INGENIERÍA DE SISTEMAS

SISTEMA DE ADMINISTRACIÓN DE INVENTARIOS DE INSUMOS PARA LABORATORIO DE ÓPTICA

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

Autor: Daniel Santiago Soto Villamil

Tutor: Maritza Netzy Paiva Zapana

La Paz - Bolivia

2024

RESUMEN

TÍTULO: SISTEMA DE ADMINISTRACIÓN DE INVENTARIOS DE INSUMOS PARA LABORATORIO DE ÓPTICA

AUTOR: DANIEL SANTIAGO SOTO VILLAMIL

PROBLEMÁTICA

Ineficiente administración de inventarios de insumos de laboratorios de 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 normas basadas en la ISO 27001 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	: Lic. Maritza Netzy Paiva Zapana
DESCRIPTORES O TEMAS	: Sistema web, Vue.js Nest.js, Node.js, PostgreSQL, TypeScript, JavaScript.
PERÍODO DE INVESTIGACIÓN	: 2024
EMAIL DE LOS AUTORES	: Santiago_SV@outlook.es

ÍNDICE

Página

CAPITULO I

INTRODUCCIÓN

1.1. ANTECEDENTES 1

1.2. PLANTEAMIENTO DEL PROBLEMA 4

1.2.1. Identificación Del Problema 5

1.2.2. Problema Central 6

1.2.3. Formulación Del Problema 7

1.3. OBJETIVOS DE LA INVESTIGACIÓN 7

1.3.1. Objetivo General 7

1.3.2. Objetivos Específicos 7

1.4. DELIMITACIÓN 8

1.4.1. Límite Temporal 8

1.4.2. Límite Espacial 8

1.5. JUSTIFICACIÓN 9

1.5.1. Justificación Social 9

1.5.2. Justificación Económica 9

1.5.3. Justificación Tecnológica 10

1.6. TIPOLOGÍA DEL PROYECTO 11

1.7. MÉTODOS DE INVESTIGACIÓN 11

1.7.1. Enfoque De La Investigación 11

1.7.2. Métodos De Investigación 11

1.7.3. Diseño De La Investigación 12

1.7.4. Tipo De Investigación 13

1.8. TÉCNICAS DE INVESTIGACIÓN Y SUS INSTRUMENTOS 13

1.8.1. Las Entrevistas en Profundidad 14

1.9. POBLACIÓN Y MUESTRA 14

1.9.1. Población 14

1.9.2. Muestra 15

CAPITULO II

MARCO TEÓRICO

2.1. SISTEMA 16

2.2. SISTEMA WEB 16

2.3. HERRAMIENTAS DE DESARROLLO 17

2.3.1. JavaScript 18

2.3.2. TypeScript 20

2.3.3. Node.JS 22

2.3.4. Nest.JS 23

2.3.5. Vue.JS 24

2.3.6. TyperORM 25

2.3.7. TailWind CSS 26

2.4. BASE DE DATOS 27

2.4.1. Sistema de Gestión de Bases de Datos 28

2.4.2. PostgreSQL 29

2.5. API Y API REST 31

2.5.1. API 31

2.5.2. REST 31

2.5.3. API REST 32

2.6. INVENTARIO 33

2.6.1. Métodos de Control de Inventarios 34

2.7. ISO 27001 36

2.7.1. Principios Fundamentales de la ISO/IEC 27001 38

2.7.1.1. Contexto de la organización 38

2.7.1.2. Necesidades y expectativas de las partes interesadas 38

2.7.2. Soporte en el Sistema de Gestión de la Seguridad de la Información (SGSI) .. 39

2.7.2.1. Recursos necesarios 39

2.7.2.2. Competencia y capacitación 40

2.7.2.3. Concienciación del personal 40

2.7.2.4. Comunicación efectiva 41

2.7.3. Contexto de la Organización 42

2.7.3.1. Comprensión de la organización y de su contexto 42

2.7.3.2. Comprensión de las necesidades de las partes interesadas 43

2.7.3.3. Sistema de gestión de la seguridad de la información 43

2.7.4. Compatibilidad con otras Normas de Sistemas de Gestión 44

2.8. MARCO DE TRABAJO SCRUM 44

CAPITULO III

MARCO PRACTICO

3.1. SCRUM 47

3.1.1. Roles Claves en Scrum 47

3.1.2. Requerimientos 48

3.1.2.1. Requerimientos funcionales 48

3.1.2.2. Requerimientos no funcionales 51

3.1.3. Pila de Producto (Product Backlog) 52

3.1.4. Diseño del Sistema 55

3.1.4.1. Diagrama de casos de uso 55

3.1.4.2. Diagrama de secuencia 56

3.2. SPRINT DE GESTIÓN DE AUTENTICACIÓN 57

3.2.1. Objetivos del Sprint 57

3.2.2. Definición de la Gestión de Autenticación 58

3.2.3. Historias del Usuario 59

3.2.4. Tareas del Sprint Backlog 60

3.2.5. Desarrollo Iterativo y Validación 61

3.2.6. Evaluación de Resultados 62

3.2.6.1. Resultados de roles 62

3.2.6.2. Resultados de usuarios....64

3.3. SPRINT DE GESTIÓN PERSONAL....66

3.3.1. Objetivos del Sprint....66

3.3.2. Definición de La Gestión De Personal....67

3.3.3. Historias del Usuario....68

3.3.4. Tareas del Sprint Backlog....69

3.3.5. Desarrollo Iterativo y Validación....70

3.3.6. Evaluación de Resultados....71

3.3.6.1. Resultados de personal....71

3.4. SPRINT DE GESTIÓN DE PROVEEDORES Y PRODUCTOS....73

3.4.1. Objetivos del Sprint....73

3.4.2. Definición de la Gestión de Proveedores y Productos....74

3.4.3. Historias del Usuario....75

3.4.4. Tareas del Sprint Backlog....76

3.4.5. Desarrollo Iterativo y Validación....77

3.4.6. Evaluación de Resultados....78

3.4.6.1. Resultados de proveedores....78

3.4.6.2. Resultados de productos 80

3.5. SPRINT DE GESTIÓN DE TRABAJOS 82

3.5.1. Objetivos del Sprint 82

3.5.2. Definición de la Gestión de Trabajos 82

3.5.3. Historias del Usuario 83

3.5.4. Tareas del Sprint Backlog 84

3.5.5. Desarrollo Iterativo y Validación 87

3.5.6. Evaluación de Resultados 88

3.5.6.1. Resultados de trabajos. 88

3.6. SPRINT DE GESTIÓN DE VENTAS 90

3.6.1. Objetivos del Sprint 90

3.6.2. Definición de la Gestión de Ventas 91

3.6.3. Historias del Usuario 92

3.6.4. Tareas del Sprint Backlog 93

3.6.5. Desarrollo Iterativo y Validación. 95

3.6.6. Evaluación de Resultados 96

3.6.6.1. Resultados de ventas 96

3.7. SPRINT DE GESTIÓN DE LA ISO 27001 98

3.7.1. Introducción 98

3.7.2. Alcance del Sistema 99

3.7.3. Contexto de la Organización 100

3.7.3.1. Análisis de factores internos 100

3.7.3.2. Análisis de factores externos 101

3.7.3.3. Identificación de partes interesadas y sus necesidades 101

3.7.4. Liderazgo 102

3.7.4.1. Política de seguridad de la información 102

3.7.4.2. Roles, responsabilidades y autoridades 102

3.7.4.3. Evidencia de liderazgo 103

3.7.4.4. Seguridad en la gestión de proyectos 104

3.7.5. Planificación 104

3.7.5.1. Acciones para tratar los riesgos y oportunidades 105

3.7.5.2. Evaluación de riesgos 105

3.7.5.3. Tratamiento de los riesgos 108

3.7.5.4. Declaración de Aplicabilidad (SoA) 109

3.7.5.5. Objetivos de seguridad de la información 111

3.7.5.6. Planificación de cambios..... 112

3.7.6. Operación..... 112

3.7.6.1. Planificación y control operacional..... 113

3.7.6.2. Evaluación de los riesgos de seguridad de la información 113

3.7.6.3. Tratamiento de los riesgos de seguridad de la información 114

3.7.7. Evaluación del Desempeño..... 114

3.7.7.1. Seguimiento, medición, análisis y evaluación 114

3.7.7.2. Indicadores clave (KPIs) 115

3.7.7.3. Tabla de evaluación de controles..... 115

CAPITULO IV

ANÁLISIS DE FACTIBILIDAD

4.1. FACTIBILIDAD TÉCNICA 117

4.1.1. Requerimientos Técnicos:..... 117

4.1.2. Evaluación de Recursos Existentes 117

4.1.3. Conclusión Técnica 118

4.2. ANÁLISIS DE FACTIBILIDAD OPERATIVA 118

4.2.1. Evaluación Operativa 118

4.2.2. Conclusión Operativa 119

4.3. ANÁLISIS DE FACTIBILIDAD ECONÓMICA 119

4.3.1. Presupuesto Inicial 119

4.3.2. Costos operativos Anuales 120

4.4. ANÁLISIS COSTO-BENEFICIO 121

4.4.1. Beneficios Cuantificables (Anuales): 121

4.4.2. Cálculo ROI 121

4.4.3. Período de Recuperación 122

4.4.4. Conclusión 122

4.5. COCOMO 2 122

4.5.1. Estudio de costos 122

4.5.2. Estimación el costo para el desarrollo 122

4.5.3. Recuento de Función 123

4.5.3.1. Determinar puntos función 123

4.6. COSTO TOTAL 124

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES 127

5.1.1. Cumplimiento de Objetivos 127

5.1.2. Integración y Eficiencia 127

5.1.3. Gestión de Seguridad 128

5.1.4. Metodología Ágil 128

5.1.5. Factibilidad del Sistema 128

5.2. RECOMENDACIONES 128

5.2.1. Mejoras en Reportes de Inventarios 128

5.2.2. Gestión Detallada de Usuarios 129

5.2.3. Ampliación de Controles de Auditoría 129

5.2.4. Exportación Personalizada de Datos 129

5.2.5. Mejoras en la Visualización de Inventarios 130

5.2.6. Respaldo Automático de Datos 130

REFERENCIAS BIBLIOGRÁFICAS 131

ANEXOS 134

APÉNDICE 141

ÍNDICE DE TABLAS

Tabla 1 Tipos de Gestión de Inventarios. 34

Tabla 2 Roles de Scrum 47

Tabla 3 Requerimientos Funcionales 48

Tabla 4 Requerimientos No Funcionales 51

Tabla 5 Product Backlog 52

Tabla 6 Requisitos De La Gestión De Autenticación. 58

Tabla 7 Historia De Usuarios De La Gestión De Autenticación. 59

Tabla 8 Tareas Del Sprint Backlog De Gestión De Autenticación. 60

Tabla 9 Desarrollo Iterativo y Validación de Gestión de Autenticación. 61

Tabla 10 Resultados del Módulo de Autenticación. 62

Tabla 11 Resultados del Módulo de Usuarios 64

Tabla 12 Requisitos De La Gestión Del Personal 67

Tabla 13 Historia De Usuarios De La Gestión De Personal. 68

Tabla 14 Tareas Del Sprint Backlog De Gestión Del Personal. 69

Tabla 15 Desarrollo Iterativo y Validación de Gestión del Personal. 70

Tabla 16 Resultados del Módulo de Personal. 72

Tabla 17 Requisitos De La Gestión De Proveedores y Productos. 74

Tabla 18 Historia De Usuarios De La Gestión De Proveedores Y Productos. 75

Tabla 19 Tareas Del Sprint Backlog De Gestión de Proveedores y Productos. 76

Tabla 20 Desarrollo Iterativo y Validación De Gestión de Proveedores Y Productos. 77

Tabla 21 Resultados del Módulo de Proveedores. 78

Tabla 22 Resultados del Módulo de Productos. 80

Tabla 23 Requisitos De La Gestión De Trabajos. 82

Tabla 24 Historia De Usuarios De La Gestión De Trabajos. 84

Tabla 25 Tareas Del Sprint Backlog De Gestión de Trabajos. 84

Tabla 26 Desarrollo Iterativo y Validación De Gestión de Trabajos. 87

Tabla 27 Resultados del Módulo de Trabajos. 88

Tabla 28 Requisitos De La Gestión De Ventas. 91

Tabla 29 Historia De Usuarios De La Gestión De Ventas. 92

Tabla 30 Tareas Del Sprint Backlog De Gestión de Ventas. 93

Tabla 31 Desarrollo Iterativo y Validación De Ventas. 95

Tabla 32 Resultados del Módulo de Ventas. 96

Tabla 33 Explicación y Resultado de las Métricas del CVSS 106

Tabla 34 Tratamientos de Riesgos 108

Tabla 35 Declaración de Aplicabilidad (SoA) 109

Tabla 36 Objetivos de la seguridad de la Información 111

Tabla 37 Evaluación de Controles 115

Tabla 38 Recursos Existentes 117

Tabla 39 Aspectos de la Evaluación Operativa 118

Tabla 40 Presupuesto Inicial 119

Tabla 41 Costos Operativos Anuales 120

Tabla 42 Beneficios Anuales 121

Tabla 43 Recuento de Función 123

Tabla 44 Factores de Peso de la Complejidad para Tipos de Objeto 123

Tabla 45 Cronograma de Gant 141

ÍNDICE DE FIGURAS

Figura 1 Diagrama Ishikawa 6

Figura 2 Casos de Uso 55

Figura 3 Diagrama de Secuencia 56

Figura 4 Resultado de Gestión de Roles 64

Figura 5 Resultados de Gestión de Usuarios 65

Figura 6 Resultados de Gestión Personal 73

Figura 7 Resultados Gestión de Proveedores 80

Figura 8 Resultados de Gestión de Productos 81

Figura 9 Resultados de Gestión de Trabajos 90

Figura 10 Resultado Gestión de Ventas 98

Figura 11 Resultados del CVSS 106

Figura 12 Calculo COCOMO II 125

Figura 13 Resultados obtenidos del COCOMO II 126

CAPITULO I

INTRODUCCIÓN

1.1. 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.

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.

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.

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.

1.2. PLANTEAMIENTO DEL PROBLEMA

En el contexto actual de las ópticas, la administración de inventarios es un proceso fundamental que, si no se gestiona de manera adecuada, puede generar pérdidas económicas, desabastecimiento de productos y una limitada capacidad para satisfacer la demanda de los clientes. Muchas ópticas aún operan con sistemas manuales para la gestión de sus inventarios, lo que dificulta el control eficiente del stock, la planificación de reposiciones y el seguimiento de productos en almacén. Esto puede derivar en costos operativos elevados y una disminución en la competitividad de estas empresas.

La implementación de un Sistema de Administración de Inventarios de Insumos para Laboratorio de Óptica tiene como objetivo optimizar la gestión del stock, favoreciendo la disponibilidad constante de insumos y mejorando los procesos operativos relacionados con el inventario. El problema principal radica en el uso de métodos manuales, que resultan ineficientes para administrar el inventario de manera efectiva, afectando la capacidad de las ópticas para responder oportunamente a las necesidades del mercado.

Evidencia de esta problemática se encuentra en estudios previos que muestran cómo las empresas que no cuentan con herramientas de administración automatizadas enfrentan pérdidas significativas en su stock, dificultades en el seguimiento de productos y una disminución en su capacidad para prever necesidades futuras (López, 2021). Esto repercute directamente en su capacidad operativa, incrementando costos innecesarios y afectando su desempeño en un mercado altamente competitivo.

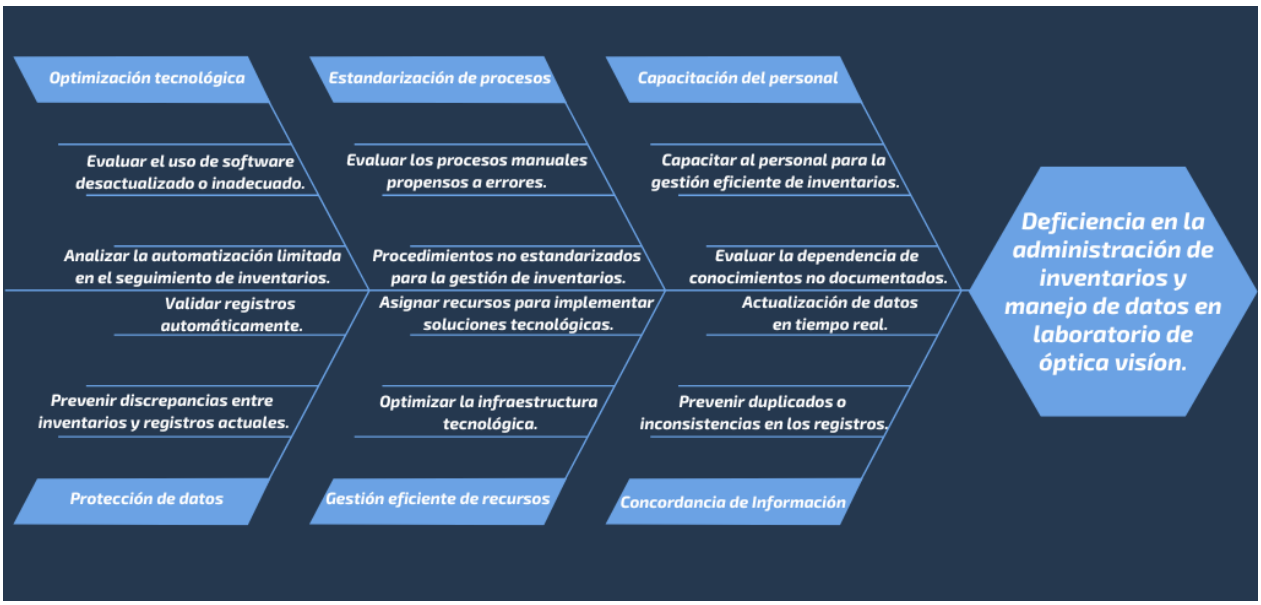
Se espera que el desarrollo de este sistema no solo optimice los procesos operativos relacionados con el manejo de inventarios, sino que también permita a las ópticas mantener un control preciso del stock, mejorar su capacidad de respuesta y reducir costos derivados de ineficiencias en la gestión de insumos.

1.2.1. 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. (miro, 2023)

Figura 1 Diagrama Ishikawa



1.2.2. Problema Central

El laboratorio de Óptica Visión enfrenta deficiencias en la administración de inventarios y el manejo de datos, causadas por el uso de procesos manuales propensos a errores y la falta de automatización en el registro y actualización de información. Estas problemáticas generan discrepancias entre los inventarios físicos, inconsistencias en los registros lo que dificulta la continuidad operativa y la toma de decisiones basada en datos precisos. Además, la falta de concordancia en la información afecta la coordinación interna, limitando la capacidad de responder eficientemente a las demandas operativas.

1.2.3. Formulación Del Problema

¿Qué deficiencias existen en la administración de inventarios y en el manejo de información en las ópticas, y de qué manera impactan estas en la eficiencia técnica y operativa del laboratorio?

1.3. OBJETIVOS DE LA INVESTIGACIÓN

1.3.1. Objetivo General

Desarrollar un sistema de administración de inventarios de insumos del Laboratorio de óptica Visión para reducir perdidas mediante alertas tempranas y hacer el seguimiento de sus productos.

1.3.2. 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 de datos alineada con las características operativas de los laboratorios de óptica, respetando los principios de organización y seguridad de los datos.
- Desarrollar los módulos de usuario, personal, productos, proveedores y ventas en el sistema de administración de inventarios para gestionar la trazabilidad de los insumos.
- Aplicar directrices basadas en las normas de la ISO 27001 en el sistema de administración de insumos para laboratorios de óptica.

- Mostrar listados de insumos prontos a acabarse y aquellos que ya llevan un tiempo determinado establecido como máximo como alertas tempranas
- Generar reportes automatizados a partir de datos de ventas, trabajos e insumos del laboratorio de óptica.

1.4. DELIMITACIÓN

1.4.1. Límite Temporal

La investigación sobre el Sistema de Administración de Inventarios para Ópticas con Implementación de Seguridad Basada en la ISO 27001 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.

1.4.2. Límite Espacial

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 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.

1.5. JUSTIFICACIÓN

1.5.1. Justificación Social

La implementación de un Sistema de Administración de Inventarios para Ópticas con Seguridad Basada en la ISO 27001 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 implementación de un sistema eficiente para la administración de inventarios puede servir como un ejemplo para otras ópticas, promoviendo mejores prácticas en el manejo y control del stock. Este avance contribuirá a fortalecer la competitividad de las ópticas, ayudándolas a gestionar sus operaciones de manera más efectiva. La optimización de los procesos beneficiará tanto a los empleados como a los consumidores, mejorando la calidad del servicio y la eficiencia operativa en el sector óptico.

1.5.2. Justificación Económica

Desde una perspectiva económica, la implementación de un Sistema de Administración de Inventarios con Seguridad Basada en la ISO 27001 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 ineficiente, 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.

1.5.3. Justificación Tecnológica

El proyecto está respaldado por una arquitectura tecnológica moderna diseñada para garantizar escalabilidad, seguridad y eficiencia, elementos esenciales para cumplir con los objetivos propuestos. Se emplea NestJS con Node.js en el backend, seleccionados por su enfoque modular y su capacidad para construir aplicaciones robustas y escalables. Para el frontend, se utiliza Vue.js, una herramienta versátil que permite crear interfaces dinámicas y amigables para el usuario. La base de datos está gestionada por PostgreSQL, reconocida por su confiabilidad y rendimiento en entornos de alta complejidad. En términos de seguridad, se implementaron autenticación con JWT, encriptación de contraseñas con bcrypt, y configuración de CORS para un control adecuado de accesos. Además, herramientas como VSCode, Postman y PlantUML fueron clave para optimizar el desarrollo, pruebas y documentación. Esta selección tecnológica asegura que el sistema no solo cumple con los requerimientos actuales, sino que está preparado para escalar y adaptarse a futuras necesidades.

1.6. 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. 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.

1.7. MÉTODOS DE INVESTIGACIÓN

1.7.1. 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)

1.7.2. 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. 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.

1.7.3. 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 de insumos para laboratorio de óptica influye en la operatividad. 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.

1.7.4. 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, 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)

1.8. TÉCNICAS DE INVESTIGACIÓN Y SUS INSTRUMENTOS

Las técnicas de investigación seleccionadas para este estudio serán:

1.8.1. 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.

1.9. POBLACIÓN Y MUESTRA

1.9.1. Población

La población de esta investigación estará compuesta por el laboratorio óptico de la "Óptica Visión" de la ciudad de La Paz, Bolivia. Este laboratorio interactúa con sistemas de administración de inventarios y se centra en la gestión y control de insumos. La

población incluye al dueño del laboratorio óptico, quien tiene conocimiento directo sobre la administración de inventarios en laboratorios de ópticas.

1.9.2. Muestra

La muestra de esta investigación será el laboratorio óptico de la "Óptica Visión". En este caso, se entrevistará exclusivamente al dueño del laboratorio óptico, quien proporciona una perspectiva clave sobre la implementación y operación del sistema.

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)

Por lo tanto, la selección de la muestra será de muestreo por criterio, permitiendo incluir al dueño del laboratorio óptico, quien interactúa directamente con el Sistema de Administración de Inventarios y cuenta con experiencia en la gestión de inventarios.

CAPITULO II

MARCO TEÓRICO

2.1. 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 (Sommerville, 2011). 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.

2.2. 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.

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 (TechTarget, 2023). 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.

2.3. 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)

2.3.1. 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" (p. 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" (p. 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. (p. 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" (p. 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" (p. 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).

2.3.2. 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" (pp. 9-10), lo que confirma la popularidad del lenguaje a nivel global.

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)

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).

2.3.3. 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).

2.3.4. Nest.JS

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: “El 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)” (kinsta, 2022, párr. 1), lo cual facilita la estructuración de aplicaciones complejas.

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).

2.3.5. Vue.JS

Vue.js, conocido comúnmente como Vue (pronunciado /vjuː/, como "view"), es un framework progresivo diseñado para construir interfaces de usuario. A diferencia de otros frameworks monolíticos, Vue ha sido creado para ser utilizado de manera incremental, lo que lo convierte en una herramienta altamente adaptable para diversos proyectos. Su librería central se enfoca únicamente en la capa de visualización, lo que facilita su integración con otras librerías o sistemas ya existentes, proporcionando flexibilidad tanto para proyectos pequeños como para aplicaciones más complejas.

Entre sus características más destacadas, Vue permite el desarrollo de aplicaciones web de una sola página (SPA, por sus siglas en inglés) cuando se combina con herramientas modernas y librerías de apoyo. Esta capacidad lo posiciona como una opción ideal para

proyectos que buscan sofisticación sin perder la simplicidad en su implementación inicial. Según el equipo de desarrollo de Vue, "la simplicidad progresiva es una de las claves que hacen de Vue una herramienta única en el ecosistema del desarrollo frontend" (Vue Team, 2024, párr. 1).

Además, Vue ha ganado popularidad gracias a su enfoque intuitivo y a su curva de aprendizaje asequible, incluso para desarrolladores que recién comienzan en el área del desarrollo frontend. Este framework también se distingue por su comunidad activa y su compatibilidad con herramientas modernas como Webpack, Babel y TypeScript, lo que lo convierte en una solución versátil para proyectos de diversa escala (Vue Team, 2024).

En resumen, Vue.js es más que una herramienta para crear interfaces: es un framework progresivo que combina simplicidad, flexibilidad y sofisticación, permitiendo a los desarrolladores adaptar su uso a las necesidades específicas de sus proyectos.

2.3.6. 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).

2.3.7. TailWind CSS

En el desarrollo de interfaces web, los desarrolladores enfrentan constantemente retos asociados al diseño y la personalización de estilos. Entre estos desafíos se encuentran la necesidad de anular estilos predefinidos, mantener una especificidad adecuada y optimizar la velocidad de desarrollo y mantenimiento, especialmente en aplicaciones de gran escala. Según Carreón (2020), "el uso de herramientas avanzadas para gestionar estilos puede simplificar procesos complejos y mejorar la eficiencia en el diseño frontend" (párr. 1). Además, crear diseños personalizados que reflejen la identidad del producto o idea es esencial para destacar en un entorno altamente competitivo.

En este contexto, Tailwind CSS se presenta como una solución innovadora. Este framework, basado en PostCSS, permite construir sitios web con estilos altamente personalizados, ofreciendo la posibilidad de ajustar colores, tamaños de borde, pesos de

fuente, espaciado, puntos de interrupción, sombras y mucho más. Según Carreón (2020), "los frameworks basados en PostCSS han transformado la manera en que los desarrolladores manejan estilos, al permitir un control granular y altamente personalizable en el diseño de interfaces" (parr. 2). Una de las principales ventajas de Tailwind CSS es su capacidad para evitar los problemas comunes de personalización que suelen presentarse en otros entornos de trabajo que utilizan componentes prediseñados, los cuales, aunque prácticos, pueden llevar a estilos genéricos y a la pérdida de originalidad en los diseños.

Tailwind CSS no solo optimiza el flujo de trabajo, sino que también asegura que los desarrolladores puedan crear interfaces visualmente atractivas y funcionales sin comprometer la identidad y valores del producto (Carreón, 2020). Esto se logra gracias a su enfoque en clases utilitarias que facilitan la creación de estilos precisos y consistentes. Como resultado, Tailwind CSS se ha consolidado como una herramienta valiosa para diseñar interfaces modernas, potentes y alineadas con las necesidades específicas de cada proyecto.

2.4. 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)

2.4.1. 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).

2.4.2. PostgreSQL

PostgreSQL es una herramienta ampliamente reconocida en el ámbito del software libre por su cumplimiento de estándares internacionales y funcionalidades avanzadas. Su

flexibilidad, escalabilidad y adaptabilidad lo convierten en una de las opciones más utilizadas para la gestión de bases de datos. Según (Gibert, 2007), "la escalabilidad y la interoperabilidad son claves en cualquier sistema de gestión de bases de datos moderno" (p. 5). Estas características han permitido que PostgreSQL se mantenga competitivo frente a herramientas comerciales.

El origen de PostgreSQL se remonta a POSTGRES, desarrollado en la Universidad de Berkeley, y desde 1994 ha evolucionado como un sistema líder en su categoría. Como se menciona, "PostgreSQL es un gestor de bases de datos orientadas a objetos (SGBDOO o ORDBMS en sus siglas en inglés) muy conocido y usado en entornos de software libre porque cumple los estándares SQL92 y SQL99, y también por el conjunto de funcionalidades avanzadas que soporta" (Gibert, 2007, p. 5).

Gibert (2021) destaca que "PostgreSQL ha sido adoptado ampliamente debido a su adaptabilidad, lo que lo posiciona como una de las principales herramientas en el mercado de bases de datos" (p. 5). Además, su capacidad para gestionar datos estructurados y no estructurados es esencial en entornos modernos, ya que "ofrece capacidades avanzadas para ambos tipos de datos" (Gibert, 2007, p. 5). La comunidad de desarrollo también juega un papel fundamental, promoviendo mejoras constantes que lo mantienen a la vanguardia.

2.5. API Y API REST

2.5.1. API

Según Red Hat (2023), "Una API es un conjunto de definiciones y protocolos que se utiliza para desarrollar e integrar sistemas de software de las aplicaciones" (párr. 2). Además, permite que las empresas compartan recursos e información mientras garantizan la seguridad y autenticación.

Frente al tema, "las API actúan como mediadores entre los usuarios o clientes y los recursos o servicios web, definiendo los accesos y permitiendo la interacción sin necesidad de conocer detalles internos" (Red Hat, 2023, párr. 3). Esto las convierte en herramientas clave para la interoperabilidad de sistemas.

Red Hat (s.f.) afirmó lo siguiente:

> Una API puede considerarse como el contrato entre el usuario y el proveedor de información, estableciendo el contenido necesario en la llamada y la respuesta requerida. Por ejemplo, una API de servicio meteorológico podría requerir un código postal como entrada y devolver una temperatura máxima y mínima como respuesta (párr. 4).

2.5.2. REST

Según Red Hat (2023), "REST no es un protocolo ni un estándar, sino un conjunto de límites relacionados con la arquitectura" (párr. 5). Este estilo arquitectónico define cómo estructurar APIs para garantizar interoperabilidad y eficiencia en la web.

Frente al tema, Red Hat (2023) afirma que "los principios fundamentales de REST incluyen una arquitectura cliente-servidor, comunicación sin estado y almacenamiento en caché, lo cual optimiza las interacciones entre cliente y servidor" (párr. 6).

Se describe que:

> Los desarrolladores de las API pueden implementar REST de diversas maneras. Cuando el cliente envía una solicitud a través de una API RESTful, esta transfiere una representación del estado del recurso requerido al cliente o extremo. La información se entrega por medio de HTTP en formatos como JSON, XML, o texto plano (Red Hat, 2023, párr. 7).

2.5.3. API REST

Frente al tema, "una API REST es una interfaz que sigue los principios arquitectónicos de REST para facilitar la comunicación entre sistemas, optimizando el uso de recursos con respuestas en formatos estándar como JSON o XML" (Red Hat, 2023, párr. 8).

Red Hat (2023) afirmó lo siguiente:

> Para que una API sea considerada RESTful, debe cumplir varios principios, como arquitectura cliente-servidor, comunicación sin estado, datos almacenables en caché, una interfaz uniforme, mensajes autodescriptivos y un sistema jerárquico en capas. Opcionalmente, puede incluir código bajo demanda para extender las capacidades del cliente (párr. 9).

Por lo tanto, "las API REST son ideales para aplicaciones modernas debido a su flexibilidad, velocidad y adaptabilidad, especialmente en entornos como el desarrollo de aplicaciones móviles y el Internet de las cosas (IoT)" (Red Hat, 2023., párr. 10).

2.6. 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 (Muller, 2003).

2.6.1. Métodos de Control de Inventarios

La gestión de inventarios es un componente esencial en la administración eficiente de recursos dentro de una organización. Los métodos de control y valorización de inventarios permiten optimizar los procesos de almacenamiento, distribución y reposición de productos, garantizando un balance entre disponibilidad y costos. Desde técnicas como el método ABC, que clasifica los productos según su impacto financiero, hasta el Just in Time (JIT), que minimiza el almacenamiento innecesario, cada metodología responde a necesidades específicas del mercado y del modelo de negocio. Su correcta implementación no solo asegura el flujo constante de bienes, sino que también reduce riesgos, mejora la toma de decisiones y potencia la competitividad empresarial. (Gonzales, 2023)

Tabla 1 Tipos de Gestión de Inventarios.

Método	Descripción

Método ABC	Clasifica las existencias en tres categorías (A, B, C) basadas en su importancia, volumen y precio. Los artículos clase A son de alta gama, los B de prioridad media, y los C de bajo valor pero alto volumen de ventas.
Método PEPS/FIFO	"Primeras entradas, primeras salidas". Prioriza las existencias más antiguas para garantizar productos frescos o evitar deterioros.
Método UEPS/LIFO	"Últimas entradas, primeras salidas". Despacha primero los lotes más recientes, para inventarios de mediano a pequeño tamaño.
Método EOQ	Busca calcular el monto de pedido que minimice los costos de inventario. Funciona con una demanda constante y reabastecimiento inmediato tras agotar el stock.
Conteo cíclico	Conteo periódico del inventario. Puede integrarse con el método ABC asignando distintas frecuencias de conteo para cada clase (A, B, C).
Stock de Seguridad	Mantiene un nivel adicional de productos como reserva para anticipar fluctuaciones de la demanda o retrasos en el suministro.
Seguimiento de Lotes	Organiza productos según la fecha de producción y materias primas utilizadas, permitiendo rastrear procedencia, destino y caducidad.

Método JIT (Just in Time)	Gestiona inventarios para que los productos estén disponibles solo en el momento necesario, reduciendo desperdicios y costos de almacenamiento.
Promedio Ponderado	Calcula el costo promedio de inventarios basado en precios y cantidades de cada lote. Fórmula: $PP = (Precio1 * Unidades1 + Precio2 * Unidades2 + \cdots)/(TotalUnidades))$

Fuente: Elaboración propia

Para el siguiente proyecto se hará uso del promedio ponderado.

2.7. 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 (ISO/IEC, 2023). 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.

Lo cual según la norma:

> 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) (ISO/IEC, 2023, p. 8).

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.

2.7.1. Principios Fundamentales de la ISO/IEC 27001

2.7.1.1. 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).

2.7.1.2. 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 (ISO/IEC, 2023). 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.

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

2.7.2.1. 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 (ISO/IEC, 2023).

2.7.2.2. 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, según la norma,

> 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 (UNE-ISO/IEC, 2023, p. 14).

2.7.2.3. 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). Haciendo así que al 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.

2.7.2.4. 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).

Siendo que 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.

2.7.2.5. Gestión de la información documentada

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

a) 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).

b) 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).

c) 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.

2.7.3. Contexto de la Organización

2.7.3.1. 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 UNE-ISO/IEC (2023), "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" (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 (UNE-ISO/IEC, 2023).

2.7.3.2. 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).

Según la norma “Estos requisitos pueden incluir obligaciones legales, regulatorias, contractuales y de cumplimiento, que deben ser considerados para garantizar la efectividad del SGSI” (UNE-ISO/IEC, 2023, p. 7). Lo cual al 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.

2.7.3.3. 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). Al tener 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.

2.7.4. 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 (UNE-ISO/IEC, 2023). Siendo así que un 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.

2.8. MARCO DE TRABAJO SCRUM

El surgimiento de la agilidad como enfoque en la gestión de proyectos puede entenderse como una respuesta a las limitaciones del modelo en cascada en entornos cada vez más complejos. Durante los años 90, el Reporte CHAOS de 1994 puso de manifiesto las bajas tasas de éxito de los proyectos gestionados bajo metodologías tradicionales, evidenciando la necesidad de enfoques más flexibles y adaptativos. Esto dio lugar a las llamadas Metodologías Livianas, entre las que destacan Extreme Programming (XP),

Scrum, Software Craftmanship y Lean Software Development, las cuales ofrecían alternativas más alineadas con la naturaleza cambiante de los proyectos de software.

En febrero de 2001, un grupo de 17 expertos en desarrollo de software y representantes de estas metodologías livianas se reunió en Utah, Estados Unidos. De esta reunión surgió el Manifiesto por el Desarrollo Ágil de Software, una declaración de valores y principios que transformó la forma de gestionar proyectos de software. Según Alaimo (2021), "el manifiesto no solo dio identidad y unidad a diversas metodologías, sino que también inició un movimiento que continúa evolucionando con el tiempo". Sobre este momento clave, se afirma lo siguiente:

> El Manifiesto para el Desarrollo Ágil de Software, más allá de dar unidad e identidad a una serie de métodos y patrones de práctica, ha determinado el surgimiento de un movimiento. Un movimiento en el que cada uno de quienes nos acercamos a él y nos sentimos cautivados, desde ese preciso momento pasamos a formar parte responsable de cómo los valores, principios y prácticas ágiles se llevan a la realidad de las organizaciones, a la vez que construimos nuevos enfoques, los probamos y mejoramos con vistas al futuro. (Alaimo, 2020, pág. 14).

El Manifiesto Ágil marcó un hito al proponer una alternativa a los procesos rígidos y dominados por la documentación que caracterizaban al desarrollo de software en esa época. Frente a una complejidad que, según DeGrace y Hulet Stahl (1990), consistía en gestionar cambios frecuentes para un número limitado de usuarios, hoy en día las aplicaciones deben adaptarse a millones de usuarios en constante demanda de nuevas

funcionalidades. Esto refleja cómo la complejidad de los años 90 ha escalado a órdenes de magnitud mayores en la actualidad.

Además de establecer valores y principios, el movimiento ágil se caracteriza por su dinamismo y evolución. Alaimo (2021) señala que "el manifiesto sigue tan vigente como en sus inicios, inspirando nuevas prácticas y enfoques que son probados y mejorados constantemente". Esta capacidad de adaptarse a los desafíos del presente asegura que los métodos ágiles sigan siendo relevantes para responder a las demandas del mercado, la tecnología y las organizaciones modernas.

CAPITULO III

MARCO PRACTICO

3.1. SCRUM

3.1.1. Roles Claves en Scrum

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

Tabla 2 Roles de Scrum

Rol	Nombre
Dueño del Producto (Product Owner)	Optica Vision
Responsable del Scrum (Scrum Master)	Maritza Netzy Paiva Zapana
Equipo de Desarrollo (Develoment Team)	Daniel Santiago Soto Villamil

Fuente: Elaboración Propia

3.1.2. Requerimientos

3.1.2.1. Requerimientos funcionales

Tabla 3 Requerimientos Funcionales

ID	Requerimiento	Descripción
RF01	Registro de personal	Permitir registrar datos del personal (nombres, apellidos, email, teléfono, dirección y tipo de persona (Natural o Jurídica)).
RF02	Actualización de personal	Editar información del personal, como datos de contacto y tipo de persona.
RF03	Eliminación lógica de personal	Permitir marcar como inactivo a personal que ya no esté asociado a los procesos del sistema.
RF04	Registro de usuarios	Asociar usuarios al personal existente, con nombre de usuario, contraseña y rol asignado.
RF05	Configuración de autenticación	Permitir el inicio de sesión mediante validación de credenciales seguras.
RF06	Gestión de roles	Crear, editar y eliminar roles, según el cada.

RF08	Registro de proveedores	Registrar nuevos proveedores con datos básicos como nombre, número de contacto y empresa asociada.
RF09	Actualización de proveedores	Editar información de los proveedores existentes.
RF10	Eliminación lógica de proveedores	Permitir marcar como inactivos a los proveedores que ya no suministran productos.
RF11	Registro de productos	Permitir registrar productos con nombre, descripción, stock, precio de compra y precio de venta.
RF12	Actualización de productos	Editar información de productos como precios, descripciones y stock.
RF13	Eliminación lógica de productos	Marcar productos como inactivos para no incluirlos en procesos posteriores.
RF14	Relación de productos con proveedores	Asignar uno o varios proveedores a los productos registrados.
RF15	Registro de trabajos	Registrar trabajos ópticos realizados, como instalación de lentes con detalles técnicos.

RF16	Gestión de parámetros técnicos	Permitir registrar y editar detalles como colores, tratamientos y características ópticas.
RF17	Actualización de trabajos	Editar información de trabajos ya registrados, como costos, detalles técnicos y fechas de entrega.
RF18	Seguimiento de estados de trabajos	Administrar el estado de los trabajos (en proceso, terminado, entregado, etc.).
RF19	Registro de ventas	Capturar detalles de ventas realizadas, incluyendo productos vendidos, cantidades y precios.
RF20	Generación de detalles de ventas	Permitir registrar los servicios ópticos asociados a cada venta, como trabajos personalizados.
RF21	Visualización de historial de ventas	Mostrar un historial detallado de las ventas realizadas, incluyendo sus productos y servicios.
RF22	Visualización en tiempo real	Mostrar datos actualizados en tiempo real, como stock de productos, ventas y estados de trabajos.

Fuente: Elaboración Propia

3.1.2.2. Requerimientos no funcionales

Tabla 4 Requerimientos No Funcionales

ID	Requerimiento	Descripción
RNF01	Tiempo de respuesta	El sistema debe responder rápidamente, asegurando que las acciones de los usuarios no generen retrasos perceptibles.
RNF02	Seguridad básica	Las contraseñas deben guardarse de manera segura para evitar accesos no autorizados.
RNF03	Disponibilidad	El sistema debe estar accesible durante las horas de trabajo habituales de la óptica.
RNF04	Compatibilidad	El sistema debe funcionar en navegadores web.
RNF05	Facilidad de uso	La interfaz debe ser clara y permitir a los usuarios realizar sus tareas de manera sencilla.
RNF06	Validación de datos	Los datos ingresados deben ser revisados automáticamente para evitar errores.
RNF07	Respaldo periódico	Se debe realizar un respaldo del sistema al una vez por mes para proteger la información.

RNF08	Acceso restringido	Cada usuario debe acceder únicamente a la información y funciones relacionadas con su rol.

Fuente: Elaboración Propia.

3.1.3. Pila de Producto (Product Backlog)

Tabla 5 Product Backlog

ID	TAREA	PRIORIDAD	MÓDULO	ESTADO
1	Registrar nuevo personal	Alta	Módulo de Gestión de Personal	Terminado
2	Actualizar datos de personal	Alta	Módulo de Gestión de Personal	Terminado
3	Eliminar lógicamente personal	Media	Módulo de Gestión de Personal	Terminado
4	Registrar nuevos usuarios	Alta	Módulo de Gestión de Usuarios	Terminado
5	Configurar autenticación de usuarios	Alta	Módulo de Gestión de Usuarios	Terminado
6	Administrar roles	Alta	Módulo de Gestión de Usuarios	Terminado

7	Registrar nuevos proveedores	Alta	Módulo de Gestión de Proveedores	Terminado
8	Actualizar datos de proveedores	Media	Módulo de Gestión de Proveedores	Terminado
9	Eliminar lógicamente proveedores	Media	Módulo de Gestión de Proveedores	Terminado
10	Registrar nuevos productos	Alta	Módulo de Gestión de Productos	Terminado
11	Actualizar datos de productos	Alta	Módulo de Gestión de Productos	Terminado
12	Eliminar lógicamente productos	Media	Módulo de Gestión de Productos	Terminado
13	Relacionar productos con proveedores	Media	Módulo de Gestión de Productos	Terminado
14	Registrar ventas	Alta	Módulo de Ventas	Terminado
15	Actualizar detalles de ventas	Media	Módulo de Ventas	Terminado
16	Generar reportes de ventas	Media	Módulo de Reportes	Terminado

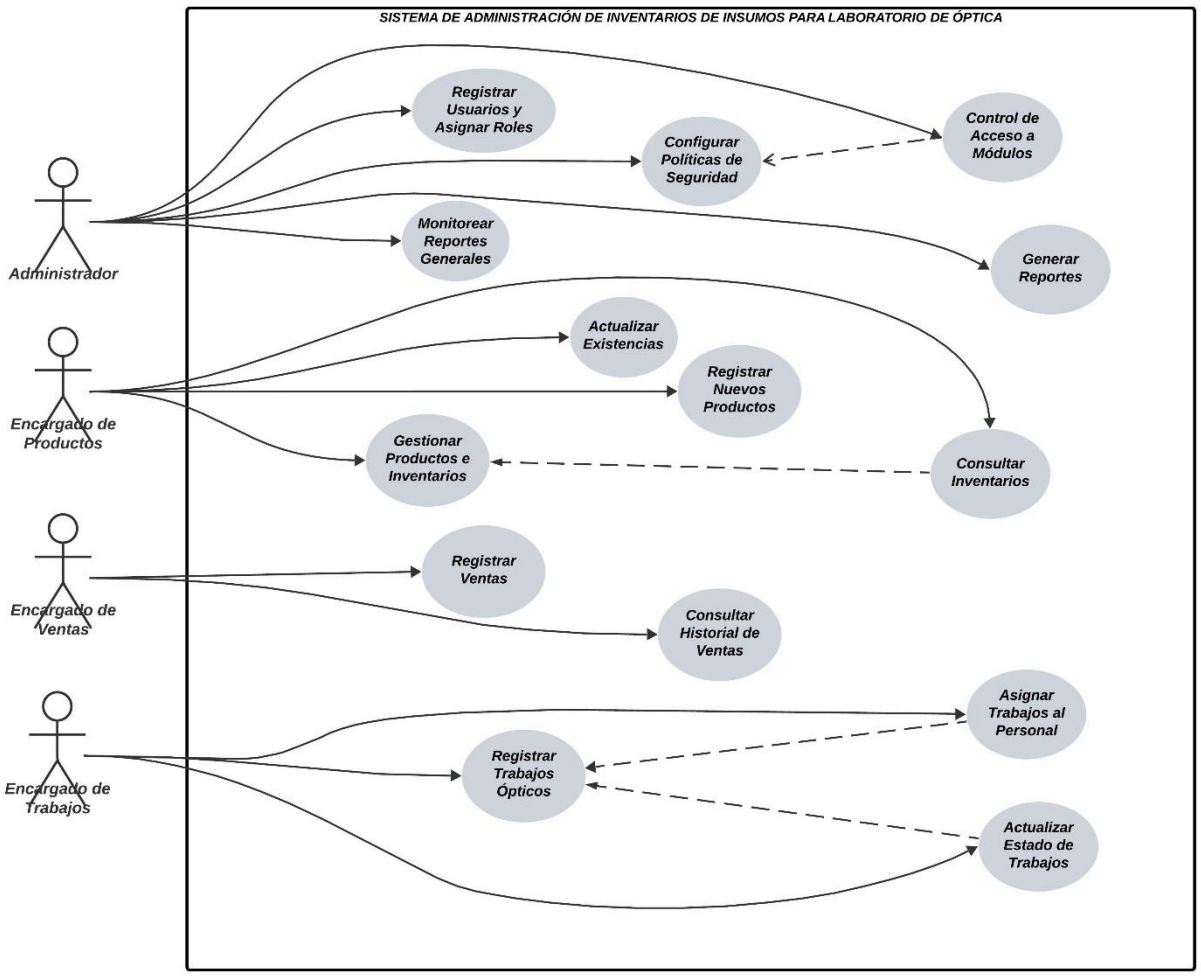
17	Registrar trabajos personalizados	Alta	Módulo de Trabajos	Terminado
18	Actualizar detalles de trabajos	Media	Módulo de Trabajos	Terminado
19	Administrar tratamientos y colores	Media	Módulo de Tratamientos y Colores	Terminado
20	Relacionar tratamientos con productos	Media	Módulo de Tratamientos y Colores	Terminado
21	Registrar ópticas	Media	Módulo de Gestión de Ópticas	Terminado
22	Actualizar detalles de ópticas	Media	Módulo de Gestión de Ópticas	Terminado
23	Visualización en tiempo real de datos	Alta	General	Terminado

Fuente: Elaboración Propia.

3.1.4. Diseño del Sistema

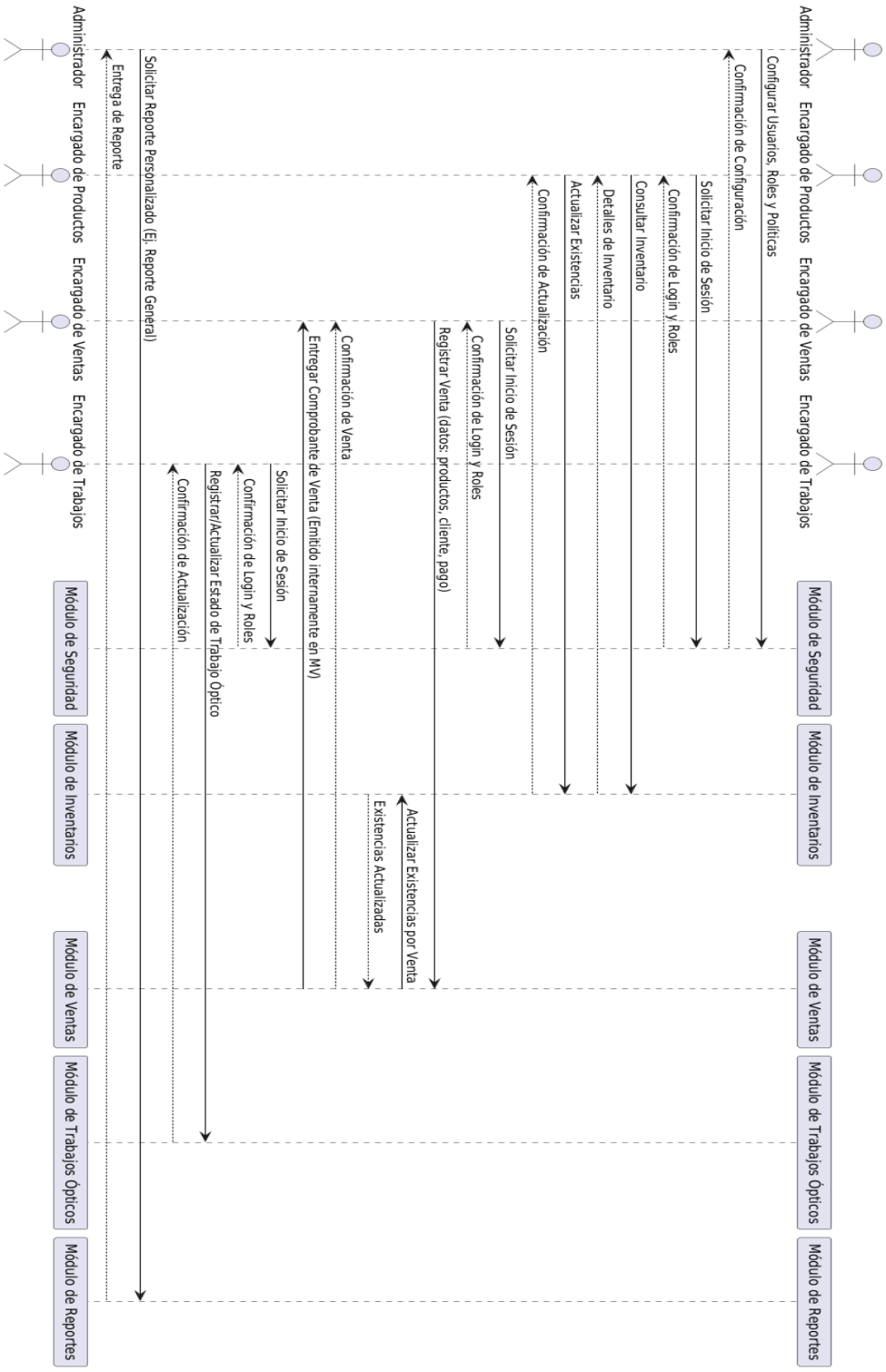
3.1.4.1. Diagrama de casos de uso

Figura 2 Casos de Uso



3.1.4.2. Diagrama de secuencia

Figura 3 Diagrama de Secuencia



3.2. SPRINT DE GESTIÓN DE AUTENTICACIÓN

3.2.1. Objetivos del Sprint

El presente sprint tiene como objetivo desarrollar y validar las funcionalidades esenciales del módulo de gestión de Autenticación, que será la base para controlar los accesos y funcionalidades del sistema. Esto incluye las siguientes metas:

a) Gestión de Roles Predefinidos:

- Implementar la creación inicial de roles predefinidos en el sistema mediante seeding (Inserción de Datos por código).
- Validar que estos roles no sean editables ni eliminables por los usuarios del sistema.

b) Gestión de Usuarios:

- Implementar la lógica para la creación, edición y eliminación de usuarios desde el sistema administrativo.
- Validar que los usuarios puedan ser asignados únicamente a roles predefinidos.
- Garantizar que los usuarios desactivados no tengan acceso al sistema.

c) Validación de Accesos:

- Implementar validaciones que aseguren que cada usuario accede únicamente a las funcionalidades permitidas según su rol asignado.

d) Seguridad en el Proceso de Autenticación:

- Implementar autenticación segura basada en tokens (JWT) y bcrypt para el manejo de contraseñas.

- Configurar restricciones para evitar accesos no autorizados mediante mecanismos de verificación como tokens de acceso con expiración y validaciones estrictas en el inicio de sesión.
- Proteger los puntos de accesos relacionados con roles y usuarios mediante middlewares de autenticación y validación de roles.

3.2.2. Definición de la Gestión de Autenticación

Identificación de las funcionalidades necesarias para el correcto funcionamiento del módulo de Autenticación.

Tabla 6 Requisitos De La Gestión De Autenticación.

REQUISITO	DESCRIPCIÓN
Gestión de roles predefinidos	Implementar roles preexistentes (Administrador, Supervisor, Encargado de Ventas, Encargado de Trabajos) que sean inmutables.
Relación roles-usuarios	Establecer la asociación entre los usuarios y los roles predefinidos para determinar accesos y funcionalidades disponibles.
Validación de accesos	Restringir accesos y funcionalidades según el rol asignado a cada usuario.

Integridad de roles	Asegurar que los roles predefinidos no puedan ser creados, editados ni eliminados desde la interfaz del sistema.
Consistencia en la asignación	Garantizar que los usuarios puedan ser asignados únicamente a roles válidos definidos en el sistema.

Fuente: Elaboración Propia.

3.2.3. Historias del Usuario

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

Tabla 7 Historia De Usuarios De La Gestión De Autenticación.

ID	Historia de Usuario
HU1	El administrador requiere que el sistema disponga de roles predefinidos para garantizar un acceso controlado y seguro a cada módulo.
HU2	El administrador necesita asignar roles a los usuarios para asegurar que cada uno tenga acceso exclusivamente a las funcionalidades correspondientes a su rol.
HU3	Los usuarios deben acceder únicamente a las funcionalidades permitidas según el rol asignado, para evitar acciones no autorizadas.

HU4	El supervisor requiere consultar los roles asignados a los usuarios para verificar que los accesos estén configurados correctamente.

Fuente: Elaboración Propia.

3.2.4. Tareas del Sprint Backlog

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

Tabla 8 Tareas Del Sprint Backlog De Gestión De Autenticación.

ID	TAREA	DESCRIPCIÓN	RESPONSABLE	ESTADO	TIEMPO ESTIMADO
1	Crear roles predefinidos	Implementar la creación de roles fijos mediante seed o código estático.	Daniel Santiago Soto Villamil	Terminado	3 días
2	Asignar roles a usuarios	Desarrollar la lógica para asignar roles a usuarios del sistema.	Daniel Santiago Soto Villamil	Terminado	4 días

3	Validar accesos por roles	Implementar validaciones que restrinjan accesos a funcionalidades según el rol asignado.	Daniel Santiago Soto Villamil	Terminado	4 días
4	Proteger la edición de roles	Asegurar que los roles no puedan ser creados, editados o eliminados desde la interfaz del sistema.	Daniel Santiago Soto Villamil	Terminado	3 días

Fuente: Elaboración Propia.

3.2.5. Desarrollo Iterativo y Validación

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

Tabla 9 Desarrollo Iterativo y Validación de Gestión de Autenticación.

TAREA	PROGRESO	VALIDACIÓN REALIZADA

Crear roles predefinidos	Terminado	Validación de la creación correcta de roles fijos (Administrador, Supervisor, Encargado de Ventas, etc.).
Asignar roles a usuarios	Terminado	Comprobación de que los usuarios tienen asignado el rol adecuado en la base de datos.
Validar accesos por roles	Terminado	Verificación de que los usuarios solo acceden a las funcionalidades permitidas según su rol asignado.
Proteger la edición de roles	Terminado	Validación de que los roles no puedan ser creados, editados o eliminados desde la interfaz del sistema.

Fuente: Elaboración Propia.

3.2.6. Evaluación de Resultados

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

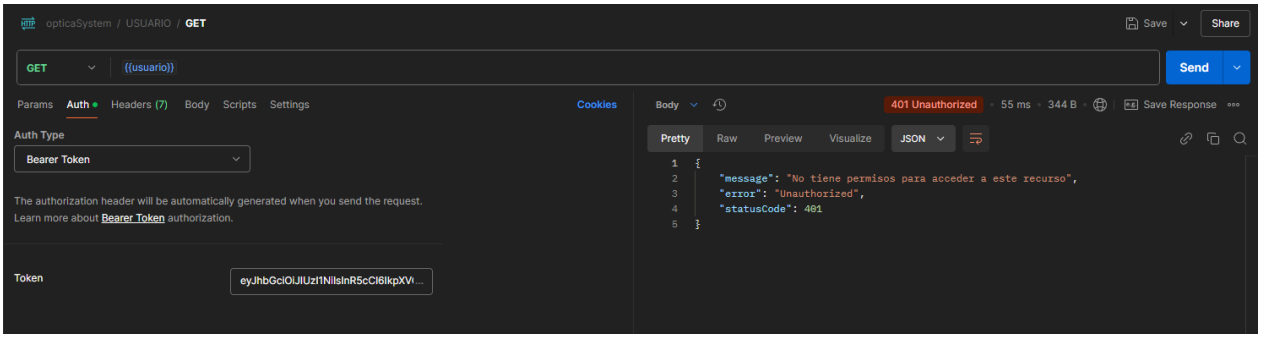
3.2.6.1. Resultados de roles

Tabla 10 Resultados del Módulo de Autenticación.

PRUEBA FUNCIONAL	REGISTRO DE ROLES
Descripción	• Permite verificar la existencia de roles predefinidos.
Objetivos	• Validar que los roles predefinidos existan en la base de datos. • Verificar que los usuarios tienen roles asignados correctamente. • Confirmar que los usuarios acceden únicamente a las funcionalidades permitidas según su rol.
Condiciones	• Los roles deben ser creados inicialmente mediante seeds. • Los roles deben estar correctamente asignados a los usuarios.
Resultado esperado	• Los roles se validan y no presentan conflictos. • Los usuarios acceden a las funcionalidades correspondientes a su rol asignado.
Resultado obtenido	• El sistema valida correctamente los roles predefinidos y su asignación. • El acceso se restringe adecuadamente, cumpliendo con las reglas de roles.

Fuente: Elaboración Propia.

Figura 4 Resultado de Gestión de Roles



3.2.6.2. Resultados de usuarios

Se obtuvieron los siguientes resultados de las pruebas funcionales al módulo de usuarios.

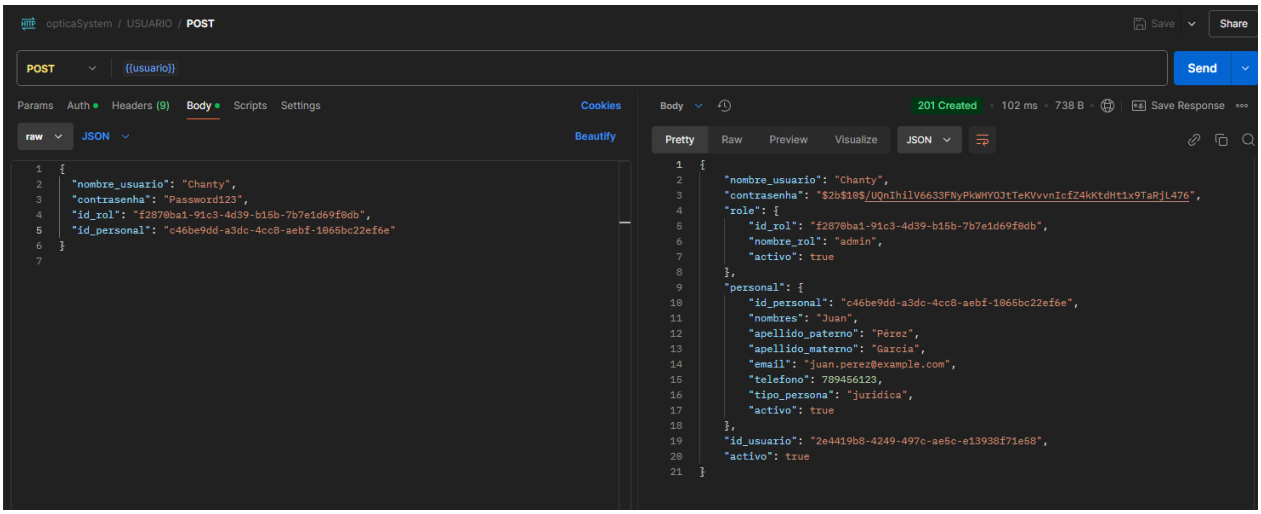
Tabla 11 Resultados del Módulo de Usuarios

PRUEBA FUNCIONAL	REGISTRO DE USUARIOS
Descripción	• Permite el registro de nuevos usuarios mediante un punto de acceso que asocia roles asignados.
Objetivos	• Registrar un nuevo usuario enviando datos válidos a través de la API. • Verificar que los datos del usuario se almacenen correctamente en la base de datos y estén asociados a un rol predefinido.

Condiciones	• Interactuar con el punto de acceso de registro de usuarios con rol de administrador. • La base de datos debe estar activa y funcional.
Resultado esperado	• Al enviar una solicitud válida, el usuario se registra exitosamente en la base de datos, asignándosele un rol predefinido según los parámetros configurados.
Resultado obtenido	• El sistema responde con un código de estado 201 Created y el usuario se registra correctamente en la base de datos, validando los datos únicos y asignando el rol correspondiente.

Fuente: Elaboración Propia.

Figura 5 Resultados de Gestión de Usuarios



3.3. SPRINT DE GESTIÓN PERSONAL

3.3.1. Objetivos del Sprint

El presente sprint tiene como propósito desarrollar y validar las funcionalidades esenciales del módulo de gestión de personal, consolidando las operaciones necesarias para administrar eficientemente los datos de los empleados y garantizar la seguridad en el sistema. Los objetivos específicos incluyen:

a) Registro del personal:

- Implementar la funcionalidad para que el administrador registre datos esenciales, como nombre, correo electrónico, tipo de empleado, y estado (activo/inactivo).
- Vincular automáticamente roles predefinidos al personal al momento de su registro, según el tipo de empleado (por ejemplo, administrador, encargado de ventas, etc.).

b) Actualización y consulta del personal:

- Proporcionar herramientas para que el administrador actualice la información del personal de manera segura, evitando duplicidad o errores en los datos.
- Permitir al administrador y supervisor consultar la información del personal activo e inactivo, con filtros para mejorar la búsqueda y el seguimiento.

c) Control de accesos mediante desactivación lógica:

- Incorporar la funcionalidad para activar o desactivar empleados sin eliminar sus registros de la base de datos, garantizando un control seguro y reversible.

- Asegurar que el personal desactivado no pueda acceder al sistema bajo ninguna circunstancia.

d) Validación de datos:

- La unicidad de los nombres de usuario asociados al personal.
- Verificar que la información del personal esté correctamente asociada en la base de datos, manteniendo una relación clara y sin conflictos

3.3.2. Definición de La Gestión De Personal

Identificación de las funcionalidades necesarias para el correcto funcionamiento del módulo de gestión de personal.

Tabla 12 Requisitos De La Gestión Del Personal

REQUISITO	DESCRIPCIÓN
Registro de personal	Permitir al administrador registrar al personal con datos básicos como nombre, correo, teléfono, tipo de persona y estado activo/inactivo.
Edición de personal	Implementar la funcionalidad para que el administrador actualice los datos del personal registrado, asegurando la integridad de los datos.
Eliminación lógica	Garantizar que el personal pueda ser desactivado sin eliminar los registros del sistema, manteniendo un historial íntegro.

Validación de datos	Asegurar la unicidad de los correos electrónicos y otros datos críticos, evitando duplicados y manteniendo la consistencia en el sistema.
Consulta de personal	Habilitar una funcionalidad para listar y buscar personal registrado, con filtros por estado, tipo de persona y otros criterios relevantes.

Fuente: Elaboración Propia.

3.3.3. Historias del Usuario

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

Tabla 13 Historia De Usuarios De La Gestión De Personal.

D	Historia de Usuario
HU1	El administrador requiere registrar nuevos miembros del personal con datos básicos para mantener un registro organizado y accesible.
HU2	El administrador necesita editar la información de los miembros del personal para garantizar que los datos se mantengan actualizados.
HU3	El administrador solicita desactivar a los miembros del personal que ya no formen parte de la organización, con el objetivo de evitar errores en la gestión.

HU4	El administrador desea consultar una lista del personal registrado con filtros, para facilitar la búsqueda y la clasificación eficiente.

Fuente: Elaboración Propia.

3.3.4. Tareas del Sprint Backlog

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

Tabla 14 Tareas Del Sprint Backlog De Gestión Del Personal.

ID	TAREA	DESCRIPCIÓN	RESPONSABLE	ESTADO	TIEMPO ESTIMADO
1	Registrar personal	Implementar funcionalidad para registrar nuevos miembros del personal.	Daniel Santiago Soto Villamil	Terminado	5 días
2	Editar información del personal	Desarrollar lógica para actualizar los datos personal, asegurando	Daniel Santiago Soto Villamil	Terminado	4 días

		validaciones y consistencia.			
3	Consultar lista del personal	Crear un módulo para consultar el listado de personal registrado, incluyendo filtros.	Daniel Santiago Soto Villamil	Terminado	3 días
4	Desactivar personal	Implementar funcionalidad para cambiar el estado del personal a inactivo sin eliminar su registro del sistema.	Daniel Santiago Soto Villamil	Termin	

Fuente: Elaboración Propia.

3.3.5. Desarrollo Iterativo y Validación

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

Tabla 15 Desarrollo Iterativo y Validación de Gestión del Personal.

TAREA	PROGRESO	VALIDACIÓN REALIZADA
Registrar personal	Completada	Validación de datos únicos (nombre, correo). Verificación de almacenamiento correcto en la base de datos.
Editar información del personal	Completada	Confirmación de actualizaciones en la base de datos con validaciones de integridad.
Consultar lista del personal	Completada	Validación de la correcta visualización del listado con filtros funcionales (estado activo/inactivo).
Desactivar personal	Completada	Comprobación de cambio de estado del personal a inactivo, garantizando la preservación de su registro en el sistema.

Fuente: Elaboración Propia.

3.3.6. Evaluación de Resultados

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

3.3.6.1. Resultados de personal

Se obtuvieron los siguientes resultados de las pruebas funcionales realizadas al módulo de Personal.

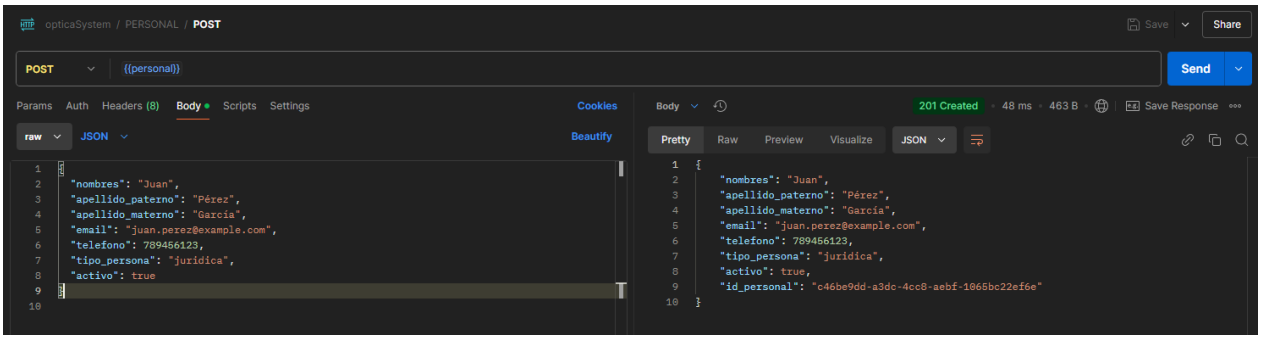
Tabla 16 Resultados del Módulo de Personal.

PRUEBA FUNCIONAL	REGISTRO DE PERSONAL
Descripción	• Permite el registro, actualización y desactivación lógica del personal mediante un punto de acceso.
Objetivos	• Registrar personal con datos válidos (nombres, apellidos, email, teléfono, tipo de persona, etc.). • Actualizar información existente de personal, como datos de contacto o tipo de persona. • Desactivar lógicamente personal que ya no esté en activo.
Condiciones	• La base de datos debe estar activa y funcional. • Los usuarios deben tener rol de administrador para gestionar el personal.
Resultado esperado	• Los datos del personal se registran correctamente en la base de datos, asociados a su tipo de persona. • Desactivación lógica sin eliminar registros del sistema.
Resultado obtenido	• El sistema responde con un código de estado 201 Created para nuevos registros y 200 OK para actualizaciones o desactivaciones.

	• Las desactivaciones lógicas restringen la interacción del personal desactivado en otros módulos del sistema.

Fuente: Elaboración Propia.

Figura 6 Resultados de Gestión Personal



3.4. SPRINT DE GESTIÓN DE PROVEEDORES Y PRODUCTOS

3.4.1. Objetivos del Sprint

El propósito del presente sprint es desarrollar y validar las funcionalidades del módulo de gestión de proveedores y productos. Las metas específicas incluyen:

a) Registro de Proveedores:

- Implementar un sistema para registrar proveedores con datos básicos (nombre, número de contacto, empresa, etc.).

b) Actualización y Desactivación de Proveedores:

- Habilitar la edición de datos existentes y la desactivación lógica de proveedores no activos.

c) Registro de Productos:

- Permitir registrar productos con información relevante (nombre, descripción, stock, precios de compra y venta).

d) Relación entre Productos y Proveedores:

- Configurar la asignación de proveedores específicos a productos registrados, garantizando la trazabilidad.

e) Validación de Datos:

- Asegurar que los datos ingresados sean únicos y consistentes con los requerimientos funcionales establecidos.

3.4.2. Definición de la Gestión de Proveedores y Productos

Identificación de las funcionalidades necesarias para el correcto funcionamiento del módulo.

Tabla 17 Requisitos De La Gestión De Proveedores y Productos.

REQUISITO	DESCRIPCIÓN
Registro de proveedores	Permitir registrar datos básicos de proveedores como nombre, contacto y empresa.
Actualización de proveedores	Modificar información existente de los proveedores registrados.
Desactivación lógica de proveedores	Marcar como inactivos a proveedores que no estén en uso.

Registro de productos	Registrar productos con detalles como nombre, descripción, precios y stock.
Actualización de productos	Editar información de productos ya registrados.
Relación productos-proveedores	Permitir asociar productos a uno o varios proveedores.

Fuente: Elaboración Propia.

3.4.3. Historias del Usuario

Tabla 18 Historia De Usuarios De La Gestión De Proveedores Y Productos.

ID	Historia de Usuario
HU1	El administrador requiere registrar trabajos ópticos con detalles técnicos para organizar y documentar los servicios ofrecidos de manera efectiva.
HU2	El usuario encargado necesita actualizar el estado de los trabajos (pendiente, en proceso, finalizado, entregado) con el fin de llevar un control claro del progreso.
HU3	El administrador solicita asociar productos, tratamientos y colores a los trabajos registrados para garantizar un seguimiento adecuado de los insumos utilizados.

HU4	El administrador requiere asignar trabajos al personal encargado para identificar responsabilidades y distribuir de manera eficiente la carga de trabajo.

Fuente: Elaboración Propia.

3.4.4. Tareas del Sprint Backlog

Tabla 19 Tareas Del Sprint Backlog De Gestión de Proveedores y Productos.

ID	TAREA	DESCRIPCIÓN	RESPONSABLE	ESTADO	TIEMPO ESTIMADO
1	Registrar nuevos proveedores	Crear formulario y lógica para registrar proveedores con datos básicos.	Daniel Santiago Soto Villamil	Terminado	5 días
2	Actualizar datos de proveedores	Implementar lógica para editar información de proveedores ya registrados.	Daniel Santiago Soto Villamil	Terminado	4 días

3	Registrar nuevos productos	Crear formulario y lógica para registrar productos con detalles completos.	Daniel Santiago Soto Villamil	Terminado	6 días
4	Relacionar productos-proveedores	Configurar la lógica para asignar proveedores específicos a productos registrados.	Daniel Santiago Soto Villamil	Terminado	5 días

Fuente: Elaboración Propia.

3.4.5. Desarrollo Iterativo y Validación

Descripción del progreso y validación de las tareas desarrolladas:

Tabla 20 Desarrollo Iterativo y Validación De Gestión de Proveedores Y Productos.

TAREA	PROGRESO	VALIDACIÓN REALIZADA
Registrar nuevos proveedores	Terminado	Validación de datos únicos y almacenamiento correcto en la base de datos.

Actualizar datos de proveedores	Terminado	Confirmar que las actualizaciones no generen duplicados ni errores en los registros.
Registrar nuevos productos	Terminado	Validación de datos ingresados y registro correcto en la base de datos.
Relacionar productos-proveedores	Terminado	Comprobar que la asignación de productos a proveedores se realiza sin conflictos.

Fuente: Elaboración Propia.

3.4.6. Evaluación de Resultados

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

3.4.6.1. Resultados de proveedores

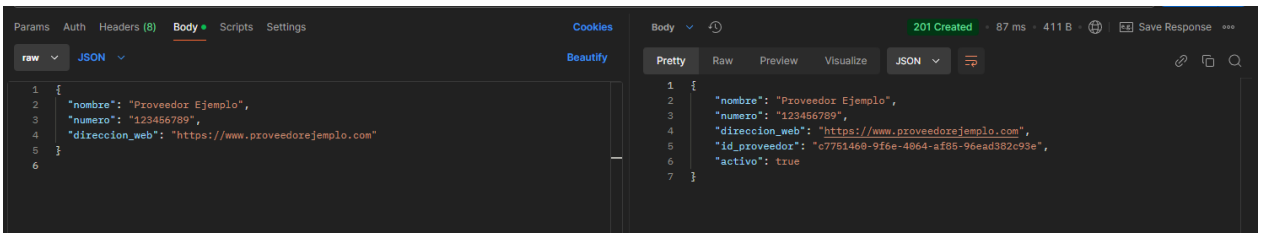
Tabla 21 Resultados del Módulo de Proveedores.

PRUEBA FUNCIONAL	REGISTRO DE PROVEEDORES
Descripción	• Permite el registro, actualización y desactivación lógica de proveedores mediante un punto de acceso.

Objetivos	• Registrar proveedores con datos válidos (nombre, contacto, empresa). • Actualizar información existente de proveedores, como datos de contacto o empresa. • Desactivar lógicamente proveedores que ya no suministran productos.
Condiciones	• La base de datos debe estar activa y funcional. • Los usuarios deben tener rol de administrador para gestionar el personal.
Resultado esperado	• Los datos de los proveedores se registran correctamente en la base de datos, asociados a los productos correspondientes. • Actualización de datos válida sin duplicados. • Desactivación lógica sin eliminar registros del sistema.
Resultado obtenido	• El sistema responde con un código de estado 201 Created para nuevos registros y 200 OK para actualizaciones o desactivaciones. • Los datos únicos del proveedor se validan correctamente. • Las desactivaciones lógicas restringen la interacción de los proveedores desactivados en otros módulos del sistema.

Fuente: Elaboración propia.

Figura 7 Resultados Gestión de Proveedores



3.4.6.2. Resultados de productos

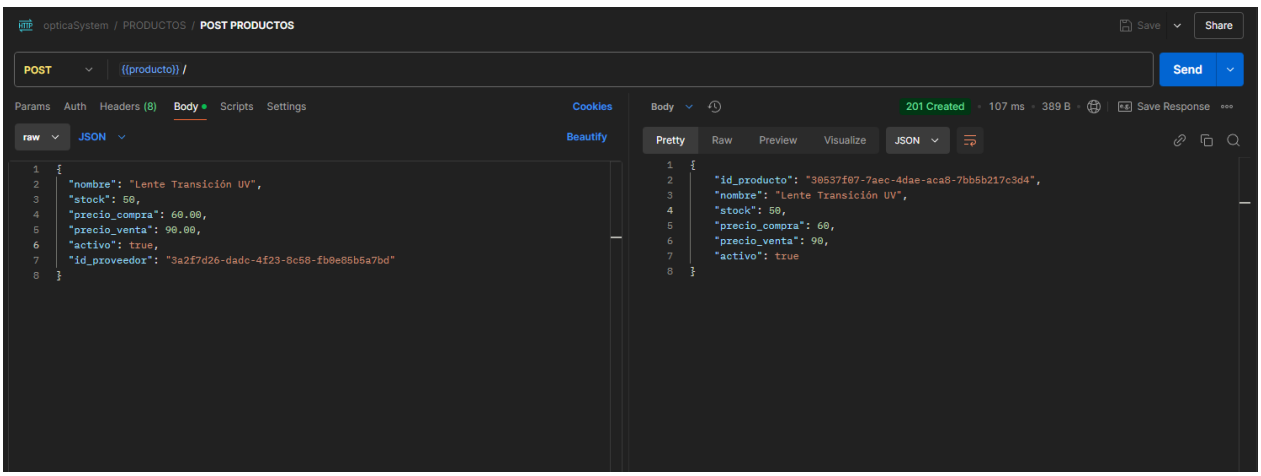
Tabla 22 Resultados del Módulo de Productos.

PRUEBA FUNCIONAL	REGISTRO DE PRODUCTOS
Descripción	• Permite el registro, actualización y desactivación lógica de productos mediante un punto de acceso.
Objetivos	• Registrar productos con datos válidos (nombre, stock, precio de compra y venta). • Actualizar información existente de productos, como precios y stock. • Desactivar lógicamente productos que ya no estén disponibles.
Condiciones	• La base de datos debe estar activa y funcional. • Los usuarios deben tener rol de administrador para gestionar los productos.

Resultado esperado	• Los datos de los productos se registran correctamente en la base de datos, asociados a proveedores cuando corresponda. • Actualización de datos válida sin duplicados. • Desactivación lógica sin eliminar registros del sistema.
Resultado obtenido	• El sistema responde con un código de estado 201 Created para nuevos registros y 200 OK para actualizaciones o desactivaciones. • Los datos únicos de los productos se validan correctamente. • Las desactivaciones lógicas restringen la interacción de los productos desactivados en otros módulos del sistema.

Fuente: Elaboración Propia.

Figura 8 Resultados de Gestión de Productos



3.5. SPRINT DE GESTIÓN DE TRABAJOS

3.5.1. Objetivos del Sprint

a) Registro de trabajos ópticos:

- Implementar funcionalidades para registrar trabajos con detalles técnicos específicos.

b) Gestión de colores:

- Permitir la administración y asociación de colores a los trabajos registrados.

c) Gestión de tratamientos:

- Desarrollar un sistema que permita gestionar los tratamientos ópticos disponibles y asociarlos a trabajos.

d) Gestión de parámetros técnicos:

- Implementar lógica para capturar detalles técnicos (esfera, cilindro, prisma, etc.) en cada trabajo.

e) Actualización de trabajos:

Permitir modificar información existente de trabajos registrados.

f) Seguimiento de estados de trabajos:

- Implementar funcionalidades para cambiar y visualizar el estado de los trabajos (en proceso, finalizado, entregado).

3.5.2. Definición de la Gestión de Trabajos

Tabla 23 Requisitos De La Gestión De Trabajos.

REQUISITO	DESCRIPCIÓN

Registro de trabajos	Permitir registrar trabajos ópticos con detalles técnicos y asignación al personal encargado del trabajo.
Gestión de detalles técnicos	Capturar parámetros técnicos como esfera, cilindro, eje, prisma, base y altura de los trabajos ópticos.
Gestión de colores y tratamientos	Permitir registrar y asociar colores y tratamientos a trabajos específicos, según requerimiento del cliente.
Actualización de trabajos	Editar información existente sobre un trabajo, como parámetros técnicos, costos y fechas.
Seguimiento de estado de trabajos	Administrar y actualizar el estado del trabajo (pendiente, en proceso, finalizado o entregado).
Relación con personal	Asociar trabajos registrados al personal encargado para identificar responsables del proceso.
Relación con productos	Relacionar productos registrados en el sistema a cada trabajo óptico, como insumos o materiales utilizados.

Fuente: Elaboración Propia.

3.5.3. Historias del Usuario

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

Tabla 24 Historia De Usuarios De La Gestión De Trabajos.

ID	Historia de Usuario
HU1	El administrador necesita registrar nuevos proveedores con sus datos básicos con el propósito de gestionar adecuadamente su relación con los productos del inventario.
HU2	El administrador requiere registrar productos con información detallada para garantizar un control preciso y actualizado del inventario.
HU3	El administrador solicita asignar proveedores específicos a los productos registrados, facilitando la trazabilidad y la gestión eficiente del suministro.
HU4	El administrador desea desactivar proveedores que ya no trabajen con la empresa para mantener el sistema organizado y depurado.
ID	Historia de Usuario

Fuente: Elaboración Propia.

3.5.4. Tareas del Sprint Backlog

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

Tabla 25 Tareas Del Sprint Backlog De Gestión de Trabajos.

ID	TAREA	DESCRIPCIÓN	RESPONSABLE	ESTADO	TIEMPO ESTIMADO
1	Registrar trabajos ópticos	Crear formulario y lógica para registrar trabajos ópticos con detalles técnicos completos.	Daniel Santiago Soto Villamil	Terminado	6 días
2	Asignar trabajos al personal	Implementar funcionalidad para asignar trabajos al personal responsable, permitiendo trazabilidad.	Daniel Santiago Soto Villamil	Terminado	4 días
3	Capturar detalles técnicos	Capturar y validar parámetros técnicos como esfera, cilindro,	Daniel Santiago Soto Villamil	Terminado	5 días

		prisma, eje y altura.			
4	Actualización de trabajos	Permitir la edición de detalles técnicos y actualización del estado del trabajo.	Daniel Santiago Soto Villamil	Terminado	5 días
5	Seguimiento del estado de trabajos	Crear funcionalidad para visualizar, filtrar y actualizar el estado de trabajos asignados.	Daniel Santiago Soto Villamil	Terminado	4 días
6	Asociar productos y tratamientos	Implementar relación de productos, colores y tratamientos registrados a cada trabajo óptico.	Daniel Santiago Soto Villamil	Terminado	6 días

Fuente: Elaboración Propia.

3.5.5. Desarrollo Iterativo y Validación

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

Tabla 26 Desarrollo Iterativo y Validación De Gestión de Trabajos.

TAREA	PROGRESO	VALIDACIÓN REALIZADA
Registrar trabajos ópticos	Terminado	Validar almacenamiento de parámetros técnicos y asignación al personal.
Asociar trabajos al personal	Terminado	Verificar la asociación del trabajo con un responsable registrado.
Gestión de detalles técnicos	Terminado	Validar la captura de datos técnicos (cilindro, esfera, etc.).
Actualización de trabajos	Terminado	Confirmar la edición de detalles y actualización del estado del trabajo.
Seguimiento del estado de trabajos	Terminado	Verificar cambios en el estado del trabajo y su visualización.
Asociar productos y tratamientos	Terminado	Validar la relación entre productos registrados y los trabajos ópticos.

Fuente: Elaboración Propia.

3.5.6. Evaluación de Resultados

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

3.5.6.1. Resultados de trabajos.

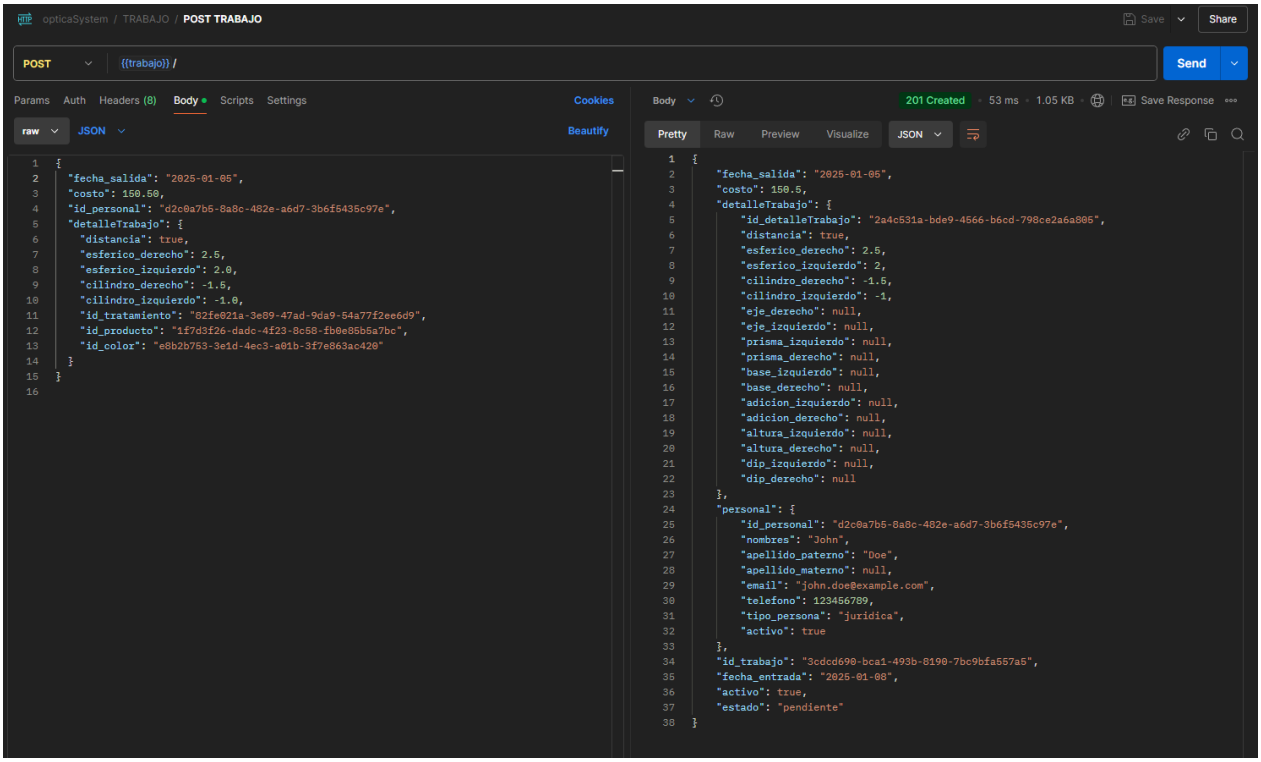
Tabla 27 Resultados del Módulo de Trabajos.

PRUEBA FUNCIONAL	REGISTRO DE TRABAJOS
Descripción	• Permite el registro, actualización y desactivación lógica de trabajos ópticos mediante un punto de acceso.
Objetivos	• Registrar trabajos con detalles técnicos válidos (esfera, cilindro, eje, altura, prisma). • Actualizar información existente de trabajos, como parámetros técnicos, costos o estados. • Desactivar lógicamente trabajos finalizados o no activos, evitando eliminaciones permanentes.
Condiciones	• La base de datos debe estar activa y funcional. • Los usuarios deben tener rol de administrador para gestionar los trabajos.

	• Productos, colores y tratamientos deben estar registrados previamente en el sistema.
Resultado esperado	• Los trabajos se registran correctamente con detalles técnicos y asignación de personal responsable. • Actualización de datos válida, reflejando los nuevos parámetros y costos sin duplicados. • Desactivación lógica que restringe la edición y visualización de trabajos inactivos en otros módulos.
Resultado obtenido	• El sistema responde con un código de estado 201 Created para nuevos registros y 200 OK para actualizaciones o desactivaciones. • Los detalles técnicos del trabajo (esfera, cilindro, prisma, etc.) se almacenan correctamente. • La desactivación lógica funciona correctamente, restringiendo trabajos inactivos en el sistema.

Fuente: Elaboración propia.

Figura 9 Resultados de Gestión de Trabajos



3.6. SPRINT DE GESTIÓN DE VENTAS

3.6.1. Objetivos del Sprint

El presente sprint tiene como objetivo desarrollar y validar las funcionalidades esenciales del módulo de ventas, garantizando un proceso eficiente de registro, gestión y seguimiento de ventas. Las metas específicas incluyen:

a) Registro de ventas:

- Implementar la funcionalidad para registrar ventas con datos esenciales como fecha, monto total y usuario responsable.

b) Detalle de ventas:

- Permitir capturar los detalles de productos y servicios vendidos, incluyendo cantidad, precio unitario y total parcial.

c) Visualización de historial:

- Desarrollar una funcionalidad para visualizar y filtrar el historial de ventas, permitiendo su seguimiento eficiente.

d) Cálculo automático del total:

- Asegurar que el monto total de las ventas se calcule automáticamente según los detalles ingresados.

e) Validación de datos:

- Garantizar la consistencia de la información registrada, evitando duplicados o registros incompletos.

3.6.2. Definición de la Gestión de Ventas

Tabla 28 Requisitos De La Gestión De Ventas**.**

REQUISITO	DESCRIPCIÓN
Registro de ventas	Permitir registrar transacciones de ventas con información básica (fecha, monto total, usuario responsable).
Registro de detalle de ventas	Capturar detalles de los productos y servicios vendidos, como cantidad, precio unitario y total parcial.
Actualización de ventas	Permitir modificar información de ventas, como ajustes en detalles o montos registrados.

Visualización de ventas	Mostrar un historial detallado de ventas registradas, con filtros por fecha y usuario.
Cálculo del monto total	Calcular automáticamente el monto total de la venta con base en los detalles proporcionados.
Asociación de ventas	Relacionar cada venta registrada con el usuario responsable y productos involucrados.

Fuente: Elaboración Propia.

3.6.3. Historias del Usuario

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

Tabla 29 Historia De Usuarios De La Gestión De Ventas.

ID	Historia de Usuario
HU1	El administrador requiere registrar ventas con detalles completos para mantener un control adecuado y preciso de las transacciones realizadas.
HU2	El usuario encargado necesita ingresar los productos y servicios vendidos con el fin de calcular correctamente el monto total de cada venta.

HU3	El administrador solicita visualizar el historial de ventas con el propósito de realizar un seguimiento eficiente de las operaciones y detectar patrones o tendencias.
HU4	El usuario encargado desea modificar una venta registrada para corregir errores en los detalles de la transacción y garantizar la exactitud de la información.
HU5	El administrador requiere filtrar las ventas por fecha y usuario con el objetivo de analizar la información de manera eficiente y facilitar la toma de decisiones.

Fuente: Elaboración Propia.

3.6.4. Tareas del Sprint Backlog

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

Tabla 30 Tareas Del Sprint Backlog De Gestión de Ventas.

ID	TAREA	DESCRIPCIÓN	RESPONSABLE	ESTADO	TIEMPO ESTIMADO
1	Registro de ventas	Crear punto de acceso y lógica para registrar ventas con fecha,	Daniel Santiago Soto Villamil	Terminado	5 días

		usuario y monto total.			
2	Registro de detalle de ventas	Implementar la captura de productos y servicios vendidos, con cantidad y precios.	Daniel Santiago Soto Villamil	Terminado	4 días
3	Cálculo automático del total	Automatizar el cálculo del monto total con base en los productos ingresados.	Daniel Santiago Soto Villamil	Terminado	3 días
4	Actualización de ventas	Permitir la edición de los datos de ventas registradas, como detalles y montos.	Daniel Santiago Soto Villamil	Terminado	4 días
5	Visualización de ventas	Crear funcionalidad para	Daniel Santiago Soto Villamil	Terminado	5 días

		mostrar y filtrar el historial de ventas registradas.			

Fuente: Elaboración Propia.

3.6.5. Desarrollo Iterativo y Validación.

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

Tabla 31 Desarrollo Iterativo y Validación De Ventas.

TAREA	PROGRESO	VALIDACIÓN REALIZADA
Registro de ventas	Terminado	Se verificará el almacenamiento correcto en la base de datos con datos válidos.
Registro de detalle de ventas	Terminado	Se validará la captura correcta de productos y su asociación con la venta registrada.
Cálculo automático del total	Terminado	Se asegurará que el cálculo del total se realice automáticamente sin errores.
Actualización de ventas	Terminado	Se confirmará que las modificaciones se reflejen correctamente en los registros.

Visualización de ventas	Terminado	Se validará la visualización ordenada y el filtrado eficiente de ventas registradas.

Fuente: Elaboración Propia.

3.6.6. Evaluación de Resultados

Análisis de los resultados obtenidos durante el sprint y alineación con los objetivos del módulo.

3.6.6.1. Resultados de ventas

Tabla 32 Resultados del Módulo de Ventas.

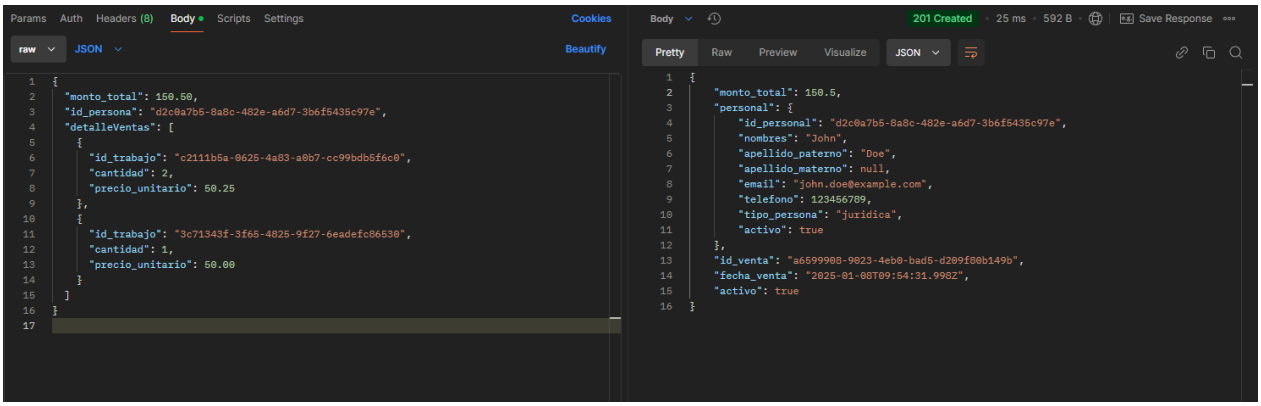
PRUEBA FUNCIONAL	REGISTRO DE PROVEEDORES
Descripción	• Permite el registro, actualización y visualización de ventas, incluyendo detalles como productos, cantidad y total.
Objetivos	• Registrar ventas con información válida (fecha, monto total y usuario responsable). • Capturar detalles de productos vendidos, incluyendo cantidad y precio unitario. • Actualizar registros de ventas existentes. • Visualizar un historial detallado y filtrable de ventas.

Condiciones	• La base de datos debe estar activa y funcional. • El usuario debe tener rol de administrador o encargado de ventas.
Resultado esperado	• Los datos de la venta se registran correctamente en la base de datos, asociados al usuario responsable. • El detalle de productos y servicios vendidos se almacena sin errores. • El monto total de la venta se calcula automáticamente con base en los detalles ingresados. • Las actualizaciones modifican los registros correctamente. • La visualización muestra el historial ordenado y permite filtros por fecha o usuario.
Resultado obtenido	• El sistema responde con un código de estado 201 Created para nuevos registros y 200 OK para actualizaciones. • Los productos y servicios vendidos se registran correctamente en la base de datos, validando los datos únicos. • El monto total se calcula sin errores, sumando correctamente los valores parciales.

	• Las actualizaciones se reflejan en tiempo real sin inconsistencias. • La visualización del historial de ventas es ordenada y funcional, permitiendo filtros eficientes.

Fuente: Elaboración Propia.

Figura 10 Resultado Gestión de Ventas



3.7. SPRINT DE GESTIÓN DE LA ISO 27001

3.7.1. Introducción

El presente sprint se enfoca en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001 y complementado con la Guía de Implementación de Sistemas de Gestión de Seguridad de la Información de NQA (National Quality Assurance). Estas herramientas proporcionarán los lineamientos necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información, mediante un enfoque estructurado que incluye el análisis del contexto organizacional, la planificación estratégica, la aplicación de controles tecnológicos y la

evaluación del rendimiento, adaptados a las necesidades específicas del laboratorio de óptica.

3.7.2. Alcance del Sistema

Para este proyecto, el alcance del Sistema de Gestión de Seguridad de la Información (SGSI) se alineará con la implementación de la norma ISO/IEC 27001, considerando las directrices de la Guía de Implementación de NQA. Este alcance estará centrado exclusivamente en la gestión de la seguridad de la información del laboratorio de una óptica en la ciudad de La Paz, abarcando los procesos relacionados con la administración de inventarios de insumos ópticos, el control de accesos y la protección de datos sensibles.

Dado que la norma es aplicable a organizaciones de cualquier tamaño o sector, este proyecto se adaptará a las características particulares del laboratorio, incluyendo su estructura organizativa y tecnológica. Se garantizará el cumplimiento de las cláusulas de la norma relevantes para este entorno, priorizando los objetivos de confidencialidad, integridad y disponibilidad de la información, como requisito indispensable para la certificación de conformidad.

La implementación considerará las siguientes áreas específicas:

- Procesos de inventario y trazabilidad de insumos.
- Acceso seguro a la información del sistema.
- Protección de datos relacionados con los productos y usuarios.

Con este alcance definido, se asegura una implementación eficaz del SGSI dentro de un marco adaptable a las necesidades y contextos del laboratorio óptico.

3.7.3. Contexto de la Organización

La organización, el Laboratorio de Óptica, opera en un entorno dinámico que requiere atención a factores internos y externos que pueden influir en su capacidad para gestionar de forma efectiva la seguridad de la información.

3.7.3.1. Análisis de factores internos

a) Madurez organizacional: El laboratorio cuenta con procesos manuales de inventario establecidos, pero está en transición hacia un sistema digital.

b) Cultura organizacional: Existe un enfoque regulado en la gestión del inventario, priorizando los datos de productos.

c) Recursos disponibles: El sistema es gestionado por diferentes personas sin un enfoque en específico.

d) Formatos de activos de información: La información se almacena principalmente en formatos físicos como cuadernos de papel.

e) Complejidad del sistema: El laboratorio no utiliza un sistema que centralice la información del inventario, ventas y trabajos.

f) Espacio físico: El laboratorio dispone de instalaciones propias, pero no con un área exclusiva donde se encuentre al almacenamiento de equipos y sistemas.

3.7.3.2. Análisis de factores externos

a) Competencia: Opera en un mercado competitivo y en crecimiento, lo que genera la necesidad de adoptar tecnología para mantenerse actualizado y ofrecer mejores servicios.

b) Reguladores: No existen requisitos regulatorios estrictos específicos para este sector en la región, pero la seguridad de los datos y la satisfacción del cliente son prioritarias.

c) Consideraciones ambientales: Las instalaciones del laboratorio no presentan riesgos significativos relacionados con desastres naturales o factores ambientales.

d) Prevalencia de ataques de seguridad de la información: Aunque el laboratorio no ha sido víctima de ciberataques, la digitalización puede aumentar su exposición a riesgos de seguridad que deben ser mitigados.

3.7.3.3. Identificación de partes interesadas y sus necesidades

a) Propietarios: Esperan un sistema eficiente y confiable que garantice la seguridad de los datos y mejore la gestión operativa del laboratorio.

b) Empleados: Requieren un sistema accesible y fácil de usar que facilite las tareas diarias de gestión del inventario, ventas y trabajos ópticos.

c) Clientes: Desean un servicio ágil y confiable que garantice precisión en los pedidos y entregas.

3.7.4. Liderazgo

3.7.4.1. Política de seguridad de la información

En alineación con la cláusula 5.1 del Anexo A de la ISO 27001, se ha definido una Política de Seguridad de la Información (PSI) para el laboratorio. Esta política ha sido aprobada por la dirección y se actualiza periódicamente en respuesta a cambios significativos en el entorno o los procesos.

La PSI establece un marco para:

- Cumplir con requisitos legales, regulatorios y contractuales.
- Implementar controles clave relacionados con la seguridad de la información, como la gestión de accesos (Anexo A 5.15), la clasificación de la información (Anexo A 5.12) y la gestión de incidentes (Anexo A 5.24-5.27).
- Promover la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

3.7.4.2. Roles, responsabilidades y autoridades

Según el Anexo A 5.2, se han definido roles y responsabilidades claras para garantizar la seguridad de la información:

a) Propietario del laboratorio: Responsable de supervisar el SGSI y asignar recursos adecuados.

b) Administrador del sistema: Coordina la implementación de controles de seguridad, supervisa los accesos y reporta a la alta dirección.

c) Encargado de ven tas: Asegura la confidencialidad de los datos relacionados con clientes y ventas.

d) Encargado de trabajos: Protege los datos técnicos generados en el laboratorio y supervisa su correcta gestión.

3.7.4.3. Evidencia de liderazgo

El liderazgo en la implementación del SGSI recae principalmente en el gestor del proyecto, quien se encarga de diseñar, implementar y supervisar los controles de seguridad necesarios para cumplir con la norma ISO 27001. La dirección del laboratorio apoya la iniciativa al proporcionar los recursos y autorizaciones requeridas para desarrollar el sistema.

Las acciones realizadas incluyen:

- Diseñar y documentar políticas de seguridad alineadas con los objetivos organizacionales.
- Supervisar la implementación de controles, como la segregación de funciones y la protección de activos (Anexos A 5.3 y A 5.12).
- Realizar revisiones internas para garantizar el cumplimiento con los requisitos establecidos en el SGSI.

De esta forma, el liderazgo necesario para el desarrollo e implementación del sistema es proporcionado por el gestor del proyecto, asegurando su alineación con los objetivos del laboratorio.

3.7.4.4. Seguridad en la gestión de proyectos

La seguridad de la información se integra en la gestión de proyectos del laboratorio conforme al Anexo A 5.8, a través de los siguientes enfoques:

a) Evaluación temprana de riesgos: Identificando posibles vulnerabilidades en cada fase del proyecto para implementar controles preventivos.

b) Asignación de responsabilidades claras: Designando roles específicos para la supervisión de la seguridad durante la planificación, ejecución y entrega de cada proyecto.

c) Monitoreo continuo: Verificando el cumplimiento de los controles de seguridad definidos en la política del laboratorio a lo largo del ciclo de vida del proyecto.

d) Gestión de cambios: Implementando procedimientos formales para evaluar y aprobar cualquier modificación en los sistemas o procesos que pueda afectar la seguridad de la información.

Estas medidas aseguran que todos los proyectos se desarrollen bajo un marco que priorice la protección de los activos de información y garantice su alineación con los objetivos del SGSI.

3.7.5. Planificación

La planificación dentro de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001 se centra en identificar riesgos, establecer objetivos de seguridad y definir controles eficaces para mitigarlos. Este proceso es fundamental para

garantizar que las medidas implementadas sean adecuadas, eficaces y alineadas con los objetivos de la organización.

3.7.5.1. Acciones para tratar los riesgos y oportunidades

La organización debe considerar las cuestiones internas y externas identificadas en el contexto de la organización (sección 4) y establecer un plan para tratar los riesgos y oportunidades.

Esto incluye:

a) Identificación de riesgos: Revisar activos, procesos y vulnerabilidades comunes.

b) Evaluación de probabilidad: Calcular la probabilidad de ocurrencia de cada riesgo de forma sistemática.

c) Evaluación del impacto: Analizar las consecuencias económicas, operativas y de seguridad que cada riesgo podría causar.

d) Clasificación y priorización: Clasificar los riesgos según probabilidad e impacto, estableciendo acciones prioritarias.

e) Integración en procesos del SGSI: Incorporar las acciones definidas dentro de los procesos operativos y evaluar su efectividad.

3.7.5.2. Evaluación de riesgos

La evaluación de riesgos debe identificar las amenazas y vulnerabilidades asociadas a los activos de información y las operaciones críticas del SGSI. Este proceso se alinea con los controles definidos en el Anexo A, documentados en la Declaración de Aplicabilidad

(SoA). Los riesgos priorizados deben estar vinculados a los controles seleccionados, asegurando coherencia en el tratamiento y monitoreo. Utilizando el estándar CVSS v4.0, los resultados obtenidos reflejan el nivel de exposición del sistema:

Figura 11 Resultados del CVSS

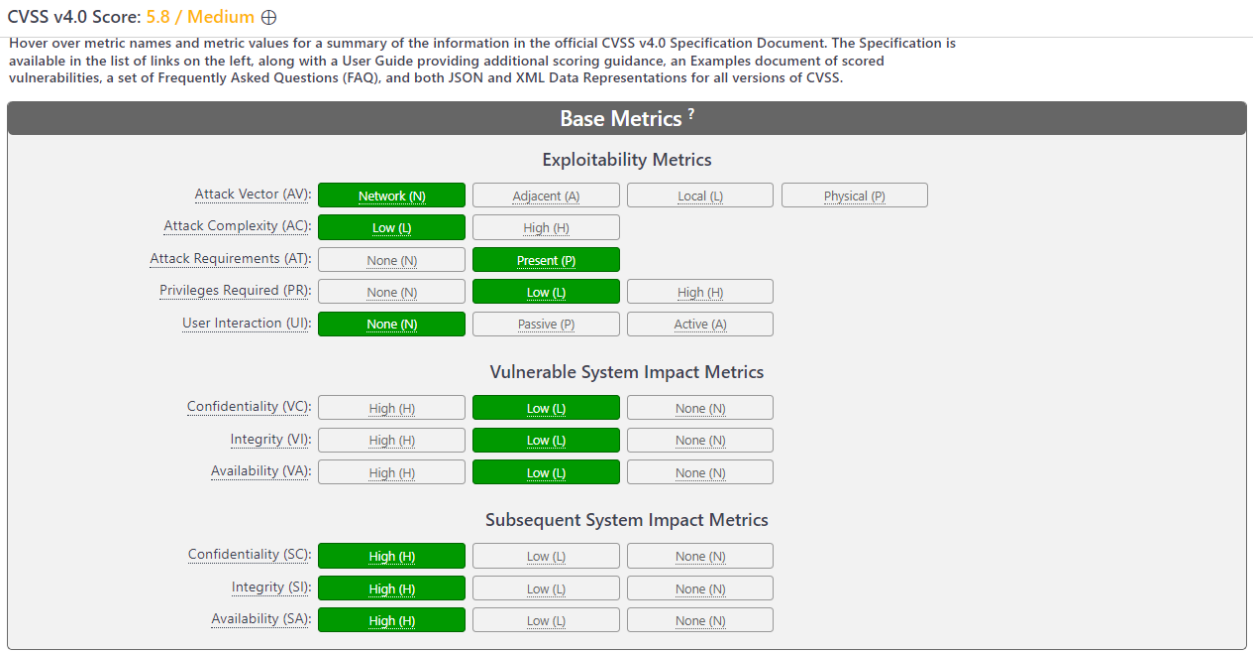


Tabla 33 Explicación y Resultado de las Métricas del CVSS

Métrica Base (CVSS)	Valor Asignado	Descripción
Attack Vector (AV)	Network (N)	El sistema puede ser atacado a través de una red pública o privada.

Attack Complexity (AC)	Low (L)	La explotación del sistema requiere baja complejidad, aunque se aplican medidas de protección.
Privileges Required (PR)	Low (L)	Con permisos bajos, un atacante puede intentar comprometer ciertas funciones.
User Interaction (UI)	None (N)	No es necesaria interacción del usuario para iniciar un ataque.
Confidentiality (VC)	Low (L)	Los datos sensibles están protegidos, pero un ataque exitoso podría comprometerlos.
Integrity (VI)	Low (L)	Existe un riesgo bajo de modificación de datos no autorizada debido a las medidas de seguridad.
Availability (VA)	Low (L)	El impacto en la disponibilidad del sistema se considera bajo.

Fuente: Elaboración Propia.

Resultado Total CVSS: 5.8/10 (Riesgo Medio)

3.7.5.3. Tratamiento de los riesgos

El plan de tratamiento de riesgos incluye la implementación de controles seleccionados para mitigar los riesgos identificados. Los controles están documentados en la Declaración de Aplicabilidad (SoA) junto con las justificaciones de su inclusión o exclusión. Este plan se actualiza periódicamente para reflejar cambios en los riesgos o controles.

El tratamiento incluye:

Tabla 34 Tratamientos de Riesgos

Método de Tratamiento	Descripción
Evitar	Eliminar actividades o procesos que generen riesgos innecesarios.
Eliminar	Modificar sistemas o eliminar vulnerabilidades específicas.
Reducir probabilidad	Implementar controles técnicos y organizativos para reducir las posibilidades de un incidente (ejemplo: autentificación segura).
Reducir consecuencias	Limitar el impacto mediante configuraciones redundantes o backups periódicos.
Transferir	Contratar seguros o delegar la actividad a un proveedor externo.

Aceptar	Documentar los riesgos residuales cuando el costo de mitigación es mayor al impacto potencial.

Fuente: Elaboración Propia.

3.7.5.4. Declaración de Aplicabilidad (SoA)

La Declaración de Aplicabilidad (SoA) es un documento clave del SGSI que identifica los controles aplicables del Anexo A y su relación con los riesgos identificados. Este documento incluye:

a) Controles seleccionados: Identificados en el Anexo A para tratar los riesgos prioritarios.

b) Justificación de inclusión/exclusión: Razones por las cuales un control es aplicable o no.

c) Estado de implementación: Si el control está implementado, en proceso o pendiente.

d) Frecuencia de revisión: El SoA se revisa y actualiza regularmente, al menos una vez al año, o cuando se produzcan cambios significativos en los riesgos o controles.

Tabla 35 Declaración de Aplicabilidad (SoA)

Control	Descripción del Control	¿Aplicable?	¿Implementado?	Justificación
8.5	Autenticación segura. Tecnologías y	Sí	Sí	Implementado para fortalecer

	procedimientos para autenticación segura basados en políticas de acceso.			la autenticación de usuarios en el sistema con JWT y bcrypt.
8.24	Uso de criptografía. Reglas para el uso eficaz de la criptografía y gestión de claves.	Sí	Sí	Implementado para proteger datos sensibles en tránsito y en reposo.
8.16	Seguimiento de actividades. Monitorización de redes, sistemas y aplicaciones para detectar comportamientos anómalos.	Sí	En proceso	Implementación en curso de herramientas de monitoreo de actividad en tiempo real.
8.13	Copias de seguridad de la información. Mantenimiento y	Sí	Sí	Para garantizar la disponibilidad.

	prueba periódica de copias de seguridad.			
8.31	Separación de entornos de desarrollo, prueba y producción.	Sí	Sí	Asegurando la separación lógica de los entornos para minimizar riesgos de contaminación entre ellos.

Fuente: Elaboración Propia.

3.7.5.5. Objetivos de seguridad de la información

Los objetivos están diseñados para ser medibles, coherentes con la política de seguridad y ajustados a las necesidades organizativas:

Tabla 36 Objetivos de la seguridad de la Información

Objetivo	Acción Planificada	Indicador
Garantizar la disponibilidad de los servicios	Implementar redundancia en infraestructura tecnológica.	Disponibilidad > 95%.

Minimizar la pérdida de datos	Realizar backups semanales y pruebas de restauración semestrales.	0 incidentes de pérdida de datos.
Proteger la confidencialidad de la información	Implementar cifrado en los datos almacenados y en tránsito (Anexo A: 8.24 - Uso de criptografía).	> 98% de datos cifrados.

Fuente: Elaboración Propia.

3.7.5.6. Planificación de cambios

La planificación de cambios en el SGSI debe incluir:

- Revisión de riesgos asociados al cambio.
- Actualización de la Declaración de Aplicabilidad (SoA) para reflejar cambios en los controles o su estado de implementación.
- Asignación de recursos necesarios.
- Designación de responsables para cada etapa del cambio.
- Monitoreo de la efectividad tras la implementación.

3.7.6. Operación

La operación de un Sistema de Gestión de Seguridad de la Información (SGSI) requiere la ejecución controlada y documentada de procesos que permitan mitigar riesgos y alcanzar los objetivos de seguridad definidos previamente. La integración de controles

tecnológicos y operacionales garantiza que el SGSI pueda adaptarse a nuevas amenazas, mantener su eficacia y gestionar de forma proactiva los riesgos asociados.

3.7.6.1. Planificación y control operacional

La organización ha planificado e implementado controles alineados con los objetivos establecidos en la sección anterior.

- Establecimiento de criterios para procesos: Los procesos clave incluyen la gestión de usuarios, autenticación segura y monitoreo de actividades.
- Control de cambios planificados: Se establecieron procedimientos para evaluar riesgos y mitigar los impactos negativos de los cambios en el sistema.

3.7.6.2. Evaluación de los riesgos de seguridad de la información

La evaluación de riesgos se realiza de forma continua y documentada. La organización aplica métodos establecidos en la sección anterior para identificar y priorizar amenazas.

Integración del CVSS en la evaluación

La metodología CVSS se aplica para evaluar riesgos de seguridad, permitiendo priorizar vulnerabilidades en función de su impacto. Los resultados obtenidos del CVSS informan decisiones sobre tratamiento y mitigación de riesgos.

Por ejemplo:

a) Autenticación segura (Anexo 8.5): Evaluación periódica del sistema de autenticación con tecnologías como JWT y bcrypt para prevenir ataques de escalamiento de privilegios.

b) Gestión de vulnerabilidades técnicas (Anexo 8.8): Implementación de un sistema continuo para la identificación y tratamiento de vulnerabilidades en el software.

3.7.6.3. Tratamiento de los riesgos de seguridad de la información

El plan de tratamiento de riesgos incluye acciones documentadas y verificables para implementar controles aplicables según el SoA. Entre las actividades clave se encuentran:

a) Autenticación segura (Anexo 8.5): Mantenimiento y revisión de mecanismos de autenticación para usuarios internos y externos.

b) Uso de criptografía (Anexo 8.24): Cifrado de datos en tránsito y reposo para garantizar la confidencialidad.

c) Gestión de vulnerabilidades técnicas (Anexo 8.8): Implementación de herramientas de escaneo de vulnerabilidades con ciclos de evaluación periódica.

La organización evalúa el impacto de estas acciones mediante pruebas de penetración.

3.7.7. Evaluación del Desempeño

3.7.7.1. Seguimiento, medición, análisis y evaluación

La organización lleva a cabo un monitoreo continuo de los procesos y controles del SGSI para garantizar que los objetivos de seguridad se cumplan de manera efectiva. Los

indicadores clave de desempeño (KPIs) son utilizados como métricas para evaluar el estado de la seguridad de la información.

a) Procesos Supervisados

- Autenticaciones: Monitoreo de autenticaciones fallidas y accesos no autorizados.
- Vulnerabilidades: Supervisión de vulnerabilidades detectadas mediante herramientas específicas.
- Actividades Críticas: Revisión de registros de actividades críticas en el sistema.

b) Frecuencia

- Monitoreo diario: Uso de herramientas para detección en tiempo real.
- Revisión mensual: Generación de reportes detallados y análisis de resultados.

3.7.7.2. Indicadores clave (KPIs)

- Tasa de vulnerabilidades mitigadas: Reducción del 20% en vulnerabilidades críticas.
- Disponibilidad del sistema: Superior al 95%.
- Proporción de datos cifrados: Superior al 98%.

3.7.7.3. Tabla de evaluación de controles

Tabla 37 Evaluación de Controles

Control Evaluado	Métrica Evaluada	Frecuencia	Método de Evaluación	Tasa de Éxito (%)

8.5 Autenticación segura	Tasa de autenticaciones fallidas detectadas	20	Revisar logs de intentos de autenticación	80%
8.24 Uso de criptografía	Proporción de datos cifrados	20	Inspección del código y pruebas técnicas	100%
8.16 Seguimiento de actividades	Número de actividades anómalas detectadas	50	Revisar logs de monitoreo	80%
8.13 Copias de seguridad	Éxito en la restauración de backups	Mensual	Pruebas de restauración	60%
8.31 Separación de entornos	Validación de acceso y segregación entre entornos	Semanal	Pruebas funcionales	100%
TOTAL	84%			

Fuente: Elaboración Propia.

CAPITULO IV

ANÁLISIS DE FACTIBILIDAD

4.1. FACTIBILIDAD TÉCNICA

El análisis de factibilidad técnica asegura que el sistema cuenta con los recursos tecnológicos, el hardware, el software, y el equipo necesario para su desarrollo e implementación. A continuación, se presentan los detalles específicos de los recursos disponibles:

4.1.1. Requerimientos Técnicos:

- Servidor en la nube (Vultr) para alojamiento del sistema.
- Conexión a Internet con 35 Mbps de velocidad.
- Herramientas de desarrollo: Node.js, NestJS, Vue.js, PostgreSQL, y TypeORM.
- Herramientas de pruebas: Postman y PlantUML.

4.1.2. Evaluación de Recursos Existentes

Tabla 38 Recursos Existentes

Recurso	Estado Actual	¿Cumple?	Acción Necesaria
Servidor en la nube	Vultr configurado	Sí	Ninguna

Computadora	ASUS i5-13400F, 16 GB RAM	Sí	Ninguna
Software	Node.js, NestJS, Postman	Sí	Ninguna
Conexión a Internet	AXS, 35 Mbps	Sí	Ninguna
Personal	2 miembros capacitados	Sí	Capacitación continua en ISO 27001

Fuente: Elaboración Propia.

4.1.3. Conclusión Técnica

El proyecto es viable con los recursos actuales y algunas capacitaciones adicionales.

4.2. ANÁLISIS DE FACTIBILIDAD OPERATIVA

Evalúa la capacidad operativa para adoptar y utilizar el sistema de gestión de inventarios. Incluye aspectos humanos, procesos organizativos y aceptación por parte de los usuarios.

4.2.1. Evaluación Operativa

Tabla 39 Aspectos de la Evaluación Operativa

Aspecto	Análisis	Estado

Resistencia al cambio	Personal comprometido con la mejora continua	Favorable
Capacitación requerida	20 horas sobre ISO 27001 y uso del sistema	Manejable
Procesos afectados	Documentación actualizada	Favorable
Tiempo de adaptación	1 mes estimado	Aceptable
Soporte post-implementación	Garantizado por equipo interno	Favorable

Fuente: Elaboración Propia.

4.2.2. Conclusión Operativa

Operativamente factible con un plan de capacitación y acompañamiento inicial.

4.3. ANÁLISIS DE FACTIBILIDAD ECONÓMICA

Determina la viabilidad económica del proyecto considerando costos iniciales, costos operativos y beneficios esperados.

4.3.1. Presupuesto Inicial

Tabla 40 Presupuesto Inicial

Componente	Costo (USD)

Servidor Vultr	$600 (6 meses)
Licencias necesarias	$300
Capacitación del personal	$500
Desarrollo e implementación	$2,500
Contingencia (10%)	$390
Total	$4,290

Fuente: Elaboración Propia.

4.3.2. Costos operativos Anuales

Tabla 41 Costos Operativos Anuales

Concepto	Costo Anual (USD)
Mantenimiento	$500
Renovación de licencias	$200
Soporte técnico	$800
Total	$1,500

Fuente: Elaboración Propia.

4.4. ANÁLISIS COSTO-BENEFICIO

4.4.1. Beneficios Cuantificables (Anuales):

Tabla 42 Beneficios Anuales

Beneficio	Valor (USD)
Reducción de errores de inventario	$1,200
Optimización de tiempo en procesos	$1,000
Mejora en la seguridad de los datos	$800
Ahorros por auditorías externas	$500
Total Beneficios Anuales	$3,500

Fuente: Elaboración Propia.

4.4.2. Cálculo ROI

ROI a 3 años:

$$ROI = \frac{Beneficios\ Totales - Costos\ Totales}{Costos\ Totales} * 100$$

Beneficios Totales (3 años): $3,500 × 3 = $10,500

Costos Totales (3 años): $4,290 + ($1,500 × 3) = $8,790

$$ROI = \frac{16{,}500\ - 8{,}790}{Costos\ Totales} * \ 100 = 19.5\%$$

4.4.3. Período de Recuperación

$$Periodo\ de\ Recuperacion = \frac{\text{Inversión Inicial}}{Beneficio\ Neto\ Anual}$$

Inversión Inicial: $4,290

Beneficio Neto Anual: $3,500 - $1,500 = $2,000

$$Periodo\ de\ Recuperacion = \frac{4{,}290}{2{,}000} = 2.145\ años\ (25.7\ meses)$$

4.4.4. Conclusión

El proyecto sigue siendo económicamente viable, pero con un ROI moderado del 19.5% en un período de 3 años. El período de recuperación es de 2.14 años, lo que representa una inversión a mediano plazo, adecuada para organizaciones con necesidades específicas en la seguridad y manejo de inventarios.

4.5. COCOMO 2

4.5.1. Estudio de costos

Los costos son los cálculos estimados de los recursos que se quiere en el sistema y tiene relación directa e indirecta con el proceso productivo en sus diferentes etapas (estudio, análisis, ejecución y administración).

4.5.2. Estimación el costo para el desarrollo

Para obtener la estimación del costo para el desarrollo del sistema, se utiliza el Método

por Puntos de Objeto.

4.5.3. Recuento de Función

Tabla 43 Recuento de Función

Objeto	Básico	Medio	Avanzado
Pantallas	4	2	1
Informes	1	3	0
Módulos de Seguridad	0	1	2

Fuente: Elaboración Propia.

4.5.3.1. Determinar puntos función

A continuación, se realiza el cálculo de puntos función con los datos obtenidos

mediante la siguiente ecuación:

$$PF = \Sigma(pantallas * peso\ de\ complejidad) + \Sigma(informes * peso\ de\ complejidad)$$

Tabla 44 Factores de Peso de la Complejidad para Tipos de Objeto

Objeto	Básico	Medio	Avanzado
Pantallas	5	10	15
Informes	4	8	12

Módulos de Seguridad	6	12	20

Fuente: Elaboración Propia.

Donde entendemos que:

PF = Puntos Funcion.

El símbolo (*) se considera el factor multiplicador de cada celda en el cual refleja el esfuerzo relativo requerido para implementar un tipo de objeto con un nivel de complejidad dado.

Se tiene un total de 78 puntos de función, definiendo los aspectos de escalas de software como nominales y los costos de software como nominales de la misma forma, se utiliza el software COCOMO II (Constructive Cost Model), se tienen los siguientes resultados:

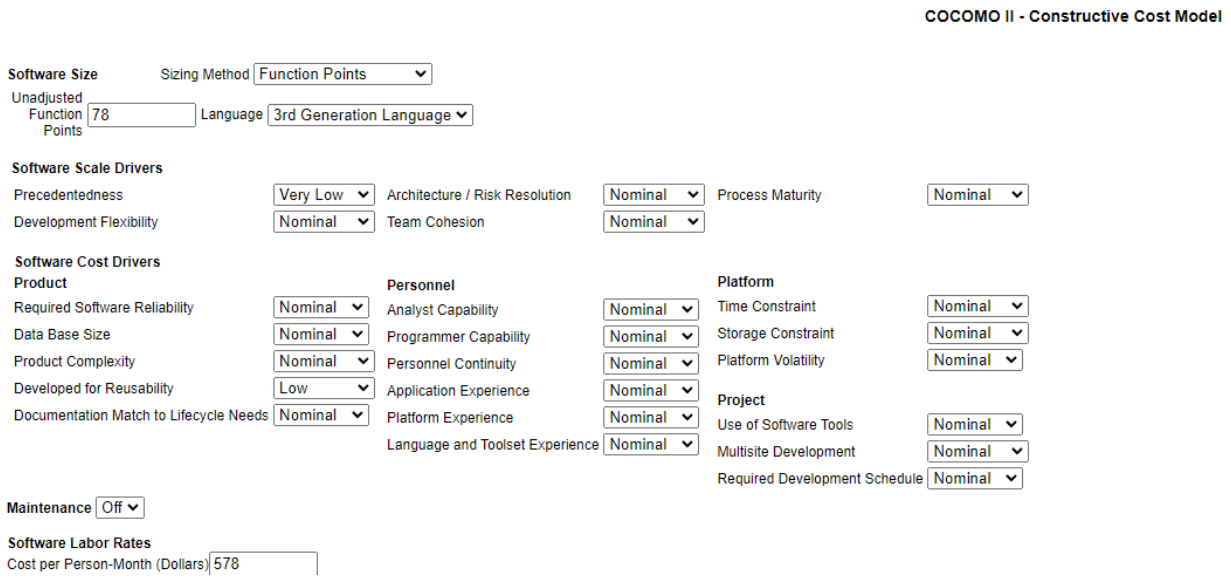
4.6. COSTO TOTAL

CT = (Costo estimado por COCOMO II) + CTH + CTS + CTO

CT = 12,984 $ + 1,485 $ + 1,080.56 $ + 1,217 $

CT = 16,766.56 USD

Figura 12 Calculo COCOMO II



- El software no considera costos de mantenimiento
- El software contempla costos de soporte al momento de desplegar el sistema.
- Se utilizó el valor del salario promedio de un ing. de sistemas junior en Bolivia para la gestión 2025 que corresponde a 4000 bs. Para realizar el cálculo y su equivalencia a 575 en dólares americanos. Con tipo de cambio a 6.96 Bs, por dólar americano.

Para aproximar el costo total de producción del software, se realiza los siguientes cálculos:

Figura 13 Resultados obtenidos del COCOMO II

Results

Software Development (Elaboration and Construction) Staffing Profile

Effort = 22.6 Person-months
Schedule = 10.0 Months
Cost = $12984

Total Equivalent Size = 6240 SLOC
Effort Adjustment Factor (EAF) = 0.98

Acquisition Phase Distribution

Phase	Effort (Person-months)	Schedule (Months)	Average Staff	Cost (Dollars)
Inception	1.4	1.3	1.1	$779
Elaboration	5.4	3.8	1.4	$3116
Construction	17.2	6.3	2.7	$9868
Transition	2.7	1.3	2.2	$1558

Software Effort Distribution for RUP/MBASE (Person-Months)

Phase/Activity	Inception	Elaboration	Construction	Transition
Management	0.2	0.7	1.7	0.4
Environment/CM	0.1	0.4	0.9	0.1
Requirements	0.5	1.0	1.4	0.1
Design	0.3	2.0	2.7	0.1
Implementation	0.1	0.7	5.8	0.5
Assessment	0.1	0.5	4.1	0.7
Deployment	0.0	0.2	0.5	0.8

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

En conclusión, se logró desarrollar un sistema integral para la administración y gestión de inventarios en la Óptica Visión, cumpliendo con los estándares de seguridad establecidos en la normativa ISO/IEC 27001. Este sistema proporciona un control eficiente de los inventarios, garantizando la protección de la confidencialidad, integridad y disponibilidad de la información. De igual manera, se lograron los siguientes objetivos:

5.1.1. Cumplimiento de Objetivos

El proyecto cumplió con los objetivos propuestos al implementar un sistema de gestión de inventarios para Óptica Visión basado en las normas ISO 27001 e ISO 27002. Esto asegura un manejo eficiente y seguro de los datos sensibles, como el inventario y la información de los proveedores, garantizando la confidencialidad, integridad y disponibilidad de la información.

5.1.2. Integración y Eficiencia

La integración de herramientas tecnológicas modernas como Nest.js, TypeORM y Vue.js, combinadas con la base de datos PostgreSQL, permitió desarrollar un sistema robusto y escalable, optimizando los tiempos de operación y minimizando los errores manuales.

5.1.3. Gestión de Seguridad

La implementación de controles tecnológicos definidos en el SoA asegura un tratamiento adecuado de los riesgos. Además, las pruebas realizadas demuestran que los niveles de seguridad implementados cumplen con los estándares propuestos, reduciendo significativamente las vulnerabilidades críticas.

5.1.4. Metodología Ágil

El uso de la metodología Scrum permitió un desarrollo organizado, con entregas incrementales que garantizaron la retroalimentación constante y ajustes oportunos en el desarrollo del proyecto.

5.1.5. Factibilidad del Sistema

A través del análisis de factibilidad técnica, económica y operativa, se concluyó que el sistema es viable, rentable y adecuado para su implementación, con un retorno de inversión favorable en los años siguientes.

5.2. RECOMENDACIONES

Como resultado del presente proyecto, se sugieren algunas recomendaciones que

pueden ser llevadas a cabo en futuros trabajos, los cuales son:

5.2.1. Mejoras en Reportes de Inventarios

Se sugiere implementar reportes avanzados que permitan filtrar por periodos personalizados y categorizar productos según movimientos recientes o históricos.

Actualmente, el sistema ofrece reportes básicos que cumplen con los requisitos funcionales iniciales, pero estas mejoras no fueron incluidas debido a la prioridad de garantizar la funcionalidad esencial antes de abordar características adicionales.

5.2.2. Gestión Detallada de Usuarios

Una funcionalidad futura podría incluir la posibilidad de establecer permisos a nivel de acciones específicas dentro del sistema (por ejemplo, permitir que ciertos usuarios visualicen, pero no editen datos). Esto no se incorporó en esta fase debido a que los roles y permisos actuales fueron diseñados de acuerdo con los requerimientos específicos del cliente, priorizando simplicidad y rapidez en la implementación.

5.2.3. Ampliación de Controles de Auditoría

Aunque el sistema ya registra las acciones principales realizadas por los usuarios, se podría incluir un módulo de auditoría más detallado que registre eventos específicos como intentos fallidos de inicio de sesión o modificaciones en configuraciones críticas. No se implementó en esta etapa debido a que el enfoque principal fue cumplir con los controles básicos de seguridad establecidos en las normativas ISO.

5.2.4. Exportación Personalizada de Datos

Actualmente, el sistema permite exportar datos en formatos predefinidos. Se recomienda en una fase futura incorporar opciones de personalización para que los usuarios puedan seleccionar columnas y formatos específicos. Esto no se incluyó porque las opciones existentes son suficientes para cumplir con los requerimientos actuales de la empresa.

5.2.5. Mejoras en la Visualización de Inventarios

Se puede considerar agregar gráficos dinámicos que resuman el estado del inventario en tiempo real. Aunque esto aportaría valor, no se priorizó en esta fase para garantizar que los recursos se destinaran a funcionalidades operativas críticas.

5.2.6. Respaldo Automático de Datos

Una mejora futura podría incluir la automatización completa de las copias de seguridad para que se realicen en intervalos más frecuentes o en base a eventos específicos. Actualmente, el sistema permite realizar respaldos mensuales, lo cual fue considerado suficiente para cumplir con los requisitos mínimos de seguridad

REFERENCIAS BIBLIOGRÁFICAS

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.

Alaimo, M. (2021). *Scrum y algo más.*

Carreón, A. (2020). dev: https://dev.to/alfredocu/tailwind-css-spanish-4lk4

Gibert, M. (2007). *Bases de datos en PostgreSQL.* https://doi.org/https://dgvs.mspbs.gov.py/files/documentos/06_06_2016_20_09_46_P06_M2109_02152.pdf

Gonzales, E. (2023). *cimatic*. https://cimatic.com.mx/blog/todo-lo-que-debes-conocer-de-sistema-de-inventarios/

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

miro. (2023). https://miro.com/es/diagrama/que-es-diagrama-ishikawa/

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/

Red Hat. (2023). *redhat*. https://www.redhat.com/es/topics/api/what-is-a-rest-api#%C2%BFqu%C3%A9-es-una-api-de-rest

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

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

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

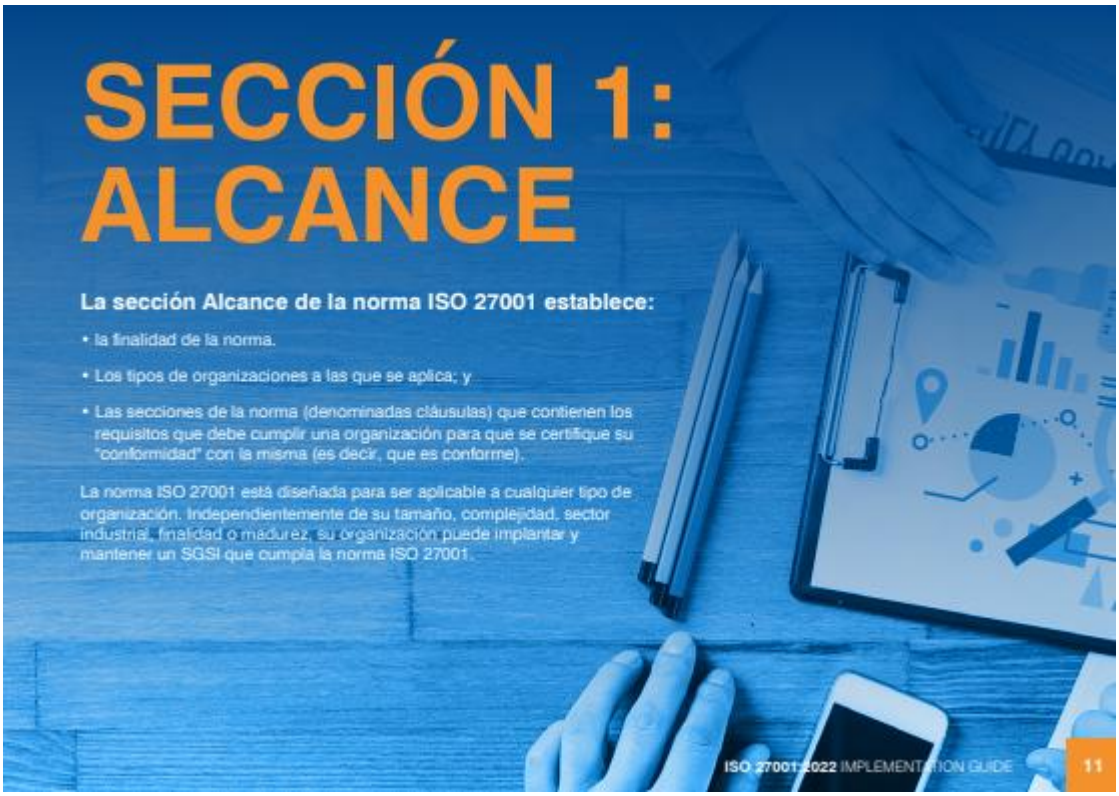
UNE-ISO/IEC. (2023). *Tecnología de la información - Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información.*

Vue.js Team. (s.f.). *vuejs*. https://es.vuejs.org/v2/guide/

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

ANEXOS

Anexo 1: Alcance ISO 27001



Anexo 2: Contexto de la Organización ISO 27001

SECCIÓN 4: CONTEXTO DE LA ORGANIZACIÓN

El propósito de su SGSI es proteger los Activos de Información de su organización, para que pueda alcanzar sus objetivos.

La forma de hacerlo y las áreas específicas de prioridad dependerán del contexto en el que opere su organización. organización:

- Internamente: las cosas sobre las que la organización tiene cierto control.
- Externamente: las cosas que la organización no controla directamente.

Un análisis cuidadoso del entorno en el que opera su organización es fundamental para identificar los riesgos inherentes a la seguridad de sus activos de información. El análisis es la base que le permitirá evaluar qué procesos debe considerar añadir o reforzar para construir un SGSI eficaz.

Contexto interno

Los siguientes son ejemplos de las áreas que pueden tenerse en cuenta al evaluar las cuestiones internas que pueden influir en los riesgos del SGSI:

- Madurez: ¿Es una empresa ágil con un lienzo en blanco en el que trabajar, o una institución con procesos y controles de seguridad establecidos?
- Cultura organizativa: ¿Es su organización relajada en cuanto a cómo, cuándo y dónde trabaja la gente, o extremadamente reglamentada?
- Gestión: ¿Existen canales y procesos de comunicación claros entre los principales responsables de la toma de decisiones y el resto de la organización?
- Tamaño de los recursos: ¿Trabaja con un equipo de seguridad de la información o lo hace todo una persona?
- Madurez de los recursos: ¿Los recursos disponibles están informados, plenamente formados, son fiables y constantes, o el personal carece de experiencia y cambia constantemente?
- Formatos de los activos de información: ¿Sus activos de información se almacenan principalmente en formato impreso o electrónicamente en un servidor o en sistemas remotos basados en la nube?
- Sensibilidad/valor de los activos de información: ¿Su organización tiene que gestionar activos de información muy valiosos?
- Coherencia: ¿Dispone de procesos uniformes en toda la organización o de una multitud de prácticas operativas diferentes con poca coherencia?
- Sistemas: ¿Tiene su organización muchos sistemas que funcionan con versiones de software que ya no son compatibles con el fabricante, o mantiene la tecnología más actualizada y mejor disponible?
- Complejidad del sistema: ¿Utiliza un sistema principal que hace todo el trabajo pesado, o varios sistemas departamentales con una transferencia de información limitada entre ellos?
- Espacio físico: ¿Disponen de una oficina propia y segura, o trabajan en un espacio compartido con otras organizaciones, o son una organización exclusivamente remota?

Contexto externo

Los siguientes son ejemplos de las áreas que pueden tenerse en cuenta al evaluar las cuestiones externas que pueden influir en los riesgos del SGSI:

- La competencia: ¿Opera en un mercado innovador y en evolución, que requiere actualizaciones de los sistemas para seguir siendo competitivo, o en un mercado maduro y estable con pocas innovaciones?
- Propietario: ¿Necesita aprobación para mejorar la seguridad física?
- Reguladores: ¿Existe en su sector la obligación de realizar cambios reglamentarios con regularidad, o hay poca supervisión por parte de los organismos reguladores?
- Económico/político: ¿Influyen las fluctuaciones monetarias en su organización? ¿Cómo afectan las situaciones geopolíticas a su organización?
- Consideraciones ambientales: ¿Están sus instalaciones en una llanura inundable y los servidores en un sótano? ¿Existen factores que hagan de sus instalaciones un posible objetivo de robo o atentado terrorista (por ejemplo, en un lugar céntrico o cerca de un posible objetivo)?
- Prevalencia de los ataques a la seguridad de la información: ¿Su organización opera en un sector que sufre ciberataques?
- Accionistas: ¿Están muy preocupados por la vulnerabilidad de la organización a las violaciones de datos? ¿Hasta qué punto les preocupa el coste de los esfuerzos de la organización por mejorar su seguridad de la información?

Partes interesadas

Una parte interesada es cualquiera que esté, pueda estar o se perciba afectado por una acción u omisión de su organización. Las partes interesadas se irán aclarando a lo largo del proceso de análisis exhaustivo de los problemas internos y externos.

Probablemente incluirá a accionistas, propietarios, reguladores, clientes, empleados y competidores. Dependiendo de su empresa, pueden incluir al público en general y al medio ambiente. No tiene que intentar comprender o satisfacer todos sus caprichos, pero sí determinar cuáles de sus necesidades y expectativas son relevantes para su SGSI.

Alcance del SGSI

Para cumplir con la norma ISO 27001, debe documentar el alcance de su SGSI. Los alcances documentados suelen describir:

- Los límites del lugar o lugares físicos incluidos (o no incluidos).
- Los límites de las redes físicas y lógicas incluidas (o no incluidas).
- Los grupos de empleados internos y externos incluidos (o no incluidos)
- Los procesos, actividades o servicios internos y externos incluidos (o no incluidos).
- Interfaces clave en los límites del ámbito de aplicación.

Si quiere priorizar recursos creando un SGSI que no cubra toda su organización, seleccionar un ámbito limitado a la gestión de los intereses de las partes interesadas clave es un enfoque pragmático. Esto se puede hacer incluyendo sólo sitios, activos, procesos y unidades de negocio o departamentos específicos. Algunos ejemplos son:

- **"Todas las operaciones realizadas por el Dpto. IT."**
- **"Soporte y gestión del correo electrónico".**
- **"Todos los equipos, sistemas, datos e infraestructuras del centro de datos de la organización, situado en la sede de Basingstoke".**

CONSEJO: Documente o mantenga un archivo de toda la información recopilada en el análisis del contexto de su organización y de las partes interesadas, como por ejemplo

- Conversaciones con un alto representante de la organización, por ejemplo, un director general, CFO, CTO...
- Actas de reuniones o planes de negocio.
- Un documento específico que identifica los problemas internos/externos y las partes interesadas, así como sus necesidades y expectativas; por ejemplo, un análisis DAFO, un estudio PESTLE o una evaluación de riesgos empresariales de alto nivel.

Nueva consideración para el cambio climático

ISO ha introducido cambios en la norma ISO 27001 para subrayar la importancia de abordar los efectos del cambio climático en el marco de los sistemas de gestión de las organizaciones.

Para mejorar la concienciación y la respuesta de las organizaciones al cambio climático, ISO ha introducido dos cambios fundamentales en la cláusula 4:

Cláusula original 4.1:
"Comprensión de la organización y su contexto. La organización debe determinar las cuestiones externas e internas que son relevantes para su propósito y que afectan a su capacidad para lograr el resultado o resultados previstos de su sistema de gestión de XXX."

Esta cláusula incluye ahora explícitamente la afirmación "La organización determinará si el cambio climático es una cuestión relevante".

Cláusula original 4.2:
"Comprender las necesidades y expectativas de las partes interesadas. La organización debe determinar:

- Las partes interesadas que son relevantes para el sistema de gestión XXX.
- Los requisitos pertinentes de estas partes interesadas.
- Cuáles de estos requisitos se abordarán a través del sistema de gestión XXX".

La cláusula ahora también dice: "Nota: Las partes interesadas pertinentes pueden tener requisitos relacionados con el cambio climático".

Anexo 3: Liderazgo ISO 27001

SECCIÓN 5: LIDERAZGO

La importancia del liderazgo

El liderazgo en este contexto significa la participación en el establecimiento de la dirección del SGSI, su aplicación y provisión de recursos. Esto incluye:

- Garantizar que los objetivos del SGSI sean claros y estén alineados con la estrategia general.
- Claridad en las responsabilidades y la rendición de cuentas.
- El pensamiento basado en el riesgo está en el centro de toda toma de decisiones
- Comunicación clara de esta información a todas las personas dentro del ámbito de su SGSI.

La norma ISO 27001 concede gran importancia al compromiso activo de la Dirección en el SGSI, partiendo de la base de que el compromiso de la Dirección es crucial para garantizar la implantación efectiva y el mantenimiento de un SGSI eficaz por parte de los empleados.

Política de seguridad info.

Una responsabilidad vital de la dirección es establecer y documentar una Política de Seguridad de la Información (PSI) que esté alineada con los objetivos clave de la organización. Debe incluir objetivos o un marco para establecerlos. Para demostrar que está alineada con el contexto de la organización y los requisitos de las principales partes interesadas, se recomienda que haga referencia o contenga un resumen de los principales problemas y requisitos que debe gestionar. También debe incluir el compromiso de:

- Cumplir los requisitos aplicables en materia de seguridad de la información, como los requisitos legales, las expectativas de los clientes y los compromisos contractuales.
- La mejora continua de su SGSI.

El PSI puede hacer referencia a, o incluir sub-políticas que cubran, los controles clave del SGSI de la organización. Algunos ejemplos son: la selección de proveedores críticos para la seguridad de la información, la contratación y formación de los empleados, clear desk y clear screen, controles criptográficos, controles de acceso, etc.

Para demostrar la importancia del PSI, es aconsejable que lo autorice el miembro de mayor rango de su Alta Dirección o cada uno de los miembros del equipo de Alta Dirección.

CONSEJO: Para asegurarse de que su PSI está bien comunicado y a disposición de las partes interesadas, recomendamos:

- Inclúyala en los paquetes de iniciación y en las presentaciones para nuevos empleados y contratistas.
- Publique la declaración clave en los tablones de anuncios internos, las intranets y el sitio web de su organización.
- Haga que su cumplimiento y/o apoyo sea un requisito contractual para empleados, contratistas y proveedores críticos para la seguridad de la información.

Funciones y responsabilidades

Para que las actividades de seguridad de la información formen parte de las actividades de la mayoría de las personas de la organización, las responsabilidades y las obligaciones de rendir cuentas deben definirse y comunicarse claramente.

Aunque la norma no exige la designación de un representante de seguridad de la información, puede ser útil para algunas organizaciones nombrar a uno que dirija un equipo de seguridad de la información para coordinar la formación, supervisar los controles e informar sobre el funcionamiento del SGSI a la alta dirección. Es posible que esta persona ya sea responsable de la protección de datos.

Sin embargo, para desempeñar su función con eficacia, lo ideal es que forme parte del equipo de alta dirección y que tenga sólidos conocimientos técnicos sobre gestión de la seguridad de la información.

Evidenciar liderazgo al auditor

La Dirección serán aquellos que establecen la dirección estratégica y aprueban la asignación de recursos para la organización o área de negocio con el alcance de su SGSI. Dependiendo de cómo esté estructurada su organización, estas personas pueden ser el equipo directivo diario. Un auditor normalmente pondrá a prueba el liderazgo mediante una entrevista, y evaluará su nivel de implicación en el:

- Evaloración de riesgos y oportunidades.
- Establecimiento y comunicación de políticas.
- Fijación y comunicación de objetivos.
- Revisión y comunicación del rendimiento del sistema.
- Asignación de recursos, responsabilidades y obligaciones adecuadas.

CONSEJO: Antes de su auditoría externa, identifique quién de la alta dirección se reunirá con el auditor externo. Prepárelos con un simulacro de entrevista que incluya las preguntas que espera que les hagan.

Anexo 4: Planificación ISO 27001

SECCIÓN 6: PLANIFICACIÓN

La norma ISO 27001 es una herramienta de gestión de riesgos que orienta a una organización para que identifique las causas de sus riesgos para la seguridad de la información. Como tal, el propósito de un SGSI es:

- **Identificar los riesgos importantes, los obvios y los ocultos pero peligrosos.**
- **Garantizar que las actividades y los procesos operativos de una organización estén diseñados, dirigidos y dotados de recursos para gestionar intrínsecamente esos riesgos.**
- **Responder y adaptarse automáticamente a los cambios para hacer frente a los nuevos riesgos y reducir continuamente la exposición al riesgo de la organización.**

Disponer de un plan de acción detallado que se supervise de forma alineada y se apoye en revisiones periódicas es crucial, y proporciona al auditor la mejor prueba de que la planificación del sistema está claramente definida.

Evaluación de riesgos

La evaluación de riesgos es el núcleo de cualquier SGSI eficaz. Ni siquiera la organización mejor dotada de recursos puede eliminar la posibilidad de que se produzca un incidente de seguridad de la información. Para todas las organizaciones, la evaluación de riesgos es esencial:

- Aumentar la probabilidad de identificar todos los riesgos potenciales mediante la participación de personas que utilicen técnicas de evaluación.
- Asignar recursos para abordar las áreas más prioritarias.
- Tomar decisiones estratégicas sobre cómo gestionar los riesgos que permitan alcanzar con mayor probabilidad sus objetivos.

La mayoría de los marcos de evaluación de riesgos consisten en una tabla que contiene los resultados de los elementos 1-4 con una tabla o matriz suplementaria que cubre el punto 5.

Un auditor externo esperará ver un registro de su evaluación de riesgos, un propietario asignado para cada riesgo identificado y los criterios que ha utilizado.

CONSEJO: El anexo A (5.9) contiene el requisito de mantener una lista de los activos de información, los activos asociados a la información (por ejemplo, edificios, archivadores, ordenadores portátiles, licencias) y las instalaciones de procesamiento de la información. Si completa su evaluación de riesgos evaluando sistemáticamente los riesgos que plantea cada elemento de esta lista, habrá cumplido dos requisitos en el mismo ejercicio.

La norma ISO 27005 - Gestión de riesgos para la seguridad de la información ofrece orientación sobre el desarrollo de una técnica de evaluación de riesgos para su organización. Sea cual sea la técnica que elija, debe incluir los siguientes elementos:

1. Proporcionan un impulso para la identificación sistemática de los riesgos (por ejemplo, revisando los activos, grupos de activos, procesos, tipos de información) uno a uno, comprobando en cada uno la presencia de amenazas y vulnerabilidades comunes, y registrando los controles que tiene actualmente para gestionarlos.
2. Proporcionar un marco para evaluar la probabilidad de que se produzca cada riesgo de forma sistemática (por ejemplo, una vez al mes, una vez al año).
3. Proporcionar un marco para evaluar las consecuencias de que se produzca cada riesgo sobre una base coherente (por ejemplo, pérdida de 1.000 £, pérdida de 100.000 £).
4. Proporcione un marco para clasificar cada riesgo identificado sobre una base coherente teniendo en cuenta su evaluación de la probabilidad y las consecuencias.
5. Establecer criterios documentados que especifiquen, para cada puntuación o categoría de riesgo, el tipo de acción que debe emprenderse y el nivel o prioridad que se le asigna.

Anexo 5: Operación ISO 27001

SECCIÓN 8: OPERACIÓN

Así que, después de toda la planificación y evaluación de riesgos, estamos listos para pasar a la fase de "hacer". La cláusula 8 trata de tener un control adecuado sobre la creación y entrega de su producto o servicio.

La gestión de los riesgos para la seguridad de la información y la consecución de sus objetivos requieren la formalización de sus actividades en un conjunto de procesos claros.

Es probable que muchos de estos procesos ya existan (por ejemplo, la iniciación y la formación) y que simplemente haya que modificarlos para incluir elementos relevantes para la seguridad de la información. Otros procesos pueden tener lugar de manera ad hoc (por ejemplo, aprobación de proveedores), mientras que algunos pueden no existir en absoluto (por ejemplo, auditoría interna).

Para aplicar procesos eficaces son cruciales las siguientes prácticas:

1. Los procesos se crean adaptando o formalizando las actividades habituales de una organización.
2. Identificación sistemática de los riesgos de seguridad de la información pertinentes para cada proceso.
3. Definición y comunicación claras del conjunto de actividades necesarias para gestionar los riesgos asociados a la seguridad de la información cuando se produce un evento (por ejemplo, la incorporación de un nuevo empleado a la empresa).
4. Asignación clara de las responsabilidades para llevar a cabo las actividades relacionadas.
5. Asignación adecuada de recursos para garantizar que las actividades relacionadas puedan llevarse a cabo como y cuando sea necesario.
6. Evaluación rutinaria de la coherencia con la que se sigue cada proceso y su eficacia en la gestión de los riesgos pertinentes para la seguridad de la información.

CONSEJO: Para cada proceso, designe a una persona responsable de garantizar que se lleven a cabo los pasos 2 a 6. Esta persona suele denominarse propietario del proceso. A esta persona se la suele denominar propietario del proceso.

Evaluación de riesgos para la seguridad de la información

Los métodos y técnicas de evaluación de riesgos descritos en la cláusula 6 deben aplicarse a todos los procesos, activos, información y actividades dentro del alcance del SGSI de la organización.

Dado que los riesgos no son estáticos, los resultados de estas evaluaciones deben revisarse frecuentemente, al menos una vez al año, o con mayor frecuencia si la evaluación identifica la presencia de uno o más riesgos significativos. Los riesgos también deben revisarse siempre que:

- Se completan todas las acciones de Tratamiento de Riesgos (véase más abajo).
- Se producen cambios en los activos, la información o los procesos de la organización.
- Se identifican nuevos riesgos.
- La experiencia o nueva información indican que la probabilidad y las consecuencias de cualquier riesgo identificado han cambiado.

CONSEJO: Para asegurarse de que su proceso de evaluación de riesgos cubre los tipos de eventos que requerirían una revisión, también debe tener en cuenta los controles del Anexo A.

Tratamiento de los riesgos para la seguridad de la información

El plan de tratamiento de riesgos que elabore no puede quedarse simplemente en una declaración de intenciones: debe aplicarse. Cuando sea necesario introducir cambios para tener en cuenta nueva información sobre riesgos y cambios en los criterios de evaluación de riesgos, el plan debe actualizarse y volver a autorizarse.

También se debe evaluar el impacto del plan y registrar los resultados de esta evaluación. Esto puede hacerse como parte de la revisión de la gestión o de los procesos de auditoría interna, o utilizando evaluaciones técnicas como pruebas de penetración en la red, auditorías de proveedores o auditorías de terceros sin previo aviso.

Anexo 6: Evaluación de Desempeño ISO 27001

SECCIÓN 9: EVALUACIÓN DEL DESEMPEÑO

Existen tres formas principales de evaluar el rendimiento de un SGSI. Éstas son:

- Supervisar la eficacia de los controles del SGSI.
- Mediante auditorías internas.
- Reuniones de revisión por la dirección.

Seguimiento, medición, análisis y evaluación

Su organización tendrá que decidir qué necesita supervisar para asegurarse de que el proceso del SGSI y los controles de seguridad de la información funcionan según lo previsto. No es práctico para una organización supervisar manualmente todo en todo momento. Si intentara hacerlo, es probable que el volumen de datos fuera tan grande que resultara prácticamente imposible utilizarlo con eficacia. Por lo tanto, tendrá que tomar una decisión informada sobre qué supervisar. Las siguientes consideraciones serán importantes:

- ¿Qué procesos y actividades están sujetos a las amenazas más frecuentes y significativas?
- ¿Qué procesos y actividades presentan las vulnerabilidades inherentes más importantes?
- ¿Qué resulta práctico controlar y generar información significativa y oportuna?
- ¿Está automatizando su supervisión?
- Con cada proceso de supervisión que ponga en marcha, para que sea eficaz debe definirlo claramente:
  - Cómo se lleva a cabo el seguimiento
  - Cuando se emprende.
  - Quién es responsable de llevarla a cabo.
  - Cómo se comunican los resultados, cuándo, a quién y qué hacen con ellos.
  - Si los resultados de la supervisión identifican un rendimiento inaceptable, ¿cuál es el proceso o procedimiento de escalada para hacer frente a esta situación?

Para demostrar a un auditor que dispone de un proceso de supervisión adecuado, deberá conservar registros de los resultados de la supervisión, los análisis, las revisiones de evaluación y cualquier actividad de escalado.

Auditorías internas

El objetivo de las auditorías internas es comprobar los puntos débiles de los procesos del SGSI e identificar oportunidades de mejora. También son una oportunidad para que la alta dirección compruebe la eficacia del SGSI. Si se hacen bien, las auditorías internas pueden garantizar que no haya sorpresas en las auditorías externas.

Las auditorías internas que realice deben comprobar

- La coherencia con que se siguen y aplican los procesos, procedimientos y controles.
- Hasta qué punto sus procesos, procedimientos y controles generan los resultados previstos.
- Si su SGSI sigue cumpliendo la norma ISO 27001 y los requisitos de las partes interesadas.

Para garantizar que las auditorías se llevan a cabo con un calidad y de forma que aporten valor añadido, es necesario que las realicen personas que sean:

- Respetadas.
- Competentes.
- Familiarizadas con los requisitos de la norma ISO 27001.
- Capaces de interpretar su documentación y conocedores de técnicas y comportamientos de auditoría sólidos.

Lo más importante es que se les asigne tiempo suficiente para completar la auditoría y se les garantice la cooperación de los empleados pertinentes. Debe mantener un plan para llevar a cabo sus auditorías internas. Un auditor externo esperará que este plan garantice que todos los procesos de su SGSI se auditan en un ciclo de tres años y que cuentan con procesos que:

- Mostrar pruebas de un rendimiento deficiente (por ejemplo, a través de auditorías previas, o resultados de supervisión o incidentes de seguridad de la información).
- Gestionar los riesgos más importantes para la seguridad de la información.
- Se auditan con mayor frecuencia.

El auditor externo también esperará que las acciones identificadas en las auditorías se registren, sean revisadas por los empleados adecuados y se apliquen a tiempo para rectificar cualquier problema significativo. En el plazo de cierre de las auditorías, los auditores deben tener en cuenta las oportunidades de mejora identificadas que requieran una inversión significativa de recursos.

APÉNDICE

	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																	

Tabla 45 Cronograma de Gant