarrolladores que buscan una solución adaptable y eficiente en la gestión de datos.

TypeORM destaca por ser el único ORM en JavaScript que admite tanto los patrones Active Record como Data Mapper, lo que permite escribir aplicaciones escalables y mantenibles de forma productiva y con un bajo acoplamiento entre componentes. Además, su diseño ha sido influenciado por otros ORMs populares, como Hibernate, Doctrine y Entity Framework, lo que le permite aprovechar las mejores prácticas de estas herramientas para mejorar la experiencia de desarrollo en aplicaciones que dependen de bases de datos (typeorm, 2023, párr. 1).

### Material UI

Material UI es una biblioteca de componentes de código abierto para React que implementa el diseño de Material Design de Google, proporcionando a los desarrolladores una colección completa de componentes listos para usar en producción. Que según The MUI team pact (2023) "Incluye una colección completa de componentes preconstruidos que están listos para su uso en producción desde el primer momento" (párr. 2). Material UI permite personalizar los componentes según las necesidades del proyecto, ofreciendo una serie de opciones de personalización que facilitan la implementación de un sistema de diseño propio. Este enfoque permite a los desarrolladores integrar una estética moderna y consistente en sus aplicaciones web, manteniendo la flexibilidad para ajustar y adaptar los estilos según los requerimientos específicos de cada proyecto.

## BASE DE DATOS

Una base de datos es un sistema que organiza y almacena datos de manera centralizada, permitiendo que distintos usuarios accedan a la información de manera consistente y controlada. En contraste con los sistemas de ficheros descentralizados, una base de datos centraliza y reduce la duplicidad de información dentro de la organización. Esto permite que los datos sean compartidos y utilizados por diferentes departamentos, eliminando inconsistencias y facilitando la independencia lógica-física de los datos. Como se menciona en el texto:

Una base de datos se puede percibir como un gran almacén de datos que se define y se crea una sola vez, y que se utiliza al mismo tiempo por distintos usuarios. En una base de datos todos los datos se integran con una mínima cantidad de duplicidad. De este modo, la base de datos no pertenece a un solo departamento, sino que se comparte por toda la organización. Además, la base de datos no sólo contiene los datos de la organización, también almacena una descripción de dichos datos. (Marqués, 2011, p. 2)

Los metadatos que contiene una base de datos proporcionan un diccionario de datos que describe la estructura y facilita la independencia lógica-física, evitando los problemas comunes de los sistemas de ficheros tradicionales.

### Sistema de Gestión de Bases de Datos

Un Sistema de Gestión de Bases de Datos (SGBD) es una aplicación que permite a los usuarios definir, crear, mantener y controlar el acceso a una base de datos, además de gestionar la estructura física y lógica de los datos almacenados. Este sistema separa la estructura física de la lógica, almacenando la definición de datos en un diccionario o catálogo.

Que según Marqués (2011):

El SGBD permite la inserción, actualización, eliminación y consulta de datos mediante un lenguaje de manejo de datos. El hecho de disponer de un lenguaje para realizar consultas reduce el problema de los sistemas de ficheros, en los que el usuario tiene que trabajar con un conjunto fijo de consultas, o bien, dispone de un gran número de programas de aplicación costosos de gestionar. Hay dos tipos de lenguajes de manejo de datos: los procedurales y los no procedurales. Estos dos tipos se distinguen por el modo en que acceden a los datos. Los lenguajes procedurales manipulan la base de datos registro a registro, mientras que los no procedurales operan sobre conjuntos de registros. En los lenguajes procedurales se especifica qué operaciones se debe realizar para obtener los datos resultados, mientras que en los lenguajes no procedurales se especifica qué datos deben obtenerse sin decir cómo hacerlo. El lenguaje no procedural más utilizado es el SQL (Structured Query Language) que, de hecho, es un estándar y es el lenguaje de los SGBD relacionales. (p. 3)

Lo cual nos da esta capacidad de manejar datos de manera relacional mediante SQL que resuelve los problemas de los sistemas de ficheros, donde los datos se duplicaban y no existía un control de consistencia. Además, el SGBD incluye sistemas de seguridad, integridad, concurrencia y recuperación para garantizar el acceso controlado y confiable a la información, adaptándose a las necesidades de los usuarios mediante vistas personalizadas de la base de datos. Esto permite que el sistema sea accesible y comprensible para los usuarios sin necesidad de interactuar directamente con la estructura física de los datos, asegurando la independencia lógica-física (Marqués, 2011, pp. 3-4).

### SQL

SQL (Structured Query Language) es un lenguaje estándar que permite la gestión y manipulación de datos en bases de datos relacionales. A través de SQL, los usuarios pueden realizar operaciones de consulta y administración de datos, como crear, insertar, actualizar y eliminar información en las tablas de la base de datos. "La mayor parte de los SGBD relacionales implementan este lenguaje y mediante él se realizan todo tipo de accesos a la base de datos" (Marqués, 2011, p. 41). Las sentencias SQL más utilizadas incluyen CREATE TABLE, INSERT, UPDATE, DELETE y SELECT, las cuales permiten a los desarrolladores responder a consultas y mantener la integridad de los datos. SQL, al ser declarativo, facilita el acceso a la información requerida sin necesidad de especificar cómo obtenerla, optimizando así las operaciones en sistemas de bases de datos relacionales.

Tabla 2 Tipos de Comandos SQL

|  |  |  |
| --- | --- | --- |
| **Tipo de Comando SQL** | **Descripción** | **Ejemplos** |
| DDL (Data Definition Language) | Define la estructura de la base de datos, incluyendo tablas, índices y esquemas. | CREATE TABLE, ALTER TABLE, DROP TABLE, CREATE INDEX, DROP INDEX |
| DML (Data Manipulation Language) | Maneja los datos dentro de las tablas (consulta, inserción, actualización, eliminación). | SELECT, INSERT, UPDATE, DELETE |
| DCL (Data Control Language) | Controla los permisos y accesos a los datos de la base de datos. | GRANT, REVOKE |
| TCL (Transaction Control Language) | Administra las transacciones en la base de datos para garantizar la integridad de los datos. | COMMIT, ROLLBACK, SAVEPOINT, SET TRANSACTION |
| DQL (Data Query Language) | Se enfoca en la consulta de datos específicos de la base de datos (a menudo categorizado dentro de DML, pero a veces considerado aparte). | SELECT |

Fuente: Elaboración propia

## INventario

El inventario representa un activo esencial para las empresas, actuando como respaldo en la cadena de suministro y asegurando la continuidad de las operaciones. Los inventarios son materiales o productos almacenados que las organizaciones mantienen para cubrir la demanda en momentos específicos, protegiéndose contra posibles interrupciones en el flujo de suministro.

Según Muller (2003), se destaca lo siguiente:

El inventario es un activo, pero un tipo de activo del cual las empresas no quieren en exceso. Sin embargo, no tener 'en exceso' pondría a la organización en riesgo de posibles interrupciones en la cadena de suministro y de costos extremos imprevistos. Entonces, la clave para una administración efectiva de los inventarios es el equilibrio: mantener los inventarios adecuados para garantizar la producción continua y los flujos comerciales, al mismo tiempo que se minimiza la inversión de inventario para asegurar un desempeño financiero sólido (p. 4).

Así, los inventarios cumplen un rol de equilibrio: permiten a las empresas responder a la demanda y asegurar la estabilidad en el suministro de productos y materiales, al mismo tiempo que facilitan la planificación y administración de recursos. Este activo es una parte integral del sistema productivo, ya que su existencia garantiza que los materiales y productos necesarios estarán disponibles en el momento adecuado, sin depender completamente de las fluctuaciones en la producción o el transporte. A medida que las cadenas de suministro se vuelven más complejas y las empresas enfrentan demandas variables, el inventario se convierte en un recurso estratégico que, si se gestiona adecuadamente, puede minimizar los riesgos y contribuir al éxito operativo.

### Inventario en la Cadena de Suministro

El inventario juega un papel crítico en la administración de la cadena de suministro, al servir como un punto de equilibrio entre la demanda de los clientes y la oferta de los proveedores. Este equilibrio permite gestionar eficazmente los flujos hacia adelante y hacia atrás en la cadena de suministro, asegurando la continuidad operativa. "Gran parte de la actividad implicada en la administración de las relaciones se basa en la compra, transferencia o administración del inventario" (Waller, 2015, p. 5). Este enfoque permite a las empresas atender tanto las demandas variables de los clientes como las necesidades de adquisición de materiales, minimizando riesgos y optimizando recursos.

Un ejemplo clave de este equilibrio es el uso de procesos de planeación de ventas y operaciones (S&OP), los cuales integran pronósticos de ventas y marketing con las funciones operativas, como manufactura, logística y compras. Estos procesos incluyen análisis detallados del inventario disponible, en tránsito y en proceso, permitiendo a las empresas ajustar estratégicamente sus planes de producción y adquisición para satisfacer las necesidades del mercado. Otro caso destacado es el uso de datos del punto de venta (POS) en el sector minorista, donde cada venta registrada actualiza automáticamente el nivel de inventario, facilitando la reposición de productos en colaboración con los proveedores. Este enfoque asegura que las decisiones de inventario estén alineadas con la demanda del cliente, optimizando tanto el tiempo como los recursos necesarios para mantener la continuidad en la oferta.

### Tipos de Inventario y su Clasificación

Existen diversos tipos de inventario, y su clasificación depende de varios factores, como su uso, su función en la cadena de suministro y su administración. Aunque las definiciones suelen traslaparse, este análisis busca ofrecer un marco completo para una comunicación más efectiva sobre la administración de inventarios. Según Muller (2003), "la manera de administrar el inventario depende, en gran medida, del tipo de inventario, en qué se utiliza y qué lo afecta" (p. 9).

La siguiente tabla no define de manera clara los diferentes tipos de inventarios:

Tabla 3 Tipos de Inventarios

|  |  |
| --- | --- |
| **Tipo de Inventario** | **Descripción** |
| |  | | --- | |  |   Inventario de ciclo | |  | | --- | |  |   Cantidad promedio de productos entre reabastecimientos. Calculado como la cantidad del pedido dividida entre dos para unidades discretas como cajas. |
| Inventario de seguridad | |  | | --- | |  |   Productos reservados para enfrentar incertidumbres en demanda o retrasos en suministro. Permite garantizar un nivel de servicio aceptable en condiciones adversas. |
| Inventario en tránsito | Productos en movimiento hacia un nodo de almacenamiento o entre ubicaciones. Calculado como el tiempo promedio de entrega multiplicado por las ventas diarias. |
| |  | | --- | |  |   Inventario promocional | Destinado a campañas de marketing o promociones específicas. Gestionado cuidadosamente para evitar exceso o escasez. |
| |  | | --- | |  |   Inventario de demostración | Inventario para exhibición, que puede contribuir al inventario de seguridad si se vende en caso de agotamiento. |
| |  | | --- | |  |   Inventario minorista en bodega | Ubicado en la bodega de una tienda, incluye inventarios en tránsito, de ciclo o de seguridad. Un manejo adecuado minimiza costos asociados. |
| |  | | --- | |  |   Inventario Estacional | Utilizado en periodos específicos del año. Calculado generalmente con el modelo del vendedor de periódicos para maximizar el retorno de inversión. |

Fuente: Elaboración propia

## ISO 27001

La Norma ISO/IEC 27001 establece los requisitos para la creación, implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI). Según la norma, la adopción de un SGSI es una decisión estratégica que permite a las organizaciones proteger sus activos más valiosos: la información. Esta protección se logra preservando la confidencialidad, integridad y disponibilidad de los datos a través de un proceso continuo de gestión de riesgos. Como señala el documento, "el sistema de gestión de la seguridad de la información preserva la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos y otorga a las partes interesadas confianza sobre la adecuada gestión de los riesgos" (ISO/IEC, 2023, p. 6)

El establecimiento de un SGSI se ajusta a las necesidades específicas de la organización, considerando sus objetivos, requisitos de seguridad, procesos internos, tamaño y estructura. Estos factores cambian con el tiempo, lo que obliga a las organizaciones a mantener un enfoque dinámico y adaptativo. Además, el SGSI no es un sistema aislado; su implementación debe estar completamente integrada con los procesos organizativos y la estructura de gestión general. Este enfoque asegura que la seguridad de la información esté presente desde la fase de diseño de procesos y sistemas, fortaleciendo la confianza y eficiencia en la protección de datos.

La norma no establece un orden estricto para la implementación de los requisitos, lo que permite a las organizaciones priorizar en función de sus contextos y necesidades específicas. Además, se alienta a las partes interesadas, tanto internas como externas, a utilizar el SGSI para evaluar la capacidad de la organización de cumplir con sus requisitos de seguridad. La ISO/IEC 27000, como parte de la misma familia de normas, proporciona una visión general y un vocabulario común, incluyendo referencias a normas complementarias como la ISO/IEC 27003 (guía de implementación), ISO/IEC 27004 (métricas de seguridad) y ISO/IEC 27005 (gestión de riesgos).

En esencia, la implementación de un SGSI según la ISO/IEC 27001 fortalece la capacidad de las organizaciones para gestionar los riesgos relacionados con la información, ofreciendo un marco sólido y reconocido internacionalmente para la protección de datos en un entorno dinámico y competitivo.

### Principios Fundamentales de la ISO/IEC 27001

#### Contexto de la Organización

El éxito de un Sistema de Gestión de la Seguridad de la Información (SGSI) depende de su capacidad para adaptarse al contexto organizacional, tanto interno como externo. La norma ISO/IEC 27001 establece que las organizaciones deben identificar y comprender las condiciones y factores que impactan su propósito y capacidad para alcanzar los resultados deseados del SGSI. Este análisis incluye aspectos económicos, legales, tecnológicos y culturales que afectan la seguridad de la información. Según la norma, "la organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan su capacidad para lograr los resultados previstos de su sistema de gestión de la seguridad de la información" (UNE-ISO/IEC, 2023, p. 8).

La norma también sugiere referirse a la ISO 31000:2018 para establecer un enfoque sistemático que permita evaluar riesgos en relación con el contexto organizacional. Este análisis es fundamental para anticipar desafíos, aprovechar oportunidades y definir estrategias efectivas para gestionar la seguridad de la información.

#### Necesidades y Expectativas de las Partes Interesadas

La norma requiere que las organizaciones identifiquen las partes interesadas que son relevantes para el SGSI, junto con sus necesidades y expectativas específicas. Estas partes interesadas pueden incluir:

* Clientes, que demandan confidencialidad y protección de datos.
* Reguladores, que exigen cumplimiento normativo.
* Proveedores, que necesitan garantías de integridad en las transacciones.
* Empleados, que buscan herramientas seguras para manejar información.

Según la norma, "la organización debe determinar las partes interesadas relevantes para el SGSI y cuáles de sus requisitos se abordarán mediante este sistema" (UNE-ISO/IEC, 2023, p. 8). Esto permite al SGSI alinearse con los objetivos estratégicos y operativos de la organización, garantizando una gestión efectiva de los riesgos relacionados con la seguridad de la información.

Al incorporar estas expectativas, las organizaciones logran construir confianza con las partes interesadas, mejorar su resiliencia ante riesgos y mantener la integridad de sus procesos operativos.

### Soporte en el Sistema de Gestión de la Seguridad de la Información (SGSI)

#### Recursos Necesarios

Un Sistema de Gestión de la Seguridad de la Información (SGSI) requiere recursos adecuados para su establecimiento, implementación, mantenimiento y mejora continua. Según la norma ISO/IEC 27001, "la organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de la seguridad de la información" (UNE-ISO/IEC, 2023, p. 13). Estos recursos incluyen infraestructura, tecnología, personal capacitado y soporte técnico. La disponibilidad de estos recursos es esencial para garantizar la eficacia y continuidad del SGSI, promoviendo una gestión adecuada de la seguridad de la información.

#### Competencia y Capacitación

La competencia del personal que opera bajo el SGSI es un factor clave para su éxito. La norma establece que "la organización debe determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta a su desempeño en seguridad de la información" (UNE-ISO/IEC, 2023, p. 13). Además, se debe garantizar que el personal posea la formación, educación o experiencia adecuada, y cuando sea necesario, implementar acciones como programas de formación o tutorías para cubrir cualquier brecha en las competencias. También se debe conservar evidencia documentada de la competencia del personal, asegurando el desempeño efectivo del SGSI.

#### Concienciación del Personal

La concienciación es un componente fundamental para el éxito del SGSI. Según la norma, "las personas que trabajan bajo el control de la organización deben ser conscientes de la política de la seguridad de la información, su contribución a la eficacia del SGSI, y las implicaciones de no cumplir con los requisitos del sistema" (UNE-ISO/IEC, 2023, p. 13). Promover una cultura organizacional que valore la seguridad de la información asegura un mayor compromiso por parte de los empleados, lo que fortalece el sistema y reduce riesgos relacionados con fallos humanos.

#### Comunicación Efectiva

La comunicación interna y externa desempeña un papel crucial en la gestión del SGSI. Las organizaciones deben determinar el contenido, los destinatarios, los tiempos y los medios adecuados para transmitir la información. Como señala la norma, "la organización debe determinar la necesidad de comunicaciones internas y externas pertinentes al sistema de gestión de la seguridad de la información, incluyendo su contenido, cuándo comunicar, con quién comunicar y cómo comunicar" (UNE-ISO/IEC, 2023, p. 14). Un flujo de comunicación claro asegura que todos los involucrados estén alineados con los objetivos de seguridad de la organización, facilitando la implementación de medidas de seguridad eficaces.

#### Gestión de la Información Documentada

La información documentada es un componente esencial del SGSI. La norma detalla varios aspectos clave para su gestión:

* **Requisitos Generales**: "El sistema de gestión de la seguridad de la información de la organización debe incluir la información documentada requerida por este documento y aquella que la organización ha determinado como necesaria para la eficacia del sistema" (UNE-ISO/IEC, 2023, p. 14).
* **Creación y Actualización**: "Cuando se crea y actualiza la información documentada, la organización debe asegurarse de la identificación, descripción, formato y revisión adecuada para su idoneidad y adecuación" (UNE-ISO/IEC, 2023, p. 14).
* **Control de Documentación**: La norma indica que "la información documentada debe estar disponible y protegida contra pérdida de confidencialidad, uso inadecuado o pérdida de integridad, y controlada mediante actividades como distribución, almacenamiento y control de cambios" (UNE-ISO/IEC, 2023, p. 14).

La correcta gestión de la documentación asegura que los procesos del SGSI sean consistentes y rastreables, permitiendo un monitoreo efectivo de su implementación.

### Contexto de la Organización

#### Comprensión de la Organización y de su Contexto

El éxito de un Sistema de Gestión de la Seguridad de la Información (SGSI) depende de su capacidad para adaptarse al contexto organizacional. Según la norma ISO/IEC 27001, "la organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan a su capacidad para lograr los resultados previstos de su sistema de gestión de la seguridad de la información" (UNE-ISO/IEC, 2023, p. 7). Estas cuestiones pueden incluir factores económicos, tecnológicos, legales, culturales y sociales, así como aspectos internos como la estructura organizativa, los procesos y las capacidades existentes. Además, la norma recomienda referirse al apartado 5.4.1 de la ISO 31000:2018 para un análisis sistemático y estructurado del contexto organizacional, permitiendo anticipar riesgos y oportunidades.

#### Comprensión de las Necesidades de las Partes Interesadas

El SGSI debe alinearse con las expectativas y requisitos de las partes interesadas clave. La norma establece que "la organización debe determinar las partes interesadas que son relevantes para el sistema de gestión de la seguridad de la información, así como sus requisitos relevantes" (UNE-ISO/IEC, 2023, p. 7). Estos requisitos pueden incluir obligaciones legales, regulatorias, contractuales y de cumplimiento, que deben ser considerados para garantizar la efectividad del SGSI. Identificar y priorizar estas necesidades permite a las organizaciones diseñar un sistema que no solo cumpla con los estándares internacionales, sino que también se alinee con sus objetivos estratégicos.

#### Determinación del Alcance del SGSI

Para garantizar la eficacia del SGSI, la organización debe establecer claramente sus límites y aplicabilidad. Según la norma, "la organización debe determinar los límites y la aplicabilidad del sistema de gestión de la seguridad de la información para establecer su alcance" (UNE-ISO/IEC, 2023, p. 8). Este proceso debe considerar factores como las cuestiones externas e internas previamente identificadas, los requisitos de las partes interesadas, y las interfaces y dependencias entre las actividades internas y externas. El alcance debe ser documentado y servir como referencia para guiar la implementación y evaluación continua del sistema.

#### Sistema de Gestión de la Seguridad de la Información

El núcleo de la norma ISO/IEC 27001 reside en el establecimiento y mantenimiento de un SGSI. Como se indica, "la organización debe establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información, incluyendo los procesos requeridos y sus interacciones de acuerdo con los requisitos de este documento" (UNE-ISO/IEC, 2023, p. 8). Este enfoque integrado permite a las organizaciones gestionar la seguridad de la información de manera coherente y efectiva, incorporando procesos como la gestión de riesgos, la evaluación de controles y la mejora continua, asegurando así la protección de la información crítica frente a amenazas internas y externas.

### Compatibilidad con otras Normas de Sistemas de Gestión

La norma ISO/IEC 27001 está diseñada para garantizar la compatibilidad con otras normas de sistemas de gestión mediante el uso de la estructura de alto nivel, términos y definiciones comunes establecidos en el Anexo SL de las Directivas ISO/IEC. Según la norma, "este enfoque común definido en el Anexo SL será útil para aquellas organizaciones que deciden implantar un sistema de gestión que cumpla con los requisitos de dos o más normas de sistemas de gestión" (UNE-ISO/IEC, 2023, p. 6).

Esto permite a las organizaciones integrar múltiples sistemas de gestión, como ISO 9001 (gestión de calidad) o ISO 14001 (gestión ambiental), de manera más eficiente, reduciendo duplicidades y mejorando la coherencia entre procesos. El marco compartido proporciona una base estandarizada para gestionar distintos aspectos organizacionales bajo un enfoque integrado, facilitando la implementación y el mantenimiento de varios estándares en una única estructura operativa.

## ISO 27002

### Introducción y Conceptos Generales

Un Sistema de Gestión de Seguridad de la Información (SGSI) se presenta como un marco integral para proteger los activos de información de las organizaciones, sin importar su tipo o tamaño. Este sistema es aplicable tanto en el sector público como en el privado, y puede adaptarse a industrias con entornos de riesgo específicos, sirviendo como referencia para determinar e implementar controles orientados al tratamiento de riesgos en la seguridad de la información (ISO/IEC, 2023, párr. 1).

La seguridad de la información abarca la protección de datos en múltiples formas, desde electrónicas hasta verbales, reconociendo que su valor no solo reside en palabras y números, sino también en conceptos, ideas y marcas.

Como señala la norma:

El valor de la información va más allá de las palabras escritas, los números y las imágenes: conocimientos, conceptos, ideas y marcas son ejemplos de formas intangibles de información. En un mundo interconectado, la información y otros activos asociados merecen o requieren protección frente a diversas fuentes de riesgo, ya sean naturales, accidentales o deliberadas. (ISO/IEC, 2023, p. 10).

Este enfoque holístico asegura la preservación de la confidencialidad, integridad y disponibilidad de los datos mediante un conjunto de controles adecuados.

Un SGSI no solo se limita a medidas tecnológicas; requiere el respaldo de políticas, normas, procesos y procedimientos integrados en la gestión organizativa. Además, “un SGSI eficaz requiere el apoyo de todo el personal de la organización y, en algunos casos, la participación de otras partes interesadas, como accionistas o proveedores” (UNE-ISO/IEC, 2023, p. 10). Este enfoque colaborativo permite identificar y mitigar riesgos con atención a los detalles, garantizando un entorno seguro que respalde los objetivos estratégicos de las organizaciones.

En conclusión, la implementación de un SGSI alineado con la norma ISO/IEC 27001 no solo protege los activos de información, sino que también fortalece la confianza de las partes interesadas, permitiendo alcanzar los objetivos de negocio en un entorno seguro y controlado (ISO/IEC, 2023, p. 10).

### Objeto y campo de aplicación

La Norma ISO/IEC 27002:2023 proporciona un marco de referencia para implementar controles genéricos de seguridad de la información. Está diseñada para ser utilizada por organizaciones de cualquier tipo y tamaño, con el objetivo de garantizar la protección de los activos de información en diversas áreas. Entre sus aplicaciones, destacan:

1. Implementación en SGSI basados en la ISO/IEC 27001: Proporciona los controles necesarios para gestionar la seguridad de la información en el contexto de un Sistema de Gestión de Seguridad de la Información (SGSI) (UNE-ISO/IEC, 2023, p. 13).
2. Mejores prácticas internacionales: Facilita la adopción de controles basados en estándares globalmente reconocidos. (UNE-ISO/IEC, 2023, p. 13).
3. Directrices específicas para organizaciones: Ayuda en el desarrollo de lineamientos adaptados a las necesidades y riesgos específicos de cada entidad. (UNE-ISO/IEC, 2023, p. 13).

### Términos, definiciones y abreviaturas

La norma detalla términos clave que son esenciales para la comprensión y aplicación de los controles. Algunos ejemplos incluyen:

Tabla 4 Términos, definiciones y abreviaturas ISO 27002

|  |  |
| --- | --- |
| **Término** | **Definición** |
| Activo | Cualquier cosa que tenga valor para la organización. |
| Control de acceso | Medios para garantizar que el acceso a los activos está autorizado y restringido según requisitos de seguridad. |
| Autenticación | Aportación de garantías de que las características que una entidad reivindica para sí misma son correctas. |
| Vulnerabilidad | Debilidad de un activo o control que puede ser explotada por una amenaza. |

Fuente: Elaboración Propia

### Políticas de seguridad aplicadas al desarrollo y mantenimiento

La gestión organizacional para el desarrollo seguro de software requiere la implementación de políticas de seguridad sólidas que orienten y regulen las actividades relacionadas con la protección de la información en el ámbito del desarrollo y mantenimiento.

Según la UNE-ISO/IEC (2023):

Las políticas de seguridad de la información deben ser definidas y aprobadas por la alta dirección, documentadas, comunicadas a todas las partes interesadas y revisadas periódicamente para garantizar su adecuación y efectividad en respuesta a cambios en el entorno técnico, normativo o de riesgo (p. 23).

Una política de seguridad debe incluir declaraciones sobre objetivos de seguridad, principios orientadores, compromisos con la mejora continua, y asignación de responsabilidades para la gestión de la seguridad de la información. Además, estas políticas generales se apoyan en políticas específicas que profundizan en áreas concretas como el control de acceso, gestión de activos, criptografía, seguridad de la red y desarrollo seguro (UNE-EN ISO/IEC, 2023).

Estas políticas específicas deben ser desarrolladas y revisadas por personal con autoridad y competencia técnica, tomando en cuenta factores como los cambios en la estrategia empresarial, riesgos emergentes y lecciones aprendidas de incidentes previos. Es esencial que las políticas sean comprensibles, accesibles, y comunicadas de manera adecuada a los empleados y partes externas relevantes (UNE-EN ISO/IEC, p. 25).

### Comunicación y Capacitación en Seguridad de Software

La formación y concienciación en seguridad de software son pilares fundamentales para garantizar que los desarrolladores y otros actores clave en el desarrollo de software comprendan sus responsabilidades. Según la norma:

El personal de la organización y las partes interesadas pertinentes deberían recibir una adecuada concienciación, educación y formalización sobre la seguridad de la información, así como actualizaciones periódicas sobre las políticas y procedimientos específicos según corresponda a su puesto de trabajo (UNE-ISO/IEC, 2023, p. 90).

Esto implica no solo proporcionar conocimiento técnico, sino también reforzar la cultura organizacional hacia la seguridad.

Los programas de capacitación deben incluir actividades diversas como sesiones informativas, módulos de aprendizaje electrónico, boletines, y simulacros basados en incidentes reales. Además, es crucial medir la efectividad de estas actividades mediante evaluaciones que aseguren la transferencia de conocimientos y permitan ajustes en el programa formativo. Este enfoque garantiza que el personal no solo sepa qué hacer, sino también por qué es importante, fomentando un compromiso proactivo hacia la comunicación efectiva complementando estas iniciativas al establecer canales claros para el reporte y manejo de incidentes. Por ejemplo, la organización debe implementar sistemas automatizados de notificación y puntos de contacto accesibles, promoviendo una cultura de respuesta ágil y coordinada ante cualquier amenaza o vulnerabilidad detectada.

Los servicios en la nube representan otro desafío crítico. Las políticas específicas deben definir roles y responsabilidades entre los proveedores y clientes, asegurando la confidencialidad, integridad y disponibilidad de los datos. Tal como se detalla en la norma:

La organización debería definir y comunicar cómo pretende gestionar los riesgos de seguridad de la información asociados con el uso de los servicios en la nube. Esto incluye controles específicos como administración de accesos, protección contra código malicioso y estrategias de salida para garantizar la continuidad del negocio en caso de finalización de servicios (UNE-ISO/IEC, 2023, p. 64).

# CAPITULO III

# MARCO PRACTICO

## FuNDAMENTOS de scrum

### Roles Claves en Scrum

La siguiente tabla describe el equipo Scrum para el desarrollo del proyecto.

Tabla 5 Roles de Scrum

|  |  |
| --- | --- |
| **Rol** | **Nombre** |
| Dueño del Producto (Product Owner) | Optica Vision |
| Responsable del Scrum (Scrum Master) | Daniel Santiago Soto Villamil |
| Equipo de Desarrollo (Develoment Team) | Daniel Santiago Soto Villamil |

Fuente: Elaboración Propia

### Artefactos de Scrum

#### Pila de Producto (Product Backlog)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **TAREA** | **PRIORIDAD** | **MÓDULO** | **ESTADO** |
| 1 | Registrar nuevos usuarios | Alta | Módulo de Gestión de Usuarios | Terminado |
| 2 | Administrar roles y permisos | Alta | Módulo de Gestión de Usuarios | Terminado |
| 3 | Actualizar stock de productos | Alta | Módulo de Gestión de Productos | Terminado |
| 4 | Registrar ventas | Alta | Módulo de Ventas | Terminado |
| 5 | Registrar logs de actividades | Media | Módulo de Auditoría y Logs | Terminado |
| 6 | Generar reportes de ventas | Media | Módulo de Reportes | Terminado |
| 7 | Auditoría de operaciones | Alta | Módulo de Auditoría y Logs | Terminado |
| 8 | Asignar productos a proveedores | Media | Módulo de Gestión de Proveedores | Terminado |
| 9 | Administración de tratamientos | Media | Módulo de Tratamientos y Colores | Terminado |
| 10 | Registrar trabajos personalizados | Alta | Módulo de Trabajos | Terminado |
| 11 | Generar reportes de trabajos personalizados | Media | Módulo de Reportes | Terminado |
| 12 | Registrar ópticas | Media | Módulo de Gestión de Ópticas | Terminado |
| 13 | Relacionar tratamientos con productos | Media | Módulo de Tratamientos y Colores | Terminado |
| 14 | Visualización de usuarios activos | Baja | Módulo de Gestión de Usuarios | Terminado |
| 15 | Control de permisos asignados | Media | Módulo de Gestión de Usuarios | Terminado |

## Modulo de gestion de usuarios y roles

### Definición de Requisitos del Modulo

Identificación de las funcionalidades necesarias para el correcto funcionamiento del módulo de gestión de usuarios y roles.

|  |  |
| --- | --- |
| **REQUISITO** | **DESCRIPCIÓN** |
| Registrar nuevos usuarios | Permitir al administrador registrar usuarios con nombre, contraseña y rol. |
| Configurar autenticación de usuarios | Implementar inicio de sesión con validación de credenciales seguras. |
| Administrar roles y permisos | Crear, editar y eliminar roles con sus respectivos permisos asignados. |
| Seguridad en contraseñas | Las contraseñas deben ser encriptadas antes de ser almacenadas. |
| Validación de roles | Restringir accesos y funcionalidades según el rol asignado al usuario. |

### Historias del Usuario

Detalle de las necesidades del usuario final expresadas como historias simples para guiar el desarrollo.

|  |  |
| --- | --- |
| ID | Historia de Usuario |
| HU1 | Como administrador, quiero registrar nuevos usuarios con roles asignados, para gestionar su acceso al sistema. |
| HU2 | Como administrador, quiero gestionar los roles existentes para modificar o eliminar permisos según sea necesario. |
| HU3 | Como usuario, quiero iniciar sesión con mi nombre de usuario y contraseña, para acceder al sistema según mi rol asignado. |

### Tareas del Sprint Backlog

Listado de las tareas seleccionadas del Product Backlog para ser implementadas durante este Sprint.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | TAREA | DESCRIPCIÓN | RESPONSABLE | ESTADO | TIEMPO ESTIMADO |
| 1 | Registrar nuevos usuarios | Crear formulario y lógica para agregar usuarios con roles asignados. | Daniel Santiago Soto Villamil | Terminado | 5 días |
| 2 | Configurar autenticación de usuarios | Implementar inicio de sesión seguro con validaciones de credenciales. | Daniel Santiago Soto Villamil | Terminado | 5 días |
| 3 | Administrar roles y permisos | Desarrollar funcionalidades para crear, editar y eliminar roles y permisos. | Daniel Santiago Soto Villamil | Terminado | 7 días |

### Desarrollo Iterativo y Validación

Descripción del progreso de las tareas desarrolladas y validación de las funcionalidades implementadas.

|  |  |  |
| --- | --- | --- |
| TAREA | PROGRESO | VALIDACIÓN REALIZADA |
| Registrar nuevos usuarios | Completada | Validación de datos únicos y almacenados en la base de datos correctamente. |
| Configurar autenticación de usuarios | Completada | Inicio de sesión exitoso con credenciales válidas; Negación para intentos fallidos. |
| Administrar roles y permisos | Completada | Creación, edición y eliminación de roles con permisos verificados correctamente. |

### Evaluación de Resultados

Análisis de los resultados obtenidos en el Sprint y su alineación con los objetivos del módulo.

|  |  |
| --- | --- |
| **PRUEBA UNITARIA** | **REGISTRO DE USUARIOS** |
| Descripción | Permite el registro de nuevos usuarios con sus respectivos roles asignados. |
| Objetivos | - Registrar un nuevo usuario con datos válidos.  - Verificar que el usuario sea almacenado correctamente en la base de datos. |
| Condiciones | Tener acceso al sistema como administrador y conexión a la base de datos activa. |
| Resultado esperado | El usuario es registrado exitosamente con sus credenciales y rol asignado. |
| Resultado obtenido | El sistema registra al usuario correctamente, validando los datos únicos y asignando el rol adecuado. |

|  |  |
| --- | --- |
| **PRUEBA UNITARIA** | **ADMINISTRAR ROLES Y PERMISOS** |
| Descripción | Permite crear, editar y eliminar roles y sus respectivos permisos. |
| Objetivos | - Crear un nuevo rol con permisos específicos.  - Editar un rol existente para agregar o eliminar permisos.  - Eliminar roles que no estén asignados a usuarios. |
| Condiciones | Tener acceso como administrador al módulo de roles y permisos. |
| Resultado esperado | Los roles y permisos son gestionados correctamente según las modificaciones realizadas. |
| Resultado obtenido | Se lograron crear, editar y eliminar roles y permisos sin errores ni conflictos. |

|  |  |
| --- | --- |
| **PRUEBA UNITARIA** | **AUTENTICACIÓN DE USUARIOS** |
| Descripción | Permite que los usuarios inicien sesión con credenciales válidas. |
| Objetivos | - Validar que solo usuarios registrados puedan iniciar sesión.  - Restringir el acceso a usuarios inactivos o con credenciales incorrectas. |
| Condiciones | El sistema debe estar en funcionamiento y conectado a la base de datos de usuarios. |
| Resultado esperado | Solo los usuarios registrados y activos pueden acceder al sistema. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **PRUEBA UNITARIA** | **DESCRIPCIÓN** | **OBJETIVOS** | **CONDICIONES** | **RESULTADO ESPERADO** | **RESULTADO OBTENIDO** |
| **Registro de Usuarios** | Permite el registro de nuevos usuarios con sus respectivos roles asignados. | Registrar un nuevo usuario con datos válidos. | Tener acceso al sistema como administrador y conexión a la base de datos activa. | El usuario es registrado exitosamente con sus credenciales y rol asignado. | El sistema registra al usuario correctamente, validando los datos únicos y asignando el rol adecuado. |
| **Administrar Roles y Permisos** | Permite crear, editar y eliminar roles y sus respectivos permisos. | - Crear un nuevo rol con permisos específicos.  - Editar un rol existente para agregar o eliminar permisos.  - Eliminar roles que no estén asignados a usuarios. | Tener acceso como administrador al módulo de roles y permisos. | Los roles y permisos son gestionados correctamente según las modificaciones realizadas. | Se lograron crear, editar y eliminar roles y permisos sin errores ni conflictos. |
| **Autenticación de Usuarios** | Permite que los usuarios inicien sesión con credenciales válidas. | - Validar que solo usuarios registrados puedan iniciar sesión.  - Restringir el acceso a usuarios inactivos o con credenciales incorrectas. | El sistema debe estar en funcionamiento y conectado a la base de datos de usuarios. | Solo los usuarios registrados y activos pueden acceder al sistema. | La autenticación funciona correctamente, permitiendo el acceso solo con credenciales válidas. |

**BIBLIOGRAFÍA**

Coarite Tumiri, V. (2007). Sistema Integrado de Control de Inventario 'ATIPAJ' Compañía Cervecera Boliviana S.A. Universidad Mayor de San Andrés, Carrera de Informática.

La Fuente Choque, J. (2008). Sistema para la Gestión de Ventas e Inventario Caso: Importadora Soluciones Médicas Lifemed S.R.L. Universidad Mayor de San Andrés, Carrera de Informática.

Ramos Paye, J. L. (2005). Sistema de Control de Inventarios para Laboratorios Crespal S.A. Regional Sucre. Universidad Mayor de San Andrés, Carrera de Informática.

Choque Chambilla, R. F. (2007). Sistema de Información de Compras e Inventarios SAMA. Universidad Mayor de San Andrés, Carrera de Informática.

Suarez Marin, V. (2008). Sistema de Control y Seguimiento de Almacenes para la Corte Departamental Electoral La Paz, Sala Provincias. Universidad Mayor de San Andrés, Carrera de Informática.

Chiri Honorio, C. (2009). Sistema de Entradas y Salidas e Inventario Caso: BOLITAL S.R.L. Universidad Mayor de San Andrés, Carrera de Informática.

Callisaya Apaza, W. D. (2017). Software de Gestión y Control de Inventarios Caso: AGADON S.R.L. Universidad Mayor de San Andrés, Carrera de Informática.

Deyimar. (Junio de 2023). hostinger: https://www.hostinger.es/tutoriales/que-es-react

Haverbeke, M. (2018). *Eloquent JavaScript.* No Starch Press. https://doi.org/https://eloquentjs-es.thedojo.mx/Eloquent\_JavaScript.pdf

Jiménez, C. D. (2020). *Ciberseguridad.* Marcombo. Ciberseguridad.

kinsta. (Julio de 2022 ). *Kinsta Inc.* https://kinsta.com/es/base-de-conocimiento/nestjs/

López, I. (2021). *Node.js Javascript del lado del servidor.* https://doi.org/https://annas-archive.li/md5/f8a2c5d2aeca418927b369aff0133096

Marqués, M. (2011). *Bases de Datos.* https://doi.org/https://bdigital.uvhm.edu.mx/wp-content/uploads/2020/05/Bases-de-Datos.pdf

Meta Platforms, I. (2023). React – A JavaScript library for building user interfaces: https://reactjs.org/docs/getting-started.html

Muller, M. (2003). *Fundamentos de administración de inventarios.* FreeLibros.

NestJS, C. (2023). NestJS - A progressive Node.js framework: https://docs.nestjs.com

PostgreSQL, G. D. (2023). PostgreSQL Documentation: https://www.postgresql.org/docs/

Roberto Hernández Sampieri, C. F. (2010). *Metodología de la investigación.* México: McGraw-Hill.

Salas, H. G. (2009). *Inventarios: manejo y control.* Ecoe Ediciones.

Sampieri, H. (2018). *METODOLOGÍA DE LA INVESTIGACIÓN: LAS RUTAS CUANTITATIVA, CUALITATIVA Y MIXTA* (Sexta ed.). McGraw-Hill.

Sommerville, I. (2011). *Ingeniería de software.* Pearson Educación. https://doi.org/https://annas-archive.li/md5/e1cb1c2ff784861f5dfc329bfae04be8

Standardization, I. O. (2022). *Controles de seguridad para la información.* ISO.

Talaminos, A. (2022). *TypeScript para todo.* https://doi.org/https://annas-archive.li/md5/a0a3b6094645a448e33e8bfb986fb67e

TechTarget. (Enero de 2023). *web application (web app)*. TechTarget: https://www.techtarget.com/searchsoftwarequality/definition/Web-application-Web-app

The MUI team pact. (2023). mui: https://mui.com/material-ui/getting-started/

typeorm. (2023). typeorm: https://typeorm.io/

UNE-ISO/IEC. (2023). *Sistema de Gestión de la Seguridad de la Información.*

UNE-ISO/IEC. (2023). *Tecnología de la información - Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información.*

Waller, M. A. (2015). *Administración de inventarios.* Pearson.