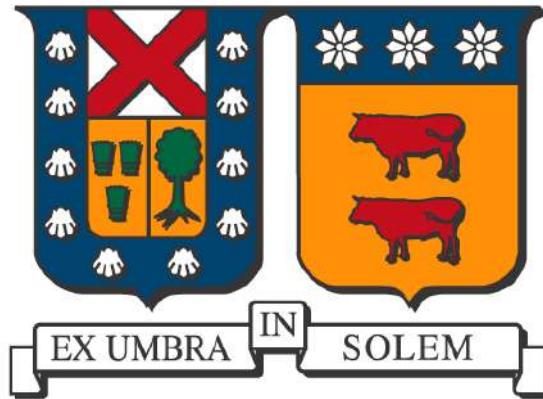


UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA
DEPARTAMENTO DE ELECTRÓNICA
SANTIAGO - CHILE



**“DISEÑO Y DESARROLLO DE UNA PLATAFORMA
INTEGRAL SST PARA METRO DE SANTIAGO”**

DIEGO ISMAEL DE LA SOTTA MONTERO

**MEMORIA DE TITULACIÓN PARA OPTAR AL TÍTULO DE INGENIERO CIVIL
TELEMÁTICO**

PROFESOR GUÍA:

NICOLÁS TORRES RUDLOFF

PROFESOR CORREFERENTE:

PATRICIO OLIVARES

AGOSTO - 2026



CONSTANCIA DE VALIDACIÓN Y CONFIDENCIALIDAD DE MONOGRAFÍA A REPOSITORIO ACADÉMICO

1.- IDENTIFICACIÓN DEL TRABAJO ACADÉMICO

Tipo de monografía (marcar una opción): ☒ Memoria o trabajo de título ☐ Tesis de Postgrado

Título del trabajo: DISEÑO Y DESARROLLO DE UNA PLATAFORMA INTEGRAL SST PARA METRO DE SANTIAGO

Nombre del candidato(a): DIEGO ISMAEL DE LA SOTTA MONTERO

Carrera / Grado: INGENIERÍA CIVIL TELEMÁTICA

Campus: SAN JOAQUÍN Departamento: ELECTRÓNICA

2.- VALIDACIÓN DEL PROFESOR GUÍA/DIRECTOR DE TESIS

Yo, Nicolás Torres Rudloff, en mi calidad de profesor(a) guía/director(a) del trabajo académico mencionado anteriormente

DEJO CONSTANCIA que:

- He revisado esta versión del documento y corresponde a la versión final aprobada del trabajo.
- El trabajo cumple con los requisitos académicos y de formato establecidos por la institución.

3.- EVALUACIÓN DE CONFIDENCIALIDAD POR PROPIEDAD INDUSTRIAL (marcar una opción)

☒ El trabajo **NO contiene** información que amerite confidencialidad y puede ser publicado de inmediato en repositorio con acceso abierto.

☐ El trabajo **CONTIENE** información con potenciales implicancias de propiedad industrial o intelectual y requiere un periodo de confidencialidad (**embargo**) por (**marcar una opción**):

☐ 6 meses ☐ 12 meses ☐ 2 años ☐ 3 años ☐ 5 años ☐ 10 años

Fundamentación de la necesidad de confidencialidad (obligatorio si se solicita embargo):

4.- FIRMAS

Profesor(a) guía o director(a) de memoria o tesis:

Fecha: 31/07/2026 Firma: _____

Estudiante o Candidato(a):

Fecha: 31/07/2026

Firma: _____

Este formulario debe ser insertado como página 2 de la memoria o tesis, completado y firmado por estudiante y profesor(a) antes de la entrega en portal PRISMA de Biblioteca USM.

Agradecimientos

En primer lugar, deseo expresar mi más profunda gratitud a mis padres, cuyo amor, sacrificio y fe inquebrantable han sido fundamentales para mí. Gracias por enseñarme el valor de la perseverancia y por darme la oportunidad de formarme como profesional; este título les pertenece tanto a ustedes como a mí. Les agradezco por su apoyo incondicional durante todos estos años de estudio y por creer en mí incluso en los momentos de mayor dificultad. Sin su sacrificio y amor, este logro no sería posible.

A mis amigos y compañeros de carrera, con quienes compartí extensas jornadas de estudio y cuya amistad hizo que este camino fuera una experiencia inigualable y divertida. Un agradecimiento especial a aquellos compañeros que conocí en el aula y que con el tiempo se convirtieron en amigos, y luego en lo que podría denominar como “hermanos”, a los cuales agradezco profundamente por todas las experiencias vividas tanto dentro como fuera de la universidad, esperando que estas vivencias perduren en el futuro.

También agradezco a todos los profesores de los cuales tuve el privilegio de aprender durante mi formación como estudiante universitario, por compartir su conocimiento y guiar mi camino académico.

Finalmente, me agradezco a mí mismo por la determinación de seguir siempre hacia adelante y nunca rendirme, independientemente de los obstáculos o situaciones personales complicadas que se presentaron en el camino.

*Esta memoria está dedicado a mis padres,
los cuales son la razón de que yo esté
aquí. Ojalá que podamos salir adelante, los
amo.*

Resumen

El presente trabajo de memoria aborda el diseño y desarrollo de una plataforma integral para la gestión del Sistema de SST en Metro de Santiago. La problemática central radica en la dispersión de información técnica y legal en múltiples soportes, lo que dificulta la trazabilidad y el cumplimiento normativo en una infraestructura de transporte masivo.

Para resolver esta necesidad, se diseñó una arquitectura de software basada en el framework *Flutter* para el desarrollo móvil y *Firebase* como infraestructura de servicios en la nube (*Backend as a Service*). La metodología de trabajo siguió el marco ágil *Scrum*, permitiendo iteraciones constantes para validar los requerimientos operativos de la organización.

Los resultados demuestran un prototipo funcional capaz de centralizar los 10 componentes estratégicos del SGSST de Metro, permitiendo la autenticación segura de usuarios, la consulta de documentación técnica y la carga de evidencias fotográficas en terreno. Se concluye que la implementación de esta herramienta optimiza significativamente la disponibilidad de la información y sienta las bases para futuras integraciones tecnológicas, como el procesamiento de lenguaje natural para la consulta de normativas.

Palabras Clave: Seguridad y Salud en el Trabajo (SST), Flutter, Firebase, Metro de Santiago, Transformación Digital, Gestión Preventiva.

Abstract

This thesis project presents the design and development of a comprehensive platform for managing the Occupational Safety and Health (OSH) at Metro de Santiago. The core problem lies in the fragmentation of technical and legal information across multiple platforms, which hinders traceability and regulatory compliance in a mass transit infrastructure.

To address this need, a software architecture was designed using the *Flutter* framework for mobile development and *Firebase* as the cloud services infrastructure (*Backend as a Service*). The work methodology followed the *Scrum* agile framework, allowing for constant iterations to validate the organization's operational requirements.

The results showcase a functional prototype capable of centralizing Metro's 10 strategic OSH components, enabling secure user authentication, technical documentation retrieval, and the uploading of field evidence. It is concluded that the implementation of this tool significantly optimizes information availability and establishes a foundation for future technological integrations, such as natural language processing for regulatory inquiries.

Keywords: Occupational Safety Health, Flutter, Firebase, Metro de Santiago, Digital Transformation, Preventive Management.

Glosario

Backend as a Service Modelo de servicio en la nube donde los desarrolladores delegan la gestión de servidores a terceros para enfocarse en la lógica del cliente.

Framework Conjunto estandarizado de conceptos, prácticas y criterios de diseño que ofrece una estructura base para el desarrollo de software. Proporciona componentes predefinidos y herramientas que facilitan la resolución de problemas comunes, permitiendo al desarrollador enfocarse en la lógica de negocio específica (como es el caso de *Flutter* en esta memoria).

Siglas

API Application Programming Interface.

FCM Firebase Cloud Messaging.

HTTPS Hypertext Transfer Protocol Secure.

HU Historias de Usuario.

ID Identity Document.

iOS iPhone Operating System.

ISO International Organization for Standardization.

LLM Large Language Model.

NLP Procesamiento del Lenguaje Natural.

NoSQL Not Only SQL.

PMM Programa de Memoria Multidisciplinaria.

QR Quick Response.

RAG Retrieval-Augmented Generation.

REST Representational State Transfer.

SaaS Software as a Service.

SDK Software Development Kit.

SGSST Sistema de Gestión de Seguridad y Salud en el Trabajo.

SSL Secure Socket Layer.

SST Seguridad y Salud en el Trabajo.

TLS Transport Layer Security.

UID User ID.

Tabla de Contenido

1	Introducción	1
1.1	Objetivos	1
1.1.1	Objetivo Principal	1
1.1.2	Objetivos Específicos	2
2	Estado del Arte	3
2.1	Soluciones de Gestión Preventiva y Cumplimiento Legal	3
2.2	Inteligencia de Datos y Gestión de Riesgos Críticos	3
2.3	Tecnologías de Soporte y Estándares Globales	4
2.4	Brecha Tecnológica y Propuesta de Valor	5
3	Propuesta de Solución	7
3.1	Responsabilidad y Contribución Individual	7
3.2	Justificación Tecnológica	8
3.3	Descripción Conceptual de la Plataforma	8
4	Requisitos del Sistema	10
4.1	Requisitos funcionales	10
4.2	Requisitos no funcionales	12
5	Diseño de Arquitectura del Sistema	13
5.1	Arquitectura General	13
5.2	Diagrama de Bloques	13
5.3	Flujo de Interacción y Comunicación	14
5.4	Estrategia de Persistencia y Disponibilidad	15
5.5	Seguridad de la Información	15
5.6	Descripción de Módulos	16
5.7	Modelo de Datos Not Only SQL (NoSQL)	16
5.7.1	Descripción de la Estructura	17

TABLA DE CONTENIDO

5.8	Cumplimiento Normativo y Protección de Datos (Ley 19.628)	18
5.8.1	Autenticación y Control de Acceso	18
5.8.2	Seguridad en el Almacenamiento de Evidencias	18
5.8.3	Cifrado de Datos en Tránsito	19
6	Metodología	20
6.1	Ciclo de Desarrollo	20
6.2	Hitos de la Memoria	21
6.3	Herramientas de Gestión	21
7	Resultados	22
7.1	Flujo de Navegación y Experiencia de Usuario	22
7.1.1	Acceso y Seguridad	22
7.1.2	Panel Principal (Hub de Seguridad)	23
7.1.3	Navegación por Componentes del Sistema de Gestión de Seguridad y Salud en el Trabajo (SGSST)	24
7.1.4	Gestión Documental y Carga de Archivos	25
7.2	Análisis de Cumplimiento Técnico	26
7.3	Análisis de Cumplimiento de Objetivos	27
7.4	Validación de Requisitos de Segunda Etapa	27
8	Conclusiones	28
8.1	Cumplimiento de Objetivos	28
8.2	Eficacia del Stack Tecnológico	28
8.3	Lecciones Aprendidas y Proyecciones	29

Referencias

Índice de figuras

5.1	Diagrama de Arquitectura de la Plataforma Seguridad y Salud en el Trabajo (SST). Fuente: Elaboración propia.	14
5.2	Diagrama de arquitectura de colecciones y documentos en Cloud Firestore. Fuente: Elaboración propia.	17
7.1	Interfaz de inicio de sesión de la aplicación.	23
7.2	Vista del menú principal con los módulos de SST.	24
7.3	Interfaz detallada del Módulo de Liderazgo y Compromiso.	25
7.4	Flujo de selección y carga de archivos hacia el repositorio en la nube. . .	26

Índice de tablas

1	Comparativa de Soluciones del Estado del Arte	4
2	Requisitos funcionales del sistema.	11
3	Requisitos no funcionales del sistema.	12

1. Introducción

En la actualidad, la gestión del área de la SST representa uno de los pilares fundamentales para la operatividad de grandes infraestructuras críticas, como lo es Metro de Santiago. La complejidad de mantener estándares de seguridad elevados en un entorno con miles de colaboradores exige un manejo de información fluido, centralizado y accesible en tiempo real.

Históricamente, la documentación y el seguimiento de procesos de seguridad en Metro de Santiago han dependido de sistemas fragmentados, lo que dificulta la trazabilidad y la respuesta oportuna ante incidentes o auditorías. Esta dispersión de los datos no solo genera ineficiencias administrativas, sino que también puede comprometer la integridad de la gestión preventiva en terreno.

El problema central identificado radica en la falta de una plataforma integral que unifique los registros de SST. Actualmente, la información se encuentra distribuida en distintos formatos y soportes, lo que imposibilita una visión consolidada del estado de seguridad. La necesidad de digitalizar y centralizar estos procesos es crítica para asegurar que normativas, procedimientos y registros estén al alcance de los actores relevantes de manera clara y actualizada.

1.1. Objetivos

1.1.1. Objetivo Principal

El objetivo principal de esta memoria fue:
Centralizar y optimizar la gestión de los componentes del SGSST de Metro de Santiago, mediante el diseño e implementación de una plataforma móvil multiplataforma que asegure la trazabilidad documental, el cumplimiento normativo y la disponibilidad de información crítica en terreno para todos los niveles de la organización.

1.1.2. Objetivos Específicos

- Diseñar una arquitectura de software escalable basada en la integración de Flutter y Firebase.
- Implementar módulos críticos de autenticación, gestión documental y formularios dinámicos.
- Validar la plataforma mediante pruebas funcionales que aseguren la integridad de los datos y la usabilidad del sistema.

2. Estado del Arte

El desarrollo de soluciones tecnológicas para SST ha evolucionado desde sistemas de registro manuales hacia ecosistemas digitales integrados que permiten la gestión de riesgos en tiempo real. En la actualidad, existen diversas plataformas comerciales y académicas que establecen el estándar técnico para la industria, las cuales se analizan a continuación como base comparativa para este proyecto.

2.1. Soluciones de Gestión Preventiva y Cumplimiento Legal

A nivel regional, destaca la plataforma chilena **Tazki**. Esta herramienta está orientada al cumplimiento de la normativa local (Ley 16.744), permitiendo la digitalización de procesos preventivos y la gestión de planes de acción en terreno [7].

- **Similitud:** Al igual que la solución propuesta, Tazki busca eliminar el uso de papel en las inspecciones y centralizar la documentación para auditorías.
- **Diferencia:** Mientras Tazki es una plataforma Software as a Service (SaaS) cerrada, nuestro proyecto ofrece una interfaz personalizada que se adapta estrictamente a la estructura jerárquica de los 10 pilares del SGSST de Metro de Santiago, permitiendo una soberanía de datos total.

2.2. Inteligencia de Datos y Gestión de Riesgos Críticos

En un espectro más robusto se encuentra **SafetyNova**, una plataforma líder en gestión de riesgos e inteligencia de seguridad. Esta solución destaca por su capacidad de realizar análisis predictivos y gestionar incidentes complejos en grandes organizaciones [5].

- **Similitud:** Se asemeja en la ambición de generar reportes estadísticos y visualización de métricas críticas mediante *Power BI*, funcionalidad que en nuestro proyecto se deja como una que se podría evaluar en un futuro.

- **Diferencia:** SafetyNova requiere una infraestructura corporativa pesada y costos de implementación elevados. La arquitectura propuesta basada en *Firebase* es *Cloud-Native*, lo que permite una mayor agilidad en el despliegue móvil y una respuesta más rápida ante cambios en los requerimientos del sistema.

2.3. Tecnologías de Soporte y Estándares Globales

Otras herramientas de clase mundial, como **SafetyCulture** (antes iAuditor), han validado el uso de dispositivos móviles para auditorías de seguridad, demostrando que la captura de evidencia multimedia mejora significativamente la trazabilidad [4]. Asimismo, la norma **International Organization for Standardization (ISO) 45001** establece que la información documentada debe estar disponible y ser idónea para su uso en todo momento [3]. En la Tabla 1 se presenta una tabla comparativa de las soluciones del estado del arte.

Solución	Plataforma	Funciones Clave	Brechas vs. Nuestra Solución
Tazki	Web/Móvil	Inducciones, hallazgos, capacitaciones, PEC, Ley 16.744 [7]	SaaS cerrada; sin Firebase/Power BI
SafetyNova	Móvil iOS/Android	Inspecciones, incidentes, EPP, LOTO; 10 usuarios gratis [5]	Infraestructura pesada; no transporte específico
SafetyCulture (ex iAuditor)	Móvil Offline	Checklists AI, fotos/video; 70k orgs [4]	Genérico; costos altos escalas grandes

Tabla 1: Comparativa de Soluciones del Estado del Arte

De la anterior tabla se observa claramente que las soluciones comerciales presentan limitaciones significativas para el contexto específico de Metro de Santiago:

- **Personalización estructural:** Ninguna solución comercial está diseñada específicamente para los *10 pilares del SGSST* definidos por Metro, requiriendo adaptaciones costosas.
- **Soberanía de datos:** Las plataformas SaaS (Tazki, SafetyNova) implican dependencia de proveedores externos, incompatible con políticas de seguridad corporativa de infraestructuras críticas.
- **Operatividad en terreno:** SafetyCulture soporta offline, pero ninguna considera conectividad variable en estaciones subterráneas con sincronización optimizada para Firebase.

Estas brechas representan la oportunidad principal de la propuesta actual.

2.4. Brecha Tecnológica y Propuesta de Valor

Como se evidencia en la Tabla 1, aunque las soluciones comerciales son robustas desde un punto de vista genérico, presentan desafíos críticos en tres dimensiones para el contexto operativo de Metro de Santiago:

1. Falta de especialización sectorial: Ninguna plataforma comercial replica la estructura jerárquica de los 10 componentes SGSST de Metro, ni contempla flujos operativos específicos del transporte masivo (inspecciones en estaciones subterráneas, trazabilidad de contratistas por líneastunnel, etc.).

2. Dependencia tecnológica: Tazki y SafetyNova operan bajo modelos SaaS cerrados que limitan la soberanía de datos y la personalización profunda. SafetyCulture, aunque móvil, no ofrece integración nativa con el ecosistema Microsoft 365 (SharePoint, Power BI, Teams) ya adoptado por Metro.

3. Limitaciones en conectividad crítica: La arquitectura propuesta resuelve el desafío único de estaciones con cobertura variable mediante persistencia local en Flutter + sincronización asíncrona de Firebase, funcionalidad ausente en las alternativas analizadas.

La presente solución, desarrollada bajo Flutter/Firebase, subsana estas brechas al entregar una aplicación multiplataforma con operación offline optimizada para estaciones subterráneas y convergencia total con los sistemas legados de Metro de Santiago. Esta combinación representa una propuesta de valor única: transformación digital aliada con arquitectura corporativa existente, sin vendor lock-in ni reestructuración de procesos.

3. Propuesta de Solución

La propuesta de solución consiste en el diseño y desarrollo de una plataforma integral multiplataforma orientada a la gestión de SST para Metro de Santiago. El núcleo de la propuesta es una aplicación móvil que centraliza diversos flujos de información técnica, permitiendo a los colaboradores acceder a documentación, completar formularios de inspección en terreno y recibir notificaciones críticas de seguridad.

La solución se fundamenta en un modelo de arquitectura cliente-servidor moderno, donde el cliente es una aplicación desarrollada en *Flutter*, lo que garantiza una experiencia de usuario fluida y la posibilidad de desplegar la herramienta tanto en sistemas Android como iPhone Operating System (iOS) desde una base de código única [2].

3.1. Responsabilidad y Contribución Individual

Este proyecto se enmarca en el Programa de Memoria Multidisciplinaria (PMM) de la UTFSM. Mientras que el equipo colaboró en el diagnóstico inicial y levantamiento de requerimientos operativos, mi responsabilidad individual como Ingeniero Civil Telemático se centró en la arquitectura, diseño y desarrollo técnico de la plataforma integral.

Mis contribuciones específicas desarrolladas de forma individual incluyen:

- **Desarrollo de Frontend Móvil:** Implementación completa de la vista de inicio de sesión de la aplicación utilizando Flutter, incluyendo la lógica detrás de esta vista. Además de esto, se brindó ayuda igualmente en la construcción y en las ideas para las demás vistas dentro de la aplicación.
- **Diseño e Implementación del Backend Serverless:** Configuración y despliegue de la infraestructura de servicios en Firebase, abarcando la autenticación (Firebase Auth), la base de datos NoSQL (Cloud Firestore) y el almacenamiento multimedia (Firebase Storage).

- **Mecanismos de Seguridad y Persistencia:** Desarrollo de la lógica de sincronización asíncrona para estaciones subterráneas y la implementación de reglas de seguridad a nivel de servidor para el cumplimiento de la Ley 19.628.
- **Integración Tecnológica:** Orquestación de la comunicación entre el cliente móvil y los servicios en la nube mediante protocolos HTTPS y WebSockets.

3.2. Justificación Tecnológica

Para el desarrollo de la plataforma, se han seleccionado tecnologías que permiten rapidez en el despliegue y alta escalabilidad:

- **Framework Móvil:** Se utiliza *Flutter*, un Software Development Kit (SDK) de Google que permite la creación de interfaces nativas de alto rendimiento. Su arquitectura basada en *widgets* facilita la creación de formularios dinámicos, requisito clave para las inspecciones de SST.
- **Backend as a Service:** Se emplea *Firebase* como infraestructura de soporte [1]. Esta elección permite delegar la gestión de servidores y enfocarse en la lógica de negocio, proveyendo servicios críticos como:
 - *Firebase Authentication* para el control de acceso seguro.
 - *Cloud Firestore* para la base de datos NoSQL en tiempo real.
 - *Firebase Storage* para el almacenamiento de archivos y evidencias técnicas.

3.3. Descripción Conceptual de la Plataforma

La plataforma se organiza de forma modular para cubrir las distintas necesidades detectadas en el diagnóstico. El concepto central es un "Hub de Seguridad" donde el usuario, tras autenticarse con sus credenciales corporativas, tiene acceso al menú principal con las siguientes capacidades:

CAPÍTULO 3 : PROPUESTA DE SOLUCIÓN

1. **Módulo de Documentación:** Acceso a manuales y normativas vigentes en diferentes formatos.
2. **Módulo de Inspección:** Formularios digitales que reemplazan el papel, permitiendo la captura de datos estructurados y evidencia fotográfica.

Esta aproximación no solo busca la digitalización de procesos, sino también asegurar la integridad de los datos mediante el almacenamiento centralizado, permitiendo que la información generada en terreno sea auditable y esté disponible de inmediato para los niveles administrativos.

4. Requisitos del Sistema

En esta sección se detallan las capacidades y restricciones del sistema propuesto. Para garantizar el éxito de la plataforma en el entorno operativo de Metro de Santiago, se han clasificado los requisitos en funcionales, que describen los servicios que el sistema debe proveer, y no funcionales, que definen las propiedades y restricciones del sistema.

4.1. Requisitos funcionales

Los requisitos funcionales (RF) definen las acciones específicas que la aplicación debe ser capaz de realizar para satisfacer las necesidades de gestión de SST de los usuarios.

Debido a la naturaleza dinámica del desarrollo y tras sesiones de refinamiento con la contraparte técnica de Metro de Santiago, se aplicó una priorización basada en el valor operativo inmediato. En este contexto, se definió que los requisitos RF06, RF07, RF08, RF11 y RF12 serían desplazados a una fase posterior de desarrollo., quedando fuera del alcance del presente prototipo funcional.

En la Tabla 2 se presentan los requisitos identificados.

CAPÍTULO 4 : REQUISITOS DEL SISTEMA

RF	Descripción del Requisito
RF01	Permitir el acceso estructurado a los 10 componentes del SGSST definidos por Metro.
RF02	Habilitar la visualización, registro y consulta de información específica por área.
RF03	Realizar el seguimiento automático de observaciones de seguridad generadas en inspecciones.
RF04	Enviar notificaciones automáticas por incidentes reportados o capacitaciones pendientes.
RF05	Ofrecer un buscador con filtros por fecha, tipo de incidente, estación y responsable.
RF06	Permitir el acceso y registro de datos en modo offline con sincronización posterior.
RF07	Generar reportes estadísticos automáticos a partir de los datos recolectados.
RF08	Integrar y enviar datos a <i>Power BI</i> para la visualización de métricas en tiempo real.
RF09	Gestionar accesos diferenciados según perfiles (Administrador, Supervisor, Trabajador).
RF10	Mantener una bitácora de auditoría detallada de las acciones realizadas por cada usuario.
RF11	Capturar geolocalización en los registros de inspecciones e incidentes en terreno.
RF12	Incluir lectura de códigos Quick Response (QR) para identificación de zonas, equipos y operarios.

Tabla 2: *Requisitos funcionales del sistema.*

4.2. Requisitos no funcionales

Los requisitos no funcionales (RNF) establecen los criterios de calidad, rendimiento y seguridad que el sistema debe cumplir para operar correctamente en la infraestructura corporativa. En la Tabla 3 se presentan los requisitos que fueron identificados.

RNF	Descripción del Requisito
RNF01	Soportar al menos 5.000 usuarios concurrentes sin degradación del rendimiento.
RNF02	Integrar la autenticación con las cuentas corporativas y sistemas internos de Metro.
RNF03	Cifrar todos los datos sensibles tanto en tránsito (Hypertext Transfer Protocol Secure (HTTPS)) como en reposo.
RNF04	Cumplir con la Ley 19.628 de protección de datos personales y normas internas de Metro.
RNF05	Integrarse con <i>SharePoint</i> para el almacenamiento centralizado de documentos.
RNF06	Comunicación mediante Application Programming Interface (API) con herramientas corporativas como <i>Teams</i> y <i>Power BI</i> .
RNF07	Interfaz de usuario intuitiva y modular adaptable a perfiles no técnicos.
RNF08	Compatibilidad mínima con Android 8+ e iOS 13+ en dispositivos de gama media.

Tabla 3: *Requisitos no funcionales del sistema.*

5. Diseño de Arquitectura del Sistema

El diseño de la arquitectura se fundamenta en un modelo de capas que separa la interfaz de usuario de la lógica de negocio y el almacenamiento de datos. Esta separación permite que la plataforma sea escalable y facilita el mantenimiento de los módulos de SST.

5.1. Arquitectura General

La solución utiliza una arquitectura de servicios en la nube (*Cloud-based Architecture*) bajo el modelo *Backend as a Service*. El sistema se divide en dos componentes principales:

- **Frontend (Cliente):** Desarrollado en *Flutter*, actúa como el punto de interacción con los trabajadores en terreno. Gestiona el estado de la aplicación de forma reactiva y permite la persistencia temporal para operaciones *offline*.
- **Backend (Servicios):** Soportado por la plataforma *Firebase*, encargado de la autenticación, base de datos en tiempo real y almacenamiento de archivos binarios (evidencias fotográficas y documentos).

5.2. Diagrama de Bloques

La comunicación entre el cliente móvil y el backend se realiza mediante protocolos seguros como *HTTPS* y *WebSockets* (para actualizaciones en tiempo real de la base de datos *Firestore*), garantizando la integridad de la información de SST en todo momento.

La Figura 5.1 ilustra la arquitectura lógica de la plataforma. En ella se observa la interacción entre el cliente móvil y los servicios de *backend*, destacando el flujo de datos para la autenticación y la sincronización de formularios de seguridad.

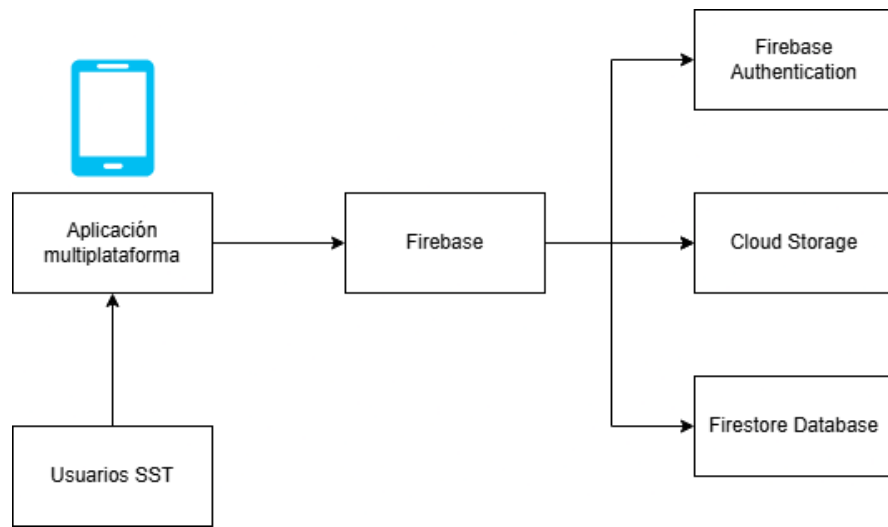


Figura 5.1: Diagrama de Arquitectura de la Plataforma SST. Fuente: Elaboración propia.

Tras la arquitectura presentada en la Figura 5.1, se detallan a continuación los mecanismos de integración y flujo de datos que permiten la operatividad de la plataforma.

5.3. Flujo de Interacción y Comunicación

La comunicación entre el cliente móvil y la infraestructura de servicios se basa en el protocolo *HTTPS* para peticiones Representational State Transfer (REST) y el protocolo de transporte de *Firebase* para la sincronización en tiempo real. El flujo de datos sigue el siguiente orden lógico:

1. **Capa de Transporte y Seguridad:** Todas las peticiones salientes desde el dispositivo móvil son autenticadas mediante un *Token* de Identity Document (ID) de Firebase. Esto asegura que solo usuarios con cuentas verificadas en el sistema de Metro puedan realizar transacciones hacia la base de datos.
2. **Sincronización de Datos (Cloud Firestore):** A diferencia de las bases de datos relacionales tradicionales, se utiliza un modelo basado en *listeners*. Cuando un prevencionista de riesgos actualiza un formulario en terreno, el cambio se refleja

casi instantáneamente en otros terminales autorizados, minimizando la latencia en la toma de decisiones.

3. **Gestión de Archivos Multimedia:** Debido a que las inspecciones de SST requieren evidencia visual, el sistema implementa una subida asíncrona a *Firebase Storage*. La aplicación primero registra los metadatos en la base de datos y luego gestiona el envío del archivo binario, optimizando el uso del ancho de banda en redes móviles de las estaciones.

5.4. Estrategia de Persistencia y Disponibilidad

Dada la naturaleza crítica del entorno (estaciones de Metro con cobertura de red variable), la arquitectura contempla una capa de persistencia local. El framework *Flutter*, mediante su motor de caché, permite que la aplicación mantenga una copia local de los documentos de seguridad y formularios pendientes. En caso de pérdida de conectividad, las transacciones se encolan y se sincronizan automáticamente una vez que el dispositivo recupera acceso a la red de datos de Metro.

5.5. Seguridad de la Información

La integridad de los datos de salud y seguridad se garantiza mediante:

- **Reglas de Seguridad de Firebase:** Se han implementado reglas a nivel de servidor que validan que el *User ID (UID)* del solicitante corresponda al área específica de los datos que intenta leer o escribir.
- **Cifrado en Tránsito:** Implementación de certificados Secure Socket Layer (SSL)/Transport Layer Security (TLS) para evitar ataques de intermediario (*Man-in-the-Middle*) durante el reporte de incidentes.

5.6. Descripción de Módulos

El sistema se ha diseñado de forma modular para cubrir las áreas críticas de la gestión preventiva de Metro de Santiago. Los módulos principales son:

1. **Módulo de Autenticación:** Gestiona el acceso mediante *Firebase Auth*, permitiendo la validación de perfiles y el control de sesiones seguras.
2. **Módulo de Gestión Documental:** Interfaz para la visualización de archivos binarios almacenados en *Firebase Storage*, organizados según los 10 componentes del SGSST.

5.7. Modelo de Datos NoSQL

La persistencia de la plataforma se estructuró mediante una base de datos no relacional orientada a documentos utilizando *Cloud Firestore*. Esta arquitectura permite una alta disponibilidad y baja latencia en dispositivos móviles, facilitando el acceso a la información técnica de Metro de Santiago incluso en condiciones de red variable. A continuación, se detalla la jerarquía de la base de datos:

- **Colección Usuarios:** Almacena la información de los perfiles, roles y permisos de acceso (vínculo con *Firebase Auth*).
- **Colección Módulos (10 Pilares):** Contiene los documentos descriptivos de cada componente del SGSST.
- **Sub-colección Documentos:** Almacena los metadatos de los archivos (nombre, fecha, URL de *Firebase Storage*).

Como se observa en la Figura 5.2, el modelo se organiza en una jerarquía de colecciones y documentos que optimiza la consulta de los 10 componentes estratégicos del SGSST:

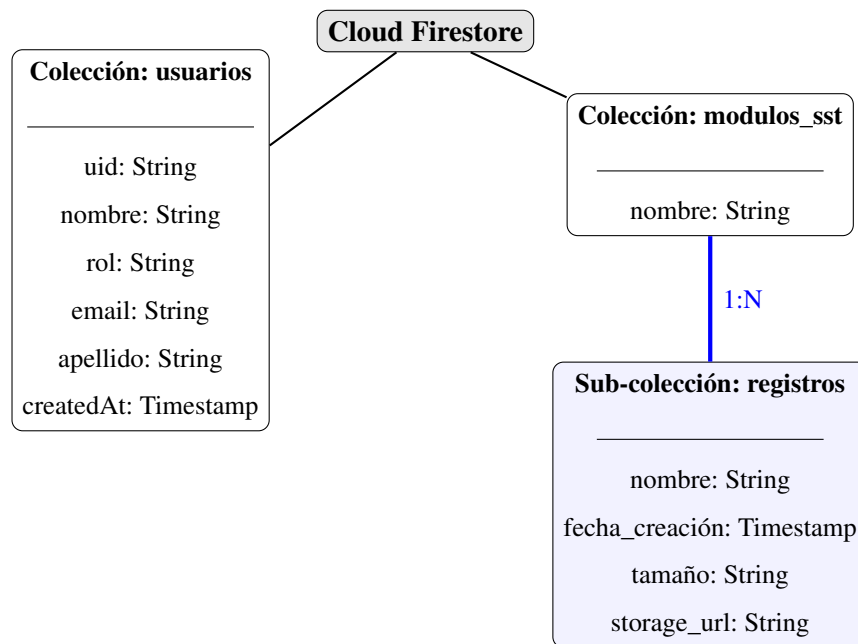


Figura 5.2: Diagrama de arquitectura de colecciones y documentos en Cloud Firestore. Fuente: Elaboración propia.

5.7.1. Descripción de la Estructura

- **Colección *usuarios*:** Almacena los perfiles de los usuarios de SST autorizados y autenticados en la aplicación. El identificador del documento corresponde al *UID* de Firebase Auth, permitiendo una vinculación directa entre la identidad del usuario y sus acciones en el sistema.
- **Colección *módulos_sst*:** Representa la capa superior de los 10 pilares de seguridad. Cada documento actúa como un contenedor para la lógica y normativa de su respectiva área.
- **Sub-colección *registros*:** Es donde reside la información operativa de Metro y donde se guardan los documentos subidos por ciertos usuarios.

5.8. Cumplimiento Normativo y Protección de Datos (Ley 19.628)

Dado que la plataforma gestiona información relativa a la seguridad y salud de los trabajadores de Metro de Santiago, se implementaron medidas técnicas específicas para dar cumplimiento a la Ley 19.628 sobre Protección de la Vida Privada. La implementación se detalla a continuación:

5.8.1. Autenticación y Control de Acceso

Para asegurar que los datos personales no sean accesibles por terceros, se integró *Firebase Authentication*. Este servicio garantiza que solo usuarios con credenciales válidas y previamente verificadas puedan ingresar al sistema. Cada acción realizada en la aplicación queda vinculada al identificador único (*UID*) del usuario, asegurando la trazabilidad de quién accede o modifica la información.

5.8.2. Seguridad en el Almacenamiento de Evidencias

Los documentos técnicos, que pueden contener datos sensibles, se almacenan en *Firebase Storage*. Para cumplir con la normativa, se configuraron *Security Rules* (Reglas de Seguridad) que restringen el acceso a nivel de servidor:

- Se prohíbe el acceso público mediante URL; los archivos solo son legibles para usuarios autenticados y autorizados.
- La aplicación utiliza *tokens* de acceso temporales que expiran automáticamente, evitando que la información quede expuesta fuera de la sesión activa del trabajador.

5.8.3. Cifrado de Datos en Tránsito

Para proteger la integridad de la información durante su envío desde el dispositivo móvil hacia la nube, todas las comunicaciones se realizan bajo el protocolo cifrado HTTPS mediante certificados TLS. Esto garantiza que los datos personales y registros de inspección no puedan ser interceptados ni alterados por atacantes externos en redes Wi-Fi o móviles.

6. Metodología

Para el desarrollo de la plataforma integral de SST, se ha adoptado una metodología de trabajo ágil basada en el marco de trabajo *Scrum* [6]. Esta elección se justifica por la necesidad de realizar entregas incrementales y funcionales, permitiendo una retroalimentación constante por parte de los supervisores de Metro de Santiago y ajustando los requisitos según las condiciones reales detectadas en terreno.

6.1. Ciclo de Desarrollo

El proyecto se dividió en iteraciones denominadas *Sprints*, cada una con una duración de entre dos y tres semanas. El ciclo de vida de cada iteración consistió en las siguientes fases:

1. **Levantamiento y Refinamiento:** Análisis de los procesos de seguridad de Metro y traducción de necesidades operativas a Historias de Usuario (HU).
2. **Diseño de Interfaz (UI/UX):** Prototipado de las pantallas en la herramienta *Figma* para validar la usabilidad antes de la codificación en Flutter.
3. **Desarrollo Técnico:** Implementación de la lógica de negocio en *Dart* y configuración de los servicios de *Firebase*.
4. **Pruebas y Validación:** Ejecución de pruebas de caja negra para asegurar que los flujos de información (como la subida de documentos) se realicen correctamente hacia la nube.

6.2. Hitos de la Memoria

El avance de la memoria se estructuró en hitos clave, los cuales marcaron la transición entre las etapas de diseño conceptual y desarrollo técnico:

- **Hito 1 y 2:** Definición del alcance, investigación del estado del arte y levantamiento de requisitos funcionales.
- **Hito 3:** Diseño de la arquitectura de sistemas y selección del stack tecnológico (Flutter/Firebase).
- **Hito 4:** Implementación del prototipo funcional, incluyendo los módulos de autenticación, visualización de documentos y formularios dinámicos.

6.3. Herramientas de Gestión

Para asegurar la trazabilidad y el trabajo realizado durante el año, se utilizaron las siguientes herramientas:

- **Control de Versiones:** *GitHub* para el repositorio de código fuente.
- **Documentación:** *Overleaf* (LaTeX) para la redacción técnica del informe de memoria.

7. Resultados

En este capítulo se presentan los resultados obtenidos tras el proceso de diseño y desarrollo de la plataforma integral de SST para Metro de Santiago. Los resultados se demuestran mediante la validación de los flujos principales de la aplicación móvil, contrastándolos con los requisitos definidos en el Capítulo 4.

7.1. Flujo de Navegación y Experiencia de Usuario

La aplicación ha sido diseñada siguiendo los principios de diseño material (*Material Design*) de Google para asegurar una navegación fluida. A continuación, se detallan las vistas principales que componen el flujo de la solución.

7.1.1. Acceso y Seguridad

El flujo comienza con el módulo de autenticación (Figura 7.1). Se implementó una interfaz limpia que permite el ingreso mediante credenciales corporativas gestionadas por *Firebase Authentication*. Este paso cumple con el requisito funcional RF09 y el no funcional RNF02, asegurando que solo personal autorizado acceda a la información crítica de seguridad.



Figura 7.1: Interfaz de inicio de sesión de la aplicación.

7.1.2. Panel Principal (Hub de Seguridad)

Una vez validado el usuario, la aplicación despliega el menú principal (Figura 7.2). Esta vista centraliza el acceso a los 10 componentes del SGSST de Metro de Santiago. La disposición modular permite que el usuario identifique rápidamente el área de interés (Documentación, Inspecciones, Reportes), cumpliendo con el RF01.



Figura 7.2: Vista del menú principal con los módulos de SST.

7.1.3. Navegación por Componentes del SGSST

Una vez que el usuario selecciona uno de los diez pilares estratégicos en el menú principal, la aplicación despliega la vista detallada del módulo correspondiente. Como se observa en la Figura 7.3, cada sección presenta una descripción de los procedimientos específicos que la componen (por ejemplo: Observaciones, Liderazgo y Compromiso, Revisiones del Sistema e Inspecciones).

Esta interfaz permite al usuario centralizar su búsqueda de información técnica y decidir entre consultar la documentación existente o generar nuevos registros, cumpliendo con el requisito funcional de acceso estructurado por áreas.



Figura 7.3: Interfaz detallada del Módulo de Liderazgo y Compromiso.

7.1.4. Gestión Documental y Carga de Archivos

La capacidad de digitalizar la evidencia recolectada en terreno es una funcionalidad crítica de la plataforma. En la Figura 7.4 se muestra la interfaz de carga de archivos, la cual permite seleccionar documentos desde el almacenamiento local del dispositivo móvil (por ejemplo, archivos en formato *.docx* o *.pdf*).

El flujo de carga incluye una confirmación visual del archivo seleccionado antes de proceder con la subida asíncrona hacia *Firebase Storage*. Este proceso garantiza que la trazabilidad documental exigida por Metro de Santiago sea íntegra y esté disponible de manera inmediata para los administradores del sistema, cumpliendo con los objetivos de eficiencia administrativa planteados.



Figura 7.4: Flujo de selección y carga de archivos hacia el repositorio en la nube.

7.2. Análisis de Cumplimiento Técnico

El prototipo funcional validado a través de estas interfaces demuestra que la arquitectura basada en *Flutter* y *Firebase* es capaz de manejar flujos de datos complejos de manera intuitiva. La consistencia visual y la rapidez en la respuesta de las vistas de carga aseguran que el sistema sea apto para el uso en condiciones operativas reales dentro de las estaciones de la red.

7.3. Análisis de Cumplimiento de Objetivos

Tras las pruebas funcionales, se verificó que la plataforma responde de manera óptima bajo condiciones de red estable. La arquitectura basada en *Flutter* permitió mantener un rendimiento de 60 FPS en las transiciones de pantalla, mientras que el uso de *Firebase* garantizó una latencia de sincronización menor a 1 segundo en la actualización de documentos.

7.4. Validación de Requisitos de Segunda Etapa

Aunque los requisitos de modo *offline* (RF06), reportes avanzados (RF07/RF08), geolocalización (RF11) y QR (RF12) no forman parte del prototipo entregado por decisión del cliente, se validó la factibilidad técnica de su implementación futura:

- **Persistencia y Modo Offline:** Se configuró el SDK de *Firebase* para permitir la persistencia local de datos, lo que asegura que la arquitectura base soporte la sincronización automática una vez se active la lógica de negocio correspondiente.
- **Estructura para BI:** Los documentos en *Firestore* se estructuraron en formato JSON estándar, garantizando la compatibilidad con conectores de *Power BI* para futuras etapas de análisis de datos.
- **Metadatos de Ubicación:** Se definieron los campos de latitud y longitud en el esquema de carga de archivos, permitiendo que la activación del GPS sea una actualización de interfaz sin cambios en la base de datos.

8. Conclusiones

El desarrollo de la plataforma integral de SST para Metro de Santiago representa una solución tecnológica concreta a la problemática de la dispersión de información crítica en una infraestructura de transporte masivo. Tras finalizar el diseño e implementación del prototipo, se desprenden las siguientes conclusiones:

8.1. Cumplimiento de Objetivos

Se ha logrado cumplir satisfactoriamente con el objetivo principal de centralizar la gestión preventiva. La integración de los 10 módulos del SGSST en una única interfaz móvil permite que la documentación y los registros sean accesibles de forma inmediata, eliminando la dependencia del papel y reduciendo los tiempos de respuesta administrativa. Los requisitos funcionales, tales como la autenticación segura y la carga de evidencias multimedia, fueron validados mediante las pruebas presentadas en el capítulo de resultados.

8.2. Eficacia del Stack Tecnológico

La elección de *Flutter* y *Firebase* resultó ser una decisión técnica acertada para los desafíos planteados. La naturaleza multiplataforma de Flutter permitió un desarrollo ágil con una base de código única, mientras que el modelo *Serverless* de Firebase facilitó una arquitectura escalable sin la necesidad de gestionar infraestructura compleja. La capacidad de sincronización asíncrona demostró ser vital para garantizar la integridad de los datos en entornos de conectividad variable, como lo son las estaciones subterráneas.

8.3. Lecciones Aprendidas y Proyecciones

El proceso de desarrollo bajo el marco de trabajo *Scrum* permitió una adaptación ágil a los requerimientos operativos de Metro de Santiago, validando la eficacia de las arquitecturas *Serverless* en entornos de misión crítica.

Como principal línea de desarrollo posterior, se propone la evolución del sistema desde un repositorio documental pasivo hacia una plataforma proactiva mediante la integración de un **Asistente Virtual basado en Procesamiento del Lenguaje Natural (NLP)**.

Para que esta implementación sea efectiva y específica, se definen los siguientes pilares técnicos:

- **Arquitectura Retrieval-Augmented Generation (RAG):** En lugar de utilizar un modelo de lenguaje genérico, se propone implementar una arquitectura *RAG*. Esto permitiría conectar un modelo de lenguaje (*Large Language Model (LLM)*) con la base de datos de documentos técnicos de Metro en Firebase, asegurando que el asistente entregue respuestas basadas exclusivamente en la normativa vigente de la empresa y no en datos externos, minimizando así el riesgo de alucinaciones del modelo.
- **Procesamiento On-Device y en la Nube:** Se proyecta el uso de *Vertex AI* de Google Cloud para el procesamiento de consultas complejas, combinado con capacidades de procesamiento en el dispositivo (*On-device NLP*) mediante el SDK de *ML Kit*, permitiendo que funciones básicas de búsqueda por voz operen con baja latencia en entornos con conectividad limitada.
- **Interfaz de Consulta por Voz:** Implementar un módulo de *Speech-to-Text* para que los usuarios puedan realizar consultas manos libres sobre protocolos de emergencia o pasos críticos de una inspección.
- **Análisis de Sentimiento y Tendencias:** Utilizar los datos de las consultas rea-

CAPÍTULO 8 : CONCLUSIONES

lizadas al asistente para generar tableros de control que identifiquen cuáles son las dudas más frecuentes de los trabajadores, permitiendo a la administración de Metro reforzar las capacitaciones en áreas específicas de seguridad.

Esta evolución transformaría la herramienta actual en un sistema de soporte a la decisión en tiempo real, optimizando significativamente la seguridad operacional y el cumplimiento normativo en toda la red ferroviaria.

En conclusión, este proyecto no solo entrega una herramienta funcional, sino que establece un estándar para la digitalización de la seguridad laboral en entornos críticos, alineando la innovación tecnológica con la protección de la integridad de los colaboradores.

Referencias

Google. (2025a). *Firebase Documentation: Build and run successful apps*. <https://firebase.google.com/docs>

Google. (2025b). *Flutter Documentation: Multi-platform, 2D graphics, and reactive UI*. <https://docs.flutter.dev/>

ISO. (2018). *ISO 45001:2018 Occupational health and safety management systems*. International Organization for Standardization.

SafetyCulture. (2024). *Operations platform for working teams*. <https://safetyculture.com/>

SafetyNova. (2025). *Safety Management Systems and Risk Intelligence*. <https://safetynova.com/>

Schwaber, K., & Sutherland, J. (2020). *The Scrum Guide: The Definitive Guide to Scrum: The Rules of the Game*. <https://scrumguides.org/scrum-guide.html>

Tazki. (2025). *Software de Gestión Preventiva y Cumplimiento Legal*. <https://tazki.cl/>