HERRAMIENTA DIGITAL BASADA EN EL ESTÁNDAR ISO/IEC 27001 PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES.

Documento De Trabajo De Grado

Sebastián Buesaco

Alejandro Alcaraz Gaviria

INSTITUCIÓN UNIVERSITARIA COLEGIO MAYOR DEL CAUCA

FACULTAD DE INGENIERÍA

INGENIERÍA INFORMÁTICA

POPAYÁN-CAUCA

2024

HERRAMIENTA DIGITAL BASADA EN EL ESTÁNDAR ISO/IEC 27001 PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES

Documento De Trabajo De Grado

Sebastián Buesaco

Alejandro Alcaraz Gaviria

Director:

ING. Juan José Caiza Narváez

Codirector:

ING. Katherine Márceles Villalba

INSTITUCIÓN UNIVERSITARIA COLEGIO MAYOR DEL CAUCA

FACULTAD DE INGENIERÍA

INGENIERÍA INFORMÁTICA

POPAYÁN-CAUCA

2024

Tabla de contenido

ANTECEDENTES **1**

I. 11

II. 14

Objetivo General 4

Objetivo Específico 4

III. 14

1. 15

2. 18

2.1. 21

3. 22

4. 24

4.1. 25

· 26

· 27

· 27

5. 27

CAPÍTULO 1. MAPEO SISTEMÁTICO **22**

1.1. 33

1.2. 33

1.2.1. 34

A. 34

B. 35

C. 37

1.2.2. 37

D. 37

E. 40

F. 41

1.2.3. 42

G. 42

H. 46

I. 50

1.2.4. 52

J. 52

CAPÍTULO 2. HERRAMIENTA DIGITAL 56

2.1. 63

2.1.1. 64

2.1.2. 65

2.1.3. 66

2.1.4. 67

· 67

· 68

· 68

· 68

· 71

· 71

➢ 72

➢ 72

➢ 73

➢ 74

2.1.5. 74

2.1.6. 75

2.1.7. 93

2.1.7.1. 93

· 93

· 94

· 94

2.1.7.2 94

2.1.7.3 95

2.1.7.4. 100

2.1.7.5. 105

CAPÍTULO 3. PRUEBAS FINALES 104

3.1 111

3.1.1 111

I. 112

· 115

II. 126

3.1.2. 135

3.1.2.1. 135

· 135

· 136

· 137

3.1.3. 140

4. 145

5. 147

Índice de Tablas

Tabla 1. Principales sistemas operativos. Fuente: Propia. 8

Tabla 2. Criterios de Evaluación Lenguaje de programación. Fuente: Propia. 9

Tabla 3. Cuadro Comparativo. Fuente: Propia. 10

Tabla 4. Características de Dart. Fuente: [78]. 11

Tabla 5. Criterios de Evaluación Base de datos. Fuente: Propia. 13

Tabla 6. Cuadro Comparativo. Fuente: Propia. 14

Tabla 7. Cuadro Comparativo. Fuente: Propia. 19

Tabla 8. Criterios de Evaluación Metodología. Fuente: Propia. 20

Tabla 9. Cuadro Comparativo. Fuente: Propia. 20

Tabla 10. Preguntas de investigación. Fuente: Propia. 28

Tabla 11. Motores de Búsqueda. Fuente : Propia. 28

Tabla 12. Criterios de Inclusión. Fuente: Propia. 32

Tabla 13. Criterios de Exclusión. Fuente: Propia. 32

Tabla 14. Cadenas básicas de búsqueda. Fuente: Propia. 35

Tabla 15. Resultados de la búsqueda. Fuente: Propia. 36

Tabla 16. Artículos primarios producto de la búsqueda. Fuente : Propia. 38

Tabla 17. Tabla de evaluación de calidad de los artículos primarios. Fuente: Propia. 42

Tabla 18. Tabla de tipo de artículos y evaluación de las palabras claves. Fuente Propia. 45

Tabla 19. Principales modelos y/o estándares establecidos en los países de Europa y Latinoamérica Fuente: Propia. 47

Tabla 20. Tendencias empleadas en los países de Europa y Latinoamérica Fuente: Propia. 48

Tabla 21. Definición de roles del Proyecto. Fuente: Propia. 62

Tabla 22. Definición de roles del Proyecto. Fuente: Propia. 62

Tabla 23. Historias de Usuario. Fuente: Propia. 65

Tabla 24. Ítems del product backlog para el primer sprint. Fuente: Propia. 66
Tabla 25. Ítems del product backlog para el segundo sprint. Fuente: Propia. 67
Tabla 26. Ítems del product backlog para el tercer sprint. Fuente: Propia. 68
Tabla 27. Ítems del product backlog para el cuarto sprint. Fuente: Propia. 68
Tabla 28. Se describen los tiempos del experto en las tareas de rol empresa y auditor. Fuente: Propia. 107
Tabla 29. Rangos de tiempos de las tareas de rol empresa. Fuente: Propia. 108
Tabla 30. Rangos de tiempos en las tareas de rol auditor. Fuente: Propia. 108
Tabla 31. Se describen los tiempos en segundos de los usuarios. Fuente: Propia. 120

Índice de Figuras

Figura 1. Logo del lenguaje de programación Dart y frameworks Flutter. Fuente: [81]. 11
Figura 2. Logo del lenguaje de programación Dart. Fuente [78]. 12
Figura 3. Diagrama de arquitectura de software de 3 Capas. Fuente: Propia. 16
Figura 4. Metodología de desarrollo de software. Fuente: Propia. 18
Figura 5. Etapas del proceso para el mapeo sistemático adaptado por los autores. Fuente : Propia. 24
Figura 6. Definición de palabras clave y sinónimos PICOC. Fuente: [93] 29
Figura 7. Palabras clave con sus sinónimos. Fuente. [93]. 30
Figura 8. Criterios de evaluación. Fuente: Propia. 33
Figura 9. Metodología de Trabajo. Fuente: Propia. 58
Figura 10. Diagrama de artefactos y reuniones en la metodología scrum. Fuente [86]. 60
Figura 11. Diagrama fases de evolución de la aplicación. Fuente: Propia. 61
Figura 12. Gestión visual de Kanban Flow. Fuente [87]. 65
Figura 13. Modelo MER. Fuente: Propia. 69
Figura 14. Prototipo inicial del módulo de inicio de sesión, diseño básico. 71
Figura 15. Interfaz final del módulo de inicio de sesión. 71
Figura 16. Prototipo inicial del módulo de programación de auditorías, con campos básicos para fechas y objetivos. 72
Figura 17. Versión final del módulo de programación de auditorías, diseño refinado. 73

Figura 18. Prototipo inicial del historial de evaluaciones, con una lista básica de auditorías. 74
Figura 19. Versión final del historial de evaluaciones, con filtros, gráficos y detalles avanzados. 74
Figura 20. Prototipo inicial de la gestión de documentos, con funcionalidad básica de carga de archivos. 75
Figura 21. Versión final del módulo de gestión de documentos, con opciones de carga, actualización y visualización. 76
Figura 22. Prototipo inicial del módulo de identificación de activos con funcionalidad limitada. 77
Figura 23. Versión final del módulo de identificación de activos, con diseño mejorado y funcionalidades avanzadas. 78
Figura 24. Prototipo inicial de gestión de riesgos con una lista estática de riesgos. 79
Figura 25. Versión final del sistema de gestión de riesgos, con la matriz de impacto. 79
Figura 26. Prototipo inicial de acceso a resultados de pruebas, con listado básico. 80
Figura 27. Versión final del módulo de acceso a resultados de pruebas, con diseño visual e interactividad. 81
Figura 28. Prototipo inicial con una interfaz básica para registrar riesgos sin priorización automatizada. 82
Figura 29. Interfaz final con el formulario y opciones de editar y eliminar. 82
Figura 30. Interfaz inicial con campos básicos de controles. 83
Figura 31. Módulo final con registro detallado e integración completa. 84
Figura 32. Interfaz inicial del generador de informes, mostrando un formulario básico con campos manuales para rellenar los hallazgos y recomendaciones. 85
Figura 33. Interfaz final del módulo, con gráficos integrados, plantillas dinámicas. 86
Figura 34. Logo de la base de datos PostgreSQL. Fuente [83]. 87
Figura 35. Logo Visual Studio Code. Fuente [88]. 88
Figura 36. Logo Postman. Fuente [89]. 88
Figura 37. Opción paleta de Comandos. Fuente: Propia. 90
Figura 38. Opción de un nuevo proyecto. Fuente: Propia. 90
Figura 39. Opción aplicación. Fuente: Propia. 90
Figura 40. Estructura del proyecto. Fuente: Propia. 91
Figura 41. Líneas del código de instalación de dependencias. Fuente: Propia. 92
Figura 42. Carpetas de los archivos creados para el frontend. 93

Figura 43. Código main.dart. 94
Figura 44. Código package.json. 95
Figura 45. Carpeta Backend. 96
Figura 46. Código Carpeta Backend/src/index.js. 97
Figura 47. Código Carpeta Backend/src/database.js. 98
Figura 48. Código Carpeta Backend/.env. 99
Figura 49. Imagen de Bienvenida. Fuente Propia. 100
Figura 50. Imagen de Registro. Fuente Propia. 100
Figura 51. Imagen de Inicio de sesión. Fuente propia. 101
Figura 52. Imagen de Inicio. Fuente Propia. 101
Figura 53. Funciones Dashboard. Fuente Propia. 102
Figura 54. Imagen de Total Registro. Fuente Propia. 102
Figura 55. Imagen de Perfil. Fuente Propia. 103
Figura 56. Pruebas de laboratorio. Fuente propia. 105
Figura 57. Pruebas de laboratorio. Fuente propia. 106
Figura 58. Tarea 1 rol empresa. Fuente: Propia. 109
Figura 59. Tarea 2 rol empresa. Fuente: Propia. 110
Figura 60. Tarea 3 rol empresa. Fuente: Propia. 110
Figura 61. Tarea 4 rol empresa. Fuente : Propia. 111
Figura 62. Tarea 5 rol empresa. Fuente : Propia. 112
Figura 63. Tarea 6 rol empresa. Fuente : Propia. 112
Figura 64. Tarea 7 rol empresa. Fuente : Propia. 113
Figura 65. Tarea 1 rol auditor. Fuente : Propia. 114
Figura 66. Tarea 2 rol auditor. Fuente : Propia. 115
Figura 67. Tarea 3 rol auditor. Fuente : Propia. 116
Figura 68. Tarea 4 rol auditor. Fuente : Propia. 116
Figura 69. Tarea 5 rol auditor. Fuente: Propia. 117
Figura 70. Categorización pregunta 1. Fuente : Propia. 121
Figura 71. Categorización pregunta 2. Fuente : Propia. 121
Figura 72. Categorización pregunta 3. Fuente : Propia. 122
Figura 73. Categorización pregunta 5. Fuente : Propia. 123
Figura 74. Categorización pregunta 9. Fuente: Propia. 124
Figura 75. Categorización pregunta 11. Fuente: Propia. 124
Figura 76. Categorización de preguntas efectividad. Fuente: Propia 132

Figura 77. Categorización de preguntas eficiencia. Fuente: Propia 133
Figura 78. Resultados ataque spidering Front-end. Fuente Owasp-zap. 135
Figura 79. Gráfica tabla de respuesta - ataque spidering. Fuente Owasp-zap. 135
Figura 80. Resultados ataque spidering Backend. Fuente Owasp-zap. 136
Figura 81. Gráfica tabla de respuesta - ataque spidering. Fuente Owasp-zap. 137

ANTECEDENTES

I. DEFINICIÓN DEL PROBLEMA

La seguridad de la información desempeña un papel crucial en entornos empresariales y gubernamentales en la era digital, para garantizar una gestión efectiva de esta seguridad, se han adoptado ampliamente modelos y estándares como ISO/IEC 27001, COBIT y NIST en Europa y Latinoamérica [67] [66]. A pesar de la prominencia de la ISO/IEC 27001, existen interrogantes sobre sus fortalezas y debilidades, así como sobre su impacto real en la protección de datos y la ciberseguridad.

Para realizar un buen análisis de la documentación se realizó un mapeo sistemático con el objetivo de identificar y evidenciar posibles fallos mejorando la seguridad frente a accesos no autorizados. La importancia de la implementación de un mapeo sistemático, para poder realizar la solución del Servidor de Identidad otorgando un nivel elevado de seguridad frente al acceso no autorizado en aplicaciones web y móviles, lo cual representa una mejora en la seguridad [65].

De acuerdo con lo anterior, la gestión de la seguridad de la información ha evolucionado de manera significativa a lo largo de los años, y uno de los marcos más influyentes para abordar estos desafíos es la norma ISO/IEC 27001 [68]. Esta norma internacional ha experimentado tres etapas de actualización clave: en 2005, 2013 y 2022. Cada una de estas actualizaciones ha respondido a la dinámica cambiante de las amenazas cibernéticas y ha introducido mejoras para fortalecer la seguridad de la información en entornos organizacionales.

Por esta razón las buenas prácticas de seguridad basadas en normas internacionales reconocidas, como ISO/IEC 27001 e ISO/IEC 27002 en el cual llevó a cabo la investigación, donde se aplicó la metodología Magerit v3 y se emplearon técnicas de inteligencia de negocios para integrar y procesar información proveniente de diversas fuentes en las organizaciones estudiadas [63].

La versión de 2005 estableció los cimientos para un Sistema de Gestión de Seguridad de la Información (SGSI), proporcionando un marco para la identificación, evaluación y tratamiento de riesgos de seguridad de la información. En 2013, la norma se sometió a una revisión integral, introduciendo cambios significativos para adaptarse a las crecientes amenazas cibernéticas y reflejar las mejores prácticas emergentes en seguridad de la información. Por último, la versión de 2022 representa la última actualización, incorporando avances tecnológicos y respondiendo a las cambiantes demandas del panorama de ciberseguridad.

Ahora bien, al comparar entre las dos últimas versiones, examinamos la implementación de los nuevos controles establecidos en estas versiones dándole un enfoque en analizar la estructura actualizada de los 114 controles y la incorporación de 11 nuevos controles, proporcionando ejemplos con perfiles de clientes en diferentes sectores. El trabajo destaca la eliminación del "Código de Prácticas" y la introducción de prácticas basadas en ciberseguridad y protección de datos. Se aborda la adaptación de tratamientos de riesgos, métricas, objetivos, políticas y procedimientos dentro de los Sistemas de Gestión de Seguridad de la Información (SGSI). El enfoque principal está en la implementación, específicamente en las categorías organizativas y tecnológicas, anticipando la puesta en marcha para abril de 2024 [62].

Como podemos evidenciar la norma ISO/IEC 27001 se destaca como una tendencia dominante en la gestión de la seguridad de la información. La amplitud de su adopción subraya la confianza depositada en este estándar para establecer y mejorar los sistemas de gestión de seguridad en ambas regiones. Sin embargo, la falta de comprensión exhaustiva sobre cómo aplicar la norma, adaptarla a contextos específicos y evaluar su impacto real en la mitigación de riesgos y la prevención de vulnerabilidades, crea un escenario en el que las organizaciones pueden enfrentar dificultades en el establecimiento y mantenimiento de sistemas de seguridad [68].

Asimismo, la implementación de un sistema de gestión de seguridad de la información bajo esta norma puede ayudar a identificar debilidades empresariales y promover

prácticas administrativas adecuadas como destaca el estudio de Arévalo, Bayona y Bautista donde llegan a la conclusión proponiendo una aplicación de herramientas para el análisis de sistemas de información usando la norma ISO 27001:2005, mediante el uso de tecnologías de información más apropiadas para las organizaciones del estudio, que protejan su activo más importante: la información [64].

Es decir que los auditores con la norma ISO/IEC 27001 de la seguridad de la información, hacen que las organizaciones cumplan con los requisitos establecidos en este estándar internacional. Sin embargo, la realización de auditorías manuales puede ser un proceso laborioso y propenso a errores [69].

Por lo anterior se propone abordar esta problemática identificando los desafíos clave en la implementación de la ISO/IEC 27001 en distintos entornos organizacionales. En este contexto, surge la necesidad de desarrollar una herramienta digital, que facilite y optimice el proceso de auditoría basado en la norma ISO/IEC 27001. La implementación de esta herramienta busca no solo agilizar el proceso de auditoría, sino también garantizar una aplicación consistente y efectiva de los requisitos de la norma.

Los modelos y estándares como ISO/IEC 27001, COBIT y NIST destacan que, aunque la ISO 27001 provee prácticas reconocidas globalmente, no es la respuesta definitiva a la seguridad de la información. Se sugiere un enfoque holístico utilizando otros modelos de gestión de la seguridad, como el framework de ciberseguridad de NIST para ayudar en el diseño de los controles de TI de ISO 27001 [66].

En este contexto, la herramienta digital innovadora, pretende abordar los desafíos actuales, proporcionando un enfoque eficiente para la evaluación de la seguridad de la información en organizaciones. Por último, evaluar la herramienta digital diseñada para optimizar la ejecución de auditorías de seguridad de la información basadas en esta norma. Al hacerlo, se espera mejorar la eficacia, consistencia y accesibilidad de las auditorías, asegurando un cumplimiento más efectivo con los estándares internacionales.

De acuerdo con lo mencionado anteriormente, surge la pregunta, **¿Cómo se puede desarrollar e implementar una herramienta digital, que facilite y optimice el proceso de auditoría basado en la norma ISO/IEC 27001, asegurando una aplicación coherente y efectiva de los requisitos de la norma?**

II. OBJETIVOS

Objetivo General

- Desarrollar una herramienta digital innovadora basada en un marco metodológico de desarrollo seguro para optimizar la implementación del estándar ISO/IEC 27001, permitiendo una gestión más eficiente y efectiva de la seguridad de la información en diversos contextos organizacionales.

Objetivo Específico

- Caracterizar la Seguridad de la Información bajo la norma ISO/IEC 27001 mediante una revisión sistemática de literatura para identificar patrones, tendencias esenciales en su implementación y gestión en diferentes contextos.

- Diseñar una herramienta digital para optimizar los procesos de implementación del estándar ISO/IEC 27001 mediante el uso de un marco metodológico de desarrollo seguro

- Evaluar la herramienta digital a través de un grupo focal que permita aportar sugerencias y mejoras a estas.

III. ALCANCE

Este trabajo de investigación tiene como propósito principal desarrollar una herramienta digital que optimice la implementación del estándar ISO/IEC 27001 en el

contexto de la gestión de la seguridad de la información. El alcance de la tesis se define a partir de tres objetivos específicos, cada uno orientado a un aspecto clave del proceso investigativo y de desarrollo.

El primer objetivo específico busca caracterizar la Seguridad de la Información bajo la norma ISO/IEC 27001 mediante una revisión sistemática de literatura. Este proceso implica identificar autores, enfoques metodológicos, técnicas y herramientas relacionadas con la implementación y gestión de la seguridad de la información en diversos contextos organizacionales. Dado el impacto y la evolución de los estándares de seguridad, esta etapa permitirá construir un marco teórico que fundamente los principios y enfoques que guiarán el desarrollo de la herramienta digital [21][22]. La revisión también se enfocará en identificar retos y buenas prácticas asociadas con la implementación del estándar ISO/IEC 27001 [19].

Para cumplir el segundo objetivo específico, se diseñará una herramienta digital innovadora orientada a optimizar la implementación del estándar ISO/IEC 27001 [23]. Este diseño estará respaldado por un marco metodológico como lo es Scrum, considerando aspectos como la evaluación de riesgos y la usabilidad en contextos organizacionales. La herramienta incluirá módulos integrados que faciliten la gestión de controles, activos, procesos y riesgos, alineados con los requisitos de la norma.

A continuación, se describen los aspectos clave relacionados con las tecnologías y herramientas seleccionadas:

1. **Sistemas Operativos**

Los sistemas operativos son plataformas diseñadas para interactuar con el hardware y el software donde se ejecutan las aplicaciones. Estos sistemas operativos tienen un conjunto de características y funcionalidades únicas que se describen a continuación en la tabla 1.

La relevancia de los sistemas operativos radica en optimizar el rendimiento y la seguridad de los dispositivos siendo clave para realizar un diseño adecuado para la eficiencia [70].

Sistemas Operativos	Logo	Características	Ventajas	Desventajas
Windows (Microsoft)	*Fuente Tomada de: (Enciclopedia Concepto) [71].*	Windows es un sistema operativo desarrollado por Microsoft, conocido por su interfaz gráfica intuitiva y amplia compatibilidad con software y hardware. Sus características incluyen una variada gama de aplicaciones y soporte para dispositivos diversos.	Su accesibilidad para principiantes, una gran cantidad de software disponible y un soporte técnico extenso.	Mayor vulnerabilidad a malware y virus, el costo asociado a las licencias y un consumo elevado de recursos del sistema.
Linux (GNU)	*Fuente Tomada de: (Juegos Linux) [72].*	Linux es un sistema operativo de código abierto que se basa en el núcleo Linux y es conocido por su flexibilidad y personalización. Sus características incluyen una variedad de distribuciones, como Ubuntu y Fedora, y una potente terminal para usuarios avanzados.	Es gratuito, tiene una mayor seguridad y estabilidad, y cuenta con una comunidad activa que ofrece soporte.	Curva de aprendizaje pronunciada para nuevos usuarios, menor compatibilidad con software comercial y la necesidad de configuración técnica en algunos casos.

Mac OS (Apple)	macOS *Fuente Tomada de: (Universidad del Pacifico) [73].*	Mac OS es el sistema operativo exclusivo de Apple, diseñado para sus computadoras. Ofrece una interfaz elegante y cohesiva, así como una integración perfecta con otros dispositivos de Apple.	Rendimiento y estabilidad superiores, menor vulnerabilidad a virus, y una excelente plataforma para diseño y edición multimedia.	Alto costo del hardware, la limitada personalización y el acceso restringido a software exclusivo de Apple.
FreeBSD (Universidad de Berkeley)	FreeBSD *Fuente Tomada de: (FreeBSD Foundation) [74].*	FreeBSD es un sistema operativo basado en Unix, conocido por su robustez y seguridad. Sus características incluyen un sistema de archivos avanzado, como ZFS, y un enfoque en la estabilidad.	Alto rendimiento en servidores, su licencia permisiva de código abierto y su excelente soporte de redes.	Comunidad más pequeña en comparación con Linux, menor compatibilidad con software de escritorio y una curva de aprendizaje para nuevos usuarios.
iOS (Apple)	iOS *Fuente Tomada de: (Universidad del Pacifico) [75].*	iOS es el sistema operativo móvil exclusivo de Apple, diseñado para iPhone y iPads. Se caracteriza por su interfaz intuitiva y fluida, así como por una alta integración de hardware y software.	Robusta seguridad que reduce el riesgo de malware, una excelente experiencia de usuario y acceso a un ecosistema de aplicaciones de alta calidad.	Alto costo de los dispositivos, limitaciones en la personalización y un sistema cerrado que restringe la flexibilidad.
Android	*Fuente Tomada de:*	Android es un sistema operativo móvil basado en Linux, utilizado principalmente en smartphones y tabletas. Sus características	Android incluye ser gratuito, su gran compatibilidad con diferentes hardware y la extensa personalización	Fragmentación entre dispositivos y versiones, vulnerabilidades de seguridad en algunas aplicaciones y la dependencia de

	(Tecnología Wiki) [76].	incluyen una interfaz personalizable y acceso a una amplia variedad de aplicaciones a través de Google Play.	que ofrece a los usuarios.	servicios de Google.
Firefox OS	Firefox OS *Fuente Tomada de: (Wikipedia) [77].*	Firefox OS era un sistema operativo móvil basado en HTML5, diseñado para dispositivos de bajo costo. Sus características incluían una interfaz simplificada y un enfoque en aplicaciones web.	Gratuito y de código abierto, ligero y rápido, y fomentar estándares abiertos.	Falta de soporte oficial, escasa disponibilidad de aplicaciones y limitaciones en comparación con otros sistemas operativos móviles más populares.

Tabla 1. Principales sistemas operativos. Fuente: Propia.

Aunque en la tabla anterior se presentan algunos de los sistemas operativos que se utilizaran para desplegar la aplicación, se destaca el sistema operativo Windows. Este se caracteriza por su alta accesibilidad y su capacidad de adaptarse a diversas necesidades, lo que facilita la adopción de aplicaciones móviles y web.

2. Lenguaje De Programación

Para escoger la mejor opción fue necesario hacer una evaluación cualitativa y cuantitativa para ofrecer una comparación clara y simplificada de diferentes lenguajes de programación, con el fin de facilitar la toma de decisiones en contextos de desarrollo de software. La evaluación busca identificar qué lenguajes proporcionan las herramientas y el soporte necesario para diversos tipos de desarrollo (web, móvil, sistemas, etc.).

Con esta evaluación se espera poder obtener como resultado el lenguaje que mejor se adapte al proyecto. Para ello, es necesario establecer unas características que

reflejan el criterio de evaluación, las cuales se utilizaran para poder evaluar todos los lenguajes de programación, como se puede observar en la tabla 2.

Se utilizará un sistema de puntaje binario (0 = No aplica y 1 = Si Aplica) aplicado a diferentes lenguajes de programación, con el fin de identificar qué opción es más viable para el proyecto, como se puede identificar en la tabla 3.

N°	Característica	Criterio	Puntuación de la Respuesta	
			1	0
C1	**Desarrollo web**	Capacidad del lenguaje para crear y mantener sitios y aplicaciones web.	SI	NO
C2	**Desarrollo de aplicaciones móviles**	Aptitud del lenguaje para desarrollar aplicaciones nativas o híbridas en plataformas móviles.	SI	NO
C3	**Comunidad**	Tamaño y actitud de la comunidad de desarrolladores, lo que afecta el soporte, la disponibilidad de recursos y la resolución de problemas.	SI	NO
C4	**Facilidad de aprendizaje**	Dificultad percibida por los nuevos desarrolladores para aprender el lenguaje, incluyendo la simplicidad de sintaxis y la calidad de la documentación disponible.	SI	NO
C5	**Rendimiento**	Capacidad del lenguaje para ejecutar procesos de manera eficiente en términos de velocidad y uso de recursos.	SI	NO
C6	**Biblioteca y herramientas**	Disponibilidad de bibliotecas, frameworks y herramientas que facilitan el desarrollo en diferentes áreas.	SI	NO
C7	**Conocimiento**	Cuenta con excelentes conocimientos en el desarrollo de aplicaciones móviles o web del lenguaje.	SI	NO

Tabla 2. Criterios de Evaluación Lenguaje de programación. Fuente: Propia.

Lenguaje	C1	C2	C3	C4	C5	C6	C7	Total
Dart	1	1	1	1	1	1	1	7
JavaScript	1	1	1	1	1	1	0	6
Kotlin	0	1	1	1	1	1	0	5
Swift	1	1	1	1	0	1	0	5
Python	1	0	1	1	0	1	0	4

Tabla 3. Cuadro Comparativo. Fuente: Propia.

Basado en la evaluación realizada y considerando los criterios específicos para desarrollo web y desarrollo de aplicaciones móviles, Dart emerge como una opción altamente recomendable para ambos ámbitos. Dart es una excelente elección para proyectos que requieran tanto desarrollo web como de aplicaciones móviles, ya que ofrece un equilibrio óptimo entre eficiencia de desarrollo, rendimiento de la aplicación y facilidad de mantenimiento. Por lo tanto, el uso de Dart es la mejor opción para el proyecto debido a su fácil uso para multiplataformas (móvil y web). A continuación, en la tabla 4, se muestran algunas características del lenguaje de programación.

Característica	**Descripción** *Fuente tomada de: (EDteam [78])*
Tipado estático opcional	Puedes especificar tipos de datos de forma estática para mejorar la seguridad y la detección de errores en tiempo de compilación, o puedes dejar que el sistema de tipos de forma dinámica.
Eficiencia y rendimiento	Ofrece un rendimiento sólido en aplicaciones móviles y web. Su compilador AOT (Ahead-of-Time) puede generar código nativo altamente optimizado para ejecutar aplicaciones más rápidas y eficientes.
Sintaxis clara y concisa	Lo hace atractivo para desarrolladores por su facilidad de lectura. Además, su estilo de codificación limpio y organizado facilita el mantenimiento del código y la colaboración en equipos.
Programación orientada a objetos	Utiliza conceptos como clases, herencia, encapsulación y polimorfismo para organizar y estructurar el código. Esto facilita la creación de aplicaciones escalables y mantenibles.
Soporte para programación funcional	Dart admite la programación funcional. Esto permite el uso de funciones de alto orden, expresiones lambda y operaciones de transformación de datos, lo que facilita el desarrollo de código más expresivo y modular.
Multiplataforma con Flutter	Una de las principales ventajas de Dart es su integración con el framework Flutter para el desarrollo de aplicaciones móviles

	multiplataforma. Flutter utiliza Dart como su lenguaje principal y proporciona un conjunto completo de herramientas y widgets para crear interfaces de usuario hermosas y fluidas en iOS, Android y web.

Tabla 4. Características de Dart. Fuente: [78].

2.1. Framework De Flutter Para Dart

Flutter es un framework de código abierto desarrollado por Google para el lenguaje de programación Dart, utilizado principalmente en el desarrollo de aplicaciones móviles multiplataforma. Ofrece una amplia variedad de widgets personalizables y flexibles que permiten construir interfaces de usuario atractivas y fluidas. Su característica de Hot Reload permite ver los cambios en tiempo real, agilizando el proceso de desarrollo. Utiliza el motor de renderizado Skia para un rendimiento rápido y suave, proporcionando una experiencia nativa tanto en Android (Material Design) como en iOS (Cupertino). Flutter simplifica el desarrollo con un código base compartido para múltiples plataformas, lo que resulta en un desarrollo ágil y eficiente de aplicaciones móviles [80] [82].

Figura 1. Logo del lenguaje de programación Dart y frameworks Flutter. Fuente: [81].

Dart es un lenguaje de programación desarrollado por Google, utilizado principalmente en el desarrollo de aplicaciones móviles y web con Flutter. Dart es conocido por su rendimiento y eficiencia, y ofrece características como tipado opcional, recolección de basura y soporte para programación orientada a objetos y funcional [79].

Figura 2. Logo del lenguaje de programación Dart. Fuente [78].

3. Base De Datos

Teniendo en cuenta lo anterior, se opta por una evaluación cuantitativa y cualitativa para obtener las opciones óptimas a las necesidades específicas del proyecto. A continuación, se describen las cinco mejores bases de datos que podrían adaptarse al lenguaje de programación.

Para ello, se establecen unas características en donde se refleja el criterio de evaluación, las cuales se utilizarán para poder evaluar todas las bases de datos, así como se puede observar en la tabla 5.

Por último, se utiliza un sistema de puntaje binario (0 = No aplica y 1 = Si Aplica), aplicado a las bases de datos para identificar la opción más viable para el proyecto como se observa en la tabla 6.

N°	Área	Criterio	Puntuación de la Respuesta	
			1	0
C1	**Facilidad de uso**	Se refiere a la simplicidad en la configuración, el manejo y el aprendizaje del sistema de gestión de base de datos.	SI	NO
C2	**Rendimiento**	Evalúa la eficiencia en el procesamiento de consultas y la gestión de grandes volúmenes de datos, así como la rapidez en la respuesta a las operaciones de entrada/salida.	SI	NO
C3	**Escalabilidad**	Capacidad de la base de datos para manejar incrementos en la	SI	NO

		carga de trabajo, ya sea aumentando el tamaño de los datos o el número de usuarios concurrentes, sin perder rendimiento.		
C4	**Soporte para Transacciones ACID**	Cumplimiento de los principios ACID (Atomicidad, Consistencia, Aislamiento, Durabilidad) que garantizan transacciones seguras y estables.	SI	NO
C5	**Extensibilidad y soporte de funciones avanzadas**	Facilidad con la que se pueden añadir nuevas funcionalidades, soporte para procedimientos almacenados, triggers y vistas, entre otros.	SI	NO
C6	**Comunidad**	Existencia de una comunidad activa y recursos disponibles para soporte técnico, tutoriales, foros de discusión y documentación.	SI	NO
C7	**Seguridad**	Medidas y herramientas disponibles para proteger la base de datos contra accesos no autorizados y garantizar la integridad de los datos.	SI	NO
C8	**Mantenimiento**	Herramientas y facilidades ofrecidas para la administración rutinaria, el mantenimiento y la monitorización de la base de datos.	SI	NO
C9	**Conformidad con estándares**	Grado en que la base de datos sigue los estándares internacionales de SQL y otros protocolos relacionados, asegurando compatibilidad e interoperabilidad.	SI	NO
C10	**Compatibilidad con el lenguaje Dart**	Disponibilidad y eficiencia de interfaces y bibliotecas para conectar y operar la base de datos desde aplicaciones desarrolladas en Dart.	SI	NO

Tabla 5. Criterios de Evaluación Base de datos. Fuente: Propia.

Base de Datos	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	Total
SQLite	1	1	0	1	0	0	0	1	0	1	5
PostgreSQL	1	1	1	1	1	1	1	1	1	1	10
MySQL	1	1	1	1	1	1	1	1	0	1	9

Tabla 6. Cuadro Comparativo. Fuente: Propia.

Con base en los resultados finales de la evaluación, PostgreSQL se destaca como la opción más adecuada para este proyecto, gracias a su alto rendimiento y capacidad de escalabilidad. Estos factores son esenciales para gestionar el crecimiento progresivo del volumen de datos y el número de usuarios. La capacidad de PostgreSQL para escalar sin afectar el rendimiento es crucial en aplicaciones que requieren un procesamiento intensivo y operaciones constantes, como en las evaluaciones de riesgo. Además, su soporte robusto para transacciones ACID, garantiza la integridad y precisión de los datos, evitando errores que podrían comprometer los resultados.

PostgreSQL muestra una excelente compatibilidad con Dart, el lenguaje de programación utilizado con Flutter para el desarrollo de aplicaciones web y móviles. Esto se debe a la disponibilidad de bibliotecas robustas, como el paquete “postgres” en Dart, que facilitan una conexión fluida y eficiente entre la aplicación y la base de datos. Esta compatibilidad asegura que los desarrolladores puedan aprovechar al máximo las características de PostgreSQL sin enfrentar problemas de integración, permitiendo un desarrollo cohesivo y sin interrupciones.

4. Arquitectura Web

La arquitectura de software en aplicaciones web nos permite saber cómo interactúa el sistema con diferentes componentes, como se comunican para cada necesidad y requisitos técnicos que tiene el usuario. Es por eso que la arquitectura web tiene un papel fundamental para un diseño que nos permite escalabilidad, seguridad, disponibilidad, rendimiento y mantenimiento, favoreciendo la experiencia del usuario.

De acuerdo con lo anterior encontramos múltiples sistemas web con diversas ventajas dependiendo del proyecto como arquitectura monolítica, arquitectura en tres capas, arquitectura microservicios, arquitectura serverless, y arquitectura jamstack. Para adentrarnos a los diferentes modelos de arquitectura web es necesario saber algunos componentes que trabajan en conjunto garantizando la experiencia del usuario, a continuación, se describen los componentes:

- **Cliente o interfaz de usuario (Frontend):** Aquí es donde el usuario interactúa con la presentación visual de la aplicación. Para realizar el enfoque visual se puede utilizar tecnologías de desarrollo web como HTML, CSS, JavaScript con un apoyo de diferentes frameworks como React, Angular [85]. Esta interfaz consume Apis que facilita interfaces dinámicas y responsivas.

- **Servidor (Backend):** Esta capa maneja la lógica y la interacción con la base de datos el cual se comunica con el front-end mediante Apis. Se suele desarrollar con Node JS, Python (Django, Flask), entre otros [85].

- **Base de Datos:** La base de datos es el que utilizamos para el almacenamiento de los diferentes datos de la aplicación de manera estructurada permitiéndonos consultas y operaciones. Algunos tipos de SQL (PostgreSQL, MySQL) o NoSQL (MongoDB, Cassandra) dependiendo de lo que pida la aplicación en cuanto a los requisitos [85].

4.1. Arquitectura Tres Capas

Esta arquitectura divide la aplicación en tres componentes independientes:

- **Capa de Presentación (Frontend):** Donde el usuario interactúa con el sistema.

- **Capa de Lógica de Negocio (Backend):** Donde se procesan las solicitudes y se aplica la lógica empresarial.

- **Capa de Persistencia (Base de Datos):** Donde se almacenan los datos.

Esta metodología nos permite mayor modularidad y escalabilidad, por lo que puede desarrollarse y desplegarse de forma independiente. Esta arquitectura es especialmente utilizada en aplicaciones empresariales debido a su estructura y capacidad de escalar [84].

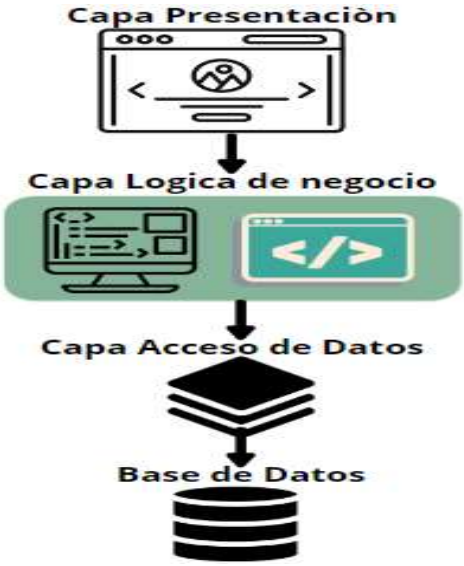

Figura 3. Diagrama de arquitectura de software de 3 Capas. Fuente: Propia.

De acuerdo con lo anterior, se ha escogido para mayor comodidad de la aplicación el modelo de tres capas, como se muestra a continuación:

- **Capa de Presentación (Front-end)**

En una aplicación desarrollada con Dart y Flutter, la capa de presentación se implementa en el front-end de la aplicación, que incluye las pantallas, widgets y componentes visuales que interactúan con los usuarios. En Flutter, esto se logra mediante la creación de widgets que representan la interfaz de usuario y responden a las acciones del usuario. La interacción entre la capa de presentación (frontend) y PostgreSQL (backend) se realiza a través de solicitudes HTTP (para aplicaciones web) o mediante consultas directas a la base de datos. Las respuestas o datos

recuperados de PostgreSQL se utilizan para actualizar la interfaz de usuario en Flutter.

- **Capa de Lógica de Negocio (Backend)**

La capa de lógica de negocio, responsable de gestionar las reglas y procesos específicos de la aplicación. Aquí se llevan a cabo operaciones como validaciones de datos, cálculos, procesamiento de información, etc. Esta capa nos sirve como intermediaria entre la capa de presentación y la base de datos garantizando que la información sea procesada correctamente.
Además, para diseñar esta capa fue necesario utilizar Node Js con Express, JavaScript para organizar el código.

- **Capa de Almacenamiento de Datos (Base de Datos)**

La capa de acceso a datos es el nivel encargado de gestionar el almacenamiento y recuperación de datos en el sistema. En esta capa utilizamos una base de datos relacional como lo es PostgreSQL donde se llevan a cabo las operaciones de consulta permitiendo almacenar la información y la consistencia de los datos

5. Metodología Para El Desarrollo De Software

La elección entre metodologías tradicionales y ágiles depende del contexto del proyecto, la naturaleza de los requisitos y la dinámica del equipo. Ambos enfoques tienen sus ventajas y desventajas, y es crucial considerar estos aspectos al seleccionar la metodología más adecuada para garantizar el éxito del proyecto y la satisfacción del cliente, como se puede observar en la siguiente figura 4.

Figura 4. Metodología de desarrollo de software. Fuente: Propia.

Por lo anterior, se enfocaron en la elección de una metodología ágil para el desarrollo de software debido a su capacidad para adaptarse rápidamente a los cambios en los requisitos del proyecto, la facilidad de trabajo entre el equipo y el cliente permitiéndonos entregas incrementales de valor dejando mayor satisfacción tanto para el cliente como para el equipo de desarrollo.

Para la elección de la metodología a utilizar, fue necesario realizar un análisis previo, profundo y detallado de cada una de ellas, considerando tanto sus características cualitativas como cuantitativas, con el fin de identificar la que mejor se adapta a las necesidades específicas del proyecto. Por lo tanto, se inició comparando las metodologías como se observa en la tabla 7, la cual permite profundizar en las características y beneficios de cada metodología, evaluando aspectos como la flexibilidad, la transparencia, la colaboración y el enfoque en la calidad del producto.

Características	**Scrum**	**Kanban**	**Extreme Programming (XP)**	**Lean Software Development (LSD)**
Ciclo	Sprint: Ciclos cortos de 1 a 4 semanas.	Sin ciclos definidos, flujo continuo de trabajo.	Ciclos cortos de desarrollo y pruebas.	Ciclos de entrega de valor al cliente.

Plan	Planificación del sprint al inicio del ciclo.	Sin plan definido al inicio, se adapta a las necesidades.	Planificación incremental, se ajusta en cada ciclo.	Planificación basada en el valor para el cliente.
Alcance	Alcance definido al inicio del sprint, puede ajustarse en la revisión.	Alcance flexible, se adapta a las necesidades del cliente.	Alcance definido en cada ciclo, se ajusta según la retroalimentación.	Alcance basado en el valor para el cliente, se ajusta según las prioridades.
Tipo	Estructurada, con roles y responsabilidades definidos.	Flexible, sin roles ni responsabilidades definidas.	Colaborativa, con énfasis en la programación en pares.	Basada en principios Lean, enfoque en el flujo de valor.
Herramientas	Tablero Scrum, gráficos de burndown, herramientas de gestión de tareas.	Tablero Kanban, métricas de flujo de trabajo, herramientas de visualización.	Herramientas de programación en pares, herramientas de pruebas unitarias, herramientas de integración continua.	Herramientas de análisis de valor, herramientas de gestión de flujo de trabajo, herramientas de entrega continua.
Ventajas	Estructura clara para la comunicación y colaboración.	Flexibilidad y adaptabilidad a cambios constantes.	Alta calidad del código y reducción de errores.	Enfoque en el valor para el cliente y satisfacción.
Desventajas	Puede ser rígido e inflexible ante cambios.	La falta de estructura puede generar confusión en el equipo.	Curva de aprendizaje alta para la implementación.	Requiere un cambio cultural en la organización.

Tabla 7. Cuadro Comparativo. Fuente: Propia.

Por último, se utilizaron puntuaciones numéricas (0 = No Aplica, 1 = Aplica y 0.5 = Parcialmente), lo que proporciona una forma clara y concisa de comparar las características específicas de cada metodología. Esto les permite identificar fácilmente cuál se ajusta mejor, teniendo en cuenta el costo de tiempo para el presente proyecto, como se observa en la tabla 10. A continuación, se enumeran cada una de las características para facilitar la comparación, como se observa en la tabla 8.

Características	Aspectos
C1	Participación del cliente en la planificación del sprint.
C2	Validación de funcionalidades por parte del cliente.
C3	Reuniones diarias con el equipo.
C4	Planificación del sprint.
C5	Revisión del sprint.
C6	Retrospectiva del sprint.
C7	Visualización del flujo de trabajo en un tablero.
C8	Límite de trabajo en progreso (WIP).
C9	Métricas de flujo de trabajo.
C10	Programación en pares.
C11	Refactorización constante.
C12	Pruebas unitarias.
C13	Integración continua.
C14	Definición del valor para el cliente.
C15	Métricas de éxito del producto.
C16	Demostraciones del producto.

Tabla 8. Criterios de Evaluación Metodología. Fuente: Propia.

	C1	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**	**C8**	**C9**	**C10**	**C11**	**C12**	**C13**	**C14**	**C15**	**C16**	**Resultados**
Scrum	1	1	1	1	1	1	0	0.5	0.5	0	0	1	1	0	0.5	0.5	**10**
Kanban	0	0.5	0	0	0	0	1	1	1	0	0	0.5	0.5	0	0	0	**4.5**
XP	1	1	0	0	0	0	0	0	0	1	1	1	1	0	0	0	**6**
LSD	1	1	0	0	0	0	0	0	0.5	0	0	0.5	0.5	0	0	0	**3.5**

0	**No aplica**
0.5	**Parcialmente**
1	**Aplica**

Tabla 9. Cuadro Comparativo. Fuente: Propia.

En resumen, la metodología Scrum fue la opción más adecuada de las cuatro, ya que te proporciona la flexibilidad, la transparencia y la capacidad de respuesta necesarias para desarrollar una herramienta digital efectiva que optimice los procesos de implementación del estándar ISO/IEC 27001. Su enfoque en la colaboración, las

entregas incrementales y la calidad del producto ayudará a alcanzar los objetivos de manera eficiente y efectiva.

A pesar de las desventajas que presenta Scrum, estas se superan con creces debido a su capacidad para proporcionar un marco ágil efectivo, que permita mejorar continuamente durante el transcurso del proyecto y desarrollo de manera eficiente y efectiva.

El último objetivo específico se centra en la evaluación de la herramienta mediante un enfoque participativo y técnico, que incluye:

Grupo focal: Se formará un grupo focal compuesto por usuarios como personas del común, estudiantes y profesores de la Institución Universitaria Colegio Mayor del Cauca, quienes interactuaron con la herramienta y proporcionarán retroalimentación sobre su funcionalidad y usabilidad de la aplicación.

Pruebas de usabilidad: Se llevarán a cabo evaluaciones que permitan analizar la eficiencia, efectividad y satisfacción del usuario al interactuar con la interfaz de la herramienta.

Pruebas de seguridad: Tanto en el frontend como en el backend, se realizan pruebas técnicas para garantizar que la herramienta cumpla con los estándares de seguridad, protegiendo los datos sensibles y minimizando riesgos de vulnerabilidades. Estas pruebas incluirán análisis de penetración, escaneos automáticos (ataque araña y fuzz) y de inyección SQL.

Las sugerencias obtenidas del grupo focal, así como los resultados de las pruebas, servirán para realizar ajustes y mejoras en la herramienta, garantizando su calidad, funcionalidad y relevancia en entornos organizacionales reales.

CAPÍTULO 1. MAPEO SISTEMÁTICO

1.1. INTRODUCCIÓN

La norma ISO/IEC 27001 es un estándar internacional que establece los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI). Se centra en proteger los activos de información de una organización mediante la identificación, control y mitigación de riesgos de seguridad.

Este estándar opera como un marco estructurado que orienta a las organizaciones en la implementación de controles de seguridad de la información. Se basa en un ciclo continuo de mejora que involucra la identificación de activos, la evaluación de riesgos, la aplicación de controles adecuados y revisiones periódicas con el fin de perfeccionar los sistemas de seguridad.

Este estudio se enfoca en recopilar información pertinente y relevante sobre Seguridad de la Información basada en la Norma o Estándar de la ISO/IEC 27001, con el propósito de ofrecer una visión general y útil para otros investigadores en este campo. Se estructura en varias etapas que abarcan el protocolo de investigación, una discusión permite explorar y contextualizar los hallazgos descubiertos durante el estudio y por último las conclusiones.

1.2. PROTOCOLO DE INVESTIGACIÓN

Un Mapeo sistemático es un procedimiento que cumple la función de recopilar, clasificar y organizar la información existente acerca de un tema de interés investigativo. De esta manera, para la elaboración del presente Mapeo se adoptó como base el protocolo propuesto por [90], teniendo en cuenta ese modelo y adecuando modificaciones al estudio sistemático de los Marcos de Ciberseguridad basados en riesgos. En consecuencia, se llevaron a cabo las siguientes fases: (1) aplicación del enfoque GQM la cual implica establecer objetivos, formular preguntas y definir métricas , (2) definición de las estrategias de búsqueda y selección se encarga de establecer métodos para encontrar y elegir información relevante durante un estudio, (3) ejecución de la revisión se basa en recopilada información según el plan establecido, buscando obtener conclusiones clave para el estudio y (4) elaboración del informe de revisión se enfoca en resumir y presentar de manera clara

los hallazgos y conclusiones obtenidos durante el proceso de revisión. En las secciones siguientes, se ofrece una explicación detallada de cada una de las etapas realizadas.

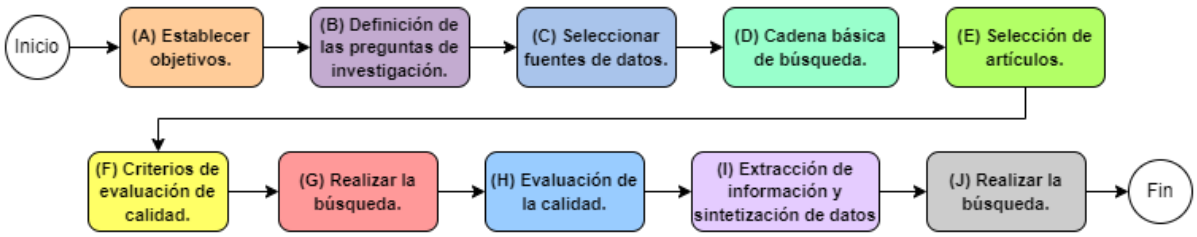

Figura 5. Etapas del proceso para el mapeo sistemático adaptado por los autores. Fuente : Propia.

1.2.1. Aplicación del enfoque GQM

A. Establecer Objetivos

Con el fin de garantizar adecuadamente este mapeo sistemático, se han establecido los siguientes Objetivos de Búsqueda (OB):

- **OB 1:** Caracterizar los modelos o estándares que utilizan algunos países de Europa y Latinoamérica frente al proceso de medición de la seguridad de la información mediante una revisión de literatura con el fin de conocer e identificar estos.

- **OB 2:** Analizar los diferentes enfoques de medición de la seguridad de la información utilizados en diversos sectores (por ejemplo, financiero, gubernamental, industrial) mediante la categorización de estos, para identificar buenas prácticas y desafíos comunes.

- **OB 3:** Establecer los lineamientos y/o estándares que debería tener un modelo de evaluación de la seguridad de la información basado en la caracterización de los modelos de seguridad de la información identificados con el fin de proponer parámetros para un nuevo modelo.

- **OB 4:** Recomendar las investigaciones encontradas acerca de los estándares y/o marcos de seguridad mediante la búsqueda exhaustiva realizada con el fin de proporcionar información relevante y actualizada a los interesados entre ellos organizaciones e investigadores.

Con estos objetivos fundamentan la búsqueda exhaustiva de información, facilitando el planteamiento de las siguientes (13) preguntas de investigación (PI) presentadas en la tabla 10, donde cada pregunta está mapeada a los objetivos planteados, junto a su respectiva motivación.

B. Definición de las preguntas de investigación

N°	Pregunta de investigación	Motivación	OB
PI1	¿Cuáles son las fortalezas y debilidades de los diferentes modelos o estándares utilizados en Europa y Latinoamérica para medir la seguridad de la información?	Identificar los puntos fuertes y débiles de los estándares existentes permitiendo comprender sus limitaciones y beneficios, lo que puede contribuir a mejorar los enfoques de seguridad de la información en estos territorios.	OB1
PI2	¿Cuáles son los principales modelos y/o estándares establecidos en los países de Europa y Latinoamérica en cuanto al proceso de medición de seguridad de la información?	Caracterizar y listar los modelos o estándares más relevantes en el proceso de medición de seguridad de la información.	OB1
PI3	¿En qué fuentes bibliográficas y en qué años se establecieron los instrumentos de medición de la seguridad de la información relacionados en las investigaciones encontradas?	Conocer las fuentes y el tiempo en que se originaron estos instrumentos proporcionando un contexto histórico y de origen con su evolución y aplicación actual.	OB1
PI4	¿Cuáles son las tendencias y los avances en cuanto a estándares de la seguridad de la información empleados por los diferentes países en Europa y Latinoamérica?	Comprender las tendencias y los avances permite identificar hacia dónde se dirige la seguridad de la información, proporcionando ideas valiosas para el desarrollo futuro en estas regiones.	OB1
PI5	¿Qué impacto tienen los modelos o estándares de seguridad de la información en la protección de los datos	Evaluar el impacto de estos modelos o estándares ayuda a entender su eficacia en la protección de datos además la	OB1

	y la ciberseguridad en algunos países de Europa y Latinoamérica?	prevención de amenazas, contribuyendo a mejorar la seguridad de la información.	
PI6	¿Cuáles son los principales enfoques y metodologías utilizados en el modelo de la evaluación de la seguridad de la información, efectivos y confiables?	Identificar los enfoques y metodologías efectivas y confiables para obtener las prácticas exitosas, mejorando así la seguridad de la información.	OB2
PI7	De acuerdo con lo investigado ¿Qué información importante se puede obtener de las prácticas exitosas de medición de la seguridad de la información en los diferentes sectores?	Extraer información valiosa de las prácticas exitosas permite generar conocimiento útil y aplicable en diversos sectores, contribuyendo a la mejora continua de la seguridad de la información en los diversos sectores.	OB2
PI8	¿Cuáles son las mejores prácticas identificadas en los diferentes modelos o estándares de seguridad de la información utilizados en algunos países de Europa y Latinoamérica?	Identificar las mejores prácticas proporciona ejemplos concretos que podrían servir como referencia y guía para mejorar la seguridad de la información en los diversos contextos.	OB2
PI9	¿Qué lineamientos y estándares son utilizados en los modelos de evaluación de la seguridad de la información encontrados en la caracterización utilizados en algunos países de Europa y Latinoamérica?	Conocer los lineamientos y estándares utilizados proporciona una base para entender los criterios que se aplican en la evaluación de la seguridad de la información, facilitando la identificación de áreas de mejora.	OB3
PI0	¿Cómo se podría adaptar el instrumento de evaluación de la seguridad de la información basado en la diferentes estándares y/o marcos de seguridad para evaluar la madurez y la efectividad de las medidas de seguridad implementadas en organizaciones?	Explorar la posibilidad de adaptar los instrumentos de evaluación existentes para medir la madurez y efectividad de las medidas de seguridad implementadas en organizaciones.	OB3
PI11	¿Cómo se abordan los principales requisitos y/o estándares del modelo de evaluación de la seguridad de la información en Europa y Latinoamérica?	Comprender cómo se abordan los requisitos y estándares principales proporciona información valiosa sobre el cumplimiento normativo y las prácticas adoptadas en diferentes regiones.	OB3
PI12	De acuerdo a lo investigado ¿Qué investigaciones abordan específicamente la evaluación de efectividad y eficacia de los estándares	Identificar investigaciones específicas sobre la evaluación efectiva de estándares de seguridad ofrece información crucial para	OB 4

	y/o marcos de seguridad en la protección de la información?	entender su impacto real en la protección de la información.	
PI13	Según los estudios encontrados ¿En qué año fue actualizada y mejorada la evaluación de la seguridad de la información en los diferentes países de Europa y Latinoamérica, ¿cuál fue el estudio?	Identificar los estudios que abordan la actualización y mejora de la evaluación de la seguridad de la información para comprender la evolución y los cambios de seguridad a lo largo del tiempo.	OB 4

Tabla 10. Preguntas de investigación. Fuente: Propia.

C. Seleccionar fuentes de datos

En la actualidad, se encuentran varios motores de búsqueda disponibles, no obstante, la elección del navegador adecuado depende en gran medida de las necesidades y preferencias del usuario. Algunos de los criterios que se toman en cuenta para elegir ciertos navegadores incluyen la calidad de los resultados de búsqueda, la interfaz de usuario, la velocidad de carga de las páginas, la privacidad y la seguridad. Con base en estos aspectos, optamos por los siguientes:

NOMBRES DE LOS MOTORES DE BÚSQUEDA BIBLIOGRÁFICA
Google Académico
IEEExplore
ScienceDirect

Tabla 11. Motores de Búsqueda. Fuente : Propia.

1.2.2. Definición en la búsqueda y estrategias de selección

D. Cadena básica de búsqueda

La cadena básica de búsqueda es una formulación cuidadosamente estructurada de términos clave y operadores lógicos que se utiliza al realizar consultas en motores de búsqueda en línea, ya sea para un mapeo sistemático o cualquier otro tipo de investigación. Esta combinación de elementos tiene como objetivo principal optimizar y dirigir la búsqueda hacia resultados específicos y relevantes a la consulta del usuario. Incluye la utilización de términos específicos relacionados con la temática de interés, el uso de comillas para buscar frases exactas, así como la incorporación de

operadores booleanos como AND y OR. Al personalizar la cadena de búsqueda, los usuarios pueden refinar su búsqueda y obtener resultados más precisos, mejorando la efectividad del proceso de obtención de información en la vastedad de la web.

Para desarrollar la cadena básica de búsqueda, se empleó la herramienta "Parsifal", la cual facilitó el análisis a través del enfoque "Picoc" (Población, Intervención, Comparación, Resultado, Contexto). Este método permitió identificar de manera sistemática los términos clave necesarios para la construcción de la cadena de búsqueda. Las figuras a continuación ilustran el proceso, evidenciando cómo la herramienta y el enfoque Picoc fueron fundamentales para la identificación y selección de los elementos esenciales que conforman una cadena de búsqueda.

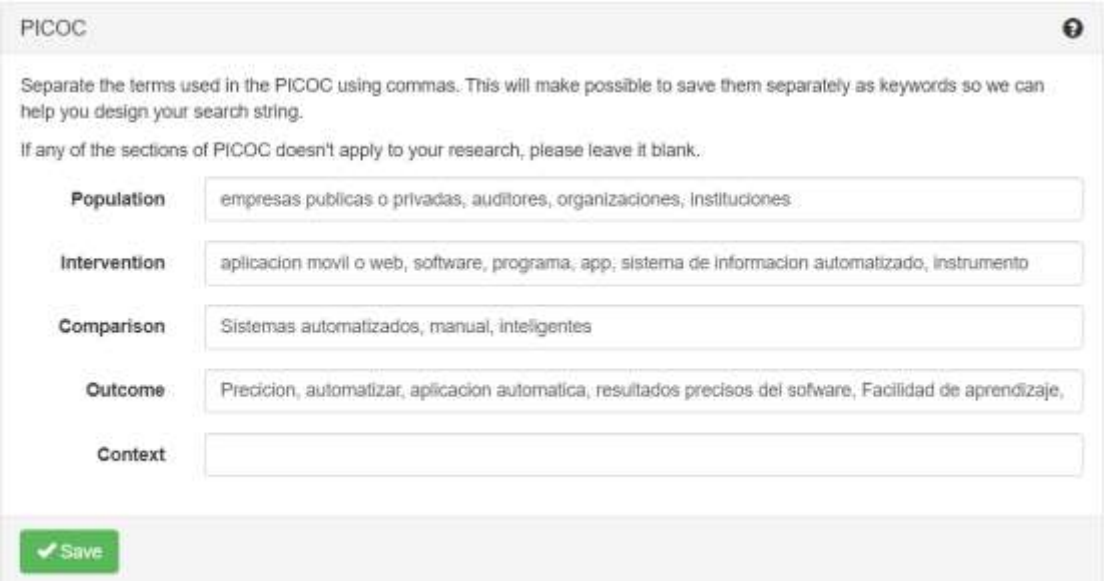

Figura 6. Definición de palabras clave y sinónimos PICOC. Fuente: [93]

Keywords and Synonyms

To edit or remove a certain keyword or synonym you may click on it's description to enable the field.

Keyword	Synonyms	Related to	
Facilidad de aprendizaje		Outcome	
Precicion		Outcome	
Sistemas automatizados		Comparison	
aplicacion automatica		Outcome	
aplicacion movil o web		Intervention	
app		Intervention	
auditores		Population	
automatizar		Outcome	
disminucion de tiempo para la evaluacion de la seguridad de la evaluacion		Outcome	
empresas		Population	

Figura 7. Palabras clave con sus sinónimos. Fuente. [93].

Al utilizar la herramienta se generó la siguiente cadena básica de búsqueda, la cual tuvo algunas modificaciones y se tradujo al idioma inglés, siendo la siguiente:

- ("auditors" OR "public or private companies" OR "institutions" OR "organizations") AND ("mobile or web application" OR "app" OR "instrument" OR "program" OR "automated information system" OR "software ") AND ("Automated systems" OR "intelligent" OR "manual") AND ("Easy to learn" OR "Precise" OR "automatic application" OR "automate" OR "decreased time for security evaluation of the evaluation" OR "optimization in results" OR "automated results" OR "precise software results")

Después de realizar la búsqueda y no obtener los resultados esperados con la cadena básica principal, se le realizaron algunos ajustes en la misma, creando así las siguientes cadenas de búsqueda para aplicar en los motores de búsqueda previamente seleccionados.

- "Auditors" OR "public or private companies" AND "Information Security Management System" OR "ISMS" OR "ISO/IEC 27001 Standard" OR "ISO 27001" AND "assessment instrument" OR "instrument" OR "Automated

information system" OR “Model” or “Framework” OR "Intelligent systems" AND "Ease of learning" OR "automated results" OR "optimization in results" AND "Mobile” OR “web application" AND "decreased time for evaluation security evaluation"

- "Information Security Management System" OR "ISO/IEC 27001 Standard" AND "Auditors" OR "public or private companies" AND "Intelligent systems" OR "framework" AND "Mobile or web application" AND "Ease of learning" or "automated results" AND "decreased time for evaluation security evaluation"

- "Auditors" OR "public or private companies" AND "Information Security Management System" OR "ISO 27001” AND "assessment instrument" OR "Automated information system" OR "Intelligent systems" AND "Mobile or web application" AND "Ease of learning" OR "automated results" OR "optimization in results" AND "decreased time for evaluation security evaluation" AND “Model” or “Framework”

E. Selección de artículos

Para garantizar la amplitud en la selección de artículos, se implementó un enfoque de dos niveles: (Nivel 1) se evaluaron los títulos de los artículos, (Nivel 2) análisis más detallado de los resúmenes o abstract, introducciones y conclusiones. Para realizar esta revisión se debió identificar los artículos que cumplían al menos con uno de los criterios de inclusión detallados en la Tabla 12, excluyendo aquellos que satisfacían alguna condición de la Tabla 13, asegurando así la relevancia y calidad de los estudios primarios. Para garantizar los objetivos planteados, se aplicó un (Nivel 3), que consistió en una revisión minuciosa del texto completo. Esto nos garantiza una selección rigurosa y precisa de la literatura necesaria para alcanzar los objetivos propuestos en el estudio.

ID	CRITERIOS DE INCLUSIÓN (CI)
CI1	Artículos relacionados con la seguridad de la información de la norma iso 27001
CI2	Artículos en inglés y español
CI3	Artículos que estén dentro el periodo 2020-2024
CI4	Estudios que hayan sido publicados en trabajos de pregrado y de postgrado.

Tabla 12. Criterios de Inclusión. Fuente: Propia.

ID	CRITERIOS DE EXCLUSIÓN (CE)
CE1	Artículos o estudios duplicados
CE2	Artículos o estudios que abordan superficialmente el tema o no aborden el tema de investigación.
CE3	Estudios cuyo contenido no es accesible al tema
CE4	Estudios que tengan una fecha inferior a 2020
CE5	Estudios diferentes al tema inglés o español

Tabla 13. Criterios de Exclusión. Fuente: Propia.

F. Criterios de evaluación de Calidad

Con el fin de poder medir y determinar la calidad y grado de pertinencia con respecto al Sistema de Gestión de Seguridad de la Información ISO 27001, se ha formulado un cuestionario que consta de 12 preguntas con un manejo de un sistema de calificación de puntos (1-0-1), en donde 1 vendría siendo SI, donde 0 es parcialmente y -1 siendo NO. Así mismo cada artículo podrá tener una calificación superior de hasta 12 o una calificación menor de -12, además luego de obtener las puntuaciones totales de los artículos podemos escoger los que nos darán una mayor relevancia y soporte en la investigación.

N°	Area	Criterio	Puntuacion de la respuesta		
			1	0	-1
C1	Motivacion	El estudio ofrece una descripcion sobre las razones de la investigacion en la tematica propuesta.	SI	Parcialmente	NO
C2	Planificacion	El estudio aplica una estructura o planificación de procesos para desarrollo de la investigación	SI	Parcialmente	NO
C3	Tematica	El estudio se enfoca en tecnicas, modelos o intrumentos de la seguridad de la informacion basado en la norma ISO 27001	SI	Parcialmente	NO
C4		En el estudio ofrece una descripcion clara de la problematica abordada.	SI	Parcialmente	NO
C5		El estudio ofrece una descripcion clara de las soluciones o tecnicas abordadas en el tema.	SI	Parcialmente	NO
C6	Solucion	La solución propuesta se ha materializado en modelos, patrones, prototipos, etc.	SI	Parcialmente	NO
C7		El estudio describe tecnologías o tecnicas utilizadas en la solución planteada	SI	Parcialmente	NO
C8		La solución propuesta del estudio ha sido probada dentro de entornos reales	SI	Parcialmente	NO
C9	Dificultades	El estudio describe limitaciones de la investigación y análisis de los resultados	SI	Parcialmente	NO
C10		El estudio describe problemáticas ligadas a la solución planteada	SI	Parcialmente	NO
C11	Resultados y Recomendaciones	El estudio expone de manera clara y detallada los resultados y concluciones obtenidas.	SI	Parcialmente	NO
C12		El estudio describe trabajos futuros o alternativas de investigacion.	SI	Parcialmente	NO

Figura 8. Criterios de evaluación. Fuente: Propia.

1.2.3. Realizar la Revisión

G. Realizar las búsquedas

Después de varias modificaciones de 10 iteraciones de búsqueda para cada cadena de búsqueda en las bases de datos preseleccionadas: Google Scholar, IEEE Xplore y ScienceDirect. Dada la variedad de opciones y configuraciones en cada base de datos, se adaptaron las cadenas de búsqueda iniciales para optimizar los resultados obtenidos. En la Tabla 14 se detallan las diversas adaptaciones realizadas a la cadena original para mejorar la precisión de los resultados. El recuento completo de los hallazgos se presenta en la Tabla 15, donde se incluye la cantidad de artículos descartados durante esta fase inicial del proceso de revisión.

N°	Cadena	Fuente

1	("Persons" OR "public" AND "private companies" OR "auditors using iso 27001 information security" OR "ISMS iso 27001" AND "Development of a "app mobile" OR "app web" OR "program" OR "software"")	Google Scholar
2	("Persons" OR "public" AND "private companies" OR "auditors using iso 27001 information security" AND "evaluation instrument iso 27001" OR "iso 27001" AND "Development of a "app mobile" OR "app web" OR "program" OR "software"")	IEEE Xplore
3	("evaluation instrument iso 27001" OR "iso 27001") AND ("Ease of learning" OR "time" OR "automated results")	ScienceDirect
4	("auditors" OR "companies" OR "institutions" OR "organizations") AND ("Information security management system" OR "ISMS") AND ("iso 27001 standard" OR "standard") AND (" assessment instrument" OR "iso 27001 standard software") AND ("Software development" OR "app" OR "program")	Google Scholar
5	("public companies" AND "private companies" OR "auditors using iso 27001 information security" AND "evaluation instrument iso 27001" OR "iso 27001" AND "Development of a "program" OR "software"")	IEEE Xplore
6	"Auditors" OR "companies" AND "Information Security Management System" OR "ISMS" AND "assessment instrument" OR "instrument" AND "Automated information system" AND "Intelligent systems" AND "Mobile or web application" AND "application"	ScienceDirect
7	"Auditors" OR "public or private companies" AND "Information Security Management System" OR "ISMS" OR "ISO/IEC 27001 Standard" OR "ISO 27001" AND "assessment instrument" OR "instrument" OR "Automated information system" OR "Model" or "Framework" OR "Intelligent systems" OR "Mobile" OR "web application" AND "Ease of learning" OR "automated results" OR "optimization in results" AND "decreased time for evaluation security evaluation"	Google Scholar
8	"Auditors" OR "public or private companies" AND "Information Security Management System" OR "ISO 27001" AND "assessment instrument" OR "Automated information system" OR "Intelligent systems" AND "Mobile or web application" AND "Ease of learning" OR "automated results" OR "optimization in results" AND "decreased time for evaluation security evaluation" AND "Model" or "Framework"	IEEE Xplore

9	"Information Security Management System" OR "ISO/IEC 27001 Standard" AND "Auditors" OR "public or private companies" AND "Intelligent systems" OR "framework" AND "Mobile or web application" AND "Ease of learning" or "automated results" AND "decreased time for evaluation security evaluation"	ScienceDirect
10	"Auditors" OR "public or private companies" AND "Information Security Management System" OR "ISMS" OR "ISO/IEC 27001 Standard" OR "ISO 27001" AND "assessment instrument" OR "instrument" OR "Automated information system" OR "Model" or "Framework" OR "Intelligent systems" AND "Ease of learning" OR "automated results" OR "optimization in results" AND "Mobile" OR "web application" AND "decreased time for evaluation security evaluation"	Google Scholar

Tabla 14. Cadenas básicas de búsqueda. Fuente: Propia.

BASES DE DATOS	ESTUDIOS			
	ENCONTRADOS	MÁS RELEVANTES	N° REPETIDOS	PRIMARIOS
GOOGLE ACADÉMICO	635	196	11	37
IEEExplore	781	264	0	35
ScienceDirect	604	175	4	20
Total	2.020	635		92

Tabla 15. Resultados de la búsqueda. Fuente: Propia.

La investigación se inició utilizando Google Académico como fuente principal de datos, lo que resultó en la recopilación de algunos resultados, con un total de 635 artículos, siendo IEEExplore con mayor resultado 781 y ScienceDirect 604 artículos, aunque la mayoría de estos no fueron seleccionados por el criterio CE2.

Sin embargo, se observó que 17 de estos artículos cumplían con al menos un criterio de inclusión (CI), pero no satisfacían ninguno de los criterios de exclusión (CE). Por otra parte, se excluyeron un total de 44 artículos debido a no cumplir con los requisitos establecidos.

La lista completa de los artículos primarios seleccionados se encuentra detallada en la tabla 16, con sus referencias correspondientes para permitir a los lectores profundizar en el contenido si así lo desean.

ID	ARTÍCULO	AÑO
A1	Create your own MUSE: A method for updating security level evaluation instruments [6]	2023
A2	Adaptation and application of the IEEE 2413-2019 standard security mechanisms to IoMT systems [15]	2022
A3	Information System Security Analysis of XYZ Company Using COBIT 5 Framework and ISO 27001:2013 [18]	2023
A4	A Dynamic and Adaptive Cybersecurity Governance Framework [22]	2023
A5	Modeling the information security management system (ISMS) of a medical organization [26]	2020
A6	The audit method of enterprise's Information security [31]	2020
A7	CAESAR8: An agile enterprise architecture approach to managing information security risks [40]	2022
A8	Information Systems Security Governance Evaluation in the Portuguese Local Public Administration [41]	2020
A9	On the Value of Information Security Policies in Organizations [43]	2023
A10	Evaluating the Impact of Metric-based Security Tools on Company Performance and Decision-making [44]	2023
A11	The Importance of Risk Management: What is Missing in ISO Standards? [45]	2021
A12	Semantic Analysis of ISO/IEC 27000 Standard Series and NIST Cybersecurity Framework to Outline Differences and	2022

	Consistencies in the Context of Operational and Strategic Information Security [27]	
A13	A novel approach for information security risk assessment maturity framework based on ISO 27001 [19]	2020
A14	NPP: A New Privacy-Aware Public Auditing Scheme for Cloud Data Sharing with Group Users [50]	2022
A15	System Analysis and Error Detection: An approach towards server monitoring using Natural Language Processing [52]	2020
A16	CIPPPA: Conditional Identity Privacy-Preserving Public Auditing for Cloud-Based WBANs Against Malicious Auditors [53]	2021
A17	Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A Web Mining-Based Analysis [54]	2021
A18	Assessment of Information Security Management System: A Case Study of Data Recovery Center in Ministry XYZ [55]	2020
A19	Organisational Information Security Maturity Assessment Based on ISO 27001 and ISO 27002 [56]	2020
A20	Análisis Preliminar De La Ciberseguridad Asociada Al Sistema Financiero En Algunos Países De Latinoamérica Y La Contribución De La Informática Forense [59]	2021
A21	Contexto de la seguridad ciudadana en América Latina y el Caribe: revisión de literatura (2007- 2017) [58]	2018
A22	Normas y estándares en auditoría: una revisión de su utilidad en la seguridad informática [60]	2023
A23	Técnicas Y Métodos Documentales En Investigación Científica [61]	2021

Tabla 16. Artículos primarios producto de la búsqueda. Fuente : Propia.

H. Evaluación de calidad

En la actualidad, caracterizada por la abundancia de información, la evaluación de calidad desempeña un papel crucial en el ámbito científico y académico, Este proceso no solo garantiza la integridad de la investigación, sino que también influye directamente en el desarrollo del conocimiento.

La implementación de criterios para la evaluación de calidad se realiza como un pilar esencial en la toma de decisiones informadas. Al aplicar criterios claros y objetivos, se busca no solo asegurar la aceptación a estándares de calidad preestablecidos, sino también proporcionar una base sólida para la selección de información. Esta rigurosidad en la evaluación contribuye a la creación de un entorno en el que la información utilizada para la investigación y desarrollo del conocimiento sea confiable y asertiva.

Además, la evaluación basada en criterios no solo se limita a la validación, sino que también se convierte en una herramienta dinámica para la mejora continua. La identificación de áreas de optimización, En resumen, la evaluación de calidad no solo actúa como un filtro, sino como un impulsor constante hacia la excelencia y la mejora continua en la era de la información.

Artículos	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	Total	Referencia
A1	1	0	-1	1	1	-1	0	0	1	0	1	1	4	[1]
A2	1	1	-1	1	0	-1	1	-1	1	0	1	1	4	[2]
A3	1	1	-1	1	1	-1	1	-1	-1	-1	1	-1	0	[3]
A4	1	0	-1	0	1	0	1	-1	1	1	1	1	5	[4]
A5	0	0	-1	1	1	1	1	-1	-1	-1	1	0	1	[5]
A6	1	1	1	-1	1	-1	1	0	1	1	1	1	7	[6]
A7	1	1	-1	-1	-1	-1	1	1	-1	-1	1	-1	-2	[7]
A8	1	-1	1	1	1	-1	1	-1	1	1	1	-1	4	[8]
A9	1	1	-1	-1	1	1	-1	-1	1	1	1	-1	2	[9]
A10	1	1	1	1	1	-1	-1	1	1	-1	1	1	6	[10]
A11	1	1	-1	1	1	1	1	0	0	0	1	-1	5	[11]
A12	1	1	-1	1	1	-1	1	-1	0	1	1	1	5	[12]
A13	0	0	-1	1	0	1	-1	1	0	-1	1	0	1	[13]
A14	1	1	-1	1	1	1	-1	1	-1	-1	1	-1	2	[14]
A15	1	1	-1	1	1	1	-1	1	1	0	1	1	7	[15]
A16	1	1	-1	1	1	1	-1	-1	0	0	1	-1	2	[16]
A17	1	1	-1	1	1	1	-1	-1	1	-1	1	1	4	[17]
A18	-1	1	0	0	1	1	1	1	1	1	1	1	8	[18]
A19	1	1	1	1	1	1	1	1	-1	-1	1	0	7	[19]
A20	1	1	1	1	1	1	-1	1	-1	-1	1	-1	4	[20]
A21	1	1	0	-1	1	1	-1	1	-1	-1	1	1	3	[21]
A22	1	1	-1	1	1	1	1	1	0	1	1	1	9	[22]
A23	1	1	-1	0	1	1	1	-1	1	0	1	0	5	[23]
A24	1	1	1	-1	1	1	-1	-1	-1	-1	1	-1	0	[24]

A25	1	1	0	-1	1	1	1	-1	-1	0	1	1	4	**[25]**
A26	1	1	0	0	1	1	-1	1	1	1	1	1	8	**[26]**
A27	1	0	1	1	0	-1	1	-1	1	-1	1	1	7	**[27]**
A28	1	1	1	1	1	0	-1	1	-1	-1	1	0	4	**[28]**
A29	1	1	1	1	1	1	-1	1	-1	-1	1	-1	4	**[29]**
A30	1	1	1	1	1	0	-1	1	0	-1	1	0	5	**[30]**
A31	1	1	-1	1	1	1	1	0	0	1	1	1	8	**[31]**
A32	0	-1	-1	0	1	-1	-1	0	-1	0	1	1	-2	**[32]**
A33	1	1	-1	1	1	1	-1	1	-1	-1	1	-1	2	**[33]**
A34	0	1	-1	1	1	0	-1	1	-1	-1	1	-1	0	**[34]**
A35	1	-1	-1	1	1	1	0	1	-1	-1	-1	-1	-1	**[35]**
A36	1	1	-1	1	1	1	-1	1	-1	-1	-1	-1	0	**[36]**
A37	1	1	1	1	1	-1	-1	1	1	0	1	-1	5	**[37]**
A38	0	1	-1	0	1	1	-1	1	-1	-1	1	1	2	**[38]**
A39	0	0	-1	1	1	1	1	1	0	1	1	0	6	**[39]**
A40	0	1	-1	1	1	-1	1	1	1	1	1	1	7	**[40]**
A41	0	1	-1	1	1	1	-1	1	1	1	1	1	7	**[41]**
A42	1	1	-1	1	1	-1	1	-1	-1	-1	-1	-1	-2	**[42]**
A43	0	1	-1	1	1	1	0	1	1	1	1	1	8	**[43]**
A44	1	1	0	1	1	1	0	1	1	1	1	1	10	**[44]**
A45	0	1	-1	1	1	1	-1	1	1	1	1	1	7	**[45]**
A46	1	0	-1	0	1	1	-1	1	-1	-1	1	-1	0	**[46]**
A47	1	0	-1	1	0	-1	-1	-1	-1	1	1	1	0	**[47]**
A48	1	1	-1	1	1	0	-1	-1	-1	-1	1	-1	-1	**[48]**
A49	1	1	0	1	1	0	0	1	-1	0	1	0	5	**[49]**
A50	1	1	0	1	1	1	1	1	-1	1	1	-1	7	**[50]**
A51	1	1	-1	1	1	-1	1	-1	1	1	1	1	6	**[51]**

A52	1	0	-1	1	1	0	1	1	1	1	1	1	8	**[52]**
A53	1	0	-1	1	1	1	1	1	0	1	1	1	8	**[53]**
A54	1	1	1	1	1	1	1	0	0	1	1	1	10	**[54]**
A55	1	0	1	1	1	1	1	1	0	1	1	1	9	**[55]**
A56	1	1	1	1	1	1	1	1	1	0	1	-1	8	**[56]**
A57	1	1	1	1	1	0	0	-1	1	0	1	0	6	**[57]**
A58	1	0	-1	1	1	0	1	1	0	1	1	1	7	**[58]**
A59	1	1	0	1	1	0	1	1	0	0	1	1	8	**[59]**
A60	1	1	1	1	1	1	1	0	0	1	1	1	10	**[60]**
A61	1	0	-1	1	1	0	1	1	1	1	1	1	8	**[61]**

Tabla 17. Tabla de evaluación de calidad de los artículos primarios. Fuente: Propia.

I. Extracción de información y sintetización de datos

La sigla PICOC refleja los elementos fundamentales de una pregunta de investigación: Participantes, Intervenciones, Comparaciones, Resultados y Contexto. La extracción de datos y la revisión de palabras clave se centran en la precisa identificación y selección de estudios que cumplen con los criterios establecidos en cada uno de estos elementos.

En el contexto de la investigación, la extracción de datos y la revisión de palabras clave, elementos clave de la metodología PICOC, son esenciales para identificar estudios relevantes. La extracción de datos implica revisar y extraer información específica de los estudios identificados, como datos demográficos, detalles de intervenciones y comparaciones entre grupos. La síntesis de datos permite condensar la información de manera coherente, ofreciendo una visión integrada de la investigación revisada. En conjunto, estos pasos aseguran una base sólida y estructurada, fundamental para la calidad y relevancia de los estudios seleccionados.

			PALABRAS CLAVE						
ID	TIPO	AÑO	P	I	C	O	C	PUBLICADO EN	NACIONALIDAD
A1	Artículo	2023	X		X	X		Elsevier BV	Estonia
A2	Artículo	2022	X	X	X	X		Elsevier BV	España
A3	Artículo	2023	X		X	X		Iopscience	Indonesia
A4	Artículo	2023	X		X	X		mdpi	Ethiopia
A5	Artículo	2020	X		X	X		E3S Web of Conferences	Rusia
A6	Artículo	2020	X		X	X		ICEMIS	Kazajstán
A7	Artículo	2022	X			X		Elsevier	Switzerland
A8	Tesis	2020	X					proquest	Portugal
A9	Tesis	2023	X		X	X		wu	Vienna
A10	Proyecto Grado	2023	X		X	X		eric lynn david	Estados Unidos
A11	Artículo	2021	X		X	X		onlinelibrary.wiley.	Países Bajos
A12	Artículo	2022	X		X			Medicon Engineering Themes	Alemania
A13	Tesis	2020	X	X	X	X		Corvinus	Hungría
A14	Artículo	2022			X	X		Ieeexplore	China
A15	Artículo	2020			X	X		Ieeexplore	India
A16	Conference	2021			X	X		Ieeexplore	China
A17	Artículo	2021	X			X		Ieeexplore	Alemania
A18	Conference	2020	X		X			Ieeexplore	Indonesia
A19	Conference	2020	X					Ieeexplore	Bulgaria
A20	Artículo	2021	X	X	X	X		Cuaderno De Investigaciones Semilleros Andina	LatinoAmérica

A21	Artículo	2018	X		X	X		ESMIC sello editorial	México
A22	Artículo	2023	X	X		X		Revista Científica PENTACIENCIAS	Alemania
A23	Artículo	2021	X	X	X	X		Revista Española de Documentación Científica	España

Tabla 18. Tabla de tipo de artículos y evaluación de las palabras claves. Fuente Propia.

1.2.4. Informe de la Revisión

J. Análisis de resultados

A continuación, se presentan los resultados obtenidos para cada una de las preguntas de investigación definidas en el mapeo sistemático.

1. **¿Cuáles son las fortalezas y debilidades de los diferentes modelos o estándares utilizados en Europa y Latinoamérica para medir la seguridad de la información?**

La comparación entre modelos y estándares específicos se basa en la información disponible en los artículos revisados, destacando tanto las fortalezas como las debilidades de los enfoques existentes.

Fortalezas:

- Algunos artículos apoyados en la ISO/IEC 27001 dicen que los modelos abordados en sus estudios son flexibles, pero deberían poder abordar dimensiones específicas y extensibles para abordar diferentes espacios y obtener mejores resultados en su aplicación.

- Algunos artículos basados en La ISO/IEC 27001 se basan en un ciclo continuo de mejora, que involucra la identificación de activos, la evaluación de riesgos, la aplicación de controles y revisiones periódicas para perfeccionar los sistemas de seguridad.

Artículos: A1, A7, A5, A14, A2, A10, A12.

Debilidades:

- Algunos artículos resaltan la importancia de la gestión de riesgos, sugiriendo que podría haber deficiencias en las normas ISO en este aspecto.

- La evaluación del impacto de las herramientas de seguridad basadas en métricas en el desempeño y la toma de decisiones destaca desafíos potenciales en la implementación práctica.

- Diferentes modelos y estándares basados en los artículos tienden a presentar una mala adaptación lo que puede generar una satisfacción menor en contextos específicos.

Artículos: A11, A3, A19, A18, A17, A8, A13, A15.

2. **¿Cuáles son los principales modelos y/o estándares establecidos en los países de Europa y Latinoamérica en cuanto al proceso de medición de seguridad de la información?**

Modelos - Estándares	Descripción	Artículos
ISO/IEC 27001	Se encuentra presente en múltiples artículos, destacando su prominencia como el estándar principal para la gestión de la seguridad de la información en ambas regiones.	A1, A9, A5, A17
Normativas y regulaciones específicas	Se identifican normativas específicas que complementan o influencian la aplicación de estándares.	A2, A16, A15, A12, A11

Marco de evaluación de riesgos	Artículos que destacan la importancia de modelos específicos de evaluación de riesgos.	A13, A19, A10, A7, A4
Auditoría y evaluación de sistemas de gestión	Existen estudios dedicados a métodos de auditoría y evaluación de sistemas de gestión de seguridad.	A6, A18, A3, A8, A14

Tabla 19. Principales modelos y/o estándares establecidos en los países de Europa y Latinoamérica Fuente: Propia.

3. **¿Cuáles son las fuentes bibliográficas y los años de publicación en los que se originaron los instrumentos de medición de seguridad de la información abordados en las investigaciones encontradas?**

Las fuentes bibliográficas y los años de publicación de los instrumentos de medición de seguridad de la información abordados en las investigaciones encontradas son variadas. Al centrar en la utilidad de las normas y estándares en auditorías informáticas, sin especificar fuentes específicas [60]. Al abordar las técnicas y métodos documentales en investigación científica, sin mencionar instrumentos de medición específicos [61].

4. **¿Cuáles son las tendencias y los avances en cuanto a estándares de la seguridad de la información empleados por los diferentes países en Europa y Latinoamérica?**

Tendencia o Avance	Artículos
La norma ISO/IEC 27001 es una tendencia destacada en la gestión de la seguridad de la información. Su adopción se evidencia en varios artículos, subrayando su relevancia y eficacia en diversos contextos organizacionales y regionales.	A1, A7, A12, A17.
Tendencia muy alta hacia métodos innovadores en la evaluación y gestión de la seguridad de la información.	A8.
Tendencia elevada hacia la adopción holística de múltiples estándares para poder abordar la seguridad de la información.	A1, A7.
Indican un enfoque creciente en la evaluación de la madurez de la seguridad de la información, destacando la importancia de obtener y aplicar una mejora continua.	A12, A19.

tendencia hacia la exploración de normativas y estándares específicos a nivel local.	A8.

Tabla 20. Tendencias empleadas en los países de Europa y Latinoamérica Fuente: Propia.

5. **¿Qué impacto tienen los modelos o estándares de seguridad de la información en la protección de los datos y la ciberseguridad en algunos países de Europa y Latinoamérica?**

Los estándares de seguridad de la información, tales como ISO/IEC 27001, COBIT y NIST, generan un impacto significativo en la protección de datos y la ciberseguridad tanto en Europa como en Latinoamérica. Su influencia radica en establecer estructuras sólidas para la gestión de la seguridad de la información, lo que ayuda a mejorar las prácticas de protección de datos y a fortalecer las defensas contra amenazas cibernéticas en estas regiones. Mientras que en Europa la adopción ha sido más amplia, en Latinoamérica, aunque puede variar, la integración de estos estándares ha contribuido a elevar el nivel de seguridad de la información en diversas organizaciones. Esto ha llevado a una mayor conciencia sobre la seguridad de los datos y ha mejorado la preparación para enfrentar desafíos cibernéticos de manera más efectiva en la región.

El impacto de modelos o estándares de seguridad de la información en la protección de los datos y la ciberseguridad en algunos países de Europa y Latinoamérica pueden ser considerables:

- **Cumplimiento normativo:** La implementación de estos estándares asegura que las organizaciones cumplan con regulaciones y leyes de protección de datos, como el GDPR en Europa o leyes de privacidad en América Latina, lo que evita sanciones legales y asegura la integridad de los datos personales.

- **Mejora en la gestión de riesgos:** Estos estándares proveen marcos sólidos para identificar, evaluar y mitigar riesgos en seguridad de la información. Esto fortalece las defensas contra amenazas cibernéticas y reduce la probabilidad de sufrir ataques o violaciones de datos.

- **Fortalecimiento de prácticas de seguridad:** Promueven la adopción de buenas prácticas en seguridad de la información, ofreciendo un marco reconocido a nivel internacional que establece estándares para la gestión de la seguridad de los datos.

- **Mejora continua:** Fomentan la evolución y adaptación constante ante las cambiantes amenazas y desafíos en ciberseguridad. Esto permite una mejora continua en las defensas y estrategias de protección de datos.

- **Confianza y credibilidad:** La implementación de estos estándares ayuda a generar confianza tanto internamente, entre los empleados y la organización, como externamente, entre los clientes y socios comerciales, al demostrar un compromiso sólido con la seguridad de los datos.

- **Reducción de riesgos financieros:** Al prevenir violaciones de datos y ataques cibernéticos, se reducen los riesgos financieros asociados con multas regulatorias, pérdida de clientes y daños a la reputación de la organización.

6. **¿Cuáles son los principales enfoques y metodologías utilizados en el modelo de la evaluación de la seguridad de la información, efectivos y confiables?**

Varios enfoques y metodologías destacan como efectivos y confiables en la evaluación de la seguridad de la información. La implementación de la norma ISO/IEC 27001 se presenta como un marco estructurado para establecer y mejorar sistemas de gestión de seguridad. Se emplearon diversas metodologías, como la implementación paso a paso de la norma, evaluación de riesgos estándar, modelos de madurez, enfoques ágiles, métodos innovadores, integración de estándares y auditorías de privacidad. Se subraya la importancia crítica de la evaluación de riesgos y la gestión proactiva para abordar los desafíos de seguridad. Como enfoques se pueden reflejar la diversidad de estrategias confiables y efectivas, utilizando enfoques como casos de estudio detallados, análisis cualitativos de contenido para identificar

patrones y desafíos, comparaciones entre casos, auditorías para evaluar la conformidad directa, desarrollo de marcos específicos y seguimiento continuo para evaluar la sostenibilidad y mejora.

7. **De acuerdo con lo investigado ¿Qué información importante se puede obtener de las prácticas exitosas de medición de la seguridad de la información en los diferentes sectores?**

Las prácticas exitosas de medición de seguridad de la información en distintos sectores incluyen el énfasis en:

- **Adaptabilidad a los cambios tecnológicos:** La capacidad de ajustarse y evolucionar junto con las innovaciones tecnológicas es crucial. Los sistemas de seguridad deben ser flexibles para incorporar nuevas tecnologías y abordar las vulnerabilidades emergentes.

- **Modelos holísticos de gestión de riesgos:** Los enfoques exitosos consideran múltiples dominios de riesgo, integrando elementos técnicos, humanos, físicos y procesuales en la evaluación de la seguridad. La visión integral ayuda a comprender y abordar los riesgos de manera más completa.
- **Evaluación continua y mejora constante:** La evaluación periódica permite identificar deficiencias y áreas de mejora en los sistemas de seguridad. La mejora continua es esencial para mantenerse actualizado frente a las amenazas cambiantes y los nuevos desafíos.

- **Auditoría pública condicional:** Métodos como la auditoría pública condicional garantizan la integridad de los datos médicos subcontratados, permitiendo a terceros de confianza verificar periódicamente la integridad sin comprometer la privacidad de los usuarios.

- **Estándares internacionales como ISO/IEC 27001 e ISO/IEC 27002:** El uso de estándares reconocidos internacionalmente proporciona una estructura

sólida para desarrollar, implementar y mejorar los sistemas de gestión de seguridad de la información.

- **Integración de tecnologías avanzadas:** El empleo de tecnologías como blockchain y herramientas de criptografía fortalece la seguridad y privacidad de la información, ofreciendo resistencia contra auditores maliciosos y garantizando la protección de los datos en entornos de nube.

8. **¿Cuáles son las mejores prácticas identificadas en los diferentes modelos o estándares de seguridad de la información utilizados en algunos países de Europa y Latinoamérica?**

Las prácticas destacan la importancia de un enfoque equilibrado y adaptativo para abordar los desafíos de seguridad de la información, combinando aspectos estructurados con la flexibilidad necesaria para enfrentar un entorno en constante cambio. Las mejores prácticas identificadas en los diferentes modelos y estándares de seguridad de la información utilizados en algunos países son:

- **Implementación Estructurada:** Adoptar un enfoque paso a paso de la norma ISO/IEC 27001 para establecer y mejorar sistemas de gestión de seguridad.

- **Gestión Proactiva de Riesgos:** Priorizar la gestión proactiva de riesgos, identificando y abordando continuamente los riesgos de seguridad.

- **Evaluación Continua de la Madurez:** Realizar evaluaciones periódicas de la madurez de la seguridad para garantizar la mejora continua de los procesos.

- **Innovación en Métodos de Evaluación:** Incorporar métodos innovadores y creativos en la evaluación de la seguridad para una visión más completa.

- **Auditorías Conscientes de la Privacidad:** Realizar auditorías conscientes de la privacidad para evaluar la seguridad, especialmente en contextos de intercambio de datos en la nube.

9. **¿Qué lineamientos y estándares son utilizados en los modelos de evaluación de la seguridad de la información encontrados en la caracterización utilizados en algunos países de Europa y Latinoamérica?**

Los estándares y marcos de referencia utilizados en modelos de evaluación de seguridad de la información en Europa y Latinoamérica incluyen:

- **ISO/IEC 27001:** Establece requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI).
- **ISO/IEC 27002:** Ofrece directrices detalladas y controles para la implementación de medidas de seguridad.

- **COBIT (Control Objectives for Information and Related Technologies):** Proporciona un conjunto de mejores prácticas para el control y gobierno de la información tecnológica en las empresas.

- **NIST CSF (Framework for Improving Critical Infrastructure Cybersecurity):** Ofrece un marco para mejorar la ciberseguridad en infraestructuras críticas, brindando orientación para la gestión de riesgos.

Estos estándares y marcos se utilizan ampliamente para establecer, evaluar y mejorar los sistemas de gestión de seguridad de la información en organizaciones y entidades gubernamentales en varios países de Europa y Latinoamérica. Su aplicación busca garantizar la integridad, confidencialidad y disponibilidad de la información en entornos empresariales y gubernamentales.

10. **¿Cómo se podría adaptar el instrumento de evaluación de la seguridad de la información basado en la diferentes estándares y/o marcos de seguridad para evaluar la madurez y la efectividad de las medidas de seguridad implementadas en organizaciones?**

Los documentos sugieren la adaptación del instrumento de evaluación de seguridad de la información basado en estándares y marcos existentes. Esto incluye:

- **Identificación y Comprensión de Estándares Relevantes:** Seleccionar los estándares apropiados como ISO/IEC 27001, NIST Cybersecurity Framework, COBIT, entre otros, y comprender sus principios, requisitos y metodologías.

- **Desarrollo de Criterios de Evaluación Flexibles:** Crear criterios de evaluación que incorporen los elementos esenciales de estos estándares. Estos criterios deben ser adaptables para abarcar las diferentes dimensiones de la seguridad de la información.

- **Diseño de un Instrumento de Evaluación Integrador:** Desarrollar un instrumento o metodología que incluya preguntas o métricas que reflejen los requisitos y prácticas delineadas en los estándares seleccionados.

- **Aplicación Personalizada en Diversos Contextos:** Asegurar que este instrumento sea flexible y pueda aplicarse a diferentes contextos organizacionales, considerando las particularidades de cada sector o industria.

- **Evaluación Continua y Adaptativa:** Implementar el instrumento y revisarlo periódicamente para asegurar su relevancia y eficacia. Debe ser capaz de adaptarse a los cambios en la tecnología y en las amenazas de seguridad.

- **Enfoque en la Mejora Continua:** Utilizar los resultados de las evaluaciones para identificar áreas de mejora y fortalecer los controles de seguridad de manera proactiva.

11. **¿Cómo se abordan los principales requisitos y/o estándares del modelo de evaluación de la seguridad de la información en Europa y Latinoamérica?**

Para enfrentar los requisitos y estándares del modelo de evaluación de la seguridad de la información en Europa y Latinoamérica, se sugiere la adopción de un enfoque riguroso basado en la norma ISO/IEC 27001. Este planteamiento implica una cuidadosa identificación y clasificación de activos, combinada con una gestión

proactiva y continua de riesgos. La aplicación de controles de seguridad específicos se integra en un marco estructurado, mientras que la evaluación constante de la madurez de la seguridad se logra mediante la implementación de enfoques ágiles e innovadores. La estrategia abarca también la integración sinérgica con otros marcos y estándares relevantes, respaldada por auditorías conscientes de la privacidad para proporcionar un enfoque completo y adaptable. Este planteamiento demuestra un compromiso sólido con las prácticas recomendadas y los estándares internacionales, asegurando una gestión efectiva y evolutiva de la seguridad de la información en ambas regiones.

12. **De acuerdo con lo investigado ¿Qué investigaciones abordan específicamente la evaluación de efectividad y eficacia de los estándares y/o marcos de seguridad en la protección de la información?**

Algunas de las investigaciones abordan la evaluación de la efectividad y eficacia de estándares y marcos de seguridad en la protección de la información. Además, algunas se plantean en la idea de proporcionar una visión un poco más crítica sobre cómo estos elementos impactan el desempeño empresarial, la toma de decisiones y la adopción en diferentes contextos organizativos. Así también indican un enfoque innovador para actualizar los instrumentos de evaluación de seguridad, proporcionando una perspectiva detallada sobre las diferencias y consistencias en el contexto de la seguridad de la información operativa y estratégica.
Artículos relevantes en investigaciones abordadas : A1, A12, A10, A3, A17.

13. **¿Cuándo se llevó a cabo la actualización y mejora de la evaluación de la seguridad de la información en diversos países de Europa y Latinoamérica, y cuál fue el estudio específico que abordó este proceso según las investigaciones encontradas?**

Una revisión de la literatura sobre programas de seguridad ciudadana en América Latina y el Caribe encontró una falta de estudios, lo que dificulta el diseño y la implementación de políticas [58]. Se destacó la necesidad de mejorar la ciberseguridad en el sector financiero de América Latina, con enfoque en la

prevención y respuesta a las ciber amenazas [59]. Sin embargo, no se proporcionó información específica sobre el momento y la naturaleza de las actualizaciones de las evaluaciones de seguridad de la información en Europa y América Latina.

CAPÍTULO 2. HERRAMIENTA DIGITAL

2.1. METODOLOGÍA

Para el desarrollo de este proyecto se aplicaron las fases propuestas por el método científico en la ingeniería de software [92]. En la fase de exploración se aplicó el método de mapeo sistemático [90]. En la fase de desarrollo fue empleando Scrum como marco de trabajo Y para la fase de evaluación se aplicó el modelo de aceptación tecnológica TAM [91]. Según lo descrito en el capítulo anterior, Scrum se enfoca en la entrega iterativa e incremental de productos, permitiendo adaptarse rápidamente a los cambios y asegurando la satisfacción del cliente. Este enfoque es clave para lograr la entrega exitosa del proyecto final, ya que prioriza la colaboración entre los equipos, la retroalimentación continua y la producción de resultados funcionales en ciclos cortos de trabajo denominados Sprint.

Para el desarrollo se utilizará una metodología ágil, empleando el proceso Scrum como marco de trabajo. Según lo descrito en el capítulo anterior, Scrum se enfoca en la entrega iterativa e incremental de productos, permitiendo adaptarse rápidamente a los cambios y asegurando la satisfacción del cliente. Este enfoque es clave para lograr la entrega exitosa del proyecto final, ya que prioriza la colaboración entre los equipos, la retroalimentación continua y la producción de resultados funcionales en ciclos cortos de trabajo denominados Sprint.

Considerando que la finalidad del presente proyecto es la implementación de una Aplicación web basada en el estándar ISO/IEC 27001 para la gestión de la seguridad de la información en las organizaciones podemos decir que el proyecto es de tipo aplicada tecnológica. A Continuación, en la siguiente figura 9 se describen las fases de trabajo a seguir.

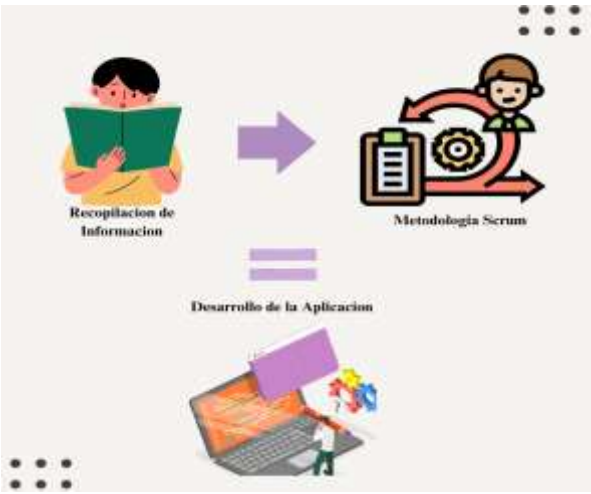

Figura 9. Metodología de Trabajo. Fuente: Propia.

2.1.1. Recopilación documental

Para la obtención de las fuentes de información fue necesario recurrir a 3 fuente de búsqueda como Google Académico, IEEExplore y ScienceDirect. para esta búsqueda que fue nuestro primer objetivo consistió en realizar un mapeo del tema a abordar como con palabras claves y operadores lógicos, también se sacaron los criterios de exclusión e inclusión.

Los criterios de inclusión aplicados fueron los siguientes:

- Artículos relacionados con la seguridad de la información de la norma iso 27001.
- Artículos en inglés y español.
- Artículos que estén dentro el periodo 2020-2024.
- Estudios que hayan sido publicados en trabajos de pregrado y de postgrado.

Los criterios de exclusión aplicados fueron los siguientes:

- Artículos o estudios duplicados.
- Artículos o estudios que abordan superficialmente el tema o no aborden el tema de investigación.
- Estudios cuyo contenido no es accesible al tema.
- Estudios que tengan una fecha inferior a 2020.
- Estudios diferentes al tema inglés o español.

2.1.2. Scrum

Es un marco de trabajo ágil utilizado principalmente en el desarrollo de software, aunque también se puede aplicar a una variedad de proyectos. Se basa en la colaboración entre los miembros del equipo para entregar productos de alta calidad de manera iterativa e incremental.

Estos procesos se componen en diferentes ciclos de trabajo llamados "Sprint", que suelen tener una duración fija de 2 a 4 semanas. Durante cada Sprint, el equipo se enfoca en entregar un conjunto de funcionalidades o "incremento de producto" que pueda ser potencialmente entregable al final del Sprint.

A continuación, se muestra el equipo de Scrum compuesto por roles definidos:

I. **Scrum Máster:** Es responsable de garantizar que el equipo comprenda y siga los principios y prácticas de Scrum. Facilita las reuniones y elimina los obstáculos que puedan afectar al equipo.
II. **Product Owner:** Representa los intereses de los stakeholders y es responsable de gestionar el Product Backlog, que es una lista priorizada de requerimientos del proyecto.
III. **Equipo de Desarrollo:** Son los encargados de realizar el trabajo para entregar los incrementos de producto.
IV. **El Product Backlog:** es una lista dinámica y priorizada de todos los requisitos, funcionalidades, mejoras y correcciones que se deben realizar en un producto. Es una herramienta fundamental en la metodología ágil Scrum y es mantenida por el Product Owner.

Scrum se caracteriza por reuniones regulares que ayudan a mantener la transparencia y la colaboración en el equipo:

- ★ **Sprint Planning:** Al comienzo de cada Sprint, el equipo selecciona las tareas a realizar y las planifica.

- ★ **Daily Standup:** Reunión diaria de 15 minutos en la que el equipo comparte qué hizo ayer, qué hará hoy y si tiene algún impedimento.

- ★ **Sprint Review:** Al final de cada Sprint, el equipo muestra al Product Owner y a los stakeholders el incremento de producto completado.

- ★ **Sprint Retrospective:** Reunión al final de cada Sprint en la que el equipo reflexiona sobre qué salió bien, qué se podría mejorar y define acciones para el próximo Sprint.

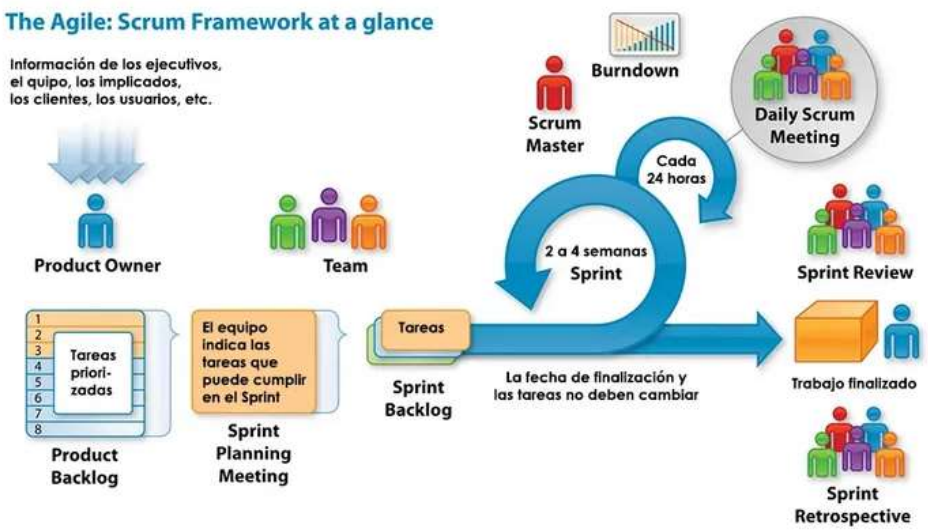

Figura 10. Diagrama de artefactos y reuniones en la metodología scrum. Fuente [86].

2.1.3. Diagrama de Bloques

A continuación, se presenta un enfoque de cada una de las fases de evolución del desarrollo de la aplicación.

Figura 11. Diagrama fases de evolución de la aplicación. Fuente: Propia.

2.1.4. Sprint 0

Inicialmente, se comienza con este sprint, que es la fase inicial del proyecto, en el cual se le dedica de una a dos semanas. Durante este tiempo, se prepara al equipo en los temas tecnológicos y metodológicos, garantizando un buen comienzo.

- **Especificación de Roles**

El presente proyecto inició formalmente en el mes de marzo de 2024. El equipo del proyecto y los roles se establecieron de la siguiente forma de acuerdo con la tabla 21, considerando los conocimientos que tiene cada integrante del equipo: Alejandro Alcaraz Gaviria responsable de atender el cliente y define el Product Backlog y prioriza las funcionalidades. De la misma manera el Scrum Máster encargado Sebastian Buesaco quien guía al equipo y por último los desarrolladores que está a cargo de los dos integrantes del equipo, quienes se encargan de diseñar y desarrollar la aplicación.

Rol	Responsabilidades	Personas
Product Owner	Representa las necesidades del cliente. Define el Product Backlog y prioriza las funcionalidades.	Alejandro Alcaraz Gaviria
Scrum Máster	Facilita las reuniones y eventos Scrum. Elimina obstáculos para el equipo.	Sebastian Buesaco

Desarrollador	Implementa las funcionalidades del Product Backlog. Realiza pruebas y asegura la calidad del código.	Equipo de trabajo

Tabla 21. Definición de roles del Proyecto. Fuente: Propia.

- **Definición del Producto**

El presente proyecto consiste en la aplicación web que facilita la implementación y el mantenimiento de un Sistema de Gestión de Seguridad de la Información (SGSI) en las organizaciones, cumpliendo con el estándar ISO/IEC 27001. El cual reduce el riesgo de ciberataques, gestiona de forma eficiente los procesos de seguridad de la información, para que los usuarios finales accedan a información de seguridad relevante.

- **Creación del Área de Trabajo**

Para el desarrollo de este proyecto fue necesario definir las herramientas que se van a utilizar en la aplicación web, con sus últimas versiones estables como se visualiza en la tabla 22.

	Descripción
Lenguaje de programación	Dart
Framework	Flutter
Base de datos	PostgreSQL

Tabla 22. Definición de roles del Proyecto. Fuente: Propia.

- **Product backlog o pila de producto**

Es una lista priorizada de funcionalidades que tu aplicación web debe incluir para cumplir con los requisitos del estándar ISO/IEC 27001. Esto servirá como base para el equipo de desarrollo para la programación web. En la siguiente tabla 23 se describen funcionalidades de la aplicación.

ID	COMO	QUIERO	PARA	PRIORIDAD
HU01	Empresa y Auditor	Identificar y organizar los activos de información.	Tener una visión clara de los activos de información que posee la organización y su valor para el negocio.	**2**
HU02	Auditor	Poder programar auditorías internas.	Evaluar el cumplimiento de la empresa con los controles de seguridad de ISO/IEC 27001.	**1**
HU03	Empresa y Auditor	Como Usuario (Auditor y Empresa), quiero poder iniciar sesión en la plataforma de manera segura con mis credenciales personales (usuario y contraseña).	Acceder de manera segura a las funcionalidades y recursos de la plataforma, según mis roles y responsabilidades como usuario.	**2**
HU4	Empresa	Poder subir y actualizar fácilmente documentos de políticas de seguridad, como políticas de acceso y uso aceptable,	Mantener la conformidad con ISO/IEC 27001.	**1**
HU05	Empresa y Auditor	Obtener información detallada sobre los activos de información de la empresa.	Tomar decisiones informadas sobre la gestión de los activos de información.	**2**
HU06	Empresa	Gestionar y tomar medidas para mitigar los riesgos identificados por el Auditor.	Garantizar la seguridad de la información y proteger los activos de la empresa ante posibles amenazas y vulnerabilidades.	**2**
HU07	Empresa	Evaluar la gravedad y el potencial de cada riesgo para la organización.	Priorizar la atención y los recursos para abordar los riesgos de seguridad de la información más importantes.	**3**
HU8	Empresa	Poder monitorear y supervisar el funcionamiento de todos los módulos de la plataforma de seguridad de la información.	Garantizar la efectividad y correcto funcionamiento de los sistemas de seguridad y protección de la información de la empresa.	**4**

HU9	Empresa y Auditor	Acceder al histórico de evaluaciones de seguridad realizadas en la plataforma para analizar tendencias, evaluar la efectividad de las medidas implementadas y realizar comparativas entre periodos.	Identificar patrones, evaluar el progreso en materia de seguridad y proporcionar recomendaciones basadas en el análisis histórico de evaluaciones.	**1**
HU10	Auditor	Registrar la información sobre los controles de seguridad, su funcionamiento y responsables.	Facilitar la gestión, auditoría y mejora continua de los controles de seguridad de la información.	**3**
HU11	Empresa	Tener acceso a los resultados de las pruebas de seguridad realizadas por el Auditor en la plataforma.	Evaluar la seguridad de la información y tomar decisiones informadas para mejorarla y mitigar riesgos.	**2**
HU12	Auditor	Poder acceder a los documentos relevantes de la empresa, como políticas de seguridad y registros de incidentes.	Realizar una revisión exhaustiva durante la auditoría.	**1**
HU13	Auditor	Generar informes detallados de auditoría que incluyan los resultados de las pruebas de seguridad, hallazgos identificados, recomendaciones de mejora y niveles de riesgo asociados.	Proporcionar información precisa y detallada a la empresa para que pueda tomar medidas efectivas para mejorar la seguridad de la información.	**4**
HU14	Empresa y Auditor	Permitir el registro de usuarios con los roles de Empresa y Auditor,	Asignarles permisos y funcionalidades específicas según su rol.	**1**
HU15	Auditor	Realizar la evaluación del cumplimiento de la norma ISO/IEC 27001	Identificar brechas y planificar acciones correctivas.	**4**
HU16	Usuario registrado (Empresa o Auditor),	Acceder únicamente a las funcionalidades correspondientes a mi rol	Evitar confusiones y asegurar una interacción fluida para el usuario.	**3**
HU17	Auditor	Visualizar un dashboard con indicadores clave de seguridad (número de riesgos, incidentes abiertos,	Tomar decisiones rápidas y basadas en datos.	**4**

		controles implementados)		
HU18	Empresa	Programar y gestionar revisiones periódicas de políticas, activos y controles	Mantener la seguridad de la información siempre actualizada.	**3**

Tabla 23. Historias de Usuario. Fuente: Propia.

- **Gestión visual**

Se utilizó la herramienta digital Kanban Flow para gestionar la metodología ágil en el proyecto. En el cual se documentará la evolución de las historias de usuario durante el sprint en curso. Este enfoque digital permitió facilitar la comunicación del equipo, la visualización del progreso y la gestión eficiente de las tareas en el contexto ágil del proyecto.

Figura 12. Gestión visual de Kanban Flow. Fuente [87].

- **Planificación de los sprint**

Como se muestra en la tabla anterior se definieron el orden de los sprint para él para el desarrollo, donde se sacaron 4 sprint definido por equipo SCRUM en conjunto, tomando en cuenta la dificultad de desarrollo, rendimiento del equipo y el número de tareas necesarias en cada ítem del product backlog, acordando así el tiempo en que se realizará en cada sprint. Con todo lo anterior se establecieron los siguientes sprints.

- **Sprint 1**

En la Tabla 24 se describen los 5 ítems del Product Backlog que son asignados al primer sprint, para lo cual se le asignó un tiempo estimado de 3 semanas por tener una dificultad alta.

ID	COMO	QUIERO	PARA
HU14	Empresa y Auditor	Permitir el registro de usuarios con los roles de Empresa y Auditor,	Asignarles permisos y funcionalidades específicas según su rol.
HU02	Auditor	Poder programar auditorías internas.	Evaluar el cumplimiento de la empresa con los controles de seguridad de ISO/IEC 27001.
HU9	Empresa y Auditor	Acceder al historial de evaluaciones de seguridad realizadas en la plataforma para analizar tendencias, evaluar la efectividad de las medidas implementadas y realizar comparativas entre periodos.	Identificar patrones, evaluar el progreso en materia de seguridad y proporcionar recomendaciones basadas en el análisis histórico de evaluaciones.
HU12	Auditor	Poder acceder a los documentos relevantes de la empresa, como políticas de seguridad y registros de incidentes.	Realizar una revisión exhaustiva durante la auditoría.
HU4	Empresa	Poder subir y actualizar fácilmente documentos de políticas de seguridad, como políticas de acceso y uso aceptable,	Mantener la conformidad con ISO/IEC 27001.

Tabla 24. Ítems del product backlog para el primer sprint. Fuente: Propia.

- **Sprint 2**

En la Tabla 25 se describen los 5 ítems del Product Backlog que son asignados al primer sprint, para lo cual se le asignó un tiempo estimado de 3 semanas por tener una dificultad media.

ID	COMO	QUIERO	PARA
HU01	Empresa y Auditor	Identificar y organizar los activos de información.	Tener una visión clara de los activos de información que posee la organización y su valor para el negocio.
HU03	Empresa y Auditor	Como Usuario (Auditor y Empresa), quiero poder iniciar sesión en la plataforma de manera segura con mis credenciales personales (usuario y contraseña).	Acceder de manera segura a las funcionalidades y recursos de la plataforma, según mis roles y responsabilidades como usuario.
HU05	Empresa y Auditor	Obtener información detallada sobre los activos de información de la empresa.	Tomar decisiones informadas sobre la gestión de los activos de información.
HU06	Empresa	Gestionar y tomar medidas para mitigar los riesgos identificados por el Auditor.	Garantizar la seguridad de la información y proteger los activos de la empresa ante posibles amenazas y vulnerabilidades.
HU11	Empresa	Tener acceso a los resultados de las pruebas de seguridad realizadas por el Auditor en la plataforma.	Evaluar la seguridad de la información y tomar decisiones informadas para mejorarla y mitigar riesgos.

Tabla 25. Ítems del product backlog para el segundo sprint. Fuente: Propia.

- **Sprint 3**

En la Tabla 26 se describen los 4 ítems del Product Backlog que son asignados al primer sprint, para lo cual se le asignó un tiempo estimado de 3 semanas por tener una dificultad alta.

ID	COMO	QUIERO	PARA
HU07	Empresa	Evaluar la gravedad y el potencial de cada riesgo para la organización.	Priorizar la atención y los recursos para abordar los riesgos de seguridad de la información más importantes.
HU10	Auditor	Registrar la información sobre los controles de seguridad, su funcionamiento y responsables.	Facilitar la gestión, auditoría y mejora continua de los controles de seguridad de la información.
HU16	Empresa	Acceder únicamente a las	Evitar confusiones y asegurar una

	o Auditor	funcionalidades correspondientes a mi rol	interacción fluida para el usuario.
HU18	Empresa	Programar y gestionar revisiones periódicas de políticas, activos y controles	Mantener la seguridad de la información siempre actualizada.

Tabla 26. Ítems del product backlog para el tercer sprint. Fuente: Propia.

- **Sprint 4**

En la Tabla 27 se describen los 5 ítems del Product Backlog que son asignados al primer sprint, para lo cual se le asignó un tiempo estimado de 3 semanas por tener una dificultad media.

ID	COMO	QUIERO	PARA
HU13	Auditor	Generar informes detallados de auditoría que incluyan los resultados de las pruebas de seguridad, hallazgos identificados, recomendaciones de mejora y niveles de riesgo asociados.	Proporcionar información precisa y detallada a la empresa para que pueda tomar medidas efectivas para mejorar la seguridad de la información.
HU8	Empresa	Poder monitorear y supervisar el funcionamiento de todos los módulos de la plataforma de seguridad de la información.	Garantizar la efectividad y correcto funcionamiento de los sistemas de seguridad y protección de la información de la empresa.
HU15	Auditor	Realizar la evaluación del cumplimiento de la norma ISO/IEC 27001	Identificar brechas y planificar acciones correctivas.
HU17	Auditor	Visualizar un dashboard con indicadores clave de seguridad (número de riesgos, incidentes abiertos, controles implementados)	Tomar decisiones rápidas y basadas en datos.

Tabla 27. Ítems del product backlog para el cuarto sprint. Fuente: Propia.

2.1.5. Modelamiento de la Base de Datos

Dado que Scrum promueve un enfoque iterativo e incremental, el modelamiento de la base de datos no es un paso aislado, sino una tarea que se aborda en los

primeros Sprint como parte del diseño inicial del sistema. Esto permite establecer una base sólida para el desarrollo técnico, adaptándose a los cambios y nuevos requisitos que puedan surgir a medida que avanza el proyecto. Es por eso que en la figura 13 podemos visualizar el modelamiento de la base de datos de la herramienta.

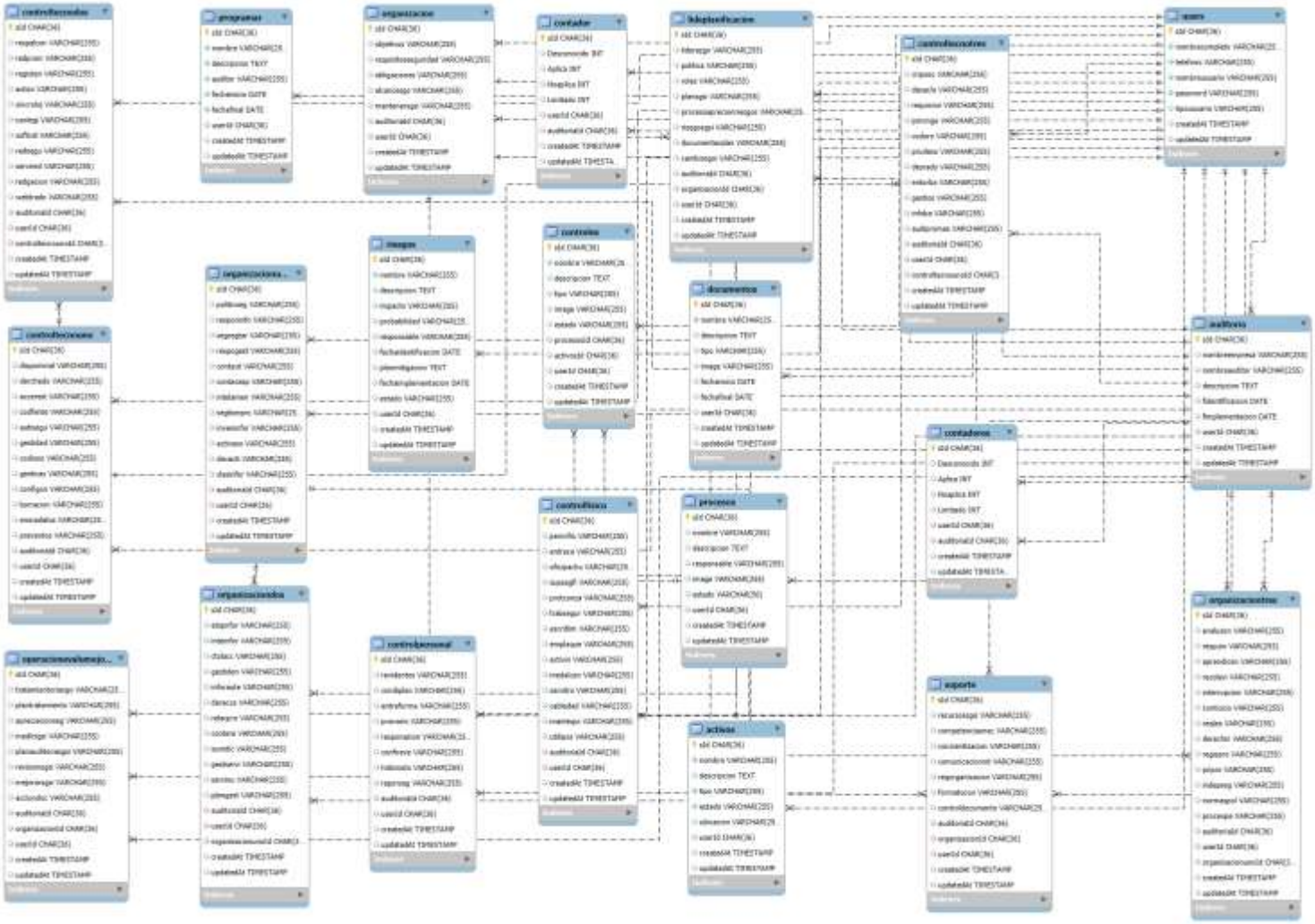

Figura 13. Modelo MER. Fuente: Propia.

2.1.6. Incrementos y Revisiones en el Desarrollo del Proyecto

En cada sprint del proyecto, se generaron incrementos tangibles que permitieron avanzar de manera iterativa y progresiva hacia el objetivo general: desarrollar una

herramienta digital basada en el estándar ISO/IEC 27001 para la gestión de la seguridad de la información en las organizaciones. Estos incrementos consisten en módulos funcionales, prototipos y documentación, los cuales fueron revisados al término de cada iteración para garantizar su alineación con los requisitos del sistema. A continuación, se describen los incrementos logrados en cada sprint, basados en los ítems seleccionados del Product Backlog, organizados según su prioridad y nivel de dificultad:

I. Sprint 1

1. Implementación de Funcionalidades Básicas del Sistema

En la Tabla 24 se presentan los 5 ítems del Product Backlog asignados al primer sprint. Durante este sprint, se trabajó en la implementación de funcionalidades básicas relacionadas con la seguridad de inicio de sesión, la programación de auditorías, el acceso al historial de evaluaciones, la gestión de documentos y la carga de políticas de seguridad. Este sprint tuvo una duración de 3 semanas debido a la alta dificultad técnica de los ítems seleccionados.

Incrementos logrados:

1. **Inicio de sesión seguro:** Este incremento consistió en implementar un sistema de autenticación seguro que permita a los usuarios (Auditor y Empresa) acceder a la plataforma utilizando credenciales personales (usuario y contraseña). El objetivo era garantizar la protección de la información sensible y proporcionar acceso según los roles definidos.

Fase inicial: En la figura 14, se desarrolló un prototipo básico de la interfaz de inicio de sesión. Este contaba con campos de entrada para el nombre de usuario y la contraseña, pero carecía de validaciones avanzadas y una conexión con la base de datos. A continuación, se muestra el prototipo inicial:

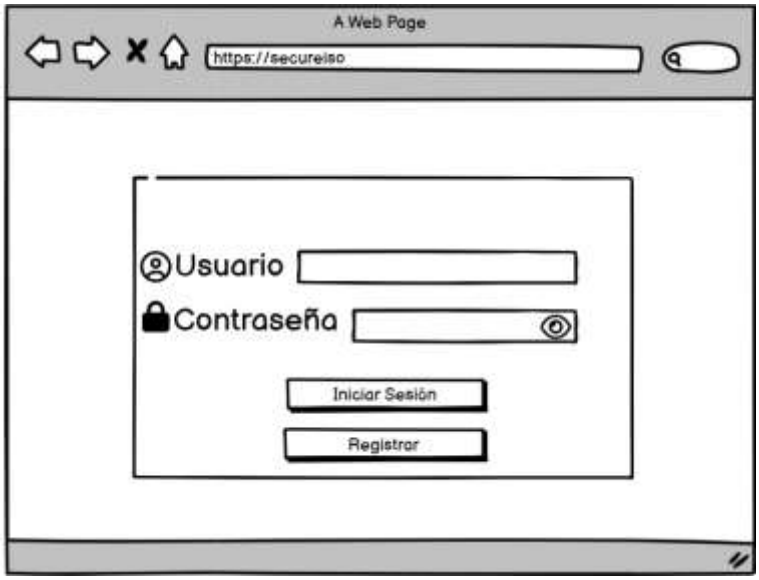

Figura 14. Prototipo inicial del módulo de inicio de sesión, diseño básico.

Fase Final: Tras implementar la lógica de negocio, se integraron mejoras como la validación de credenciales en la base de datos, la adición de mensajes de error para contraseñas o usuarios incorrectos, el uso de tokens JWT para gestionar sesiones de manera segura y un diseño mejorado con estilos y elementos de accesibilidad, logrando un módulo funcional y seguro de inicio de sesión que cumple con los requisitos definidos en la historia de usuario como se muestra en la figura 15.

Figura 15. Interfaz final del módulo de inicio de sesión.

2. **Programación de auditorías:** Este incremento se centró en desarrollar un módulo que permita a los Auditores programar auditorías internas, especificando fechas y objetivos. El objetivo era facilitar la planificación y el seguimiento de estas auditorías para evaluar el cumplimiento con ISO/IEC 27001.

Fase inicial: En la primera etapa, se creó una interfaz básica para ingresar fechas y objetivos. Este prototipo no incluía validaciones, ni opciones para asignar objetivos específicos a las auditorías como se muestra en la figura 16.

Figura 16. Prototipo inicial del módulo de programación de auditorías, con campos básicos para fechas y objetivos.

Evolución del incremento: En las iteraciones posteriores visualizamos en la figura 17 la implementación de mejoras como la validación de fechas para evitar conflictos en la planificación, la funcionalidad para asignar objetivos específicos a cada auditoría, la vinculación de las auditorías con la base de datos para su almacenamiento y consulta, así como un diseño mejorado con opciones para editar o cancelar auditorías, resultando en un módulo funcional que facilita la programación y gestión de auditorías internas.

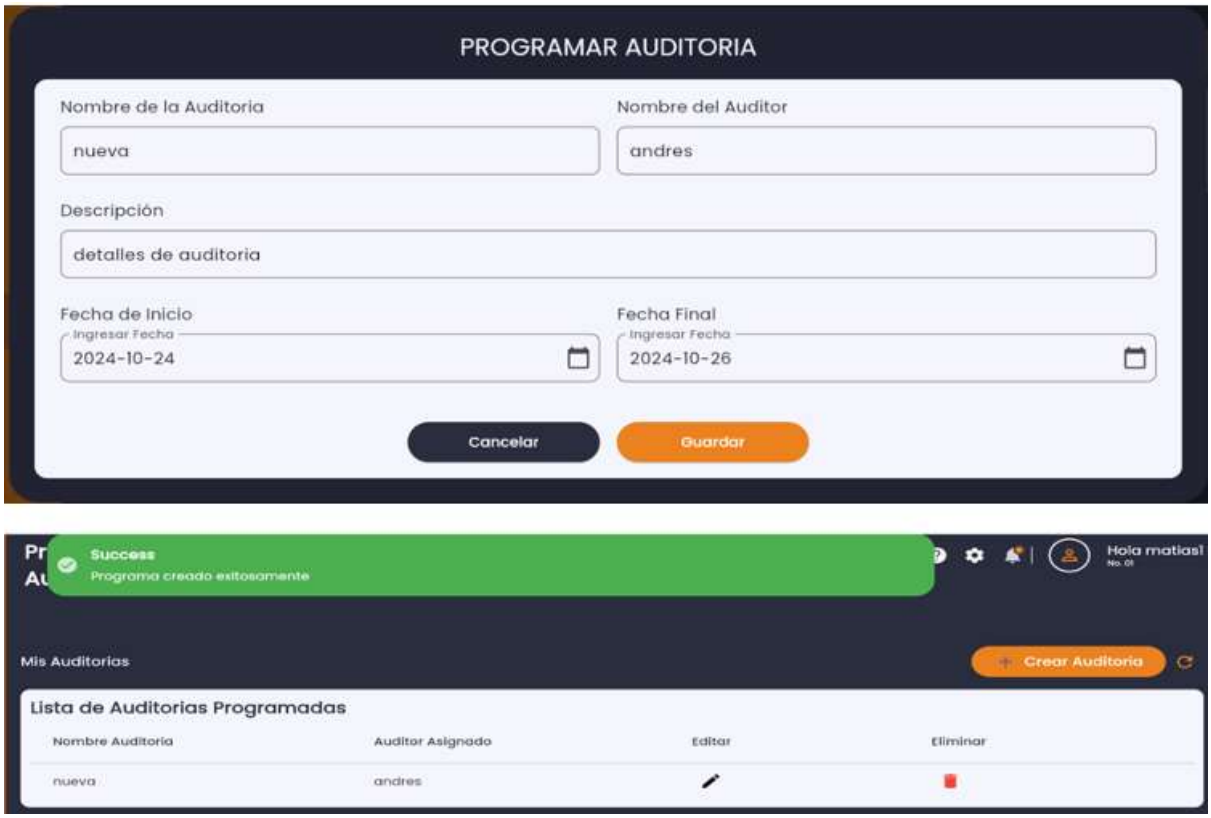

Figura 17. Versión final del módulo de programación de auditorías, diseño refinado.

3. **Historial de evaluaciones:** Este incremento abordó la configuración de un módulo para acceder al historial de auditorías y evaluaciones realizadas. Esto permite analizar tendencias y realizar comparativas entre periodos.

Fase inicial: En un primer momento, se desarrolló una interfaz inicial que mostraba una lista básica de evaluaciones, sin opciones de filtrado ni detalles avanzados. Prototipo inicial del historial de evaluaciones, con una lista básica de auditorías.

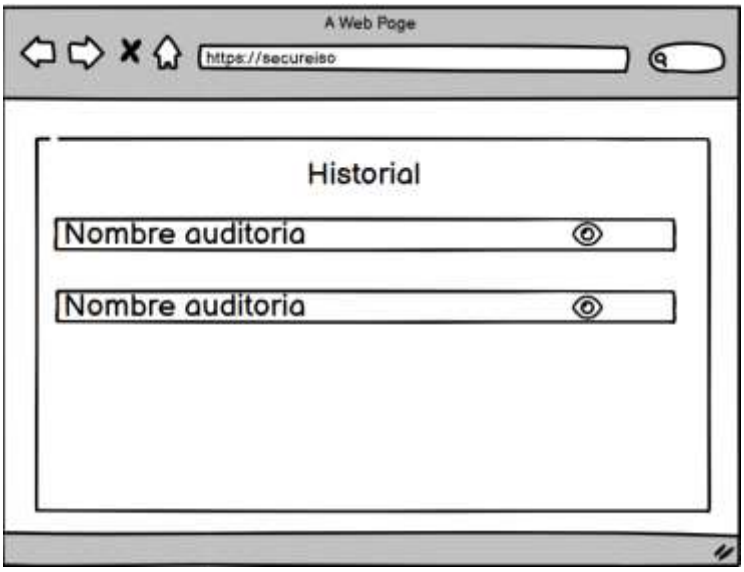

Figura 18. Prototipo inicial del historial de evaluaciones, con una lista básica de auditorías.

Evolución del incremento: Se añadieron características como filtros para buscar evaluaciones por nombre, la visualización detallada de cada auditoría con resultados y recomendaciones, gráficas para analizar tendencias de cumplimiento y áreas de mejora, y la conexión a la base de datos para recuperar datos históricos como se muestran en la figura 19.

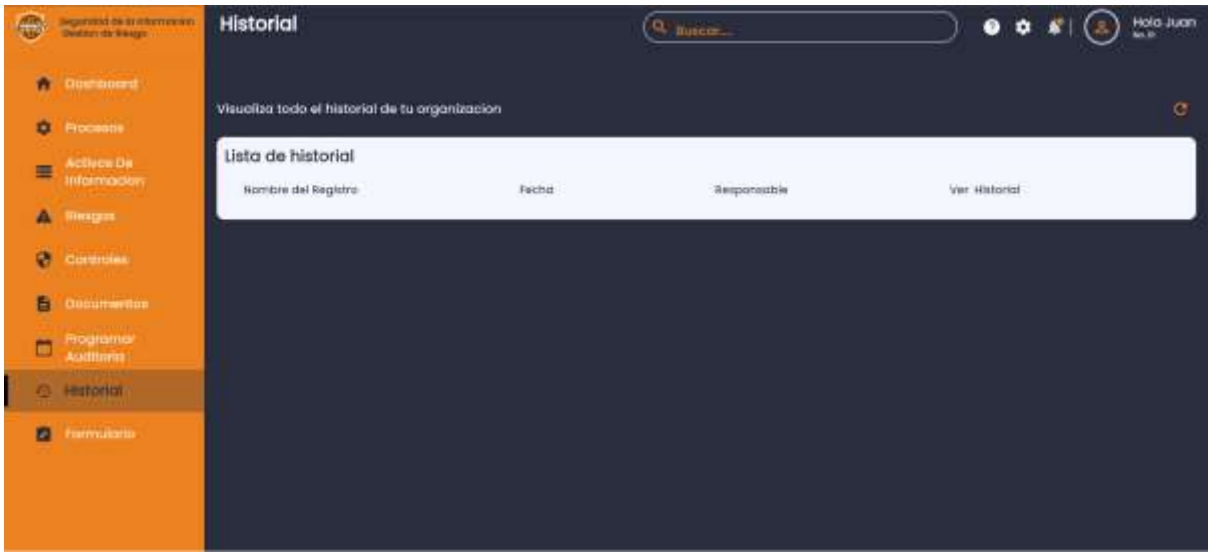

Figura 19. Versión final del historial de evaluaciones, con filtros, gráficos y detalles avanzados.

4. **Gestión de documentos:** Este incremento consistió en integrar la funcionalidad para cargar, actualizar y visualizar documentos relevantes, como políticas de seguridad y registros de incidentes.

Fase inicial: En la primera etapa, se desarrolló una interfaz básica con un botón para cargar archivos. No incluía opciones para actualizar ni visualizar documentos existentes.

Figura 20. Prototipo inicial de la gestión de documentos, con funcionalidad básica de carga de archivos.

Evolución del incremento: En la siguiente figura 21, se implementaron mejoras como la posibilidad de actualizar documentos existentes, la visualización directa de los documentos en la plataforma optimizando la gestión documental.

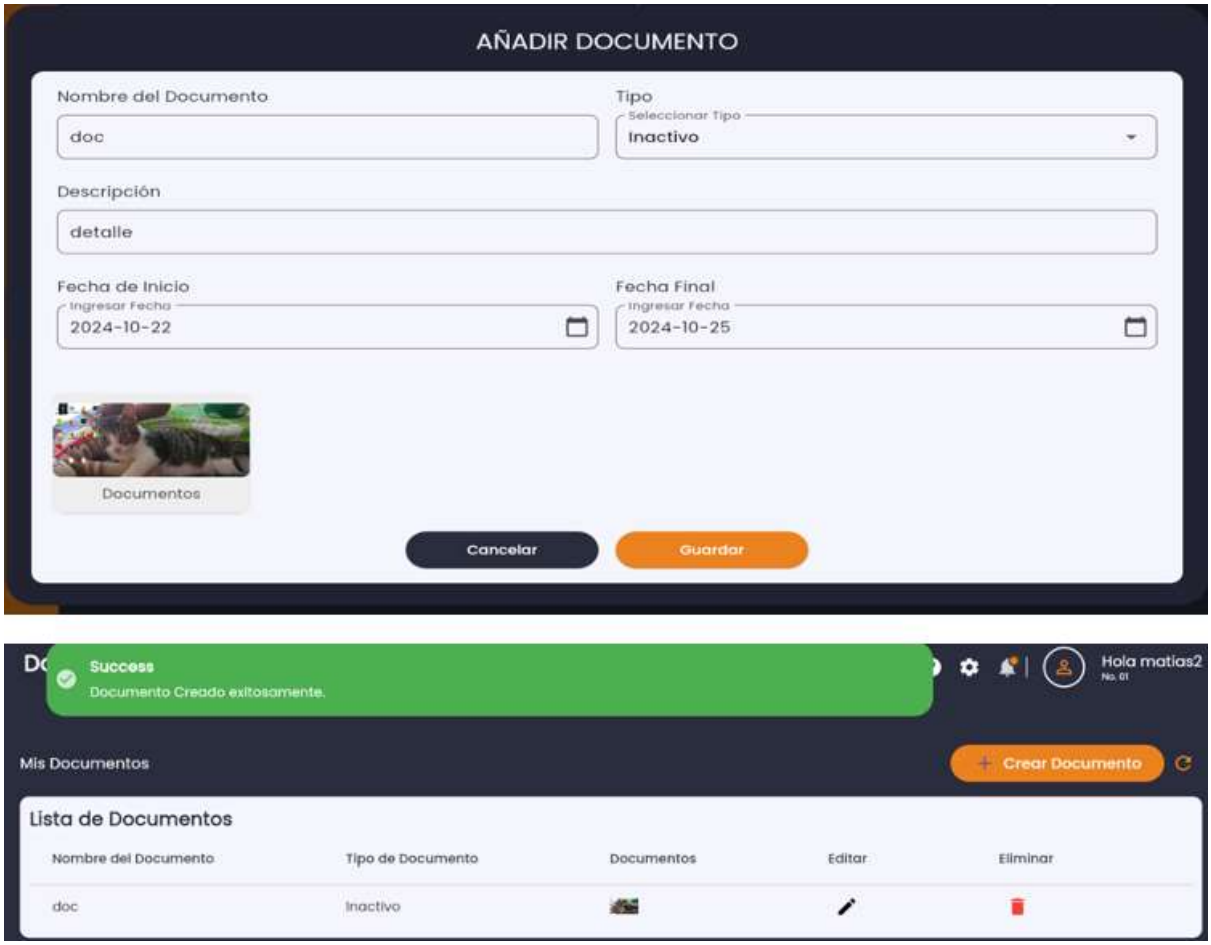

Figura 21. Versión final del módulo de gestión de documentos, con opciones de carga, actualización y visualización.

Estos incrementos proporcionaron una base funcional para garantizar el acceso seguro y facilitar las operaciones iniciales relacionadas con la ISO/IEC 27001.

II. Sprint 2

1. Gestión de Activos y Evaluaciones de Seguridad

En este sprint, descrito en la Tabla 25, se trabajó en la organización de los activos de información y en la evaluación de riesgos asociados. Los 5 ítems seleccionados tenían una dificultad media, por lo que se asignaron 3 semanas para su desarrollo.

Incrementos logrados:

1. **Identificación de activos:** El objetivo de este incremento fue desarrollar un módulo que permita registrar y organizar los activos de información de la organización. Esto incluye categorizar los activos según su importancia y vincularlos con las áreas correspondientes.

Fase inicial: El prototipo inicial de la figura 22 consiste en una tabla básica donde los usuarios podían ingresar manualmente información sobre los activos, como nombre, descripción y categoría. Sin embargo, no contaba con funcionalidades avanzadas como la edición o la vinculación con otras áreas.

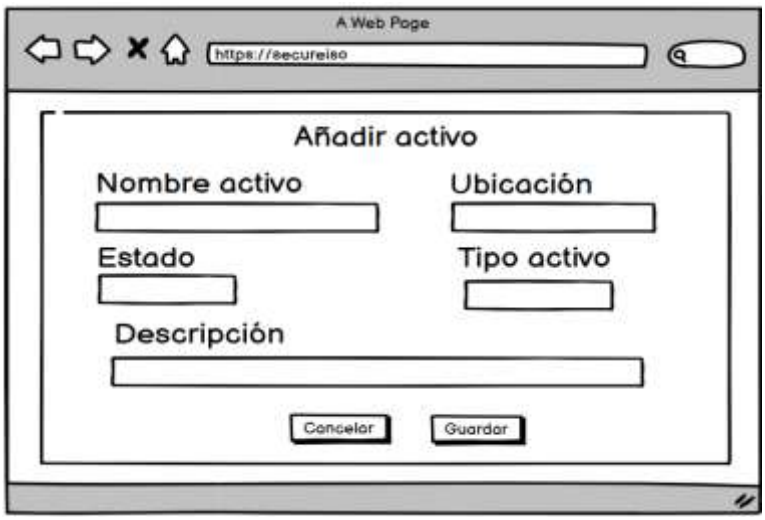

Figura 22. Prototipo inicial del módulo de identificación de activos con funcionalidad limitada.

Evolución del incremento: Durante el desarrollo, se implementaron mejoras como la inclusión de un formulario dinámico para la adición y modificación de activos, la capacidad para asociar activos a áreas específicas de la organización, y el diseño de un sistema de búsqueda optimizando la administración de los activos como se visualiza en la figura 23.

Figura 23. Versión final del módulo de identificación de activos, con diseño mejorado y funcionalidades avanzadas.

2. **Gestión de riesgos:** Este incremento tenía como objetivo implementar un sistema para que las empresas puedan evaluar los riesgos identificados y tomar medidas para mitigarlos de manera eficaz.

Fase inicial: La versión inicial de la figura 24 consistió en una lista estática de riesgos con campos para su descripción y clasificación. En esta fase, las opciones de evaluación eran limitadas y no había un sistema automatizado para calcular el impacto o la probabilidad.

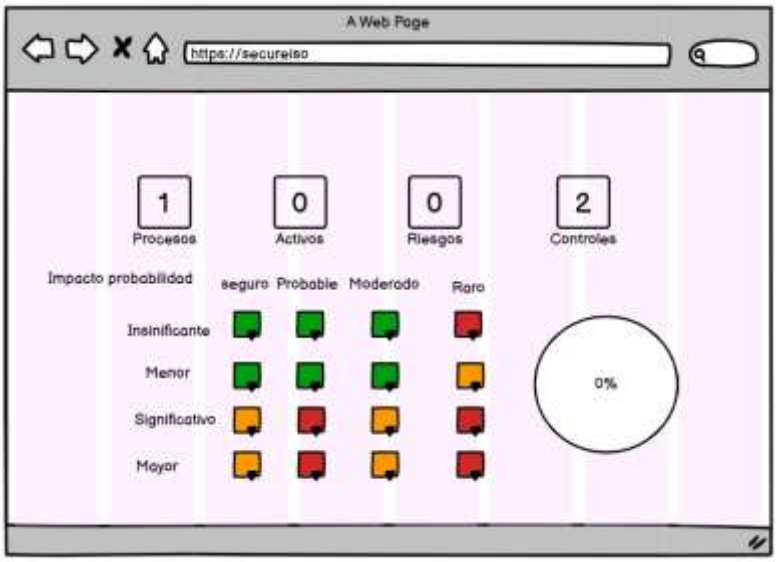

Figura 24. Prototipo inicial de gestión de riesgos con una lista estática de riesgos.

Evolución del incremento: Durante el desarrollo, se agregaron funcionalidades como un sistema de evaluación basado en matrices de impacto y probabilidad, la generación automática de prioridades para cada riesgo y reportes dinámicos que muestran el estado actual de los riesgos, mejorando significativamente la gestión de riesgos como se visualiza en la siguiente figura (25).

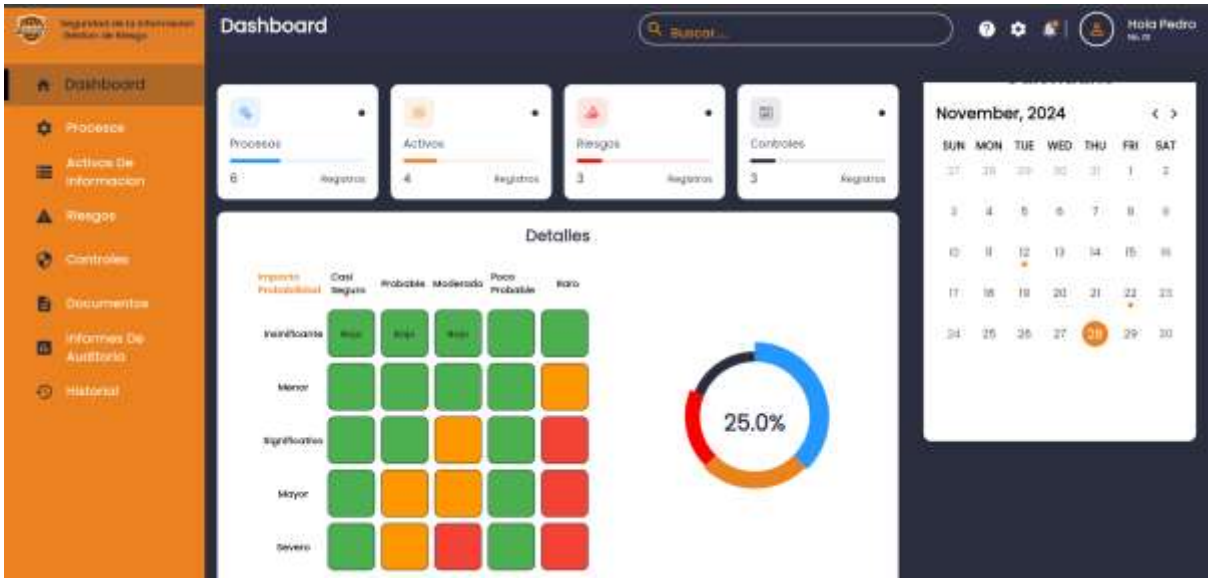

Figura 25. Versión final del sistema de gestión de riesgos, con la matriz de impacto.

3. **Acceso a resultados de pruebas:** En este incremento se desarrolló una funcionalidad para que las empresas revisen los resultados de las auditorías realizadas, proporcionando información detallada sobre las evaluaciones de seguridad.

Fase inicial: En la figura 26 se muestra un prototipo inicial mostraba un listado simple con los resultados de las pruebas. Carecía de funcionalidades para filtrar, buscar o visualizar los detalles de cada prueba.

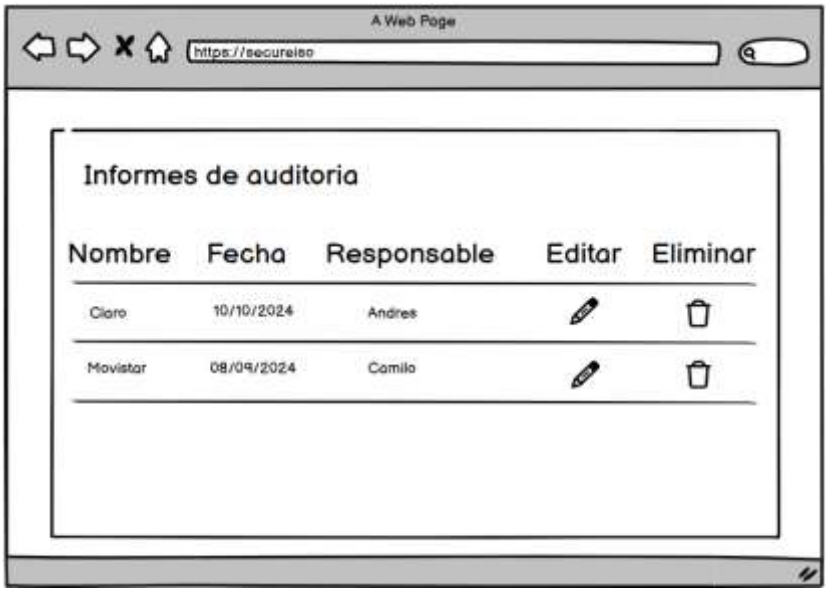

Figura 26. Prototipo inicial de acceso a resultados de pruebas, con listado básico.

Evolución del incremento: A medida que se avanzó en el desarrollo, en la figura 27 se visualiza la incorporación de funcionalidades de búsqueda y filtrado para facilitar la navegación entre los resultados, secciones detalladas que desglosan los hallazgos de las pruebas y las recomendaciones, y la generación de gráficos interactivos para visualizar áreas críticas y tendencias, mejorando la experiencia de análisis y toma de decisiones.

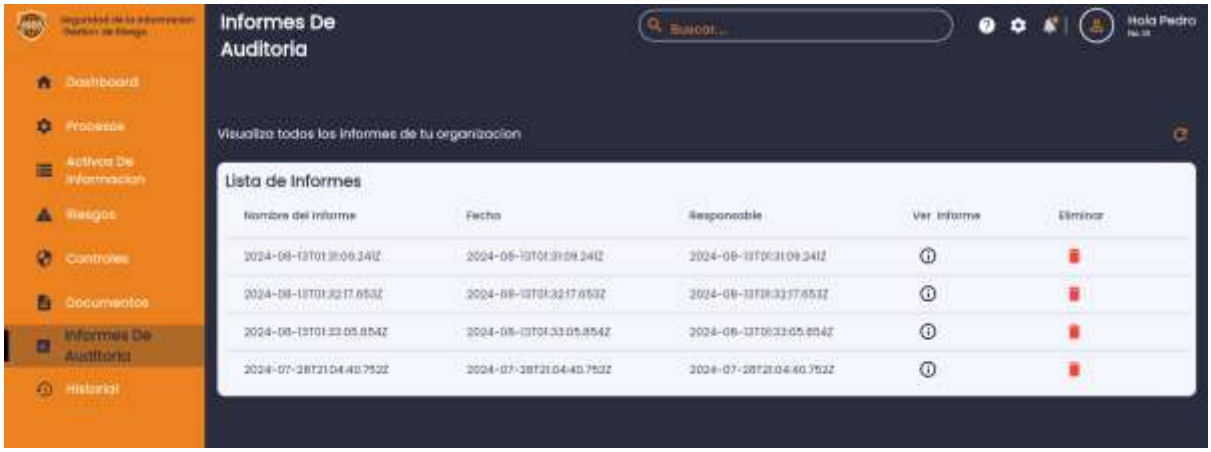

Figura 27. Versión final del módulo de acceso a resultados de pruebas, con diseño visual e interactividad.

Al finalizar este sprint, se logró una representación inicial de los activos de información, lo que permitió establecer relaciones claras entre riesgos y medidas correctivas.

III. Sprint 3

1. Priorización y Gestión de Riesgos

Como se muestra en la Tabla 26, el tercer sprint se enfocó en la priorización de riesgos y la mejora continua de los controles de seguridad. Este sprint, con 4 ítems seleccionados y una dificultad alta, tuvo una duración de 3 semanas.

Incrementos logrados:

1. **Evaluación de riesgos:** Este incremento consistió en la implementación de un módulo para priorizar riesgos según su gravedad e impacto en la organización. El objetivo era ofrecer una herramienta que permita al usuario tomar decisiones informadas para gestionar los riesgos de seguridad de la información.

Fase inicial: El prototipo inicial del módulo de evaluación de riesgos consistió en un formulario básico para ingresar manualmente los riesgos. No se incluían algoritmos de priorización ni visualizaciones claras del impacto.

Figura 28. Prototipo inicial con una interfaz básica para registrar riesgos sin priorización automatizada.

Evolución del incremento: En la figura 29 encontramos las siguientes iteraciones, se agregaron funcionalidades como un formulario más detallado basado en el impacto y probabilidad, logrando un módulo interactivo que facilita la toma de decisiones basadas en una evaluación detallada de riesgos, también la facilidad de actualizar o eliminar dicho riesgo.

Figura 29. Interfaz final con el formulario y opciones de editar y eliminar.

2. **Gestión de controles:** Registro de información sobre controles de seguridad, incluyendo responsables y detalles técnicos. El último incremento del sprint involucró el registro de información detallada sobre controles de seguridad, incluyendo responsables y detalles técnicos.

Fase inicial: El prototipo inicial de la figura 30 ofrecía una interfaz básica para agregar información de los controles, pero carecía de integración con otros módulos.

Figura 30. Interfaz inicial con campos básicos de controles.

Evolución del incremento: Las mejoras realizadas en la figura 31 incluyeron la asociación de controles a procesos y activos específicos, la integración con la opción de editar y eliminar el control, la posibilidad de subir reportes sobre el estado de los controles, optimizando la supervisión.

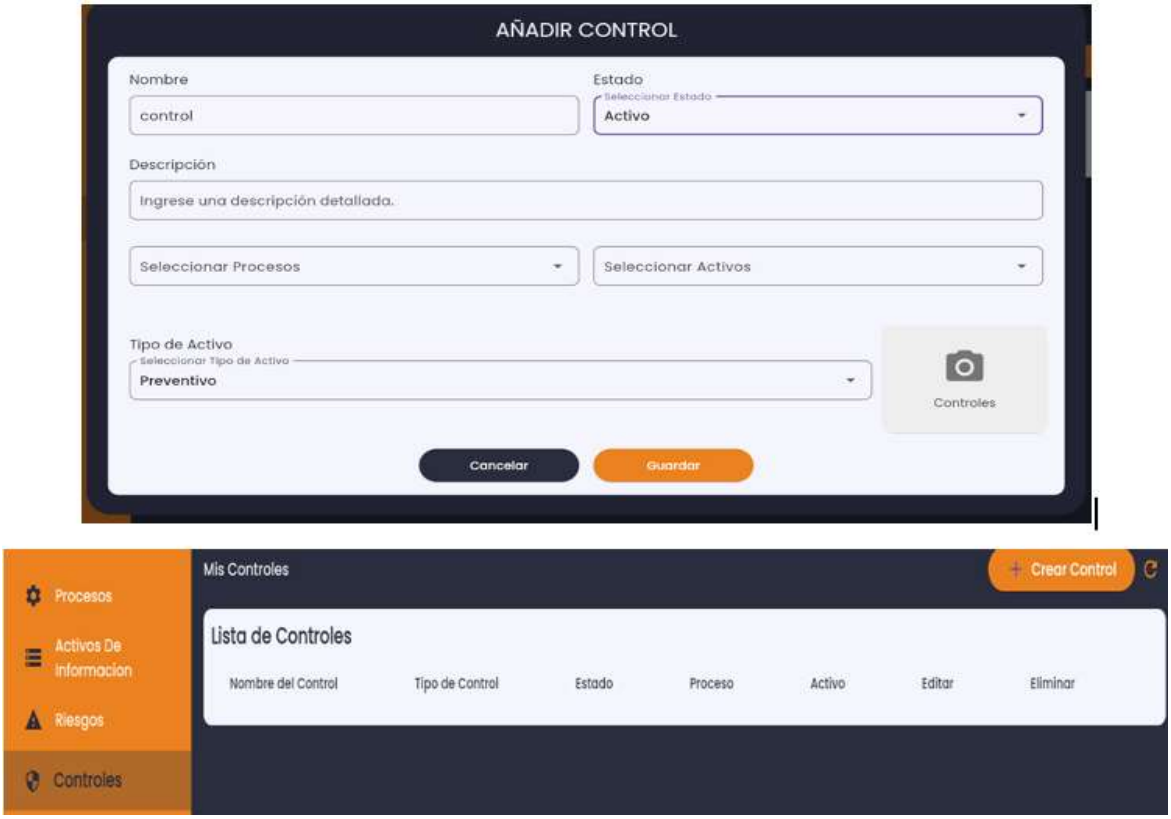

Figura 31. Módulo final con registro detallado e integración completa.

Estos incrementos permitieron integrar capacidades avanzadas para mitigar riesgos y optimizar medidas de seguridad, alineadas con ISO/IEC 27001.

IV. Sprint 4

2. Validación y Supervisión de la Seguridad

Durante el cuarto sprint, descrito en la Tabla 27, se implementan funcionalidades relacionadas con la validación de acciones correctivas y la supervisión de la seguridad en tiempo real. Este sprint incluyó 5 ítems con una dificultad media y tuvo una duración de 3 semanas.

Incrementos logrados:

- **Generación de informes:** Este incremento se enfocó en desarrollar una funcionalidad que permita al Auditor generar informes detallados sobre las auditorías realizadas. Los informes debían incluir resultados de las pruebas de

seguridad, hallazgos identificados y recomendaciones de mejora, asegurando que la información presentada sea clara y útil para la toma de decisiones por parte de la Empresa.

Fase inicial: En la primera iteración como se muestra en la figura 32, se creó un prototipo básico de los informes. Este consistía en la visualización de los resultados y la prueba del Auditor. Aunque el diseño inicial era funcional, carecía de automatización, análisis de datos y generación dinámica del informe.

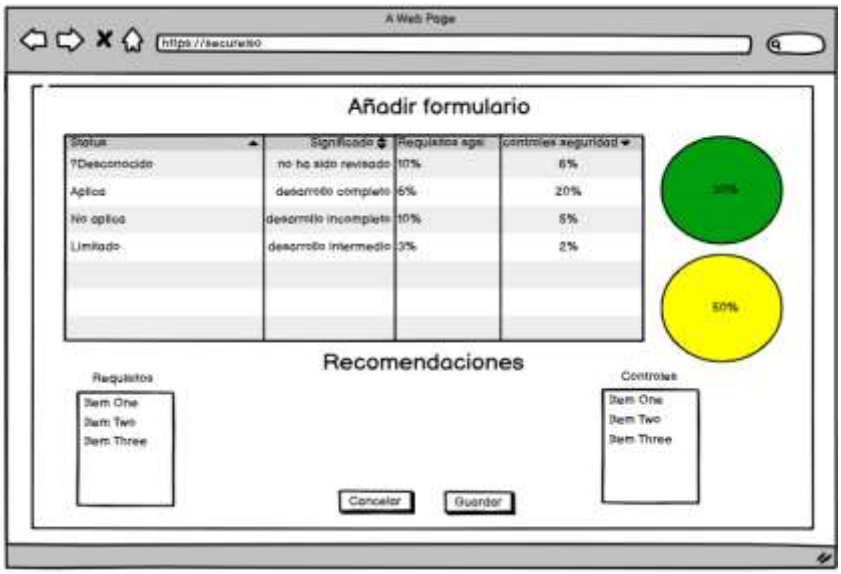

Figura 32. Interfaz inicial del generador de informes, mostrando un formulario básico con campos manuales para rellenar los hallazgos y recomendaciones.

Evolución del incremento: Durante el desarrollo, se implementaron mejoras como la automatización de datos mediante la conexión del módulo con la base de datos para extraer automáticamente los resultados de auditorías, la visualización avanzada a través de gráficos y una sección de recomendaciones con sugerencias automáticas basadas en los hallazgos mejorando la presentación de resultados, en la figura 33 se visualizan los cambios.

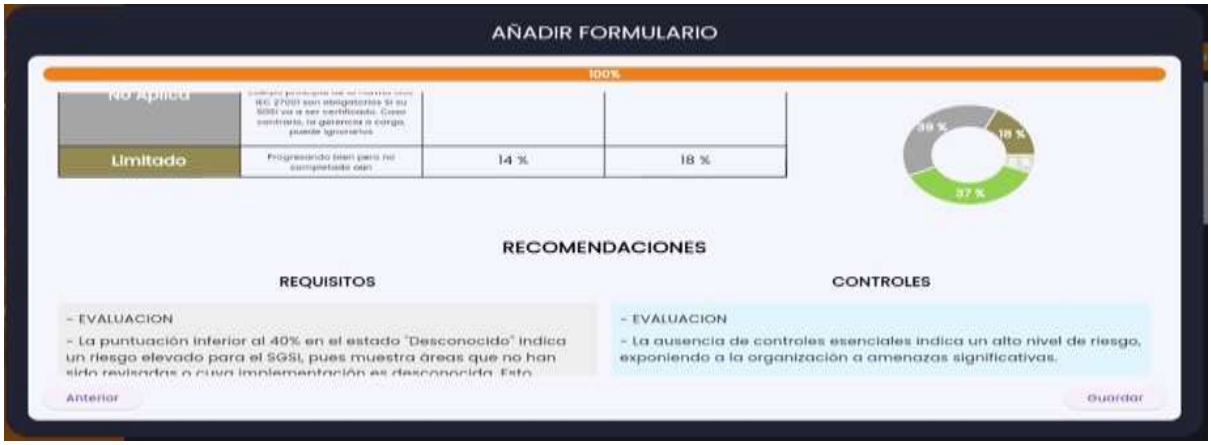

Figura 33. Interfaz final del módulo, con gráficos integrados, plantillas dinámicas.

Al finalizar este sprint, la herramienta adquirió capacidades para realizar pruebas de seguridad exhaustivas y monitorear continuamente el desempeño de los módulos.

En cada sprint, los incrementos fueron revisados por el equipo para garantizar que cumplían con los criterios de aceptación definidos en el Product Backlog. Esto incluyó pruebas funcionales, revisión de cumplimiento con ISO/IEC 27001 y validación de usabilidad con usuarios potenciales. Los ajustes necesarios fueron retroalimentados al backlog para iteraciones futuras, asegurando un proceso de mejora continua.

Por lo anterior, se presentaron algunos de los incrementos seleccionados para cada sprint dentro del marco de desarrollo de este proyecto. Estos incrementos corresponden a entregables parciales diseñados para cumplir con objetivos específicos y atender los requerimientos identificados en las historias de usuario. Cabe destacar que las historias de usuario se utilizaron principalmente como herramientas para la identificación de requisitos, proporcionando una descripción general de las necesidades del sistema desde la perspectiva del usuario final.

Sin embargo, para un entendimiento más detallado y técnico de las funcionalidades desarrolladas, se hace referencia a los casos de uso correspondientes. Estos casos de uso, que se encuentran documentados en los anexos (anexo 4), ofrecen una representación estructurada y exhaustiva de los flujos de interacción, los actores

involucrados y las respuestas esperadas del sistema. De esta manera, los casos de uso permiten profundizar en los aspectos técnicos y funcionales que subyacen a cada historia de usuario, complementando la visión inicial presentada durante el levantamiento de requisitos.

2.1.7. Implementación

Para abordar la implementación de la página web SecureIso desarrollada en esta tesis, cubriendo desde la configuración del entorno de trabajo hasta su despliegue en el servidor. Además, incluye la construcción de la página web destinada al consumo por parte de organizaciones, así como los resultados de las pruebas de funcionalidad realizadas para asegurar su correcto desempeño y usabilidad.

2.1.7.1. Herramientas De Desarrollo

Para lograr crear el proyecto fue necesario utilizar algunas herramientas que nos facilitara el desarrollo de la aplicación, tanto Froentend y Backend y herramientas que nos facilita realizar pruebas al backend. A continuación, explicaremos cada una de ellas.

- **PostgreSQL**

Esta herramienta fue utilizada para la administración de la base de datos. Nos permite gestionar las tablas y soportar relaciones complejas. PostgreSQL lo escogimos porque es compatible con diferentes programas y la posibilidad del manejo JSON.

Figura 34. Logo de la base de datos PostgreSQL. Fuente [83].

- **Visual Studio Code**

Es un editor de código desarrollado por Microsoft para Windows que es lo que utilizamos en nuestras PC, lo escogimos porque soporta diferentes lenguajes de programación como Python y Dart con Flutter. El cual para este proyecto se utilizó para realizar la aplicación con Flutter.

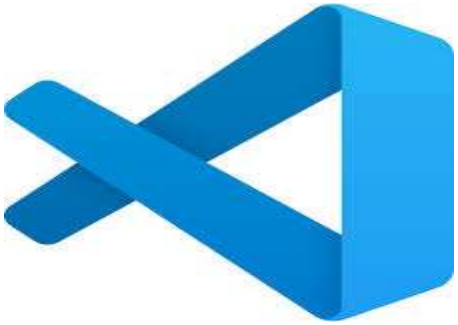

Figura 35. Logo Visual Studio Code. Fuente [88].

- **Postman**

Es una plataforma que la utilizamos para gestionar nuestro api haciendo peticiones de HTTP. Nos permite hacer peticiones como GET, POST, PUT o DELETE y ver la respuesta en formato Json. Ya que es de código abierto nos facilitó comprobar que nuestra Api funciona.

Figura 36. Logo Postman. Fuente [89].

2.1.7.2 Desarrollo Front-End

Para el desarrollo de la aplicación web fue necesario tener en cuenta los casos de uso con las historias de usuario y llevar a cabo una codificación que fue desarrollada bajo un patrón de diseño Provider (forma simplificada de implementar un observador),

ChangeNotifier (permite que los widgets se suscriban a cambios de estado) y Getx (facilita el manejo de estados, navegación e inyección de dependencias en un solo paquete).

Estándares de codificación

- **Variables:** Las variables utilizadas en el código son escritas con letras minúsculas de acuerdo con la acción que es requerido.

- **Métodos:** Los métodos son denominados de acuerdo al proceso a ejecutar y son escritas con la primera letra en mayúscula.

- **Clases:** La primera letra se escribe en mayúscula.

- **Paquetes:** Los paquetes generalmente se adicionan en minúscula.

2.1.7.3 Estructura Del Proyectos En Flutter

Al realizar la creación del proyecto podemos ver una estructura del proyecto por defecto, la cual nos sirvió como base para empezar con el desarrollo del proyecto.

A Continuación, se explicará cómo se crea un proyecto. El cual solo necesitamos como requerimiento tener todos los programas instalados, como Visual Studio Code en el cual debemos instalar la extensión de flutter, el framework Flutter que trae como lenguaje a Dart. Una vez todo instalado procedemos a crear nuestro proyecto utilizando estos sencillos pasos en Visual Studio Code, como se muestran en las imágenes 37, 38, 39.

Después seleccionamos la carpeta de ubicación y le damos un nombre al proyecto, al final obtendremos una estructura por defecto en nuestro proyecto como se muestra en la imagen 40.

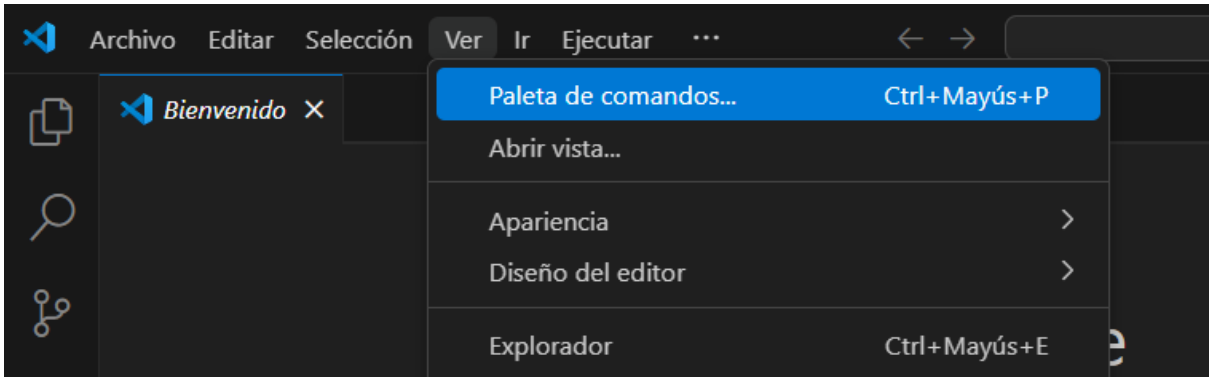

Figura 37. Opción paleta de Comandos. Fuente: Propia.

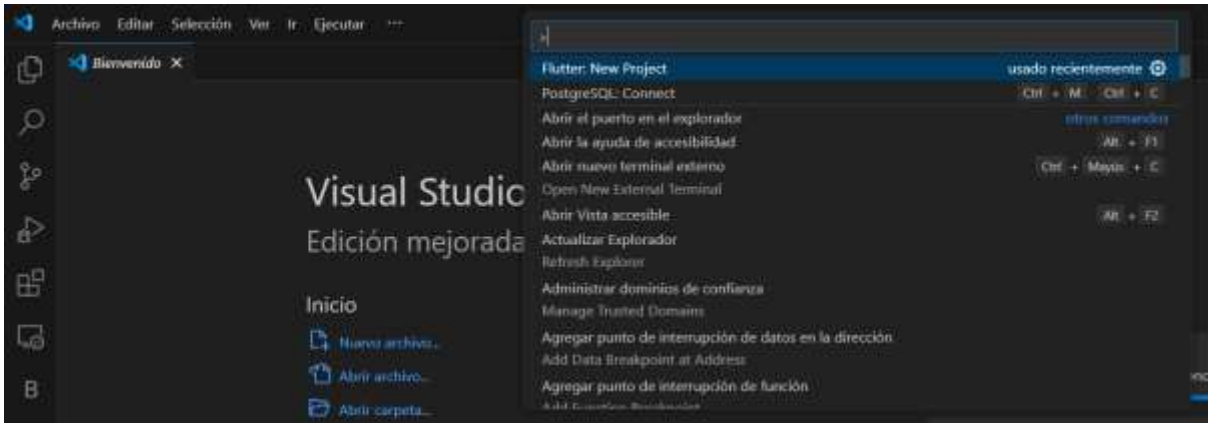

Figura 38. Opción de un nuevo proyecto. Fuente: Propia.

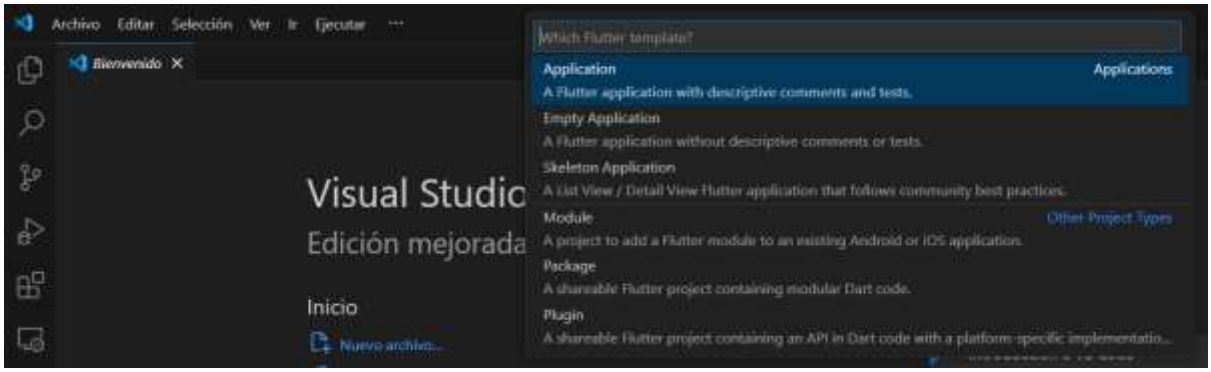

Figura 39. Opción aplicación. Fuente: Propia.

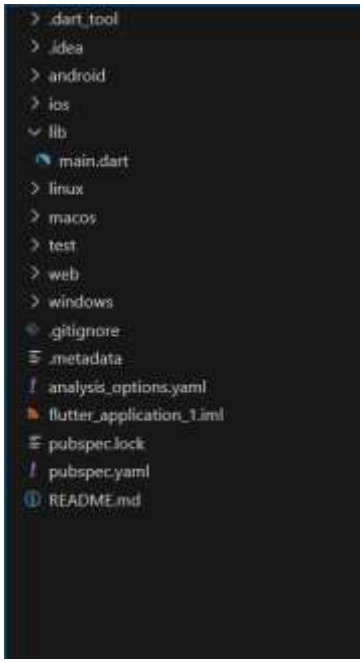

Figura 40. Estructura del proyecto. Fuente: Propia.

En esta imagen vemos todos los archivos por defecto que trae al crear un proyecto en flutter que a continuación iremos explicando.

La carpeta Android contiene el código específico para una plataforma Android, incluyendo configuraciones y archivos como el build.gradle el son necesarios para compilar la aplicación en estos dispositivos, al igual que la carpeta iOS que contiene una misma estructura, pero para dispositivos IOS.

La carpeta test y README.md, la primera es utilizada para almacenar pruebas unitarias esenciales para el funcionamiento de los widgets y funciones, ayudando a mantener la calidad del código, el último nos sirve para documentar el proyecto dando una descripción general, instalación y guías para el desarrollador.

La carpeta web para ejecutar en la web, el cual tiene archivos como index.html y configuraciones adicionales para desplegar la aplicación en los navegadores. En el archivo pubspec.yaml podemos definir las dependencias y recursos que necesite la aplicación como se muestra en la figura 41.

```
environment:
  sdk: '>=3.4.4 <4.0.0'

dependencies:
  flutter:
    sdk: flutter
  cupertino_icons: ^1.0.8
  google_fonts: ^4.0.4
  table_calendar: ^3.1.1
  provider: ^6.0.5
  flutter_svg: ^2.0.10
  fl_chart: ^0.68.0
  intl: ^0.19.0
  get: ^4.6.5
  dropdown_button2: ^2.3.9

  animations: ^2.0.11
  image_picker_for_web: ^3.0.2
  image_picker: ^1.0.0
  dio: ^5.5.0
  file_picker: ^3.0.4
  flutter_secure_storage: ^5.1.2
  shared_preferences: ^2.3.1

dev_dependencies:
  flutter_test:
    sdk: flutter

flutter:
  uses-material-design: true
  assets:
    - assets/images/
```

Figura 41. Líneas del código de instalación de dependencias. Fuente: Propia.

Una vez instaladas las dependencias podemos visualizar en la figura 42 la estructura y organización del proyecto final de nuestra aplicación web.

En la carpeta lib que es la más importante, se encuentra todo el código de la aplicación web en el cual se comienza a desplegar todo, ya que contiene el código fuente escrito por Dart. Aquí se desarrolla la lógica de la aplicación, las interfaces y los componentes principales.

```
.
..
configu
Controller
dashboard.dart
Data
main.dart
Models
Pages
Routing
Services
splash_screen.dart
style
Widgets
```

Carpeta lib.

```
.
..
data.dart
data_provider.dart
```

Carpeta lib/Data.

```
.
..
controller.dart
menuappcontroller.dart
navigation_controller.dart
```

Carpeta lib/Controller.

```
.
..
router.dart
routes.dart
```

Carpeta lib/Routing

```
.
..
http_services.dart
```

Carpeta lib/Services.

```
.
..
activos_models.dart
api_response.dart
contadorcontroles_models.dart
contadorrequisitos_models.dart
controles_models.dart
documentos_models.dart
fisico_model.dart
historial_models.dart
lideplanificacion_model.dart
menu_model.dart
myfiles.dart
operacionevalumejora_models.dart
organizacionalesdos_model.dart
organizacionalestres_model.dart
organizacionalesuno_models.dart
organizacion_model.dart
personales_model.dart
procesos_models.dart
programar_models.dart
registroformulario_model.dart
riesgos_models.dart
side_menu_data.dart
soporte_model.dart
tecnologiasdos_model.dart
tecnologiastres_model.dart
tecnologiasuno_model.dart
users_model.dart
```

Carpeta lib/Models.

```
.
..
colors.dart
extensions.dart
snack_bar_helper.dart
style.dart
```

Carpeta lib/Style.

```
.
..
custom_date.dart
custom_dropdown.dart
custom_field_text.dart
custom_text.dart
document_card.dart
pdt_view.dart
```

Carpeta lib/Widgets.

```
.
..
Componentes
controles.dart
Provider
```

Carpeta lib/Pages/Controles.

```
.
..
Activos Informacion
Controles
Dashboard
Documentos
error.dart
Formulario
Historial
Informes
Main
Procesos
Programar
Riesgos
```

Carpeta lib/Pages.

```
.
..
controles_from.dart
controles_screen.dart
sesion_list_controles.dart
```

Carpeta lib/Pages/Controles/Componentes.

```
.
..
controles_provider.dart
```

Carpeta lib/Pages/Controles/Provider

Figura 42. Carpetas de los archivos creados para el frontend.

Después de describir la estructura de la carpeta lib, procedemos a explicar los archivos .dart más importantes que garantizan el correcto funcionamiento de la aplicación. Estos archivos contienen la lógica principal, los modelos, las vistas y los

controladores que hacen posible la interacción y el flujo de datos en la aplicación. En el Anexo 2 se detalla el código completo de cada archivo para una comprensión más profunda de su implementación.

El archivo **main.dart** contiene una función main() que inicializa la aplicación Flutter, asegurando los widgets y configurando controladores clave con GetX para navegación y notificaciones. Luego, MyApp lanza la interfaz principal usando MultiProvider para gestionar el estado de múltiples módulos (como DataProvider y PanelesProvider). GetMaterialApp define rutas iniciales y de error y oculta el banner de debug. Esto organiza la estructura de la app para una gestión eficiente de navegación, estado y temas.

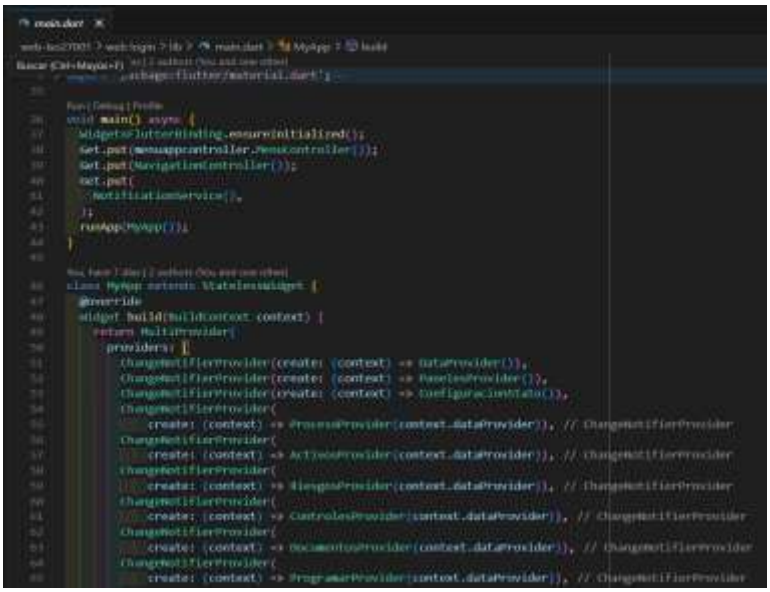

Figura 43. Código main.dart.

2.1.7.4. Construcción Del Servicio REST-API

Para el funcionamiento de la aplicación web, fue necesaria la creación de una REST API que permitiera el consumo de los recursos de la base de datos del servidor, haciendo que la aplicación sea interactiva y dinámica. Para ello, se utilizó Node.js como tecnología principal para implementar la API. En el Anexo 2 se detalla el código completo de su desarrollo para una mejor comprensión.

En la carpeta que vamos a realizar nuestra api comenzamos escribiendo en la terminal de Visual Studio Code **npm init -y** el cual me bajara todos los paquetes necesario para trabajar con Node JS, y para instalar las dependencias que utilizaremos para el funcionamiento de la API utilizamos el comando **npm install** seguido de la dependencia a instalar. A continuación, visualizamos en la imagen 58 el archivo package.json que tenemos en nuestra API.

```
{} package.json ×
Backend > {} package.json
1   {
2     "name": "backend",
3     "version": "1.0.0",
4     "description": "",
5     "main": "index.js",
6     "scripts": {
7       "dev": "nodemon src/index.js",
8       "start": "node src/index.js",
9       "test": "echo \"Error: no test specified\" && exit 1"
10    },
11    "keywords": [],
12    "author": "",
13    "license": "ISC",
14    "dependencies": {
15      "bcrypt": "^5.1.1",
16      "body-parser": "^1.20.2",
17      "cors": "^2.8.5",
18      "dotenv": "^16.4.5",
19      "express": "^4.19.2",
20      "express-async-handler": "^1.2.0",
21      "jsonwebtoken": "^9.0.2",
22      "mongoose": "^8.5.0",
23      "morgan": "^1.10.0",
24      "multer": "^1.4.5-lts.1",
25      "pg": "^8.12.0",
26      "sequelize": "^6.37.3"
27    },
28    "devDependencies": {
29      "nodemon": "^3.1.4"
30    }
31  }
```

Figura 44. Código package.json.

A continuación, visualizamos la estructura detallada de mi backend, que está organizada en carpetas y archivos clave para garantizar un funcionamiento eficiente de la aplicación. Esta estructura se ha diseñado para mantener el código organizado y modular, lo que facilita el mantenimiento y la expansión del sistema.

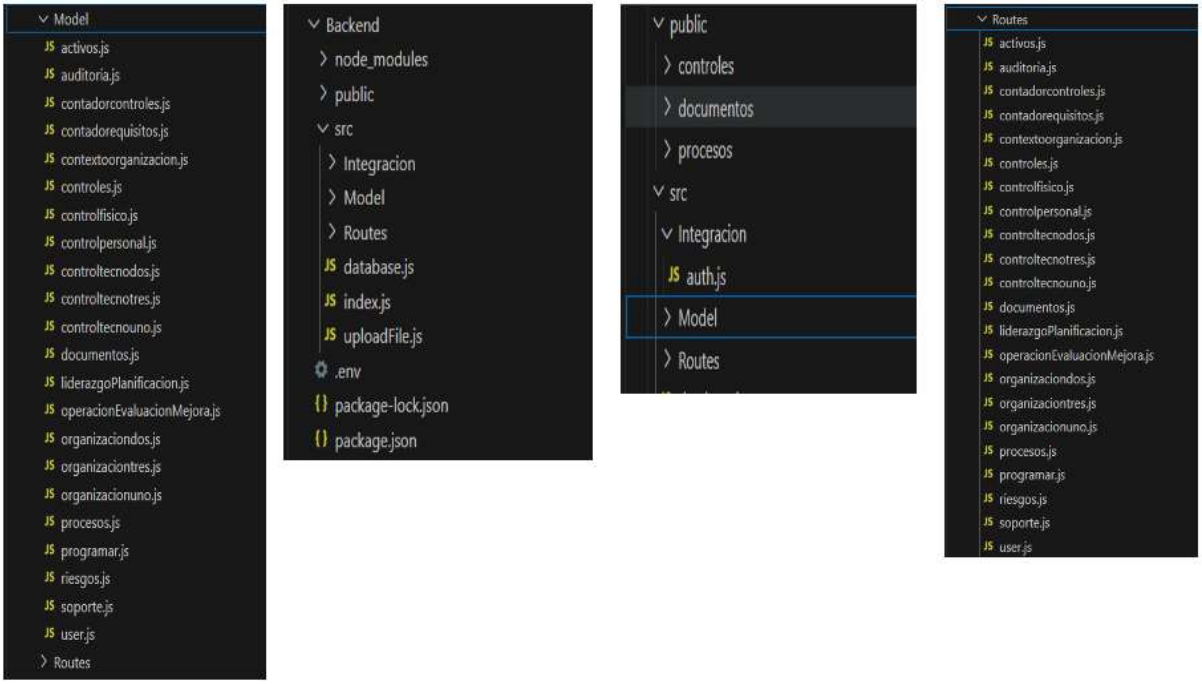

Figura 45. Carpeta Backend.

En el archivo **index.js** tenemos un código que configura una API en Node.js usando Express para manejar rutas y permitir la carga de archivos. Se inicializan Express, CORS (para permitir solicitudes externas), y body-parser para procesar datos en formato JSON. Se definen carpetas públicas (Procesos, Controles, y Documentos) para acceder a archivos subidos y se importan módulos de rutas que organizan las distintas funcionalidades del backend (como usuarios, procesos, etc.).

La ruta raíz responde con un mensaje de éxito para verificar la conexión, y un manejador de errores global captura y responde a errores del servidor. Finalmente, se configura el servidor para escuchar en un puerto definido en .env o en el 3000 por defecto.

```
index.js
Backend > src > index.js > ...
1  const express = require('express');
2  const bodyParser = require('body-parser');
3  const cors = require('cors');
4  const asyncHandler = require('express-async-handler');
5  const dotenv = require('dotenv');
6  dotenv.config();
7  const app = express();
8
9  // Middleware
10 app.use(cors({ origin: '*' }));
11 app.use(bodyParser.json());
12
13 /// setting static folder path
14 app.use('/public/procesos', express.static('./public/Procesos'));
15 app.use('/public/controles', express.static('./Public/Controles'));
16 app.use('/public/documentos', express.static('./Public/Documentos'));
17 // Routes
18 app.use('/usuarios', require('./Routes/user.js'));
19 app.use('/procesos', require('./Routes/procesos.js'));
20 app.use('/activos', require('./Routes/activos.js'));
21 app.use('/controles', require('./Routes/controles.js'));
22 app.use('/contadorequisitos', require('./Routes/contadorequisitos.js'));
23 app.use('/contadorcontroles', require('./Routes/contadorcontroles.js'));
24
25 // Ejemplo de ruta usando asyncHandler directamente en app.js
26 app.get('/', asyncHandler(async (req, res) => {
27   res.json({ success: true, message: 'API funcionando correctamente', data: null });
28 }));
29 // Manejador de errores global
30 app.use((error, req, res, next) => {
31   res.status(500).json({ success: false, message: error.message, data: null });
32 });
33
34 const PORT = process.env.PORT || 3000;
35 app.listen(PORT, () => {
36   console.log(`Server running on port ${PORT}`);
37 });
```

Figura 46. Código Carpeta Backend/src/index.js.

En el archivo **database.js** tenemos un código que configura una conexión a una base de datos PostgreSQL en Node.js utilizando el módulo pg y carga las credenciales desde variables de entorno con dotenv para mayor seguridad.

Se crea un Pool de conexiones usando estas credenciales, lo que permite gestionar múltiples conexiones de manera eficiente. Se implementa un manejador de errores para registrar y manejar cualquier error inesperado en clientes inactivos, cerrando el servidor si ocurre un problema. También se verifica la conexión inicial con pool.connect() para asegurar que el servidor puede acceder a la base de datos. Finalmente, el pool se exporta para que otras partes de la aplicación puedan ejecutar consultas.

```
JS database.js ×
Backend > src > JS database.js > ...
1   const { Pool } = require('pg');
2   const dotenv = require('dotenv');
3   dotenv.config();
4
5   const pool = new Pool({
6     user: process.env.DB_USER,
7     host: process.env.DB_HOST,
8     password: process.env.DB_PASSWORD,
9     database: process.env.DB_DATABASE,
10    port: process.env.DB_PORT,
11  });
12
13  pool.on('error', (err, client) => {
14    console.error('Unexpected error on idle client', err);
15    process.exit(-1);
16  });
17
18  // Verificar conexión a la base de datos
19  pool.connect((err) => {
20    if (err) {
21      return console.error('Error connecting to Database', err.stack);
22    }
23    console.log('Connected to Database');
24  });
25
26  module.exports = pool;
```

Figura 47. Código Carpeta Backend/src/database.js.

Este archivo **.env** almacena las configuraciones de entorno necesarias para que la aplicación se conecte a la base de datos y maneja datos sensibles de forma segura:

- **PORT=3000:** Especifica el puerto en el que el servidor Node.js escuchará las solicitudes entrantes.

- **DB_USER=postgres:** Nombre de usuario para acceder a la base de datos PostgreSQL.

- **DB_PASSWORD=12345:** Contraseña del usuario de la base de datos (se recomienda cambiarla por una contraseña segura en entornos de producción).

- **DB_HOST=localhost:** Dirección del servidor donde se encuentra la base de datos, en este caso, el servidor local.

- **DB_DATABASE=ISO27001:** Nombre de la base de datos a la que la aplicación se conectará.

- **DB_PORT=5432:** Puerto en el que PostgreSQL está escuchando conexiones.

- **SECRET_KEY='u3RfD!7wQ9Z^1Fv@8xLk0W$k2y8@Aq5H':** Clave secreta que podría usarse para firmar tokens o gestionar sesiones en la aplicación. Esta clave es fundamental para la seguridad en la autenticación y debe mantenerse privada.

Este archivo facilita la configuración sin necesidad de cambiar el código fuente y mantiene datos sensibles fuera del repositorio de código.

```
JS database.js    .env
Backend > .env
1  PORT=3000
2  DB_USER=postgres
3  DB_PASSWORD=12345
4  DB_HOST=localhost
5  DB_DATABASE=ISO27001
6  DB_PORT=5432
7
8  SECRET_KEY = 'u3RfD!7wQ9Z^1Fv@8xLk0W$k2y8@Aq5H'
```

Figura 48. Código Carpeta Backend/.env.

2.1.7.5. Presentación de Interfaces

Una vez descritos los componentes y procesos que conforman el backend y el frontend de la aplicación web, es fundamental entender cómo estos elementos se integran para proporcionar una interacción fluida para el usuario. Las interfaces de usuario, como punto de interacción entre el usuario final y el sistema, son la representación visual y funcional de la aplicación, que permiten al usuario ejecutar tareas específicas de manera intuitiva.

En esta sección, se presentarán algunas interfaces de usuario más importantes desarrolladas para la aplicación web SecureIso destacando cómo se implementan las funcionalidades y flujos definidos en el backend y frontend. En el Anexo 1 se encuentra el manual de usuario con todas las interfaces completas.

Figura 49. Imagen de Bienvenida. Fuente Propia.

I. Se llenan los campos con la información personal. Luego se procede a elegir el rol de la cuenta que se desea crear ("Auditor" o "Empresa") y finaliza haciendo clic en el botón "Registrar".

Figura 50. Imagen de Registro. Fuente Propia.

Iniciar Sesión

II. Se inicia sesión con el usuario creado en el paso anterior. Se ingresan el nombre de usuario y la contraseña, y luego se hace clic en "Iniciar Sesión".

Figura 51. Imagen de Inicio de sesión. Fuente propia.

III. Se visualiza la interfaz de la pantalla de inicio.

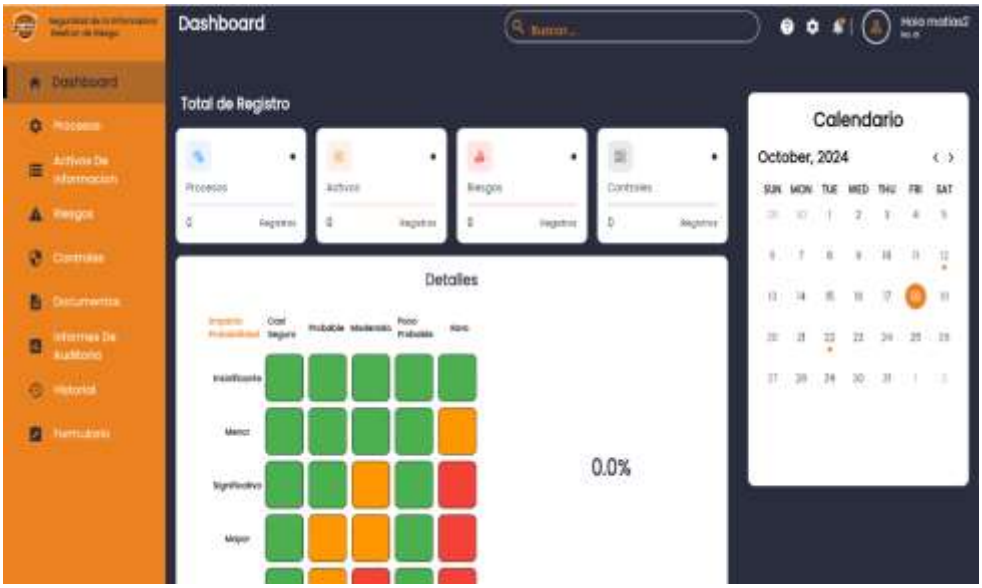

Figura 52. Imagen de Inicio. Fuente Propia.

IV. En el lado izquierdo de la pantalla de inicio, se encuentran las funciones principales para gestionar las áreas de la empresa.

Figura 53. Funciones Dashboard. Fuente Propia.

V. En el centro de la pantalla de inicio, se observa la cantidad de registros que se añaden en Procesos, Activos, Riesgos y Controles.

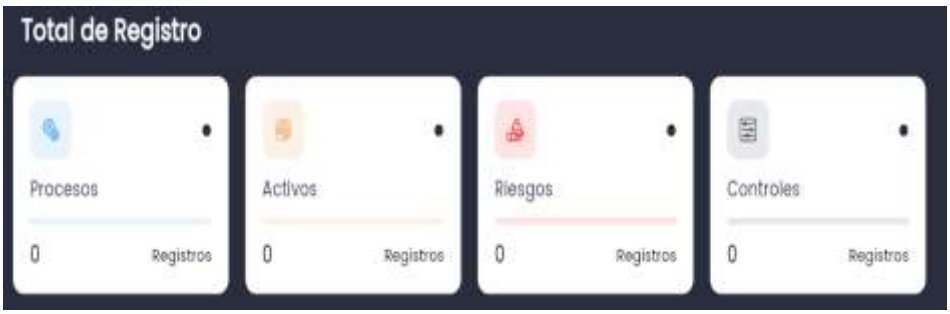

Figura 54. Imagen de Total Registro. Fuente Propia.

Perfil Del Usuario

VI. En la parte superior derecha, se encuentra el ícono de perfil. Se hace clic en él para desplegar la información personal del usuario. Debajo, se encuentra un botón "Salir" para cerrar sesión.

Figura 55. Imagen de Perfil. Fuente Propia.

CAPÍTULO 3. PRUEBAS FINALES

3.1 RESULTADOS

3.1.1 Pruebas De Usabilidad

Para validar la página web SecureIso, se formó un grupo de cinco personas, que incluía a estudiantes, profesores y miembros de la comunidad, todos de diferentes edades. A cada uno se le proporcionó un cuestionario dividido en tres partes: pre-test, test y post-test. Las tareas están especificadas para dos roles diferentes: Rol de empresa y Rol de auditor. Para las tareas del rol empresa se establece un total de 7 tareas, las cuales se dividieron en 2 partes variando así entre los usuarios, 3 usuarios con unas tareas y 2 usuarios con otras tareas diferentes con el objetivo de reducir la carga de tareas para ellos mismos. Este enfoque nos permitió evaluar si la plataforma era fácil de usar y si los participantes podían acceder a todas sus funciones sin complicaciones, o si, por el contrario, se encontraban con algunos obstáculos.

Las pruebas se llevaron a cabo en el laboratorio UX de la Institución Universitaria Colegio Mayor del Cauca, en Popayán, Cauca. Este espacio nos ofreció un ambiente ideal para observar la interacción del usuario con la página web y hacer los ajustes necesarios en base a los comentarios y resultados que obtuvimos.

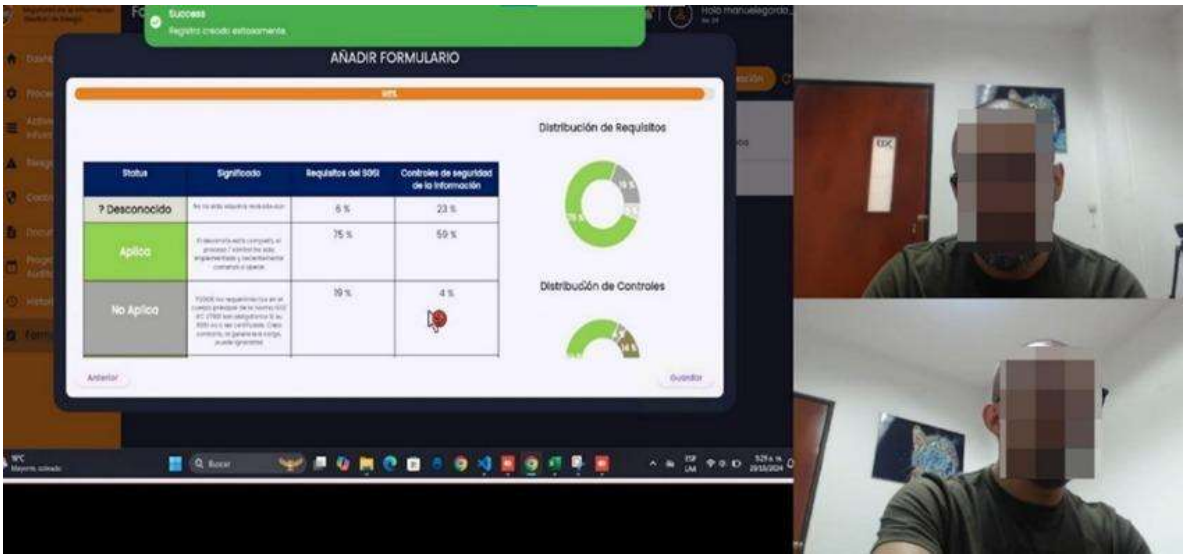

Figura 56. Pruebas de laboratorio. Fuente propia.

En la figura 56, se puede observar al usuario interactuando con la página web SecureIso, ubicada en el apartado de resultados del formulario de evaluación.

Figura 57. Pruebas de laboratorio. Fuente propia.

En la figura 57, se puede observar al usuario situado en el Laboratorio UX, resolviendo el cuestionario pre-test de las pruebas.

I. Aplicación Del Instrumento Test

- **Tiempo experto**

En la tabla 28, se presenta la realización de las tareas establecidas en el Test por el experto, correspondientes al rol de Empresa y al rol de Auditor, indicando el tiempo estipulado para cada una de ellas.

LISTA DE TAREAS			
Tareas rol empresa	**Tiempo**	**Tareas rol auditor**	**Tiempo**
Crear cuenta con rol empresa e iniciar sesión	20:10 segundos	Crear cuenta con rol auditor e iniciar sesión	20:70 segundos
Crear un nuevo riesgo con datos establecidos	35:60 segundos	Programar una nueva auditoría	16:55 segundos
Crear un nuevo documento con fechas establecidas	16:50 segundos	Modificar una auditoría programada	16:31 segundos
Eliminar un documento	15:20 segundos	Cambiar la organización a la de claro y programar una auditoría con fechas establecidas	27:55 segundos
Crear un nuevo proceso	27:93 segundos	Crear un nuevo formulario de evaluación luego visualizar resultados y sugerencias	5:30 minutos
Crear un nuevo activo con datos establecidos	23:64 segundos		
Crear nuevo control de seguridad asociado a un proceso y activo existente	35 :15 segundos		

Tabla 28. Se describen los tiempos del experto en las tareas de rol empresa y auditor. Fuente: Propia.

- **Rangos de tiempos para las tareas**

Rango de tiempo para tareas rol empresa

La tabla 29, muestra los rangos de tiempo estimados para la realización de tareas asignadas al rol de empresa, clasificándolos en tres niveles de desempeño: Alto (100%), Medio (80%) y Bajo (60%).

Lista de tareas	Alto (100 %)	Medio (80 %)	Bajo (60 %)
Crear cuenta con rol empresa e iniciar sesión	entre 20 y 30 segundos	entre 30 y 40 segundos	mayor a 40 segundos
Crear un nuevo riesgo con datos	entre 35 y 45	entre 45 y 55	mayor a 55

establecidos	segundos	segundos	segundos
Crear un nuevo documento con fechas establecidas	entre 15 y 25 segundos	entre 25 y 35 segundos	mayor a 35 segundos
Eliminar un documento	entre 15 y 25 segundos	entre 25 y 35 segundos	mayor a 35 segundos
Crear un nuevo proceso	entre 25 a 35 segundos	entre 35 y 45 segundos	mayor a 45 segundos
Crear un nuevo activo con datos establecidos	entre 20 y 25 segundos	entre 25 y 35 segundos	mayor a 35 segundos
Crear nuevo control de seguridad asociado a un proceso y activo existente	entre 35 y 45 segundos	entre 45 y 55 segundos	mayor a 55 segundos

Tabla 29. Rangos de tiempos de las tareas de rol empresa. Fuente: Propia.

Rango de tiempo para tareas rol auditor

La tabla 30, muestra los rangos de tiempo estimados para la realización de tareas asignadas al rol de auditor, clasificándolos en tres niveles de desempeño: Alto (100%), Medio (80%) y Bajo (60%).

Lista de tareas	Alto (100 %)	Medio (80 %)	Bajo (60 %)
Crear cuenta con rol auditor e iniciar sesión	entre 20 y 30 segundos	entre 30 y 40 segundos	mayor a 40 segundos
Programar una nueva auditoría	entre 15 y 20 segundos	entre 20 y 25 segundos	mayor a 25 segundos
Modificar una auditoría programada	entre 15 y 25 segundos	entre 25 y 35 segundos	mayor a 35 segundos
Cambiar la organización a la de claro y programar una auditoría con fechas establecidas	entre 25 y 35 segundos	entre 35 y 45 segundos	mayor a 45 segundos
Crear un nuevo formulario de evaluación luego visualizar resultados y sugerencias	entre 5 y 7 minutos	entre 7 y 9 minutos	mayor a 9 minutos

Tabla 30. Rangos de tiempos en las tareas de rol auditor. Fuente: Propia.

- **Resultados de las tareas del test**

Tareas Rol Empresa

- El objetivo de la tarea 1. Deseas crear una cuenta para gestionar las áreas de la organización. Accede al formulario de registro, completa los datos de registro como rol "**Empresa**" y luego inicia sesión con la cuenta recién creada.

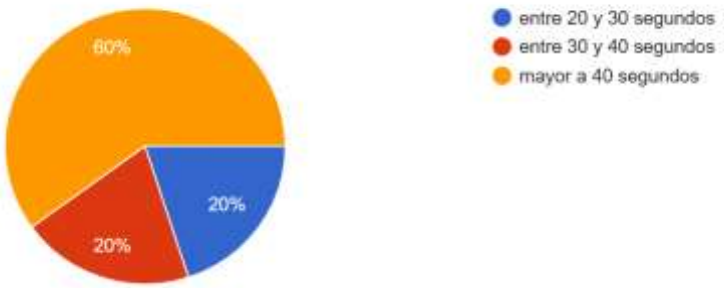

Figura 58. Tarea 1 rol empresa. Fuente: Propia.

En la figura 58, se pueden visualizar los resultados correspondientes a los 5 usuarios que realizaron la tarea, distribuidos en tres rangos de tiempo:

- **Entre 20 y 30 segundos:** El 20% de los usuarios completa la tarea en este rango de tiempo.
- **Entre 30 y 40 segundos:** Otro 20% de los usuarios terminó la tarea en este rango de tiempo.
- **Mayor a 40 segundos:** Un 60% de los usuarios tardaron más de 40 segundos en completar la tarea.

Estos resultados evidencian que la mayoría de los usuarios requirió más de 40 segundos para completar la tarea de crear una cuenta e iniciar sesión, lo que los sitúa en el rango más bajo en comparación con el tiempo óptimo alcanzado por el experto.

- El objetivo de la tarea 2. Buscas mitigar riesgos asociados al mal manejo de salarios de los empleados. Navega a la sección de "**Riesgos**", crea un nuevo riesgo con un Impacto “Severo”, con Probabilidad “Probable” y en Estado “Mitigado”.

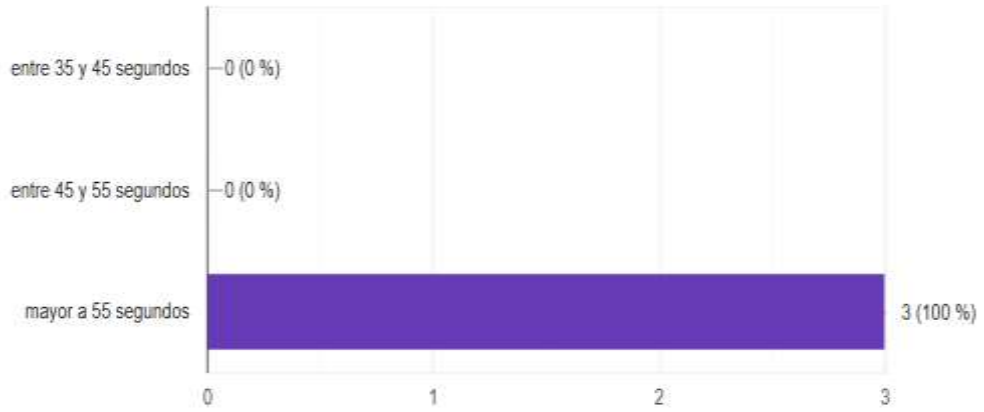

Figura 59. Tarea 2 rol empresa. Fuente: Propia.

En la figura 59, se presentan los resultados de los 3 usuarios que realizaron la tarea. El 100% de los usuarios tardó más de 55 segundos, ubicándose en el rango bajo de desempeño. Esto sugiere que la tarea presentó algún grado de dificultad que afectó la rapidez de los usuarios.

- El objetivo de la tarea 3, te propones almacenar y gestionar documentos clave para la entidad. Accede a la sección de "**Documentos**", añade un nuevo documento con la fecha de inicio 22 de octubre y fecha final 31 de octubre, y verifica que el documento se guarde correctamente.

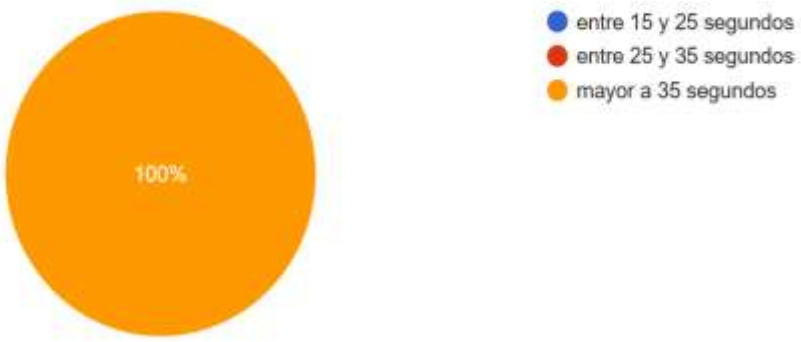

Figura 60. Tarea 3 rol empresa. Fuente: Propia.

En la figura 60, se muestran los resultados de los 3 usuarios que realizaron la tarea. El 100% de los usuarios tardó más de 35 segundos, situándose en el rango más bajo de desempeño. El tiempo fue superior al ideal (alto o medio) debido a las dificultades encontradas al adjuntar una imagen para finalizar el proceso de agregar un nuevo documento.

- El objetivo de la tarea 4, Deseas eliminar un documento que ya no es relevante. Accede a la lista de documentos, selecciona un documento y elimínalo.

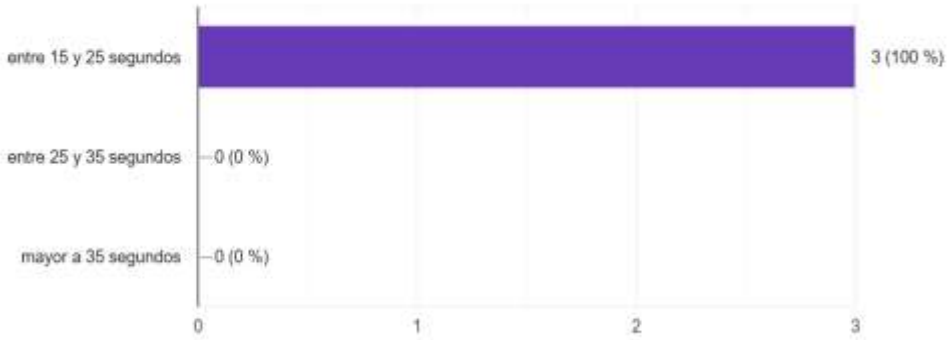

Figura 61. Tarea 4 rol empresa. Fuente : Propia.

En la figura 61, se puede observar los resultados de los 3 usuarios que completaron la tarea.

El 100% de los usuarios logró realizar la tarea en el rango de tiempo ideal (alto) de forma rápida y eficiente. Esto refleja que el proceso de eliminación de documentos es sencillo y puede realizarse sin complicaciones ni demoras.

- El objetivo de la tarea 5, Te interesa gestionar los procesos de la organización. Navega a la sección de "Procesos", crea un nuevo proceso con los respectivos datos específicos, y verifica que aparezca en la lista de procesos.

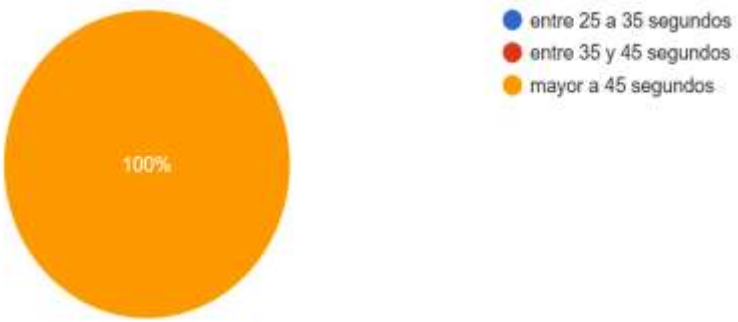

Figura 62. Tarea 5 rol empresa. Fuente : Propia.

En la figura 62, se observa los resultados de los 2 usuarios que completaron la tarea. El 100% de los usuarios necesitó más de 45 segundos para completarla, ubicándose así en el rango bajo de desempeño. Los usuarios experimentaron ligeras demoras al adjuntar una imagen al proceso, lo cual afectó considerablemente en su tiempo de añadir un nuevo proceso.

- El objetivo de la tarea 6. Quieres agregar activos de información para proteger los datos de la organización. Ve a la sección de "Activos de Información", crea un nuevo activo, completa la información y en el campo Tipo Activo coloca “Personas” y guarda.

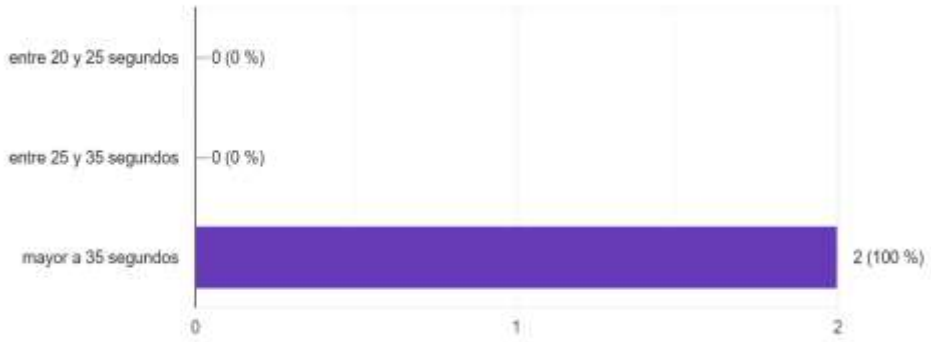

Figura 63. Tarea 6 rol empresa. Fuente : Propia.

En la figura 63, se puede observar los resultados para los 2 usuarios que realizaron la tarea.

El 100% de los usuarios necesitó más de 35 segundos para completarla, situándose así en el rango bajo de desempeño. Las demoras se debieron a dificultades al elegir las respuestas en las preguntas de selección múltiple, lo que afectó el tiempo requerido para añadir un nuevo activo.

- El objetivo de la tarea 7. Deseas gestionar los controles de seguridad de la organización. Crea un nuevo control de seguridad asociado a un proceso y un activo existente, modifica sus detalles y verifica que el control esté correctamente asignado. Es añadir un nuevo control asociado a los procesos y activos de la organización.

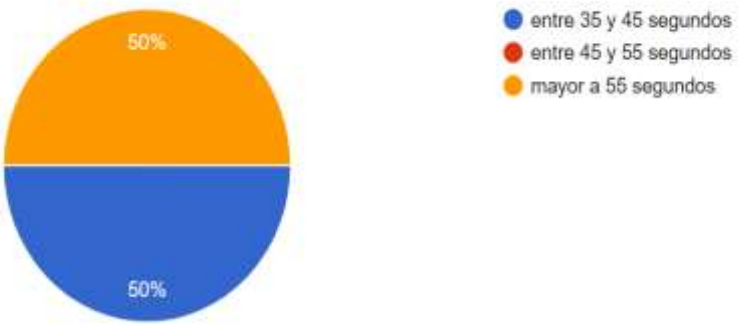

Figura 64. Tarea 7 rol empresa. Fuente : Propia.

En la figura 64, se puede observar los resultados para los 2 usuarios que realizaron la tarea, distribuidos en dos rangos de tiempo:

- **Entre 35 y 45 segundos:** El 50% de los usuarios completa la tarea en este rango de tiempo.
- **Mayor a 55 segundos:** Un 50% de los usuarios tardaron más de 55 segundos en completar la tarea.

Se observa una diferencia notable en la realización de la tarea, uno de ellos logró realizarla en un tiempo ideal (alto), mientras que el otro necesitó más de 55 segundos (bajo). Esto indica que algunos pasos en el proceso de creación o modificación de los datos del control requirieron más tiempo de lo esperado.

Tareas Rol Auditor

- El objetivo de la tarea 1. Deseas crear una cuenta para revisar el estado de una empresa, accede al formulario de registro, completa los datos de registro como rol “Auditor” y luego inicia sesión con la cuenta recién creada.

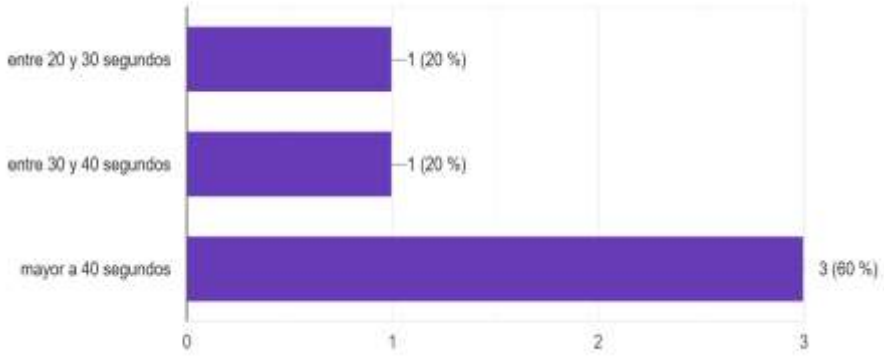

Figura 65. Tarea 1 rol auditor. Fuente : Propia.

En la figura 65, se observa los resultados para los 5 usuarios que realizaron la tarea, distribuidos en tres rangos de tiempo:

- **Entre 20 y 30 segundos:** El 20% de los usuarios completa la tarea en este rango de tiempo.

- **Entre 30 y 40 segundos:** Otro 20% de los usuarios terminó la tarea en este rango de tiempo.
- **Mayor a 40 segundos:** Un 60% de los usuarios tardaron más de 40 segundos en completar la tarea.

Estos resultados indican que la mayor parte de los usuarios necesitaron más de 40 segundos para realizar la tarea, ubicados en el rango más bajo en comparación con el tiempo óptimo (alto) alcanzado por el experto.

- El objetivo de la tarea 2. Te propones programar una nueva auditoría. Te diriges a crearla, asignándole un nombre y una fecha disponible que hayas elegido, asegurándose de que coincida con la agenda de la empresa para facilitar la coordinación y la disponibilidad de ambos.

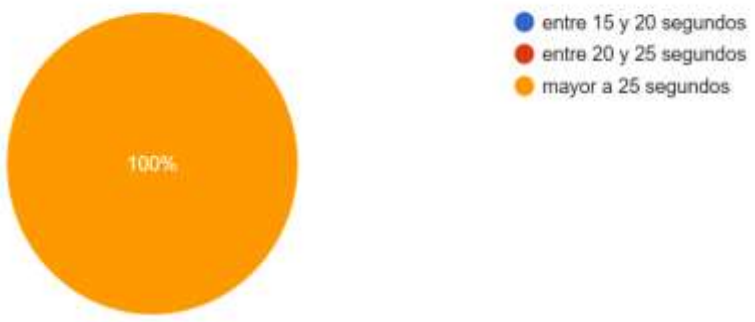

Figura 66. Tarea 2 rol auditor. Fuente : Propia.

En la figura 66, se puede observar los resultados para los 5 usuarios que realizaron la tarea.
El 100% de los usuarios necesitó más de 25 segundos para completarla, situándose en el rango bajo de desempeño. Los usuarios experimentaron una ligera demora al elegir las diferentes fechas que podrían estar disponibles para la empresa.

- El objetivo de la tarea 3. Deseas modificar una auditoría programada. Te diriges a la sección correspondiente y seleccionas la auditoría que deseas

modificar, actualizando el nombre y la fecha según sea necesario, y asegurándose de que los cambios sean coherentes con la agenda de la empresa.

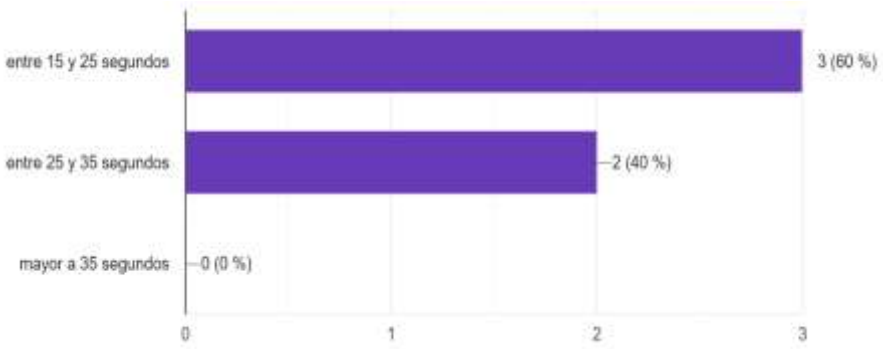

Figura 67. Tarea 3 rol auditor. Fuente : Propia.

En la figura 67, se puede visualizar los resultados para los 5 usuarios que realizaron la tarea.

Se observa que el 60% de los usuarios no experimentó dificultad alguna, logrando completar la tarea dentro del tiempo ideal definido por el experto, el 40% de los usuarios presentó una ligera demora, ubicándose en un rango de desempeño medio. En conclusión, la mayoría de los usuarios logró completar la tarea con éxito, con una diferencia mínima en los tiempos de ejecución.

- El objetivo de la tarea 4. Te interesa cambiar de empresa para evaluar una diferente. Te diriges a la sección de perfil, y en el apartado de organizaciones eliges entre las empresas a las que estás asignado. Seleccionas la empresa que esté registrada o asignada al auditor y programas una auditoría para el 10 de noviembre.

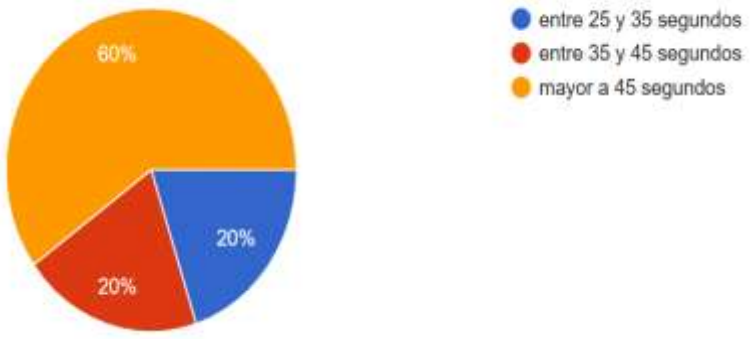

Figura 68. Tarea 4 rol auditor. Fuente : Propia.

En la figura 68, se pueden visualizar los resultados para los 5 usuarios que realizaron la tarea, distribuidos en tres rangos de tiempo:

- **Entre 25 y 35 segundos:** El 20% de los usuarios completa la tarea con rapidez, mostrando un buen dominio de la página.
- **Entre 35 y 45 segundos:** Otro 20% de los usuarios terminó la tarea pero con un ligero retraso en el tiempo.
- **Mayor a 45 segundos:** Un 60% de los usuarios tardaron más de 40 segundos en completar la tarea, tuvieron alguna dificultad en encontrar la empresa asignada.

La mayoría de los usuarios experimentaron alguna complicación en la navegación hacia el apartado de organizaciones y seleccionar una empresa, lo cual le afectó considerablemente a la hora de poder finalizar la tarea.

- El objetivo de la tarea 5. Te propones crear un formulario de evaluación para la empresa. Te diriges a la sección “Formulario” y completas los campos necesarios, incluyendo el nombre de la empresa, la fecha de la evaluación y el nombre de la persona que la realizará. Luego, seleccionas las preguntas de selección múltiple que cubrirán aspectos clave para obtener una visión detallada sobre el estado actual de la empresa. Al finalizar se visualizará los

resultados finales de tu prueba junto a unas sugerencias que te ayudarán a mejorar la estructura de la empresa.

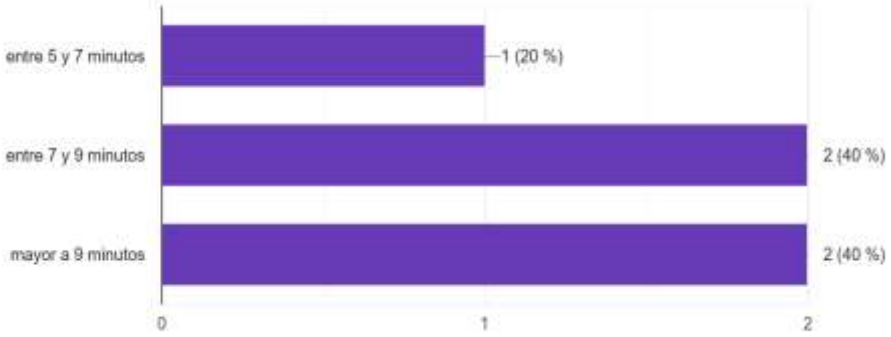

Figura 69. Tarea 5 rol auditor. Fuente: Propia.

En la figura 69, se pueden visualizar los resultados para los 5 usuarios que realizaron la tarea, distribuidos en tres diferentes rangos de tiempo:

- **Entre 5 y 7 minutos:** El 20% de los usuarios completa la tarea con rapidez, mostrando un buen nivel de fluidez en el uso del formulario.
- **Entre 7 y 9 minutos:** Un 40% de los usuarios tuvieron un retraso en el tiempo, ya que algunos se detuvieron a leer y comprender bien las preguntas antes de seleccionar una respuesta.

- **Mayor a 9 minutos:** Un 40% de los usuarios tardaron más de 9 minutos, hubo complicaciones a la hora de avanzar en el formulario ya que olvidaban responder alguna pregunta lo cual generaba un error y los obligaba a regresar y completar los campos.

La mayoría de los usuarios enfrentó complicaciones durante la navegación del formulario, especialmente al intentar avanzar sin completar todos los campos, esta situación generó cierta impaciencia en algunos usuarios, ya que se vieron obligados a regresar a completar los campos vacíos. Un 80% de los usuarios se ubicó en los rangos de tiempo medio y bajo en comparación al tiempo ideal del experto (alto).

En la tabla 31, se presentan los resultados obtenidos en el Test, indicando el tiempo en segundos, que cada usuario tardó en completar cada tarea. Los campos etiquetados como "No realiza" corresponden a tareas que los usuarios no llevaron a cabo, debido a que algunos participantes tenían asignadas tareas diferentes para el rol de empresa. Finalmente, se incluye una evaluación general sobre el nivel de usabilidad de la página web analizada.

Resultado Test					
Pregunta	**Usuario 1**	**Usuario 2**	**Usuario 3**	**Usuario 4**	**Usuario 5**
TAREA 1	21	73	35	83	92
	100%	60%	80%	60%	60%
TAREA 2	93	170	276	No Realiza	No Realiza
	60%	60%	60%		
TAREA 3	57	151	166	No Realiza	No Realiza
	60%	60%	60%		
TAREA 4	16	20	20	No Realiza	No Realiza
	100%	100%	100%		
TAREA 5	No Realiza	No Realiza	No Realiza	251	207
				60%	60%
TAREA 6	No Realiza	No Realiza	No Realiza	86	76
				60%	60%
TAREA 7	No Realiza	No Realiza	No Realiza	136	40
				60%	100%
TAREA 8	30	93	180	57	40
	100%	60%	60%	60%	80%
TAREA 9	37	55	480	60	74
	60%	60%	60%	60%	60%
TAREA 10	22	20	26	30	20

	100%	100%	80%	80%	100%
TAREA 11	61	106	69	26	43
	60%	60%	60%	100%	80%
TAREA 12	450	401	790	780	523
	80%	100%	60%	60%	60%
Resultado por usuario	**80%**	**73.3%**	**68.8%**	**66.6%**	**73.3%**
				Nivel de usabilidad	**72.4%**

Tabla 31. Se describen los tiempos en segundos de los usuarios. Fuente: Propia.

II. Aplicación del Instrumento Post – Test.

Tras la realización del Post-Test, que incluyó preguntas cuantitativas y cualitativas, se obtuvieron los siguientes resultados:

Las preguntas cuantitativas fueron formuladas de manera clara y precisa para obtener datos numéricos fácilmente medibles. Se emplearon escalas de calificación, opciones de respuesta múltiple y preguntas dicotómicas (Sí/No), asegurando que las preguntas fueran directas y sin ambigüedades. Este enfoque permitió la obtención de datos coherentes y fáciles de analizar. Por otro lado, las preguntas cualitativas se formularon para capturar las opiniones, percepciones y experiencias más detalladas de los participantes. A través de preguntas abiertas, se buscó fomentar una mayor expresión personal y reflexión por parte de los encuestados.

El Post-test cuenta con un total de 12 preguntas, de las cuales 6 son de tipo cuantitativas y 6 cualitativas, las preguntas cualitativas son categorizadas de la siguiente manera:

- La figura 70, permite categorizar la pregunta 1. **¿Cómo describirías tu experiencia al usar SECUREISO? ¿Consideras que fue fácil de usar?** En una escala del 1 al 5, donde 5 es alto y 1 el más bajo.

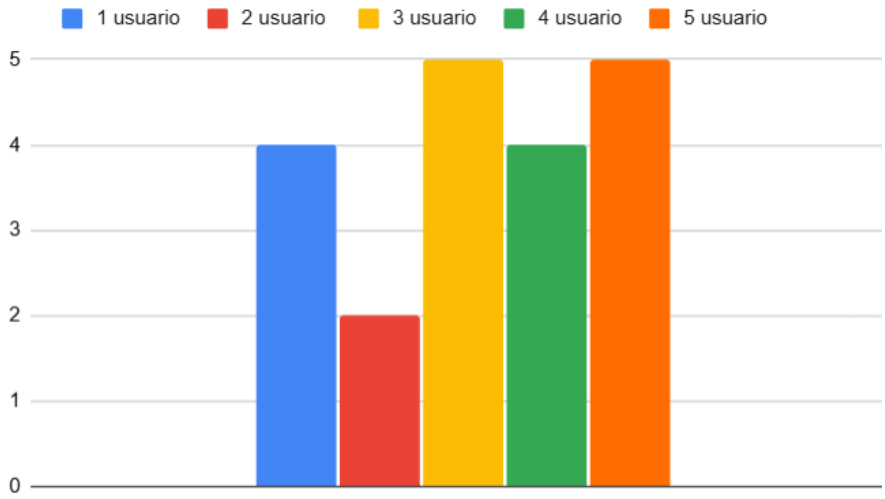

Figura 70. Categorización pregunta 1. Fuente : Propia.

Un 40% de los usuarios calificó su interacción con un 5 en una escala del 1 al 5, indicando que la encontraron muy buena y fácil de usar. Otro 40% asignó una puntuación de 4, lo que sugiere una interacción positiva y sin complicaciones. El 20% restante puntuó con un 2, reflejando cierta dificultad e insatisfacción al realizar las tareas.

- La figura 71, permite categorizar la pregunta 2. ¿Te sentiste cómodo al realizar las tareas propuestas? En una escala del 1 al 5, donde 5 es alto y 1 el más bajo.

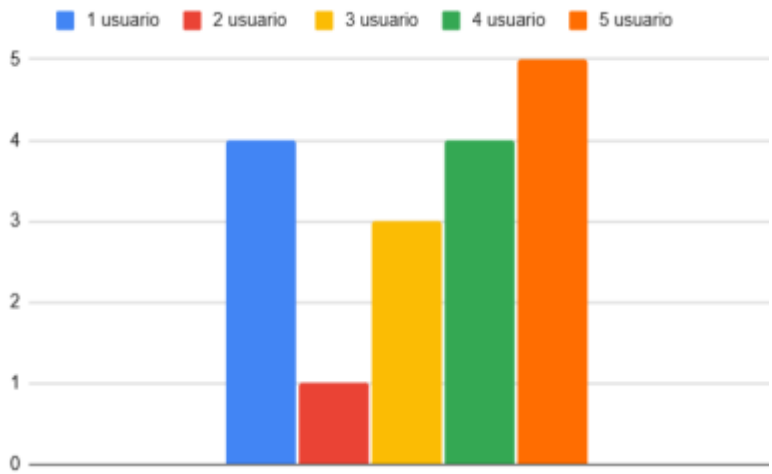

Figura 71. Categorización pregunta 2. Fuente : Propia.

Se puede observar que un 20% de los usuarios calificó su interacción con un 5, indicando que se sintieron muy cómodos al realizar las tareas. Otro 40% asignó una puntuación de 4, lo cual sugiere una interacción positiva y sin mayores dificultades. Un 20% otorgó una calificación de 3, reflejando una comodidad moderada con algunas complicaciones. Finalmente, el 20% restante calificó con un 1, lo que indica un nivel bajo de comodidad al realizar las tareas propuestas en el test.

- La figura 72, permite categorizar la pregunta 3. **¿Cuál es tu nivel de satisfacción con la experiencia en la página web (colores, tamaño y tipo de fuentes, colocación de los elementos, iconos, etc.)?** En una escala del 1 al 5, donde 5 es alto y 1 el más bajo.

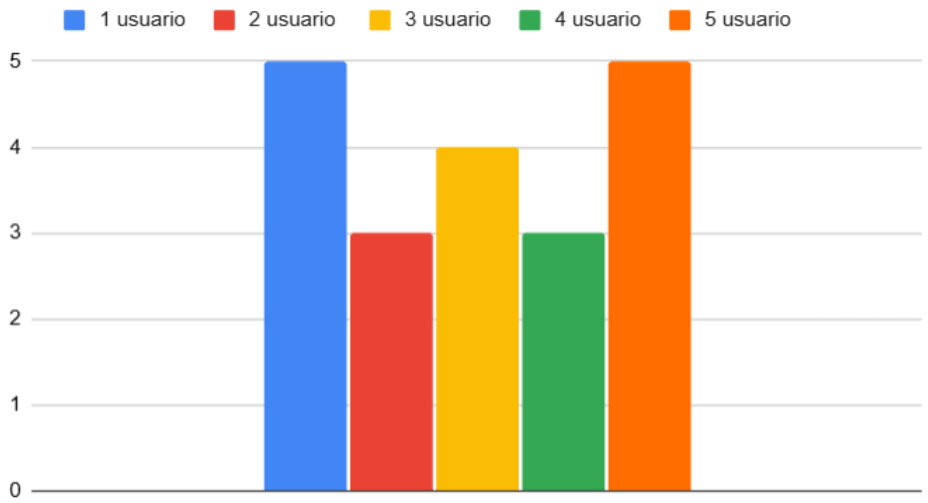

Figura 72. Categorización pregunta 3. Fuente : Propia.

La pregunta 3, recopila datos sobre la satisfacción sobre la estética de la página web, donde, se puede decir que la mayoría de los usuarios están satisfechos con la estética de la página. Un 40% calificó su experiencia con un 5, destacando su agrado por la iconografía, los tipos de fuente y la disposición de los elementos, lo que hizo que navegar en la página fuera visualmente agradable. Otro 20% le dio un 4, lo cual indica

que en general les gustó el diseño, aunque podrían notar detalles mejorables. Finalmente, un 20% puntuó con un 3, expresando una satisfacción moderada, mostrando un poco de inconformidad con los colores usados dándoles un poco de incomodidad al realizar las tareas.

- La figura 73, permite categorizar la pregunta 5. ¿Te gustaría usar SECUREISO nuevamente?

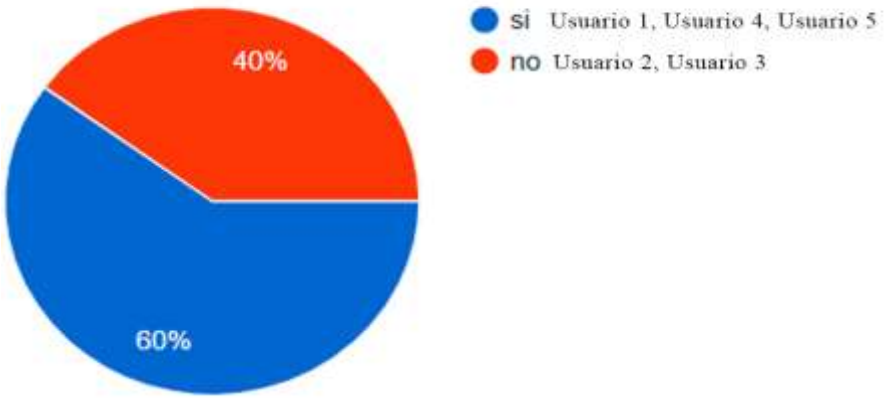

Figura 73. Categorización pregunta 5. Fuente : Propia.

El 60% de los participantes respondió que sí les gustaría usar SECUREISO nuevamente, reflejando una experiencia positiva con la plataforma y satisfacción con su utilidad y facilidad de uso. Sin embargo, el 40% indicó que no volvería a utilizarla, lo cual sugiere que algunos encontraron aspectos que no cumplieron con sus expectativas o áreas donde vieron inconformidad y quizá podría mejorar. En resumen, 3 usuarios están contentos y volverían a usarla, en comparación con 2 usuarios que no.

- La figura 74, permite categorizar la pregunta 9. ¿Recomendarías SECUREISO a otras personas para que lo utilicen en sus empresas?

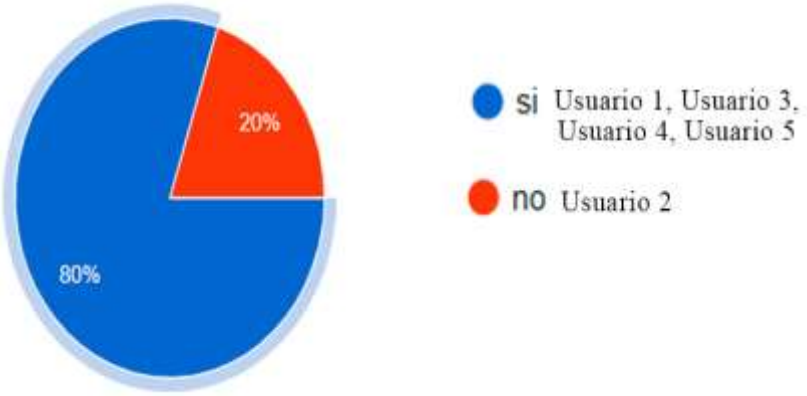

Figura 74. Categorización pregunta 9. Fuente: Propia.

Se puede evidenciar que el 80% de los usuarios afirmó que recomendaría SECUREISO, lo que muestra una percepción positiva y una gran confianza en la página web como una herramienta útil para otras empresas. Este grupo de usuarios parece estar satisfecho, ya que SECUREISO cumple con sus expectativas y creen que puede ser valioso en situaciones similares. Por otro lado, el 20% de los usuarios que hace referencia a 1 solo usuario, dijo que no lo recomendaría, lo que quizás sugiere que encontró áreas de mejora o limitaciones que le impidió tener una experiencia completamente satisfactoria.

- La figura 75, permite categorizar la pregunta 11. ¿Qué tan intuitiva consideras la interfaz de SECUREISO para nuevos usuarios?

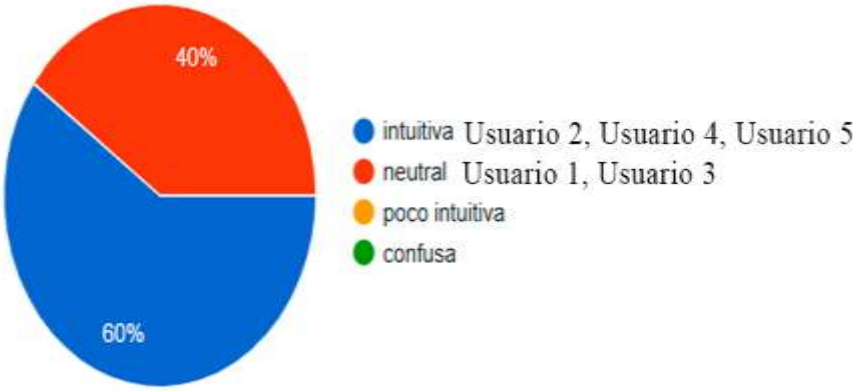

Figura 75. Categorización pregunta 11. Fuente: Propia.

El 60% de los usuarios siente que la interfaz de SECUREISO es intuitiva y fácil de usar para quienes son nuevos en la página web, lo que refleja una percepción positiva de su diseño y usabilidad. Sin embargo, el 40% restante tiene una opinión más neutral: aunque no encontraron grandes problemas, creen que la experiencia podría mejorarse en algunos aspectos como más ayudas en imágenes o una guía para que resulte más clara o accesible para todos los usuarios nuevos.

Las siguientes preguntas fueron de tipo cuantitativo, donde se incluía un espacio abierto para que los usuarios pudieran expresar libremente sus opiniones sobre posibles mejoras o inconformidades relacionadas con la página web de SECUREISO.

- **Pregunta 4. ¿Qué es lo que más le gustó de SECUREISO?**

Los usuarios resaltan varios aspectos positivos de la plataforma. Algunos mencionaron que les gustaron los resultados y sugerencias al finalizar el formulario de evaluación, mientras que otros destacaron la pantalla de registro y la estructura organizada de la página. Además, valoraron la simplicidad y facilidad de uso de la interfaz, así como el contraste, los colores y el tamaño del texto, que hacen que la aplicación sea más fácil de usar. Sin embargo, un usuario comentó que, aunque le agrada la estructura y los estilos, el color anaranjado no refleja muy bien un contraste en la interfaz, así ocasionando inconformidad al realizar las tareas.

- **Pregunta 6. ¿Hubo algún aspecto de SECUREISO que te resultara difícil o incómodo de usar en esa situación?**

Algunos de los usuarios mencionaron que les faltaba información completa sobre la empresa en el apartado de colocar las fechas disponibles, lo que hizo que ciertos procesos se sintieran un poco complejos. Además, señalaron que el formulario carece de guías claras para ayudar en la selección de opciones, lo que podría hacerlo menos intuitivo y agotador. Así mismo algunos usuarios destacaron su inconformidad con el color anaranjado de la interfaz lo que le dificulto algunas tareas, y otros percibieron que la evaluación del formulario es demasiado larga, siendo así la tarea que más tiempo les costó y mostraron algo de impaciencia por la gran totalidad de preguntas que este tenía.

- **Pregunta 7. ¿Qué opinas sobre el rendimiento de SECUREISO al realizar tareas como registrar, eliminar y editar áreas de una empresa, o crear formularios?**

Los usuarios compartieron opiniones muy positivas hacia las funciones de las áreas de la empresa, hubo unos comentarios donde reflejan que la página web es sencilla y fácil de usar para cualquier tipo de usuario, además de que responde rápido sin alguna interrupción mostrando así un funcionamiento eficiente e intuitivo. Algunos usuarios describieron que la interfaz en todo momento se sintió fluida al navegar en sus funciones y conformes al trabajar en ella.

- **Pregunta 8. ¿Qué cambiarías o añadirías a la página web?**

Algunos usuarios mencionan que sería útil reducir el número de preguntas que hay que responder para obtener los resultados, ya que simplificar el proceso podría hacerlo más rápido y menos abrumador. Otro punto que se destaca es que la página no debería borrar los datos ingresados si el usuario olvida completar algún campo, ya que, si se omite algo, hay que volver a ingresar toda la información lo cual resulta frustrante. Además, varios sugieren que se podrían cambiar los colores para hacer que la página sea más atractiva visualmente y más fácil de leer. Además, para finalizar también recomiendan usar nombres más claros para las funciones y acciones en la página web.

- **Pregunta 10. ¿Qué funcionalidades de SECUREISO encontraste más útiles?**

Los usuarios mencionan varias funcionalidades de SECUREISO que les resultan especialmente útiles. Una de las más destacadas es la opción de programar auditorías, lo que permite tener todo planificado con antelación. Además, las funciones de crear, editar y eliminar son muy prácticas, ya que dan mucha flexibilidad a la hora de gestionar muy bien las funcionalidades en la página web. La capacidad de crear perfiles, evaluar procesos internos de la empresa es un punto fuerte, ya que permite un análisis detallado de todas los procesos internos que

realice tanto en el rol “**Empresa**” como en el rol “**Auditor**”. La estética de la página web no pasa desapercibida al ofrecer una interfaz bien diseñada hace que su uso sea mucho más agradable y fácil de navegar.

- **Pregunta 12. ¿Algo adicional que quisiera comentar sobre SECUREISO?**

En general, los usuarios encuentran que SECUREISO funciona de manera bastante eficiente, aunque algunos quienes sugieren que sería útil incorporar más imágenes en la plataforma y cambiar un poco los colores, así como un sistema de ayuda contextual, que podría hacer mucho más fácil la experiencia. Cabe destacar que solo son comentarios de 2 usuarios ya que 3 usuarios no dejaron ningún tipo de comentario adicional.

El análisis de las interacciones de los usuarios en SECUREISO brinda una visión integral sobre la facilidad de uso, satisfacción general y las áreas de mejora. En las pruebas de usabilidad, los participantes completaron tareas clave en el Test, como crear cuentas, gestionar documentos, programar auditorías y crear activos de seguridad. En general, encontraron la plataforma intuitiva, aunque algunas funciones se percibieron como lentas o complicadas, lo que afectó la fluidez de la experiencia. El registro fue satisfactorio para la mayoría, aunque algunos participantes tardaron más de lo esperado, sugiriendo que simplificar este flujo podría mejorar la experiencia. En la gestión de documentos, eliminar elementos fue una tarea rápida y sin problemas, pero algunos usuarios notaron lentitud al adjuntar imágenes, lo que prolonga el tiempo de ejecución. La creación de formularios tomó entre 5 y 9 minutos, superando las expectativas. Los usuarios mencionaron que la extensión de los formularios fue considerada agotadora, y el hecho de olvidar un campo los obligaba a completar toda la información nuevamente, lo que generó frustración. Incorporar opciones para guardar el progreso parcial o reducir la cantidad de campos podría optimizar esta experiencia. En la creación de activos y controles de seguridad, algunos participantes percibieron lentitud en el proceso debido a la dificultad para identificar rápidamente las opciones desplegables.

En cuanto al nivel de usabilidad general de la página, se obtuvo un promedio de 72.4% de satisfacción en las tareas de usabilidad, considerando los resultados específicos por usuario: el usuario 1 obtuvo un 80%, el usuario 2 un 73.3%, el usuario 3 un 68.8%, el usuario 4 un 66.6%, y el usuario 5 un 73.3%. Estos datos reflejan la percepción general de la plataforma y destacan las áreas donde podría ser más ágil o intuitiva.

En la encuesta Post-Test, los usuarios calificaron su experiencia positivamente en general. Un 80% de los participantes dio calificaciones altas (4 o 5 de 5) respecto a la facilidad de uso y la experiencia general, subrayando la intuición de la plataforma y la facilidad para navegar y completar tareas. Sin embargo, un 20% informó dificultades, reflejando una experiencia menos satisfactoria.

En relación con el uso futuro, un 60% de los usuarios expresó su intención de volver a utilizar SECUREISO, valorando su utilidad para gestionar áreas clave en sus organizaciones. Sin embargo, un 40% no estaría interesado en usarla nuevamente, mencionando las áreas de mejora identificadas en las encuestas.

La mayoría de los participantes recomendaría SECUREISO a otros, reconociendo su valor en entornos profesionales. Sugerencias de mejora incluyen reducir la cantidad de preguntas en los formularios, conservar datos ya ingresados al omitir algún campo, y añadir nombres más descriptivos a las funciones. También se sugieren ajustes estéticos, como modificar ciertos colores y agregar más imágenes o ayudas contextuales que faciliten la experiencia a nuevos usuarios. La interfaz fue vista como intuitiva y rápida al realizar tareas sencillas, y valoraron la capacidad de programar auditorías y gestionar procesos internos, considerándola uno de los puntos fuertes de la plataforma.

En conclusión, SECUREISO fue bien recibida por los usuarios, quienes se mostraron satisfechos con el diseño de iconos, fuentes, colores y la disposición de elementos, lo cual facilitó una navegación visualmente agradable. Aunque algunos señalaron inconformidades menores que podrían mejorarse a futuro, en general valoraron la plataforma positivamente en cuanto a funcionalidad y facilidad de uso. La combinación de una estética atractiva y una interfaz intuitiva contribuye a una

experiencia sólida, aunque optimizar ciertos aspectos clave podría hacer la navegación aún más cómoda y eficiente, simplificando procesos y elevando la satisfacción general de los usuarios.

3.1.2. Pruebas De La Herramienta SECUREISO

La eficiencia y la efectividad son conceptos clave en la implementación de la herramienta digital según la ISO 27001, ya que definen la capacidad de optimizar recursos y alcanzar resultados esperados en la gestión de la seguridad de la información. La eficiencia se refiere al uso adecuado y racional de los recursos disponibles, minimizando el tiempo y los esfuerzos necesarios para cumplir con los requisitos de la norma. Por otro lado, la efectividad está relacionada con la capacidad de alcanzar los objetivos establecidos, asegurando que las medidas implementadas cumplan con los controles y estándares de seguridad requeridos.

En este estudio, se ha diseñado y desarrollado una herramienta digital innovadora basada en un marco metodológico de desarrollo seguro, con el objetivo de facilitar y optimizar la implementación del estándar ISO/IEC 27001 en diversos contextos organizacionales. Para evaluar su desempeño, se utilizó el Modelo de Aceptación de Tecnología (TAM), un enfoque reconocido para analizar la percepción de los usuarios respecto a la utilidad y la facilidad de uso de nuevas tecnologías.

3.1.2.1. Proceso de Evaluación Tecnológica con TAM

- **Contexto**

El estudio se llevó a cabo en el contexto de organizaciones que buscan optimizar la gestión de la seguridad de la información a través de la implementación del estándar ISO/IEC 27001. Estas organizaciones requieren soluciones digitales que no solo cumplan con los requisitos normativos, sino que también mejoren la eficiencia operativa y aseguren la efectividad en el cumplimiento de los objetivos de seguridad. Para abordar esta necesidad, se desarrolló la herramienta SECUREISO, diseñada para facilitar la implementación de controles y la gestión integral de los riesgos asociados al estándar.

- **Cuestionario y Evaluación**

Como parte de la evaluación, se elaboró un cuestionario compuesto por 14 preguntas diseñadas para medir dos factores fundamentales: la utilidad percibida y la facilidad de uso percibida de la herramienta digital SECUREISO. Estas preguntas se centraron en aspectos clave como la eficiencia en la gestión de la información, la efectividad en el cumplimiento de los requisitos de la norma, la claridad en la implementación de los controles, y la usabilidad para usuarios con diferentes niveles de experiencia.

Las preguntas relacionadas con la efectividad, que son 9 en total, se enfocan en la capacidad de la herramienta para alcanzar los objetivos de la norma ISO/IEC 27001, tales como:

- **¿Qué tan efectivo fue el uso de SECUREISO para facilitar el cumplimiento de los requisitos de la ISO 27001?**

- **¿Preferirías utilizar la herramienta SECUREISO para implementar la norma ISO 27001 en lugar del método convencional, que consiste en realizar el proceso de forma manual a través de Excel?**

Por otro lado, las preguntas relacionadas con la eficiencia, que son un total de 4, se centran en la utilización óptima de recursos, tiempo y esfuerzo durante la implementación de la norma. Un ejemplo de estas preguntas es:

- **¿Qué tan eficiente consideras que fue la gestión de la información a través de SECUREISO?**

- **¿Considera que la implementación de los controles de la ISO 27001 en la herramienta te pareció clara y bien organizada?**

El análisis de las respuestas obtenidas permitirá dar cumplimiento al objetivo general de este estudio: desarrollar una herramienta digital innovadora que, mediante su

diseño seguro y funcional, optimice la implementación de la norma ISO/IEC 27001. Este enfoque no solo busca mejorar la eficiencia operativa al reducir tiempos y recursos, sino también garantizar una gestión efectiva que cumpla con los estándares establecidos para la seguridad de la información.

Con la aplicación del modelo TAM y el análisis detallado de las percepciones de los usuarios, se espera validar que la herramienta propuesta representa una solución viable y práctica para los desafíos actuales en la implementación de la ISO/IEC 27001, beneficiando a organizaciones de distintos sectores.

- **Resultados Obtenidos y Análisis**

Los resultados obtenidos a través del cuestionario permitieron evaluar la percepción de los usuarios respecto a la utilidad y facilidad de uso de la herramienta digital desarrollada. Entre las preguntas más relevantes, se destacaron:

A. Efectiva

Estas preguntas están relacionadas con la capacidad de la herramienta para alcanzar los objetivos de la norma ISO/IEC 27001.

En la figura 76, se puede observar una percepción altamente positiva por los usuarios sobre la utilidad percibida de SECUREISO, específicamente en aspectos vinculados a su efectividad para cumplir con los objetivos de la norma ISO/IEC 27001. Las respuestas destacan su capacidad para gestionar eficazmente los riesgos requeridos por la norma, con puntuaciones máximas en esta categoría. Asimismo, los usuarios expresaron una clara preferencia por utilizar la herramienta en lugar de métodos tradicionales, como hojas de cálculo, lo que resalta su practicidad y alineación con las necesidades de las organizaciones. Otro aspecto relevante es su efectividad en la reducción del tiempo necesario para implementar la norma, evidenciando su contribución a la optimización de recursos.

Los participantes destacan la importancia de contar con herramientas tecnológicas que simplifiquen la implementación de los requisitos y controles de seguridad, una necesidad que SECUREISO satisface de manera sobresaliente. Su efectividad se estima en un 97.5%, reflejando una percepción altamente positiva por parte de los usuarios. Este resultado confirma que la herramienta cumple con su propósito de facilitar la implementación y gestión de los requisitos establecidos en la norma ISO/IEC 27001, consolidándose como una solución eficaz para optimizar la seguridad de la información.

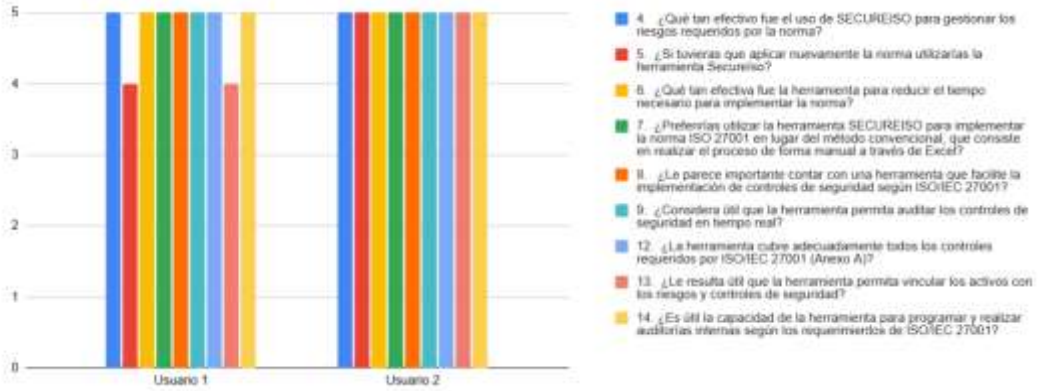

Figura 76. Categorización de preguntas efectividad. Fuente: Propia

B. Eficiente

Estas preguntas se centran en el uso óptimo de recursos, tiempo y esfuerzo en la implementación de la norma.

Los resultados de la figura 77, muestra que la herramienta SECUREISO ha sido bien recibida en general, aunque con algunas diferencias en la percepción de los usuarios. Por un lado, el Usuario 1 valoró de manera positiva la eficiencia en la gestión de la información y destacó la facilidad de navegación y uso para personas con poca experiencia, aunque encontró que la implementación de los controles de ISO 27001 podría ser más clara y organizada. Por otro lado, el Usuario 2 tuvo una experiencia completamente satisfactoria, otorgando la máxima calificación a todos los aspectos evaluados. En conjunto, esto sugiere que la herramienta es intuitiva y accesible, pero todavía hay margen para mejorar ciertos elementos, como la claridad en la

implementación de los controles de seguridad, con el objetivo de ofrecer una experiencia aún más uniforme y positiva para todos los usuarios.

Su eficiencia se estima con un promedio general del 89%, lo que sugiere que la herramienta es intuitiva y cumple con sus objetivos, aunque podría beneficiarse de ajustes para mejorar la claridad en algunos procesos específicos.

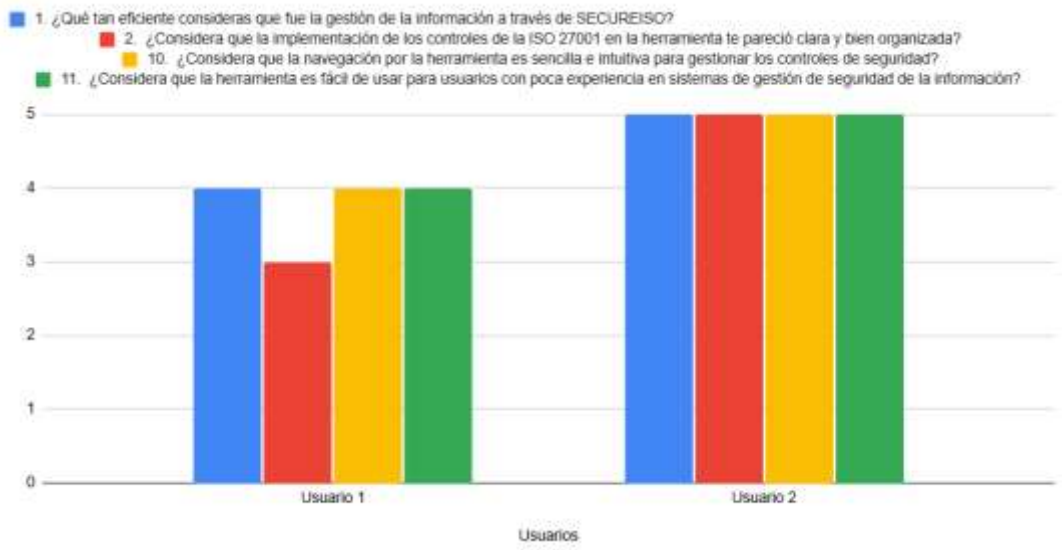

Figura 77. Categorización de preguntas eficiencia. Fuente: Propia

El análisis de las respuestas permitió identificar patrones claros que evidencian el impacto positivo de la herramienta en términos de eficiencia y efectividad. Por ejemplo, se observó que los usuarios valoran la capacidad de la herramienta para reducir el tiempo necesario para implementar los controles de seguridad, así como su facilidad para vincular activos, riesgos y controles de forma integral. Adicionalmente, las opiniones destacaron la navegación intuitiva como un factor crucial para mejorar la experiencia del usuario, incluso para aquellos con poca experiencia en sistemas de gestión de seguridad de la información.

Estos resultados se explicaron mediante el análisis de las dimensiones del Modelo de Aceptación de Tecnología (TAM), que permitió correlacionar los altos niveles de utilidad percibida con la efectividad reportada por los usuarios y los valores positivos

en facilidad de uso percibida con la reducción de barreras de adopción. Esto valida el cumplimiento del objetivo general, al demostrar que la herramienta no solo optimiza la implementación de la norma ISO/IEC 27001, sino que también facilita una gestión más estructurada y accesible, permitiendo a las organizaciones alcanzar sus metas de seguridad de la información de manera más eficiente y efectiva.

3.1.3. Pruebas De Seguridad

Para las pruebas de seguridad de la página web Secureiso, se utilizó el programa OWASP ZAP, una herramienta de seguridad gratuita y de código abierto, empleada para realizar pruebas de penetración y análisis de seguridad en aplicaciones web. El primer paso consistió en realizar un escaneo activo para identificar posibles vulnerabilidades en la página web. El análisis de seguridad mostró que la página es razonablemente segura, ya que no se encontraron vulnerabilidades críticas. Sin embargo, existen algunos aspectos que aún pueden mejorarse para hacerla más robusta frente a posibles ataques.

En la figura 78, se realizó un ataque de spidering (araña) al front-end. Se observó que se detectaron varios riesgos relacionados con inyecciones, como SQL, los cuales pueden ser aprovechados para manipular o extraer información del sitio. Aunque el riesgo se clasificó como de nivel medio, es crucial implementar validaciones más estrictas en los formularios y entradas de datos para reducir la posibilidad de que estos ataques sean efectivos. Además, se observó que algunos encabezados del servidor revelan información sobre la tecnología utilizada, lo cual podría ser útil para un atacante al planificar sus movimientos. Se recomienda configurar estos encabezados de modo que muestren la menor cantidad de información posible.

En la figura 79, se observa la gráfica de respuestas por segundo, la cual mostró que el sitio respondió adecuadamente en general, aunque se registraron algunos picos de actividad que podrían representar una sobrecarga en caso de ataques a gran escala. Mejorar la capacidad de respuesta del servidor para manejar un alto volumen de solicitudes contribuiría a proteger el sitio contra posibles intentos de saturación.

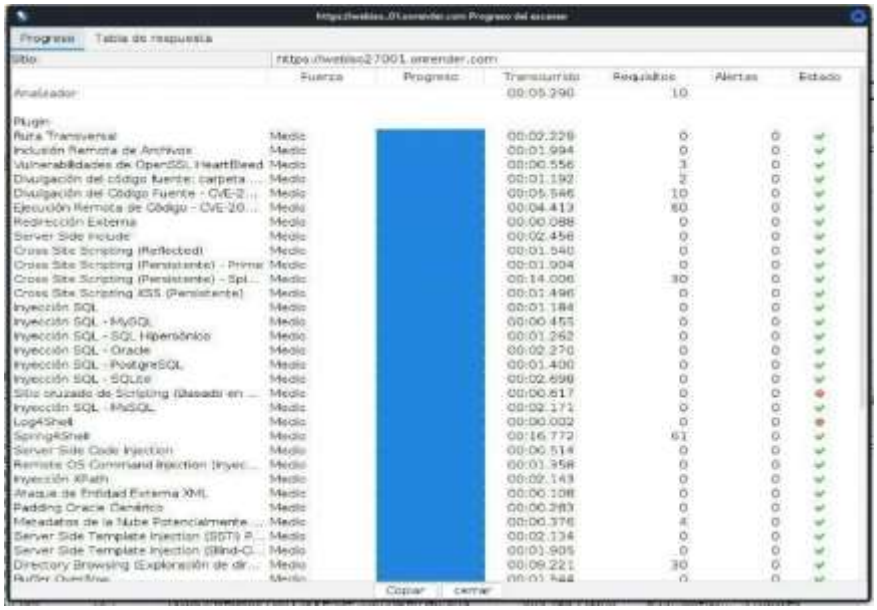

Figura 78. Resultados ataque spidering Front-end. Fuente Owasp-zap.

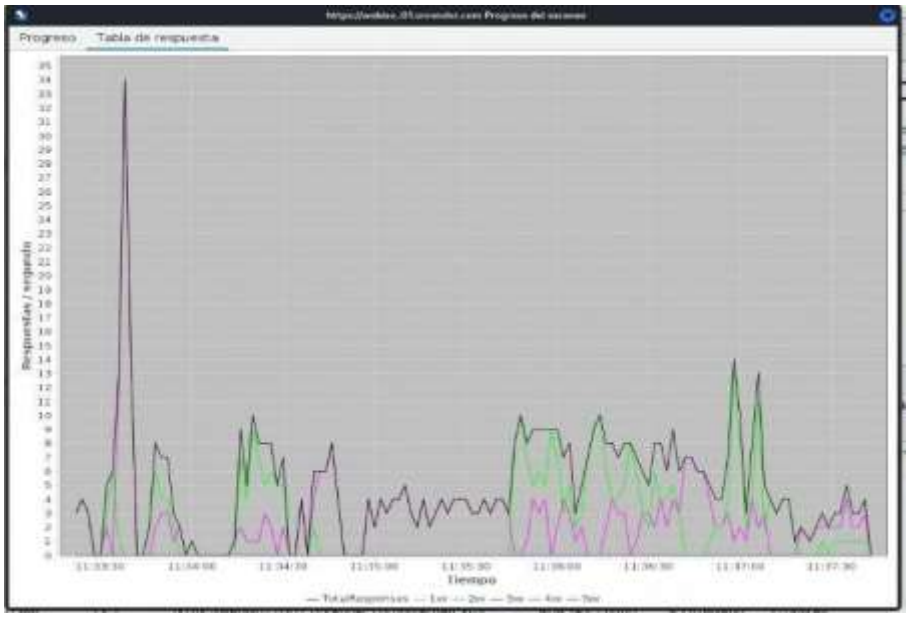

Figura 79. Gráfica tabla de respuesta - ataque spidering. Fuente Owasp-zap.

En la figura 80, se observa el ataque spidering (araña) realizado en el apartado del backend, donde se detectaron múltiples vulnerabilidades en la aplicación. Entre ellas se encuentra la vulnerabilidad de Ruta Transversal, que podría permitir el acceso a archivos no autorizados simplemente alterando la dirección en el navegador. Además, se identificaron varias formas de Inyección SQL, las cuales exponen la base de datos

a posibles manipulaciones, permitiendo que un atacante engañe a la base de datos al insertar código malicioso en los campos de entrada.

Así mismo en la figura 81, muestra cómo respondió el backend durante un "spidering", en el OWASP ZAP. En la gráfica, las líneas de colores indican el tipo de respuesta: verde para respuestas normales, morado para errores de acceso a páginas no permitidas, y naranja para errores del servidor. Los picos en la gráfica muestran momentos en que el servidor recibe muchas solicitudes de golpe, lo que podría significar que necesita ajustes para manejar alta demanda. Además, se resaltan puntos donde se detectaron vulnerabilidades, como inyecciones SQL, indicando momentos en los que el servidor podría estar en riesgo.

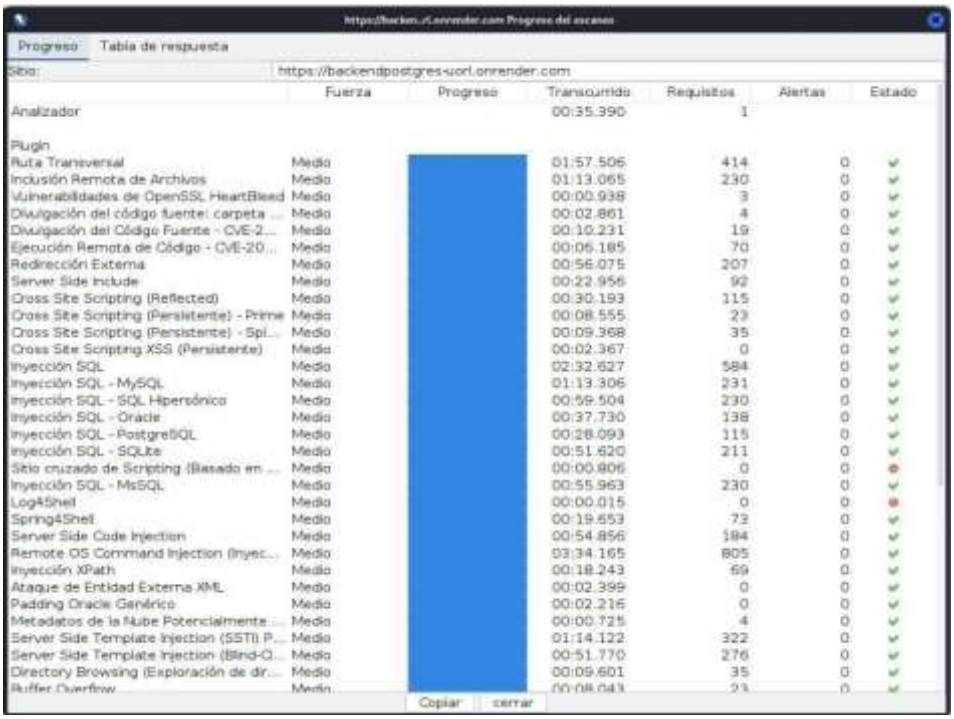

Figura 80. Resultados ataque spidering Backend. Fuente Owasp-zap.

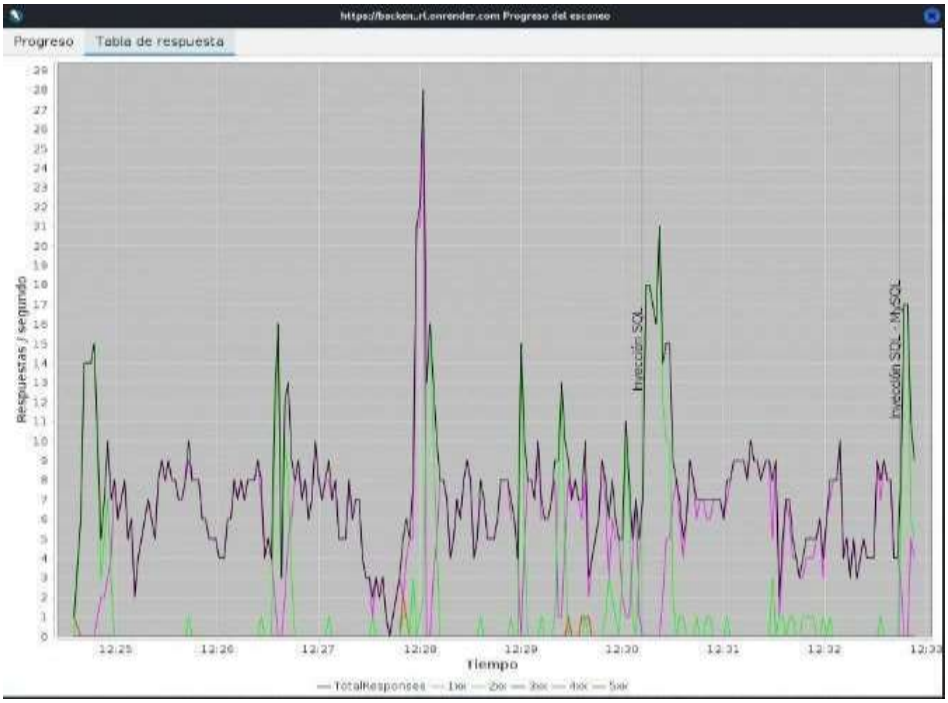

Figura 81. Gráfica tabla de respuesta - ataque spidering. Fuente Owasp-zap.

También se realizó un ataque Fuzz (User Agent Fuzzer) para el apartado del Backend, El análisis de seguridad del sitio https://backendpostgres-uorl.onrender.com reveló algunos puntos a mejorar. El sitio permite cargar contenido externo sin restricciones, lo que podría traer contenido inseguro. Los mensajes de error en el inicio de sesión muestran detalles que podrían dar pistas a atacantes sobre el sistema. Asimismo, nos refleja un riesgo informativo el cual se presenta cuando se intenta iniciar sesión, la página web devuelve información sobre cómo maneja las sesiones. Aunque esto no representa un riesgo inmediato, un atacante podría usar esa información para entender el sistema y tratar de manipular las sesiones de forma maliciosa.

Estas pruebas de seguridad se llevaron a cabo para garantizar que la página web SECUREISO esté debidamente protegida y no presente vulnerabilidades que puedan ser explotadas para acceder a información confidencial o comprometer el sistema. Se realizaron diferentes ataques en las áreas de front-end y back-end, como el spidering, que permitió explorar y analizar todas las secciones de la plataforma, proporcionando un mapeo detallado que revela rutas o enlaces ocultos, lo cual ayuda a detectar puntos de acceso que podrían pasar desapercibidos y representar riesgos

potenciales. Además, se aplicó un ataque de fuzzing, que consiste en enviar datos inesperados al sistema para observar su respuesta. Este ataque permitió identificar si el sitio maneja adecuadamente entradas inusuales y si existen posibles fallos que podrían ser explotados para obtener acceso o permisos no autorizados.

Estas pruebas son fundamentales para asegurar que la página web sea segura y esté preparada para enfrentar los ataques más comunes, permitiendo corregir cualquier debilidad de manera preventiva y brindando un entorno confiable para los usuarios.

4. CONCLUSIONES

El proyecto SECUREISO ha demostrado ser una solución innovadora y accesible para enfrentar los desafíos en la implementación de la norma ISO/IEC 27001 en la gestión de la seguridad de la información. En un contexto donde las organizaciones enfrentan amenazas constantes y cambiantes en sus sistemas de información, la creación de una herramienta digital que facilite la adopción de estándares internacionales aporta un valor significativo tanto en términos prácticos como académicos.

A lo largo de su desarrollo, se implementaron tecnologías para asegurar un diseño eficiente, seguro y adaptable. Para el front-end se utilizó el lenguaje de programación Dart junto con el framework Flutter, ofreciendo una interfaz intuitiva y accesible para los usuarios. Esto permite que SECUREISO mantenga una presentación visual moderna y fluida, facilitando la experiencia del usuario en la gestión de cuentas, documentos, auditorías y activos de seguridad. En el backend, se empleó una base de datos PostgreSQL, elegida por su robustez y capacidad para manejar grandes volúmenes de información de manera segura y escalable. Asimismo, se usó Node.js para crear la API que conecta el front-end y el backend de forma eficiente, garantizando una comunicación estable entre los distintos componentes de la página web. La herramienta Postman permitió realizar pruebas exhaustivas de la API, asegurando que cada solicitud se procese correctamente y que todas las funcionalidades fueran accesibles y seguras.

La metodología ágil SCRUM utilizada en este proyecto fue fundamental para alcanzar los objetivos planteados. La estructura de trabajo en sprints y la retroalimentación constante permitieron ajustar y perfeccionar cada funcionalidad de SECUREISO, asegurando que cumpliera con los requisitos de calidad y funcionalidad. Además garantiza que el proyecto pueda adaptarse fácilmente a cambios futuros, ya sean normativos o de seguridad, permitiendo que la herramienta mantenga su relevancia y funcionalidad.

Los resultados de las pruebas de usabilidad realizadas a SECUREISO aportan una comprensión profunda de la experiencia del usuario, la cual fue, en general, satisfactoria, ya que los usuarios evaluadores encontraron la plataforma intuitiva y útil para gestionar las distintas funcionalidades, como la creación de cuentas, la administración de documentos, la programación de auditorías y la gestión de activos de seguridad. Además, se identificaron áreas de mejora, especialmente en la optimización de tiempo en la creación de formularios y en la gestión de campos obligatorios. Estos hallazgos reflejan que la herramienta es bien recibida, aunque algunos ajustes adicionales podrían mejorar aún más su accesibilidad y eficacia en futuras versiones.

El aspecto de seguridad se abordó empleando la herramienta de prueba OWASP ZAP, que permitió evaluar la resistencia de SECUREISO frente a intentos de intrusión tanto en el front-end como en el back-end. Las pruebas de spidering y fuzzing, realizadas a través de esta herramienta, ayudaron a descubrir vulnerabilidades que no eran visibles a simple vista y a entender cómo la plataforma maneja datos inesperados. Los resultados confirmaron que SECUREISO puede resistir ataques comunes, ofreciendo a sus usuarios un entorno seguro y confiable.

Finalmente, SECUREISO representa un avance importante en el ámbito de la gestión de la seguridad de la información, ofreciendo una solución práctica, adaptable y enfocada en las necesidades reales de las organizaciones en la era digital. La herramienta no solo optimiza los procesos de auditoría y gestión de seguridad bajo la norma ISO/IEC 27001, sino que también promueve un enfoque más proactivo en la protección de datos, permitiendo a los usuarios identificar y abordar potenciales riesgos antes de que puedan comprometer la integridad de sus sistemas de información.

Este proyecto ofrece una contribución significativa tanto al ámbito académico como al profesional, al abrir camino para nuevas investigaciones y desarrollos en la aplicación de estándares de seguridad en herramientas digitales. SECUREISO no es solo una solución específica para el presente, sino un modelo adaptable que puede ser

replicado y mejorado según las necesidades futuras, brindando una base sólida para que otros investigadores y profesionales construyan soluciones cada vez más seguras y efectivas, dado el aumento continuo de los riesgos en la gestión de seguridad de la información.

5. BIBLIOGRAFÍAS

[1] A. Andersson, K. Hedström, y F. Karlsson, «“Standardizing information security – a structurational analysis”», Information & Management, vol. 59, n.o 3, p. 103623, abr. 2022, doi: 10.1016/j.im.2022.103623.

[2] A. Mas, A. L. Mesquida, y M. Pacheco, «Supporting the deployment of ISO-based project management processes with agile metrics», Computer Standards & Interfaces, vol. 70, p. 103405, jun. 2020, doi: 10.1016/j.csi.2019.103405.

[3] M. Ylönen y K. Björkman, «Integrated management of safety and security (IMSS) in the nuclear industry – Organizational culture perspective», Safety Science, vol. 166, p. 106236, oct. 2023, doi: 10.1016/j.ssci.2023.106236.

[4] F. Karlsson, E. Kolkowska, y J. Petersson, «Information security policy compliance-eliciting requirements for a computerized software to support value-based compliance analysis», Computers & Security, vol. 114, p. 102578, mar. 2022, doi: 10.1016/j.cose.2021.102578.

[5] R. Hoffmann, J. Napiórkowski, T. Protasowicki, y J. Stanik, «Measurement Models of Information Security Based on the Principles and Practices for Risk-Based Approach», Procedia Manufacturing, vol. 44, pp. 647-654, ene. 2020, doi: 10.1016/j.promfg.2020.02.244.

[6] M. Seeba, A.-A. O. Affia, S. Mäses, y R. Matulevičius, «Create your own MUSE: A method for updating security level evaluation instruments», Computer Standards & Interfaces, vol. 87, p. 103776, ene. 2024, doi: 10.1016/j.csi.2023.103776.

[7] G. Breda y M. Kiss, «Overview of Information Security Standards in the Field of Special Protected Industry 4.0 Areas & Industrial Security», Procedia Manufacturing, vol. 46, pp. 580-590, ene. 2020, doi: 10.1016/j.promfg.2020.03.084.

[8] C. Schmitz, M. Schmid, D. Harborth, y S. Pape, «Maturity level assessments of information security controls: An empirical analysis of practitioners assessment

capabilities», Computers & Security, vol. 108, p. 102306, sep. 2021, doi: 10.1016/j.cose.2021.102306.

[9] S. AlGhamdi, K. T. Win, y E. Vlahu- Gjorgievska, «Information security governance challenges and critical success factors: Systematic review», Computers & Security, vol. 99, p. 102030, dic. 2020, doi: 10.1016/j.cose.2020.102030.

[10] M. Mirtsch, K. Blind, C. Koch, y G. Dudek, «Information security management in ICT and non-ICT sector companies: A preventive innovation perspective», Computers & Security, vol. 109, p. 102383, oct. 2021, doi: 10.1016/j.cose.2021.102383.

[11] R. M. . Ferrer Dávalos, «Indicadores para la medición del desempeño administrativo en microempresas de Paraguay», PID, vol. 9, n.º 2, pp. 2–21, feb. 2022.

[12] E. K. Szczepaniuk, H. Szczepaniuk, T. Rokicki, y B. Klepacki, «Information security assessment in public administration», Computers & Security, vol. 90, p. 101709, mar. 2020, doi: 10.1016/j.cose.2019.101709.

[13] A. Shameli- Sendi, «An efficient security data-driven approach for implementing risk assessment», Journal Of Information Security And Applications, vol. 54, p. 102593, oct. 2020, doi: 10.1016/j.jisa.2020.102593.

[14] M. Brunner, C. Sauerwein, M. Felderer, y R. Breu, «Risk management practices in information security: Exploring the status quo in the DACH region», Computers & Security, vol. 92, p. 101776, may 2020, doi: 10.1016/j.cose.2020.101776.

[15] A. Talaminos-Barroso, J. Reina- Tosina, y L. M. Roa, «Adaptation and application of the IEEE 2413-2019 standard security mechanisms to IoMT systems», Measurement: Sensors, vol. 22, p. 100375, ago. 2022, doi: 10.1016/j.measen.2022.100375.

[16] K. Khando, S. Gao, M. S. Islam, y A. Salman, «Enhancing employees information security awareness in private and public organizations: A systematic literature review», Computers & Security, vol. 106, p. 102267, Jul. 2021, doi: 10.1016/j.cose.2021.102267.

[17] K. Haufe, «Maturity based approach for ISMS Governance», 1 de marzo de 2017. http://hdl.handle.net/10016/25128

[18] G. G. Prapenan y G. C. Pamuji, «Information System Security Analysis of XYZ Company Using COBIT 5 Framework and ISO 27001:2013», IOP Conference Series: Materials Science And Engineering, vol. 879, n.o 1, p. 012047, jul. 2020, doi: 10.1088/1757-899x/879/1/012047.

[19] Abazi, B. «A novel approach for information security risk assessment maturity framework based on ISO 27001», Tesis, Universidad Corvinus de Budapest, 2020. [En línea]. Disponible en: http://phd.lib.uni-corvinus.hu/1088/7/Blerton_Abazi_ten.pdf

[20] Mounia Zaydi, Bouchaib Nassereddine, «A conceptual hybrid approach for information Security governance.», International Journal Of Mathematics & Computer Science, vol. 16, n° 1, p. 47, jun. 2020

[21] Hulshof, Mike, «Information Security Certification In Context : A Strategy Selection Maturity Model», Tesis de maestría, University Of Twente Student Theses, 2021. [En línea]. Disponible en: https://purl.utwente.nl/essays/87964

[22] H. M. Melaku, «A Dynamic and Adaptive Cybersecurity Governance Framework», Journal Of Cybersecurity And Privacy, vol. 3, n.o 3, pp. 327-350, jun. 2023, doi: 10.3390/jcp3030017.

[23] A. Rusman, R. Nadlifatin, y A. P. Subriadi, «Information System Audit Using COBIT and ITIL Framework: Literature Review», Sinkron : Jurnal Dan Penelitian

Teknik Informatika, vol. 7, n.o 3, pp. 799-810, julio. 2022, doi: 10.33395/sinkron.v7i3.11476.

[24] J. Hochstetter, M. Diéguez, J. L. Fenner, y Cachero, C. «AIM Triad: A Prioritization Strategy for Public Institutions to Improve Information Security Maturity», Applied Sciences, vol. 13, n.o 14, p. 8339, jul. 2023, doi: 10.3390/app13148339.

[25] M. Diéguez, C. Cares, C. Cachero, y J. Hochstetter, «MASISCo—Methodological Approach for the Selection of Information Security Controls», Applied Sciences, vol. 13, n.o 2, p. 1094, ene. 2023, doi: 10.3390/app13021094.

[26] O. M. Safonova y N. V. Kotelnikov, «Modeling the information security management system (ISMS) of a medical organization», E3S Web Of Conferences, vol. 224, p. 01035, ene. 2020, doi: 10.1051/e3sconf/202022401035.

[27] Erfan Koza. “Semantic Analysis of ISO/IEC 27000 Standard Series and NIST Cybersecurity Framework to Outline Differences and Consistencies in the Context of Operational and Strategic Information Security". Medicon Engineering Themes 2.3 (2022): 26-39.

[28] H. A. Mangut, D. P. Luhutyit, A. D. Kalamba, y P. Mangut, «Analysis of ISO/IEC 27001 to Encourage its Adoption in Nigerian Businesses», World Journal Of Innovative Research, vol. 9, n.o 5, dic. 2020, doi: 10.31871/wjir.9.5.12.

[29] D. Nikitin, «Achieving Privacy And Iso 27001 Standard», Tesis de licenciatura, South-Eastern Finland University of Applied Sciences, 22023. [En línea]. Disponible en:
https://www.theseus.fi/bitstream/handle/10024/801074/Nikitin_Danila.pdf?sequence=2

[30] J. Marjanović, N. Dalčeković, y G. Sladić, «Blockchain-based model for tracking compliance with security requirements», Computer Science And Information Systems, vol. 20, n.o 1, pp. 359-380, ene. 2023, doi: 10.2298/csis210923060m.

[31] M. Gulzira, G. Bekmanova, A. Sharipbay, y A. Omarbekova, «The audit method of enterprise's Information security», Proceedings Of The 6th International Conference On Engineering &Amp; MIS 2020, sep. 2020, doi: 10.1145/3410352.3410761.

[32] M. Alsaleh y M. Niazi, «Evaluations of Information Security Maturity models: Measuring the NIST Cybersecurity Framework implementation status», The Sixth International Conference On Cyber-Technologies And Cyber-Systems, pp. 13-24, oct. 2021, [En línea]. Disponible en: https://www.thinkmind.org/articles/cyber_2021_1_60_80057.pdf

[33] T. Babenko, H. Hnatiienko and A. Bigdan, «Model for determining the protection level of a complex system», CEUR Workshop Proceedings, mar. 2021, [En línea]. Disponible en: https://ceur-ws.org/Vol-3132/Paper_15.pdf

[34] M. Shojaeshafiei, «A measurable cybersecurity quality framework and its application to the Department of Transportation ", Thesis, The University of Alabama in Huntsville, 2020.

[35] S. Qudsi Shehady, «A conceptual framework for discovering Instance-Spanning constraints from event logs», Thesis, University of Haifa Faculty of Social Sciences, 2023.

[36] F. Akowuah, X. Yuan, J. Xu, y H. Wang, «A Survey of Security Standards Applicable to Health Information Systems», International Journal Of Information Security And Privacy, vol. 7, n.o 4, pp. 22-36, oct. 2013, doi: 10.4018/ijisp.2013100103.

[37] S. H. Björnsdóttir, P. Jensson, S. E. Thorsteinsson, I. M. Dokas, y R. J. De Boer, «Benchmarking ISO Risk Management Systems to Assess Efficacy and Help Identify Hidden Organizational Risk», Sustainability, vol. 14, n.o 9, p. 4937, abr. 2022, doi: 10.3390/su14094937.

[38] B. Akhmetov, V. Lakhno, V. Chubaievskyi, S. Kaminskyi, S. Adilzhanova, y M. Ydyryshbayeva, «Automation of Information Security Risk Assessment», International Journal Of Electronics And Telecommunications, nov. 2023, doi: 10.24425/ijet.2022.141273.

[39] B. Alamri, K. Crowley, y I. Richardson, «Cybersecurity Risk Management Framework for Blockchain Identity Management Systems in Health IoT», Sensors, vol. 23, n.o 1, p. 218, dic. 2022, doi: 10.3390/s23010218.

[40] P. Loft, Y. He, I. Yevseyeva, y I. Wagner, «CAESAR8: An agile enterprise architecture approach to managing information security risks», Computers & Security, vol. 122, p. 102877, nov. 2022, doi: 10.1016/j.cose.2022.102877.

[41] M. R. Cavallare, «Information Systems Security Governance evaluation in the Portuguese local public administration», Master’s Thesis, University of Minho School of Engineering, 2020.

[42] E. D. Ayugi, «Information security strategies and patient data privacy among health facilities in Nairobi», Thesis, University of Nairobi, 2021. [En línea]. Disponible en: http://erepository.uonbi.ac.ke/handle/11295/157072

[43] D. Zellhofer, «On the value of information security policies in organizations», Doctoral thesis, Vienna University of Economics and Business, 2022. doi: https://doi.org/10.57938/hss.2023.001

[44] Eric David, «Evaluating the impact of metric-based security tools on company performance and decision-making», Dissertation, University of the Cumberlands, 2023.

[45] S. H. Björnsdóttir, P. Jensson, R. J. De Boer, y S. E. Thorsteinsson, «The Importance of Risk Management: What is Missing in ISO Standards?», Risk Analysis, vol. 42, n.o 4, pp. 659-691, sep. 2021, doi: 10.1111/risa.13803.

[46] B. Parengkuan, K. Tatauhe, y F. Worotijan, «Analysis of Information Security Management Systems at University», International Journal Of Information Technology And Education (IJITE), vol. 1, n.o 1, dic. 2021, [En línea]. Disponible en: https://ijite.jredu.id/index.php/ijite/article/view/10

[47] I. Mohiuddin y A. Almogren, «Security challenges and strategies for the IoT in cloud computing», 2020 11a Conferencia Internacional Sobre Sistemas de Información y Comunicaciones (ICICS), abr. 2020, doi: 10.1109/icics49469.2020.239563.

[48] L. Zhou, A. Fu, G. Yang, H. Wang, y Y. Zhang, «Efficient certificateless Multi-Copy integrity auditing scheme supporting data dynamics», IEEE Transactions On Dependable And Secure Computing, p. 1, ene. 2021, doi: 10.1109/tdsc.2020.3013927.

[49] P. Singh y S. Kr. Saroj, «A Secure Data Dynamics and Public Auditing Scheme for Cloud Storage», 2020 6th International Conference On Advanced Computing And Communication Systems (ICACCS), mar. 2020, doi: 10.1109/icaccs48705.2020.9074337.

[50] A. Fu, S. Yu, Y. Zhang, H. Wang, y C. Huang, «NPP: A New Privacy-Aware Public Auditing Scheme for Cloud Data Sharing with Group Users», IEEE Transactions On Big Data, vol. 8, n.o 1, pp. 14-24, feb. 2022, doi: 10.1109/tbdata.2017.2701347.

[51] H. Yan y W. Gui, «Efficient Identity-Based Public Integrity Auditing of Shared Data in Cloud Storage With User Privacy Preserving», IEEE Access, vol. 9, pp. 45822-45831, ene. 2021, doi: 10.1109/access.2021.3066497.

[52] D. Bansal, «System Analysis and Error Detection: An approach towards server monitoring using natural language processing», 2020 Fourth International Conference On I-SMAC (IoT In Social, Mobile, Analytics And Cloud) (I-SMAC), oct. 2020, doi: 10.1109/i-smac49090.2020.9243537.

[53] X. Zhang, J. Zhao, C. Xu, H. Li, H. Wang, y Y. Zhang, «CIPPPA: Conditional Identity Privacy-Preserving Public Auditing for Cloud-Based WBANs Against Malicious Auditors», IEEE Transactions On Cloud Computing, vol. 9, n.o 4, pp. 1362-1375, oct. 2021, doi: 10.1109/tcc.2019.2927219.

[54] M. Mirtsch, J. Kinne, y K. Blind, «Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A Web Mining-Based Analysis», IEEE Transactions On Engineering Management, vol. 68, n.o 1, pp. 87-100, feb. 2021, doi: 10.1109/tem.2020.2977815.

[55] F. Wijayanti, D. I. Sensuse, A. A. Putera, y A. Syahrizal, «Assessment of Information Security Management System: A Case Study of Data Recovery Center in Ministry XYZ», https://ieeexplore.ieee.org/xpl/conhome/9274557/proceeding, sep. 2020, doi: 10.1109/ic2ie50715.2020.9274574.

[56] V. Monev, «Organizational Information Security Maturity Assessment based on ISO 27001 and ISO 27002», 2020 International Conference On Information Technologies (InfoTech), sep. 2020, doi: 10.1109/infotech49733.2020.9211066.

[57] S. J. Putra, M. N. Gunawan, A. F. Sobri, J. Muslimin, Amilin, y D. Saepudin, «Information Security Risk Management Analysis using ISO 27005: 2011 for the telecommunication company», 2020 8th International Conference On Cyber And IT Service Management (CITSM), oct. 2020, doi: 10.1109/citsm50537.2020.9268845.

[58] C. A. Murillo, I. E. P. Escalante, y Y. R. Pedraza, «Contexto de la seguridad ciudadana en América Latina y el Caribe», Revista Científica General José María Córdova, vol. 16, n.o 24, pp. 83-106, sep. 2018, doi: 10.21830/19006586.360.

[59] M. Álvarez y D. A. H. Ladino, «Análisis preliminar de la ciberseguridad asociada al sistema financiero en algunos países de Latinoamérica y la contribución de la informática forense», Cuadernos de Investigación Semilleros Andina, vol. 1, n.o 14, dic. 2021, doi: 10.33132/26196301.1950.

[60] M. M. M. Macías, R. Macías, M. L. I. Navarrete, y J. A. I. Navarrete, «Normas y estándares en auditoría: una revisión de su utilidad en la seguridad informática», Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS, vol. 5, n.o 4, pp. 584-599, jun. 2023, doi: 10.59169/pentaciencias.v5i4.700.

[61] R. L. Carreño, Técnicas Y Métodos Documentales En Investigación Científica. 2021. doi: 10.6018/editum.2929.

[62] Salinas Suárez, Lohanna Elizabeth. Análisis entre las normativas ISO/IEC 27001:2022 versus ISO/IEC 27001:2013 Implementación de los nuevos controles de la norma en un Sistema de Gestión, en entidades financieras, desarrollo de software y una empresa de servicios de infraestructura de TI = Analysis between ISO/IEC 27001:2022 versus ISO/IEC 27001:2013 and the Implementation of the new controls in a Management System, in financial entities, software development and an IT infrastructure services company. Trabajo Fin de Máster. Universidad de Alcalá, 2023.

[63] Tasa Catanzaro, M. E., Maquera Quispe, H. G., Rojas Bujaico, J. F., & Delgado Rospigliosi, M. G. del C.(2022). Análisis de información de la gestión de incidentes de seguridad en organizaciones. Puriq, 4, e196. https://doi.org/10.37073/puriq.4.1.196

[64] J.G, Arévalo Ascanio, R. A, Bayona Trillos, D. W, Rico Bautista (2015) Implantación de un sistema de gestión de seguridad de información bajo la ISO

27001: análisis del riesgo de la información. doi:10.14483/udistrital.jour.tecnura.2015.4.a10

[65] J.L, Aguayo, R. A, Ponce, O. R, Rojas (2020) Estudio de mejora en la seguridad de aplicaciones web y de aplicaciones móviles mediante el protocolo openid connect opensource utilizado en identity server.

[66] E. Lara, F.Corella. (2018). Comparación de Modelos Tradicionales de Seguridad de la Información para centros de educación. Tierra Infinita. https://doi.org/10.32645/26028131.742

[67] Olivares, M.S., Martínez, A., & Salcedo, I.E. (2020). Framework gestión de la seguridad de la información para universidades.

[68] Babilonia Presentación, G.S. (2023). BENEFICIOS DE LAS NORMAS ISO 27000. HIGH TECH-ENGINEERING JOURNAL.

[69] De la Cruz Lopez, N., Jerónimo Jiménez, D.M., López Rodríguez, W.B., & Martínez Jiménez, R.M. (2022). Impacto de la auditoría como una herramienta de control, para el mejoramiento de la empresa. Publicaciones e Investigación.

[70] MORALES TOAPANTA, B. D. (2024). CONSTRUCCIÓN DE UNA APLICACIÓN MÓVIL PARA EVALUAR EL DESEMPEÑO DOCENTE DE LA UNIVERSIDAD POLITÉCNICA SALESIANA (p. 114) [Tesis].

[71] Raffino, Equipo editorial, Etecé (19 de noviembre de 2023). Windows. Enciclopedia Concepto. Recuperado el 24 de septiembre de 2024 de https://concepto.de/windows-2/.

[72] Anónimo. (2020). 10 razones para usar GNU/Linux. Juegos Linux; Anónimo. https://juegoslinux.org/10-razones-para-usar-gnulinux/

[73] MacOS – Edutic. (2022). Up.edu.pe; Universidad del Pacifico https://edutic.up.edu.pe/catalogo-software/macos/

[74] FreeBSD: The torchbearer of the original operating system distribution | FreeBSD Foundation. (2024, April 25). Freebsdfoundation.org. https://freebsdfoundation.org/blog/freebsd-the-torchbearer-of-the-original-operating-system-distribution/

[75] Universidad del pacifico. (n.d.). iOS. Edutic; edutic.up.edu.pe. Retrieved September 24, 2024, from https://edutic.up.edu.pe/catalogo-software/ios/

[76] to, C. (2024). Android. Tecnología Wiki; Fandom, Inc. https://tecnologia.fandom.com/wiki/Android

[77] colaboradores de Wikipedia, “Firefox OS,” Wikipedia, La Enciclopedia Libre, Jul. 18, 2024. https://es.wikipedia.org/wiki/Firefox_OS

[78] J. D. Luján, “Dart, Un Lenguaje Del Futuro,” EDteam - En Español Nadie Te Explica Mejor, 2018. https://ed.team/blog/dart-un-lenguaje-del-futuro (accessed Sep. 24, 2024).

[79] C. Darás de la Fuente, “Un Estudio Comparativo De Los Lenguajes De Programación De La Última década.,” Tesis, UNIVERSITAT POLITÈCNICA DE VALÈNCIA, 2022.

[80] nuria.canals, ¿Qué Es El Lenguaje De Programación Dart? 2020. Accessed: Sep. 24, 2024. [Online]. Available: https://inlab.fib.upc.edu/es/uncategorized-ca-es/que-es-el-lenguaje-de-programacion-dart/2020/

[81] N. Nuria, “¿Qué Es El Lenguaje De Programacion dart?,” Upc.edu, 2024. https://inlab.fib.upc.edu/wp-content/uploads/2020/05/dart_1.png (accessed Sep. 24, 2024).

[82] René Quisaguano, L., Camalle, T. G., & Toca, J. W. (2022). Análisis comparativo de entornos de desarrollo móvil. Ciencia Latina Revista Científica Multidisciplinar, 6(4), 4478-4498. https://doi.org/10.37811/cl_rcm.v6i4.2950

[83] The PostgreSQL Global Development Group, “PostgreSQL: the world’s Most Advanced Open Source Database,” Postgresql.org, 2019. https://www.postgresql.org/ (accessed Sep. 24, 2024).

[84] Y. Hernandez, “¿Cuál es la arquitectura de una aplicación web?,” Tutoriales Dongee, Jan. 24, 2023. https://www.dongee.com/tutoriales/cual-es-la-arquitectura-de-una-aplicacion-web/

[85] W. by Jaciel A, “Qué es la Arquitectura Web | Componentes y Tipos,” Niaxus, Jul. 26, 2024. https://niaxus.com/2024/07/26/que-es-la-arquitectura-web-componentes-y-tipos/ (accessed Nov. 02, 2024).

[86] Scrum.org, El Ciclo SCRUM. Accessed: Jul. 12, 2018. Available: https://www.codehoven.com/hs-fs/hubfs/SCRM-reuniones.webp?width=714&height=401&name=SCRM-reuniones.webp

[87] KanbanFlow, “KanbanFlow - Lean Project management. Simplified.,” kanbanflow.com, 2011. https://kanbanflow.com/ (accessed Nov. 2024).

[88] Microsoft, “Visual Studio Code,” Visualstudio.com, 2024. https://code.visualstudio.com/

[89] Postman, “Postman | The Collaboration Platform for API Development,” Postman, 2021. https://www.postman.com/

[90]. Kitchenham, B. (2013). Kitchenham B., Brereton P. A systematic review of systematic review process research in software engineering, Inf. Softw. Technol, 55(12), 2049-2075.

[91]. Yong Varela, L. A., Rivas Tovar, L. A. & Chaparro, J. (2010). Modelo de aceptación tecnológica (TAM): un estudio de la influencia de la cultura nacional y del perfil del usuario en el uso de las TIC. Innovar, 20(36), 187-204.

[92]. Ariel, Julio, and Hurtado Alegría. Toward a Scientific Method in Software Engineering (Position Paper).

[93] “Perform Systematic Literature Reviews.” Parsifal, parsif.al/.