



Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Firmado electrónicamente por: José Francisco
Gómez Rivera
Motivo: Autorización electrónica de trabajo de
graduación
Fecha: 03/09/2026 08:59:17
Lugar: Facultad de Ingeniería, USAC.

**SOFTWARE PARA LA PROGRAMACIÓN Y REGISTRO DE MANTENIMIENTOS
PREVENTIVOS Y CORRECTIVOS DE EQUIPOS EN INSTITUTO NACIONAL DE CIENCIAS
FORENSES**

Brandon Javier Nolberto Soto Castañeda

Asesorado por el Ing. Elmer Orlando Real Ixcayau

Guatemala, septiembre de 2026

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA



FACULTAD DE INGENIERÍA

**SOFTWARE PARA LA PROGRAMACIÓN Y REGISTRO DE MANTENIMIENTOS
PREVENTIVOS Y CORRECTIVOS DE EQUIPOS EN INSTITUTO NACIONAL DE CIENCIAS
FORENSES**

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

BRANDON JAVIER NOLBERTO SOTO CASTAÑEDA
ASESORADO POR EL ING. ELMER ORLANDO REAL IXCAYAU

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, SEPTIEMBRE DE 2026

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERÍA



NÓMINA DE JUNTA DIRECTIVA

DECANO (a. i.)	Ing. José Francisco Gómez Rivera
VOCAL II	Ing. Mario Renato Escobedo Martínez
VOCAL III	Ing. Juan Carlos Molina Jiménez
VOCAL IV	Ing. Kevin Vladimir Armando Cruz Lorente
VOCAL V	Ing. Fernando José Paz González
SECRETARIA	Mtr. Sindy Massiel Godínez Bautista

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

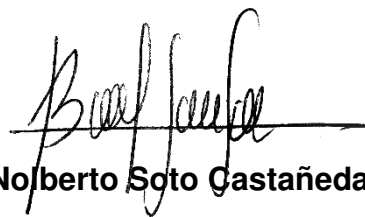
DECANO (a. i.)	Ing. José Francisco Gómez Rivera
EXAMINADORA	Inga. Floriza Felipa Ávila Pesquera de Medinilla
EXAMINADOR	Ing. Sergio Leonel Gómez Bravo
EXAMINADOR	Ing. Carlos Alfredo Azurdia Morales
SECRETARIA	Mtr. Sindy Massiel Godínez Bautista

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

**SOFTWARE PARA LA PROGRAMACIÓN Y REGISTRO DE MANTENIMIENTOS
PREVENTIVOS Y CORRECTIVOS DE EQUIPOS EN INSTITUTO NACIONAL DE CIENCIAS
FORENSES**

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha 05 de febrero de 2025.

A handwritten signature in black ink, appearing to read 'Brandon Soto', written over a horizontal line.

Brandon Javier Nolberto Soto Castañeda



VERDAD Y JUSTICIA,
NUESTRO COMPROMISO.

Guatemala, **27** de abril de 2026

Ing. Oscar Argueta Hernández
Director de la Unidad de EPS
Facultad de Ingeniería
Universidad de San Carlos de Guatemala

Estimado Ing Argueta:

Por este medio atentamente hago de su conocimiento que como Asesor de la Práctica del Ejercicio Profesional Supervisado (EPS), de la estudiante universitaria de la Carrera de Ingeniería en Ciencias y Sistemas, **Brandon Javier Nolberto Soto Castañeda** quien se identifica con DPI **3016582770101** con registro académico **201503893**, he revisado el informe final titulado ***"Desarrollo de una herramienta de software para la programación y registro de mantenimientos preventivos y correctivos de equipos en INACIF"***.

En tal virtud, lo doy por aprobado, solicitándole darle el trámite respectivo Sin otro particular, me es grato suscribirme.

Atentamente

Ing. Pablo Alejandro Martínez Gómez
Profesional I

Sección de Desarrollo de Software
Unidad Informática

Instituto Nacional de Ciencias Forenses de Guatemala -INACIF-

Ing. Pablo Alejandro Martínez Gómez
Ingeniero en Ciencias y Sistemas
Profesional I
Sección de Desarrollo de Software
Unidad de Informática
-INACIF-



Guatemala, 18 de mayo de 2026
REF.EPS.DOC.229.05.2026

Ing. Oscar Argueta Hernández
Director Unidad de EPS
Facultad de Ingeniería
Presente

Estimado Ingeniero Argueta Hernández:

Por este medio atentamente le informo que como Supervisora de la Práctica del Ejercicio Profesional Supervisado, (E.P.S) del estudiante universitario de la Carrera de Ingeniería en Ciencias y Sistemas, **Brandon Javier Nolberto Soto Castañeda, Registro Académico 201503893 y CUI 3016582770101** procedí a revisar el informe final, cuyo título es **SOFTWARE PARA LA PROGRAMACIÓN Y REGISTRO DE MANTENIMIENTOS PREVENTIVOS Y CORRECTIVOS DE EQUIPOS EN INSTITUTO NACIONAL DE CIENCIAS FORENSES.**

En tal virtud, **LO DOY POR APROBADO**, solicitando darle el trámite respectivo.

Sin otro particular, me es grato suscribirme.

Atentamente,

“Id y Enseñad a Todos”



Inga. Floriza Felipa Ávila Pesquera de Medinilla
Supervisora de EPS
Área de Ingeniería en Ciencias y Sistemas



Guatemala, 18 de mayo de 2026
REF.EPS.D.206.05.2026

Ing. Carlos Gustavo Alonzo
Director Escuela de Ciencias y Sistemas
Facultad de Ingeniería
Presente

Estimado Ing. Carlos Gustavo Alonzo:

Por este medio atentamente le envío el informe final correspondiente a la práctica del Ejercicio Profesional Supervisado, (E.P.S) titulado **SOFTWARE PARA LA PROGRAMACIÓN Y REGISTRO DE MANTENIMIENTOS PREVENTIVOS Y CORRECTIVOS DE EQUIPOS EN INSTITUTO NACIONAL DE CIENCIAS FORENSES**, que fue desarrollado por el estudiante universitario **Brandon Javier Nolberto Soto Castañeda, Registro Académico 201503893 y CUI 3016582770101** quien fue debidamente asesorado por Ing. Elmer Orlando Real Ixcayau y supervisado por Inga. Floriza Felipa Ávila Pesquera de Medinilla.

Por lo que habiendo cumplido con los objetivos y requisitos de ley del referido trabajo y existiendo la aprobación del mismo por parte del Asesor y la Supervisora de EPS, en mi calidad de Director apruebo su contenido solicitando darle el trámite respectivo.

Sin otro particular, me es grato suscribirme.

Atentamente,
“Id y Enseñad a Todos”

Ing. Oscar Argueta Hernández
Director Unidad de EPS



Universidad San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala 27 de julio de 2026

Ingeniero
Carlos Gustavo Alonzo
Director de la Escuela de Ingeniería
En Ciencias y Sistemas

Respetable Ingeniero Alonzo:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación-EPS del estudiante **BRANDON JAVIER NOLBERTO SOTO CASTAÑEDA** carné **201503893** y CUI **3016582770101**, titulado: **"SOFTWARE PARA LA PROGRAMACIÓN Y REGISTRO DE MANTENIMIENTOS PREVENTIVOS Y CORRECTIVOS DE EQUIPOS EN INSTITUTO NACIONAL DE CIENCIAS FORENSES"** y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,



Ing. Carlos Alfredo Azurdia
Coordinador de Privados
y Revisión de Trabajos de Graduación



SIST.LNG.DIRECTOR.69.EICCSS.2026

El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del Asesor, el visto bueno del Coordinador de área del trabajo de graduación titulado: **SOFTWARE PARA LA PROGRAMACIÓN Y REGISTRO DE MANTENIMIENTOS PREVENTIVOS Y CORRECTIVOS DE EQUIPOS EN INSTITUTO NACIONAL DE CIENCIAS FORENSES**, presentado por: **Brandon Javier Nolberto Soto Castañeda**, procedo con el Aval del mismo, ya que cumple con los requisitos normados por la Facultad de Ingeniería.

“ID Y ENSEÑAD A TODOS”

Una firma manuscrita en tinta negra sobre un sello circular. El sello contiene el texto "UNIVERSIDAD DE SAN CARLOS DE GUATEMALA" y "ESCUELA DE INGENIERIA EN CIENCIAS Y SISTEMAS".

Ingeniero Carlos Gustavo Alonzo
DIRECTOR
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, julio de 2026



USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

Decanato
Facultad de Ingeniería

24189101- 24189102

LNG.DECANATO.OIE.797.2026

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte de la Dirección de Escuela de Ingeniería en Ciencias y Sistemas, al Trabajo de Graduación titulado: **SOFTWARE PARA LA PROGRAMACIÓN Y REGISTRO DE MANTENIMIENTOS PREVENTIVOS Y CORRECTIVOS DE EQUIPOS EN INSTITUTO NACIONAL DE CIENCIAS FORENSES**, presentado por: **Brandon Javier Nolberto Soto Castañeda** después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:

Firmado electrónicamente por: José Francisco Gómez Rivera
Motivo: Informe final EPS
Fecha: 03/09/2026 08:59:14
Lugar: Facultad de Ingeniería, USAC.

Ing. José Francisco Gómez Rivera
Decano a.i.



Guatemala, septiembre de 2026

Para verificar validez de documento ingrese a <https://www.ingenieria.usac.edu.gt/firma-electronica/consultar-documento>

Tipo de documento: Correlativo para orden de impresión Año: 2026 Correlativo: 797 CUI: 3016582770101

Escuelas: Ingeniería Civil, Ingeniería Mecánica Industrial, Ingeniería Química, Ingeniería Mecánica Eléctrica, - Escuela de Ciencias, Regional de Ingeniería Sanitaria y Recursos Hidráulicos (ERIS). Postgrado Maestría en Sistemas Mención Ingeniería Vial. Carreras: Ingeniería Mecánica, Ingeniería Electrónica, Ingeniería en Ciencias y Sistemas. Licenciatura en Matemática. Licenciatura en Física. Centro de Estudios Superiores de Energía y Minas (CESEM). Guatemala, Ciudad

ACTO QUE DEDICO A:

Dios

Por ser mi guía constante, por brindarme fuerzas en los momentos de dificultad y por iluminar mi camino con sabiduría y esperanza.

Mi esposa

Por su amor, comprensión y apoyo incondicional, por creer en mí y por acompañarme con paciencia en este proceso.

Mi hijo

Por su amor incondicional, por enseñarme el valor del esfuerzo y la honestidad, y por ser el ejemplo que me inspira a superarme cada día.

Mis padres

Por su apoyo sincero, sus palabras de aliento y por compartir conmigo alegrías y desafíos a lo largo de este camino.

AGRADECIMIENTOS A:

**Universidad de San
Carlos de Guatemala**

Por brindarme la oportunidad de formarme académica y profesionalmente.

Mis amigos

Por su apoyo y por compartir momentos de estudio y también de alegría.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES.....	V
LISTA DE SÍMBOLOS	VII
GLOSARIO	IX
RESUMEN.....	XI
OBJETIVOS.....	XIII
INTRODUCCIÓN	XV
1. FASE DE INVESTIGACIÓN	1
1.1. Antecedentes de la empresa	1
1.1.1. Reseña histórica	1
1.1.2. Misión	2
1.1.3. Visión	2
1.1.4. Servicios que realiza.....	3
1.2. Descripción de las necesidades	3
1.3. Priorización de las necesidades	4
2. FASE TÉCNICO-PROFESIONAL	7
2.1. Descripción del proyecto	7
2.2. Investigación preliminar para la solución del proyecto	9
2.2.1. Análisis FODA	13
2.2.2. Supuestos del proyecto	14
2.2.3. Riesgos del proyecto	16
2.2.4. Plan de comunicación.....	18
2.3. Presentación de la solución del proyecto	19
2.3.1. Introducción al diseño de la solución	19

2.3.2.	Metodología de desarrollo de software (<i>Scrum</i>)	19
2.3.3.	Definición y análisis de requerimientos	20
2.3.3.1.	Requerimientos funcionales	20
2.3.3.2.	Requerimientos no funcionales	22
2.3.4.	Modelado UML	23
2.3.4.1.	Diagramas de casos de uso	23
2.3.4.2.	Diagrama de clases	25
2.3.4.3.	Diagramas de secuencia	26
2.3.4.4.	Diagrama de despliegue	27
2.3.5.	Diseño de base de datos	28
2.3.5.1.	Modelo entidad–relación	29
2.3.6.	Diseño de interfaz de usuario	32
2.3.6.1.	<i>Mockups</i> principales	32
2.3.6.2.	Criterios de usabilidad	37
2.3.7.	Tecnologías utilizadas	38
2.3.7.1.	Definición	38
2.3.7.2.	Justificación de selección	40
2.3.8.	Plan de implementación	41
2.3.8.1.	Cronograma de actividades	41
2.3.8.2.	Estrategia de pruebas	43
2.3.8.3.	Despliegue y capacitación	44
2.3.9.	Seguridad y confiabilidad	44
2.3.9.1.	Autenticación y roles con Keycloak	45
2.3.9.2.	Medidas de seguridad (VPN, TLS, <i>backups</i>)	45
2.3.9.3.	Evaluación y mitigación de vulnerabilidades	46
2.4.	Costos del proyecto	48
2.5.	Beneficios del proyecto	50

3.	FASE DE ENSEÑANZA-APRENDIZAJE	51
3.1.	Capacitación propuesta	51
3.2.	Material elaborado	52
3.2.1.	Manual de usuario	52
3.2.2.	Manual técnico.....	53
	CONCLUSIONES	55
	RECOMENDACIONES	57
	REFERENCIAS	59

ÍNDICE DE ILUSTRACIONES

FIGURAS

Figura 1.	Control de equipos antiguo	10
Figura 2.	Control de mantenimientos antiguo	11
Figura 3.	Casos de uso (vista general)	24
Figura 4.	Diagrama de clases	25
Figura 5.	Diagrama de secuencia A.....	26
Figura 6.	Diagrama de secuencia B.....	27
Figura 7.	Diagrama de despliegue	28
Figura 8.	Diagrama entidad-relación.....	31
Figura 9.	<i>Mockup</i> de pantalla de inicio de sesión	33
Figura 10.	<i>Mockup</i> de <i>dashboard</i> principal	34
Figura 11.	<i>Mockup</i> de gestión de equipos	35
Figura 12.	<i>Mockup</i> de calendario de mantenimientos.....	36
Figura 13.	Cronograma de actividades	43

TABLAS

Tabla 1.	Riesgos del proyecto	17
Tabla 2.	Plan de comunicación.....	18
Tabla 3.	Costos del proyecto	49

LISTA DE SÍMBOLOS

Símbolo	Significado
%	Porcentaje
Q	Quetzal (moneda de Guatemala)

GLOSARIO

<i>Docker</i>	Plataforma de virtualización ligera que permite empaquetar aplicaciones y sus dependencias en contenedores portables, utilizada en el desarrollo y despliegue del sistema.
<i>Keycloak</i>	Herramienta de gestión de identidades y control de acceso, utilizada en el sistema para autenticar usuarios y asignar roles mediante <i>tokens</i> de seguridad.
SQL	Lenguaje estándar para la gestión y manipulación de bases de datos relacionales.
TLS	Protocolo criptográfico que asegura la comunicación cifrada entre cliente y servidor, implementado en este sistema para proteger datos.
UML	Lenguaje de modelado estándar utilizado para representar gráficamente el diseño del sistema mediante diagramas de casos de uso, clases, secuencia y despliegue.
VPN	Red privada virtual que permite el acceso seguro y cifrado a los servicios institucionales desde ubicaciones externas.

RESUMEN

El presente proyecto consiste en el desarrollo de una herramienta de software para la programación, registro y control de mantenimientos preventivos, correctivos y calibraciones de equipos en el Instituto Nacional de Ciencias Forenses de Guatemala (Inacif). Actualmente, la gestión se realiza mediante hojas de cálculo y registros manuales, lo cual genera limitaciones en trazabilidad, eficiencia y cumplimiento de normativas internacionales como la ISO/IEC 17025.

La solución propuesta se implementará bajo una arquitectura basada en microservicios en Java, desplegados en Apache TomEE, con un *frontend* en Angular y un sistema de autenticación y roles gestionado con *Keycloak*. El sistema permitirá el registro de equipos, generación de alertas automáticas, administración de tickets de fallas, control de inventario y generación de reportes en formatos XLS/PDF (Angular Team, 2023).

El uso de *Scrum* como metodología ágil facilitará la entrega incremental del sistema en *sprints*, garantizando flexibilidad y adaptación a las necesidades de la institución. Con ello, se busca optimizar la gestión de activos del Inacif, garantizar la continuidad operativa de los laboratorios y fortalecer la calidad de los procesos periciales.

OBJETIVOS

General

Desarrollar e implementar una herramienta de software basada en la web para la gestión integral de mantenimientos preventivos, correctivos y calibraciones de equipos en el Inacif, mejorando la eficiencia operativa y asegurando el cumplimiento de normativas internacionales.

Específicos

1. Analizar los procesos actuales de mantenimiento en Inacif para identificar deficiencias y oportunidades de mejora.
2. Diseñar una arquitectura modular con *backend* en Java (*TomEE*) y *frontend* en Angular.
3. Implementar un sistema de roles y permisos con *Keycloak* que garantice seguridad y control de accesos.
4. Automatizar alertas y notificaciones de mantenimientos programados y pendientes.
5. Crear un módulo de reportes detallados en formatos PDF y Excel.
6. Capacitar al personal técnico y administrativo en el uso de la nueva herramienta para garantizar su adopción efectiva.

INTRODUCCIÓN

El Instituto Nacional de Ciencias Forenses de Guatemala (Inacif) cumple un rol esencial en el apoyo técnico-científico al sistema judicial del país. Sus laboratorios de criminalística dependen de equipos especializados que requieren un mantenimiento constante para garantizar la precisión de los análisis forenses. Sin embargo, los procesos actuales de gestión se realizan de manera semiautomatizada con hojas de cálculo, lo que limita la trazabilidad, eficiencia y control centralizado.

En este contexto, se plantea el desarrollo de un sistema de software para la gestión de mantenimientos preventivos, correctivos y calibraciones, el cual permitirá centralizar la información de los equipos y sus mantenimientos, programar tareas y generar alertas automáticas, optimizar la trazabilidad mediante bitácoras y reportes y cumplir con normativas internacionales como la ISO/IEC 17025.

La herramienta se desarrollará utilizando metodología ágil *Scrum*, permitiendo entregar resultados parciales y adaptarse a los cambios en los requerimientos. La solución contará con un *backend* en Java (*TomEE*, *EclipseLink*, *Deltaspike*), *frontend* en Angular y un sistema de seguridad basado en *Keycloak*.

De esta forma, el proyecto busca no solo mejorar la eficiencia operativa del Inacif, sino también garantizar que los resultados forenses mantengan la confiabilidad y calidad técnica que exige el sistema de justicia en Guatemala.

1. FASE DE INVESTIGACIÓN

1.1. Antecedentes de la empresa

En el primer apartado de este primer capítulo de la investigación se presenta todo lo concerniente a los antecedentes de la empresa en estudio, comenzando por una reseña de su historia.

1.1.1. Reseña histórica

El Instituto Nacional de Ciencias Forenses de Guatemala (Inacif) fue creado mediante el Decreto 32-2006 del Congreso de la República, entrando en funcionamiento en el año 2007. Su establecimiento respondió a la necesidad de contar con una entidad autónoma e independiente, capaz de unificar los servicios de criminalística y medicina forense que previamente se encontraban dispersos en diferentes instituciones del Estado.

Antes de la creación de Inacif, los servicios forenses eran prestados principalmente por el Ministerio Público y, en menor medida, por el Ministerio de Salud Pública. Esta situación generaba problemas de imparcialidad, falta de especialización y limitaciones técnicas en la investigación criminal. Con la fundación del Instituto, Guatemala dio un paso importante hacia la profesionalización de la investigación científico-forense, alineándose a estándares internacionales de justicia y derechos humanos.

Desde su creación, Inacif ha tenido como finalidad principal apoyar a la administración de justicia mediante dictámenes periciales con rigor técnico y científico. La independencia funcional y presupuestaria ha permitido a la institución modernizar progresivamente sus laboratorios, incorporar nuevas áreas de especialización y fortalecer la formación de sus peritos.

A lo largo de su trayectoria se han alcanzado logros importantes, entre los cuales destacan la acreditación de laboratorios bajo la norma internacional ISO/IEC 17025, que garantiza la calidad de los procesos científicos realizados, así como la implementación de proyectos de modernización tecnológica que fortalecen la eficiencia y la transparencia institucional. En el marco del plan de trabajo 2022-2027, la institución ha priorizado iniciativas de gobierno electrónico, orientadas a la eficiencia administrativa, la participación ciudadana y la transparencia.

1.1.2. Misión

La misión se expresa así: “Ser la institución responsable de brindar servicios de investigación científica forense fundamentada en la ciencia y el arte, emitiendo dictámenes periciales útiles al sistema de justicia, mediante estudios medicolegales y análisis técnico-científicos, apegados a la objetividad y transparencia” (Inacif, 2025, párr. 1).

1.1.3. Visión

La visión se expresa con las siguientes palabras: “Ser una institución referente a nivel nacional e internacional por su recurso humano competente, capacidad tecnológica, buenas prácticas forenses, calidad y transparencia en la gestión institucional y respeto a la dignidad humana” (Inacif, 2025, párr. 2).

1.1.4. Servicios que realiza

El Inacif presta servicios técnico-científicos en apoyo al sistema de justicia, entre los cuales destacan:

- Criminalística y análisis de evidencias físicas.
- Medicina forense y estudios medicolegales.
- Laboratorios especializados en toxicología, genética, balística, documentoscopia, entre otros.
- Dictámenes periciales que sustentan procesos judiciales.
- Apoyo técnico en la investigación de delitos a través de análisis especializados.

Estos servicios buscan garantizar que las decisiones judiciales se sustenten en pruebas objetivas, confiables y validadas bajo normas internacionales, como la ISO/IEC 17025.

1.2. Descripción de las necesidades

Actualmente, el Inacif enfrenta importantes desafíos en la gestión de sus equipos e infraestructura tecnológica:

- Procesos manuales y dispersos: la programación y registro de mantenimientos se lleva a cabo mediante hojas de cálculo, lo que genera duplicidad de datos y riesgo de pérdida de información.
- Falta de un sistema centralizado que permita coordinar y supervisar los mantenimientos preventivos y correctivos de manera uniforme en todas las dependencias.

- Limitaciones en el cumplimiento normativo: los laboratorios deben cumplir con la ISO/IEC 17025, que exige trazabilidad y documentación detallada de los mantenimientos, aspecto que actualmente no se garantiza al 100 %.
- Ausencia de alertas automatizadas para notificar sobre mantenimientos pendientes, lo que provoca retrasos y afecta la disponibilidad de equipos.
- Deficiente control de inventarios, al no existir un sistema que unifique el registro de equipos, sus estados y su historial de uso.

Estas necesidades repercuten directamente en la confiabilidad de los resultados forenses y, por lo tanto, en la credibilidad de la institución frente al sistema de justicia.

1.3. Priorización de las necesidades

Con base en el análisis realizado, las necesidades del Inacif se priorizan de la siguiente forma:

- Implementación de un sistema de gestión de mantenimientos preventivos y correctivos de equipos, que permita centralizar, automatizar y garantizar la trazabilidad de las tareas.
- Cumplimiento de la norma ISO/IEC 17025, asegurando que todos los mantenimientos queden documentados con evidencia verificable.
- Generación de reportes unificados que faciliten auditorías internas y externas, con información detallada sobre mantenimientos realizados, pendientes y estado de equipos.
- Gestión de inventarios y activos, integrando información sobre ubicación, estado y vida útil de los equipos.

- Control de accesos y roles (mediante herramientas como *Keycloak*), para garantizar la seguridad de la información y definir responsabilidades entre técnicos, administradores y proveedores.
- Notificaciones y alertas automáticas, que permitan prevenir retrasos en la ejecución de mantenimientos críticos.
- Escalabilidad del sistema, de manera que soporte la inclusión futura de más equipos, usuarios y funcionalidades.

Esta priorización permitirá atender de forma progresiva los problemas más críticos, asegurando que el Inacif fortalezca la confiabilidad de sus servicios forenses y optimice el uso de sus recursos.

2. FASE TÉCNICO-PROFESIONAL

2.1. Descripción del proyecto

El proyecto plantea el desarrollo e implementación de un sistema de software web orientado a la gestión integral de mantenimientos preventivos, correctivos y procesos de calibración de los equipos utilizados en los laboratorios y áreas de apoyo del Instituto Nacional de Ciencias Forenses de Guatemala (Inacif). La finalidad es fortalecer la trazabilidad, la planificación centralizada y la confiabilidad operativa de dichos procesos, garantizando el cumplimiento de normativas internacionales como la ISO/IEC 17025, indispensable para la validez de los análisis y peritajes realizados en los laboratorios de criminalística.

Actualmente, la administración de mantenimientos se lleva a cabo mediante hojas de cálculo y registros manuales, lo que genera duplicidad de información, riesgos de pérdida de datos y dificultad para consolidar indicadores de gestión. Esta situación limita la capacidad de respuesta institucional, afecta la vida útil de los equipos y compromete la transparencia en la administración de recursos. Ante este contexto, se vuelve prioritario modernizar el control de mantenimientos con una solución digital robusta, escalable y segura.

La solución propuesta contempla un *backend* desarrollado en Java bajo Jakarta EE/TomEE, estructurado con una arquitectura modular que permita, en etapas posteriores, evolucionar hacia microservicios. En el *frontend* se diseñará una interfaz construida en Angular, destinada a la interacción con proveedores de servicio, técnicos externos y personal del Inacif. La autenticación y

autorización estarán centralizadas en *Keycloak*, gestionando accesos de acuerdo con los distintos roles definidos (administradores, técnicos, proveedores y usuarios de consulta), con soporte para integración futura a *Single Sign-On* institucional.

En cuanto a persistencia, se hará uso de *SQL Server* o *PostgreSQL*, según disponibilidad del centro de datos institucional, con un modelo de datos que incluye catálogos de áreas, equipos, proveedores, contratos, programaciones automáticas, ejecuciones de mantenimiento, tickets de falla y bitácoras digitales de respaldo. Este diseño asegura integridad, consistencia y escalabilidad de la información, además de soportar auditorías internas y externas. Complementariamente, el sistema contará con vistas especializadas, procedimientos almacenados y disparadores que automatizan procesos como alertas, notificaciones y cálculos de próximos mantenimientos.

Las principales funcionalidades incluyen el registro y clasificación de equipos, la gestión centralizada de mantenimientos programados y correctivos, la apertura y seguimiento de tickets de fallas, el envío de notificaciones automáticas, la generación de reportes en distintos formatos (PDF/XLS) y la integración de evidencias digitales que refuercen la validez de cada procedimiento realizado. A futuro, el sistema se proyecta para soportar la firma electrónica avanzada de reportes de mantenimiento, elevando así los estándares de validez documental y confiabilidad técnica.

El proyecto será ejecutado bajo la metodología ágil Scrum, organizando el trabajo en *sprints* de dos semanas a lo largo de un período estimado de 6 meses. Este enfoque permite entregar de forma iterativa incrementos funcionales, involucrando a usuarios clave en el proceso de validación y asegurando que la solución final responda a las necesidades reales del Inacif.

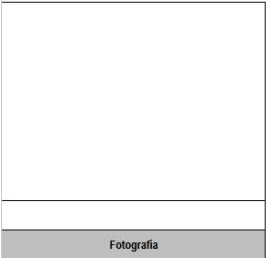
En síntesis, el desarrollo de este sistema no solo representará una modernización tecnológica, sino también un avance estratégico hacia la eficiencia institucional, la estandarización de procesos y la mejora continua en la gestión de activos críticos para la labor pericial del país.

2.2. Investigación preliminar para la solución del proyecto

Durante la etapa inicial del proyecto se llevó a cabo un análisis exhaustivo del estado actual de los procesos de mantenimiento en el Inacif, tomando en cuenta tanto la perspectiva técnica de los laboratorios como la administrativa y de soporte. El diagnóstico evidenció que los controles vigentes dependen en gran medida de hojas de cálculo dispersas y registros manuales, lo cual provoca problemas de duplicidad de datos, dificultades para consolidar información y pérdida de trazabilidad histórica. Esta dispersión de registros afecta directamente la capacidad de generar indicadores confiables, limita la transparencia en la administración y entorpece la toma de decisiones estratégicas.

Figura 1.
Control de equipos antiguo

	Formulario	Código: FOR-DG-GAC-029		FICHA
	FICHA DE IDENTIFICACIÓN DE EQUIPO	Versión: 03		
		Vigente a partir de: 5/27/2019		
		Página 1 de 2		

	Nombre del equipo		Fecha	Mantenimiento		No. de Orden de Servicio
	Código del INACIF			Preventivo	Correctivo	
	Marca					
	Modelo					
	No. de serie					
	Ubicación					
	Magnitud de medición					
	Rango o capacidad					
	Código y nombre del manual del fabricante					
	Software/Firmware					
	Condiciones de operación					

Nota. Captura de pantalla del archivo Excel para el control de equipos que se usaba previo al sistema desarrollado. Obtenido de Inacif (2025). *Información de la institución.* (p. 5) Inacif.

Se identificó también que los mantenimientos preventivos se programan de manera reactiva, es decir, únicamente cuando se presentan fallos o se detectan problemas inmediatos. Esto ha ocasionado que los equipos críticos de laboratorio estén expuestos a interrupciones que afectan la continuidad del trabajo pericial.

La falta de una calendarización estructurada de mantenimientos genera riesgos operativos y aumenta los costos a largo plazo. En la parte administrativa, se constató que existe una dificultad recurrente para dar seguimiento a contratos con proveedores, registrar adecuadamente los servicios realizados y documentar las órdenes de compra, lo que produce vacíos de información y riesgos de incumplimiento en auditorías internas y externas.

Otro hallazgo importante fue la debilidad en el cumplimiento de la norma ISO/IEC 17025, que exige trazabilidad, evidencia documental y confiabilidad en la gestión de equipos. Actualmente, la documentación de los mantenimientos carece de bitácoras digitales y respaldo electrónico de evidencias, lo que compromete el cumplimiento de dicha norma y puede afectar la acreditación de los laboratorios.

Figura 2.
Control de mantenimientos antiguo

A		B		C		D		E F G H I J K L M N O P Q R S T U V W X Y Z AA AB AC AD AE AF AG AH AI AJ AK AL AM AN AO AP AQ AR AS AT AU AV AW AX AY AZ BA BB BC BD BE BF BG BH BI BJ BK BL BM BN BO BP BQ BR BS BT BU BV BW BX BY BZ CA CB CC CD CE CF CG CH CI CJ CK CL CM CN CO CP CQ CR CS CT CU CV CW CX CY CZ DA DB DC DD DE DF DG DH DI DJ DK DL DM DN DO DP DQ DR DS DT DU DV DW DX DY DZ EA EB EC ED EE EF EG EH EI EJ EK EL EM EN EO EP EQ ER ES ET EU EV EW EX EY EZ FA FB FC FD FE FF FG FH FI FJ FK FL FM FN FO FP FQ FR FS FT FU FV FW FX FY FZ GA GB GC GD GE GF GG GH GI GJ GK GL GM GN GO GP GQ GR GS GT GU GV GW GX GY GZ HA HB HC HD HE HF HG HH HI HJ HK HL HM HN HO HP HQ HR HS HT HU HV HW HX HY HZ IA IB IC ID IE IF IG IH II IJ IK IL IM IN IO IP IQ IR IS IT IU IV IW IX IY IZ JA JB JC JD JE JF JG JH JI JJ JK JL JM JN JO JP JQ JR JS JT JU JV JW JX JY JZ KA KB KC KD KE KF KG KH KI KJ KK KL KM KN KO KP KQ KR KS KT KU KV KW KX KY KZ LA LB LC LD LE LF LG LH LI LJ LK LL LM LN LO LP LQ LR LS LT LU LV LW LX LY LZ MA MB MC MD ME MF MG MH MI MJ MK ML MN MO MP MQ MR MS MT MU MV MW MX MY MZ NA NB NC ND NE NF NG NH NI NJ NK NL NM NO NP NQ NR NS NT NU NV NW NX NY NZ OA OB OC OD OE OF OG OH OI OJ OK OL OM ON OO OP OQ OR OS OT OU OV OW OX OY OZ PA PB PC PD PE PF PG PH PI PJ PK PL PM PN PO PP PQ PR PS PT PU PV PW PX PY PZ QA QB QC QD QE QF QG QH QI QJ QK QL QM QN QO QP QQ QR QS QT QU QV QW QX QY QZ RA RB RC RD RE RF RG RH RI RJ RK RL RM RN RO RP RQ RR RS RT RU RV RW RX RY RZ SA SB SC SD SE SF SG SH SI SJ SK SL SM SN SO SP SQ SR SS ST SU SV SW SX SY SZ TA TB TC TD TE TF TG TH TI TJ TK TL TM TN TO TP TQ TR TS TT TU TV TW TX TY TZ UA UB UC UD UE UF UG UH UI UJ UK UL UM UN UO UP UQ UR US UT UU UV UW UX UY UZ VA VB VC VD VE VF VG VH VI VJ VK VL VM VN VO VP VQ VR VS VT VU VW VX VY VZ WA WB WC WD WE WF WG WH WI WJ WK WL WM WN WO WP WQ WR WS WT WU WV WW WX WY WZ XA XB XC XD XE XF XG XH XI XJ XK XL XM XN XO XP XQ XR XS XT XU XV XW XX XY XZ YA YB YC YD YE YF YG YH YI YJ YK YL YM YN YO YP YQ YR YS YT YU YV YW YX YY YZ ZA ZB ZC ZD ZE ZF ZG ZH ZI ZJ ZK ZL ZM ZN ZO ZP ZQ ZR ZS ZT ZU ZV ZW ZX ZY ZZ												Formulario		Código: FOR-DG-GAC-030 Versión: 02 Vigente a partir de: 4/2/24 Página de:	
AREA		Laboratorios de Criminalística																					
AÑO		2022																					
DESCRIPCION DEL EQUIPO	NÚMERO DE INVENTARIO	UBICACION	FRECUENCIA	ENE M C	FEB J C	MAR F C	ABR M C	MAY M C	JUN M C	JUL M C	AGO M C	SEP M C	OCT M C	NOV M C	DIC M C	OBSERVACIONES							
Cromatográfo de Gaseos 5950 equipado a sustrato de gases tipo headspace 7694 de columna y control eléctrico y mantenimiento sus ALI con doble columna y detectores FID y NPD y equipo de control eléctrico. (ITEM A)	0034214/0034220	Toxicología	Semestral			X		21/06					X										
Cromatográfo de Gaseos 7694 equipado a sustrato de gases tipo headspace 7694 de columna y control eléctrico y mantenimiento sus ALI con doble columna y detectores FID y NPD y equipo de control eléctrico. (ITEM B)	0027363C	Toxicología	Trimestral		X					X					X	ALCANCE OSA Mantenimiento Correctivo solicitado 09/03/22, mantenimiento preventivo de mayo no se realizó por no operatividad del equipo, se le requiere de realizar SIC.							
Cromatográfo de Gaseos 7694 con mantenimiento sus ALI con doble columna y detectores FID y NPD y equipo de control eléctrico. (ITEM C)	00273717	Toxicología	Anual	X						X			X			ALCANCE OSA							
MP/1																							
III CROMATOGRAFOS Y UV - I MEB - UPLC GTOF - AGITADORES - CALENTADOR AGITADOR MAGNETICO - A. DE INMUNISAGADO POR BIOCHIPs - A. GENÉTICOS - AUTOLINEAR - BARÓSCOP -																							

Nota. Captura de pantalla del control que se llevaba en archivos de Excel para la planificación y ejecución de mantenimientos. Obtenido de Inacif (2025). *Información de la institución.* (p. 8) Inacif.

Frente a este panorama, se definieron los principales objetivos que debía cumplir la nueva solución:

- Centralizar la información de equipos, mantenimientos, proveedores, contratos y tickets en una única plataforma digital.
- Garantizar la trazabilidad de los procesos mediante bitácoras digitales y evidencias documentales asociadas.

- Generar alertas y notificaciones automáticas para asegurar la ejecución oportuna de los mantenimientos preventivos.
- Facilitar el cumplimiento de auditorías y acreditaciones mediante reportes confiables y verificables que consoliden la información histórica.

La investigación incluyó también un análisis comparativo de sistemas CMMS comerciales (*Computerized Maintenance Management Systems*). Aunque algunos de estos ofrecen módulos robustos para la gestión de equipos y mantenimiento, la mayoría no se adapta al entorno normativo guatemalteco, carecen de integración con el marco institucional del Inacif y requieren costos de licenciamiento y soporte que los hacen poco sostenibles en el tiempo. Por esta razón se concluyó que un desarrollo a medida es la alternativa más viable, pues permitirá diseñar un sistema ajustado a los requerimientos legales, técnicos y de seguridad propios de la institución.

En el aspecto técnico, el Inacif puso a disposición recursos clave que facilitarán la implementación del sistema. Entre ellos se encuentra un servidor de base de datos institucional configurado en el centro de datos, el cual servirá como repositorio central para los equipos y mantenimientos. Se habilitó además un ambiente de desarrollo controlado al que se accede mediante una VPN institucional, garantizando la seguridad en la conexión y el resguardo de los datos.

Para la fase de desarrollo se definió el uso de *Visual Studio Code* como entorno de trabajo, con soporte a contenedores mediante *Docker* para la creación de ambientes replicables y aislados, y *Maven* como herramienta de gestión de dependencias y automatización del ciclo de construcción del software.

Estos recursos no solo aseguran la viabilidad técnica del proyecto, sino que permiten que el sistema se desarrolle en un entorno alineado a las políticas de seguridad informática del Inacif, garantizando desde su origen compatibilidad con la infraestructura institucional y sostenibilidad en el tiempo.

2.2.1. Análisis FODA

El análisis FODA permitió identificar los factores internos y externos que influyen en el desarrollo del sistema de gestión de mantenimientos:

- Fortalezas: experiencia técnica del equipo desarrollador en Java, Angular y *Keycloak*; uso de tecnologías libres que reducen costos; apoyo institucional del Inacif para el acceso a infraestructura de datos.
- Oportunidades: cumplimiento de normativas internacionales (ISO/IEC 17025); modernización tecnológica alineada al plan de gobierno electrónico; posibilidad de replicar la solución en otras instituciones públicas.
- Debilidades: recursos humanos limitados para pruebas y soporte; dependencia de conectividad VPN para el acceso seguro; curva de aprendizaje inicial de los usuarios finales.
- Amenazas: cambios en políticas institucionales o presupuestarias; posibles resistencias al cambio por parte del personal operativo; riesgos de ciberseguridad si no se mantienen prácticas de actualización y respaldo.

2.2.2. Supuestos del proyecto

Para la correcta planificación y ejecución del sistema de gestión de mantenimientos se establecieron los siguientes supuestos, los cuales representan condiciones que se consideran válidas durante todo el ciclo de vida del proyecto:

- Recursos técnicos y humanos

Se contará con servidores y entornos adecuados en el centro de datos institucional, así como con las herramientas de desarrollo necesarias (*Angular, TomEE, Deltaspikes, EclipseLink, Maven*). El equipo de desarrollo dispondrá de personal capacitado en dichas tecnologías para asegurar un uso eficiente y confiable.

- Información y requerimientos de los *stakeholders*

Los usuarios finales y responsables institucionales proporcionarán información clara y completa sobre formularios, flujos de trabajo y requisitos funcionales, garantizando que el sistema se diseñe acorde a las necesidades reales de la institución.

- Estabilidad y actualización de tecnologías

Las tecnologías seleccionadas (*Angular, TomEE, Deltaspikes, EclipseLink, Maven*) mantendrán soporte y estabilidad durante el desarrollo y operación del sistema, reduciendo el riesgo de incompatibilidades o necesidad de migraciones tempranas.

- Disponibilidad y compromiso de usuarios finales

Los usuarios clave estarán disponibles para participar en las pruebas de aceptación y brindarán retroalimentación oportuna, lo que permitirá realizar ajustes antes del despliegue en producción.

- Suficiencia del presupuesto

El presupuesto asignado cubrirá los costos de desarrollo, pruebas, despliegue y capacitación sin requerir incrementos significativos, asegurando la sostenibilidad del proyecto hasta su entrega final.

- Infraestructura y soporte operativo

La infraestructura de TI y el personal de soporte del Inacif estarán disponibles para el despliegue, mantenimiento y respaldo del sistema, asegurando su continuidad operativa y atención a incidentes.

- Cumplimiento de normativas y políticas

El proyecto respetará las políticas internas del Inacif, así como las regulaciones legales aplicables (por ejemplo, normas de seguridad de la información e ISO/IEC 17025), evitando conflictos legales o institucionales.

- Aceptación y adaptación a cambios

El personal del Inacif mostrará disposición a adoptar nuevas formas de trabajo y flujos digitales que introduce el sistema, facilitando la transición desde registros manuales hacia la nueva plataforma.

2.2.3. Riesgos del proyecto

Todo proyecto de software está expuesto a factores que pueden afectar su éxito. Estos riesgos pueden ser técnicos (derivados de la tecnología y la integración), organizacionales (relacionados con la participación de usuarios y gestión institucional) u operativos (ligados a la seguridad y disponibilidad del sistema).

Identificar los riesgos desde etapas tempranas permite anticipar problemas y definir medidas de mitigación, evitando retrasos o fallas en la implementación. La siguiente tabla resume los principales riesgos detectados para este proyecto:

Tabla 1.*Riesgos del proyecto*

Categoría	Riesgo identificado	Impacto	Probabilidad	Estrategia de mitigación
Técnicos	Incompatibilidad entre versiones de librerías y dependencias.	Alto	Media	Uso de integración continua (CI) y pruebas automatizadas.
Técnicos	Fallas en la integración con Keycloak.	Alto	Media	Pruebas tempranas en ambientes de preproducción y soporte de la comunidad Keycloak.
Técnicos	Limitaciones de hardware en el despliegue.	Medio	Baja	Validación previa de recursos en el Centro de Datos y escalabilidad con Docker.
Organizacionales	Rotación de personal clave durante el desarrollo.	Alto	Media	Documentación detallada y repositorios actualizados.
Organizacionales	Baja participación de usuarios en pruebas y validaciones.	Alto	Alta	Talleres de sensibilización y cronogramas de validación obligatorios.
Organizacionales	Cambios administrativos que modifiquen el alcance del proyecto.	Medio	Media	Reuniones de alineación y acuerdos formales con dirección institucional.
Operativos	Pérdida de datos por fallas en respaldos.	Alto	Media	Configuración de backups automáticos diarios y semanales.
Operativos	Ataques cibernéticos o accesos no autorizados.	Alto	Media	Implementación de VPN, TLS, autenticación con Keycloak y auditorías periódicas.
Operativos	Indisponibilidad del sistema por caídas de red o servidores.	Medio	Media	Monitoreo constante de red/servidores y plan de recuperación ante desastres (DRP).

Nota. Detalle de los posibles riesgos dentro del ciclo de desarrollo del proyecto. Elaboración propia, realizado con Microsoft Excel.

2.2.4. Plan de comunicación

La comunicación es un pilar clave en la gestión de proyectos, ya que asegura que todos los involucrados estén informados y coordinados. Un plan de comunicación define qué información se comparte, quién la transmite, con qué frecuencia y por qué medio.

En este proyecto se planteó un esquema sencillo, basado en reuniones periódicas, reportes y capacitaciones, con el fin de mantener alineados al equipo de desarrollo, la dirección institucional y los usuarios finales. La siguiente tabla presenta el plan de comunicación definido:

Tabla 2.

Plan de comunicación

Actividad	Distribución (Emisor/Receptor)	Frecuencia	Método
Reunión de seguimiento Scrum	Scrum Master ↔ Equipo de desarrollo	Semanal	Videoconferencia / Presencial
Informe de avance del proyecto	Product Owner ↔ Dirección INACIF	Quincenal	Informe escrito (PDF/Word)
Revisión de sprint e incrementos	Equipo de desarrollo ↔ Usuarios clave	Al final de cada sprint	Demostración en vivo / Documento resumen
Comunicación de incidencias técnicas	Equipo de desarrollo ↔ Unidad de Informática	Según necesidad	Correo institucional / Gestor de tickets
Entrega de manuales y documentación	Equipo de desarrollo ↔ Personal operativo	Al finalizar proyecto	Documentos PDF en intranet institucional
Talleres de capacitación	Equipo de desarrollo ↔ Usuarios finales	Una vez (post-despliegue)	Sesiones prácticas presenciales/virtuales

Nota. Detalle del plan de comunicación que se llevará a cabo a lo largo del proyecto. Elaboración propia, realizado con Microsoft Excel.

2.3. Presentación de la solución del proyecto

En el tercer apartado de este segundo capítulo del trabajo de investigación se aborda la presentación de la solución propuesta para el proyecto.

2.3.1. Introducción al diseño de la solución

La solución propuesta responde a la necesidad institucional de modernizar y sistematizar los procesos de mantenimiento del Inacif. Para lograrlo, se planteó el desarrollo de un sistema web integral basado en una arquitectura de tres capas (presentación, negocio y datos), garantizando escalabilidad, mantenibilidad y seguridad. El diseño se sustenta en la aplicación de buenas prácticas de ingeniería de software, uso de metodologías ágiles, modelado formal de requerimientos y tecnologías de vanguardia que aseguran la sostenibilidad del proyecto a largo plazo (Pressman y Maxim, 2020).

2.3.2. Metodología de desarrollo de software (*Scrum*)

La metodología seleccionada es *Scrum*, dado que permite organizar el trabajo en iteraciones cortas, entregar valor de manera temprana y adaptarse a cambios en los requerimientos.

El proyecto se desarrollará en *sprints* de dos semanas, durante un período de 6 meses, lo que permitirá entregar módulos funcionales gradualmente y recibir retroalimentación inmediata de los usuarios clave.

2.3.3. Definición y análisis de requerimientos

La etapa de definición de requerimientos constituyó uno de los pilares fundamentales en el desarrollo del sistema, ya que permitió establecer de manera clara y verificable las funcionalidades que debía cubrir, así como las características de calidad necesarias para garantizar su desempeño en el contexto institucional del Inacif. El levantamiento se realizó a través de entrevistas con personal técnico y administrativo, revisión de procesos actuales y análisis de normativas aplicables, particularmente la ISO/IEC 17025.

2.3.3.1. Requerimientos funcionales

Los requerimientos funcionales definen los servicios que el sistema proporciona al usuario y las interacciones esperadas. Estos se tradujeron en los módulos principales implementados:

- Registro y clasificación de equipos

Permite almacenar y organizar la información técnica de cada equipo, incluyendo características, ubicación y estado actual. Se implementaron categorías que facilitan la búsqueda y la trazabilidad histórica.

- Programación de mantenimientos preventivos con alertas

El sistema ofrece la posibilidad de planificar mantenimientos periódicos de forma calendarizada. Se configuraron notificaciones automáticas por correo institucional y dentro del sistema, para recordar fechas próximas de servicio.

- Registro y ejecución de mantenimientos correctivos

Brinda la opción de documentar fallas o averías, registrar la intervención técnica realizada y actualizar el estado del equipo una vez solucionado el problema.

- Creación y gestión de tickets de falla

Los usuarios pueden generar tickets que son asignados a técnicos o proveedores. El ticket mantiene un flujo de estados (abierto, en proceso, resuelto, cerrado) que garantiza trazabilidad.

- Control de contratos y proveedores

Permite administrar información de contratos de servicio, registrar su vigencia, costos y cumplimiento, así como asociarlos a proveedores responsables de los mantenimientos.

- Generación de reportes en PDF/XLS

El sistema facilita la emisión de reportes configurables sobre mantenimientos ejecutados, equipos intervenidos y estadísticas, exportables en formatos estándar para auditorías.

- Almacenamiento de evidencias digitales

Se habilitó un repositorio para guardar documentos, fotografías y certificados de calibración asociados a cada mantenimiento, garantizando respaldo digital ante auditorías internas o externas.

2.3.3.2. Requerimientos no funcionales

Los requerimientos no funcionales establecen las condiciones de calidad, seguridad y eficiencia que debía cumplir el sistema, asegurando su confiabilidad en un entorno crítico como el del Inacif:

- Seguridad: el acceso al sistema se implementó mediante autenticación y autorización con *Keycloak*, garantizando que cada usuario solo pudiera acceder a las funcionalidades asignadas a su rol. Toda la comunicación entre cliente y servidor se cifró mediante TLS 1.2+ (Red Hat, 2023).
- Rendimiento: se optimizó el tiempo de respuesta, de manera que las operaciones CRUD (crear, leer, actualizar, eliminar) se completaran en un tiempo esperado promedio, incluso bajo carga moderada.
- Disponibilidad: el sistema se ejecuta sobre la infraestructura institucional del INACIF, accesible únicamente mediante VPN, lo que garantiza continuidad de servicio y control de acceso restringido.
- Usabilidad: las interfaces se desarrollaron con diseño responsivo, accesibles desde navegadores modernos, con menús intuitivos y formularios claros, reduciendo la curva de aprendizaje del usuario final.
- Escalabilidad: gracias al uso de contenedores *Docker*, el sistema puede desplegarse en diferentes ambientes (desarrollo, pruebas, producción) y ampliarse con nuevos módulos sin afectar la operación existente.

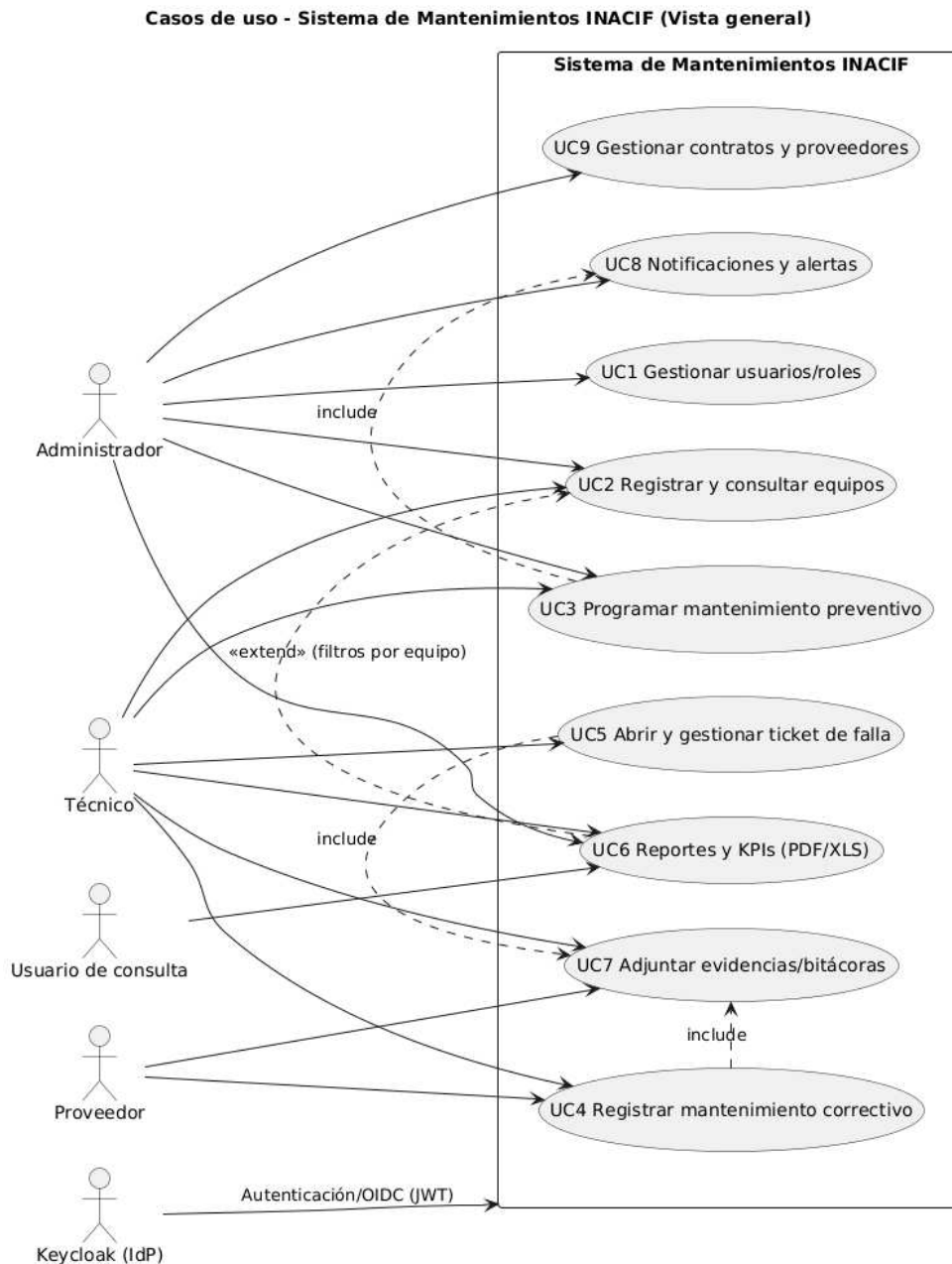
2.3.4. Modelado UML

El modelado UML formaliza la solución implementada y sirve como puente entre requerimientos, diseño e implementación. A continuación, se presentan los diagramas que describen el alcance funcional (casos de uso), la estructura estática (clases), la dinámica de procesos (secuencias) y la arquitectura física (despliegue). Estos modelos se construyeron a partir de los requerimientos validados con usuarios y del esquema de datos definido.

2.3.4.1. Diagramas de casos de uso

Los casos de uso describen las interacciones entre administrador, técnico, proveedor, usuario de consulta y el *IdP Keycloak*, con los servicios principales del sistema: gestión de equipos, mantenimientos (preventivo/correctivo), tickets, contratos/proveedores, evidencias y reportes.

Figura 3.
Casos de uso (vista general)



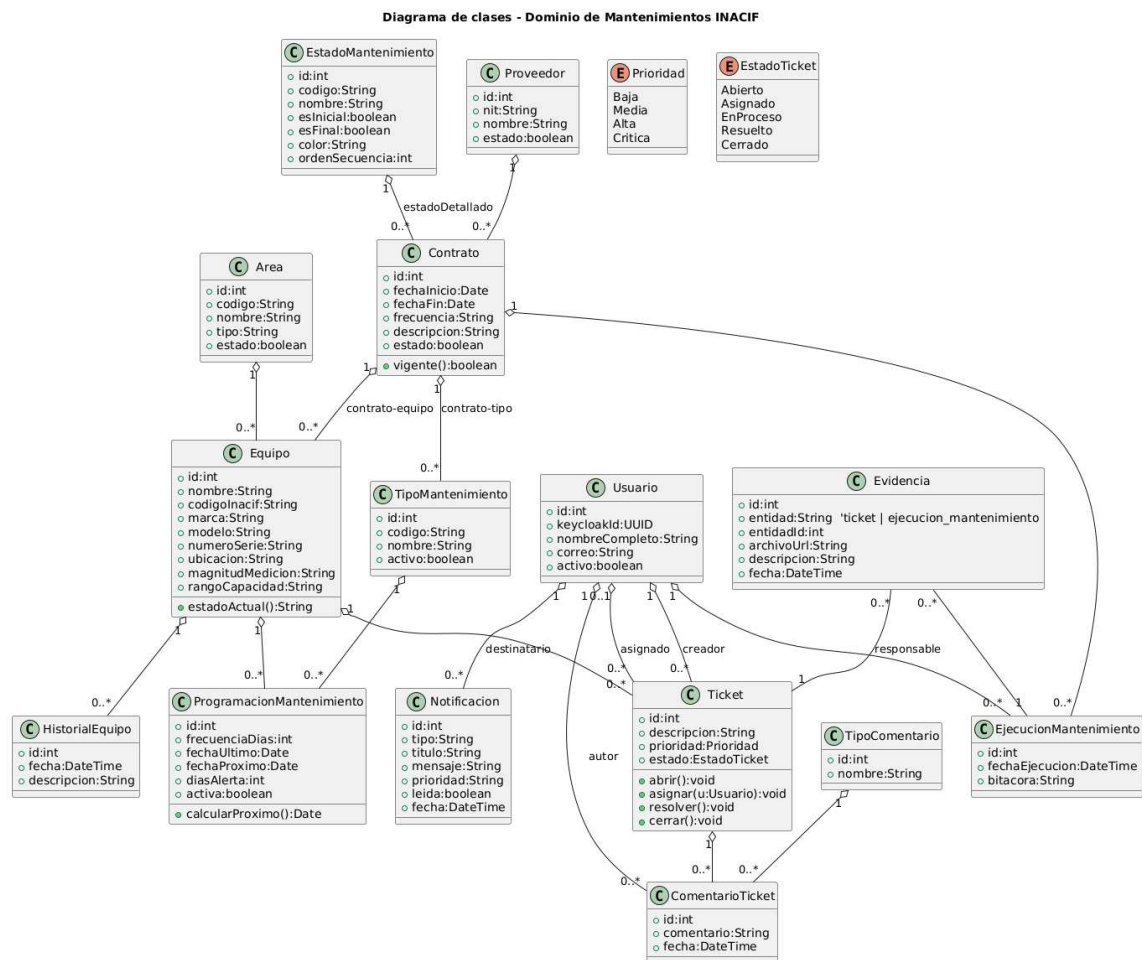
Nota. Diagrama de casos de uso, vista general. Elaboración propia, realizado con PlantUML.

2.3.4.2. Diagrama de clases

El diagrama de clases representa la estructura lógica principal. Se modelan entidades del dominio (equipo, programación, ejecución, ticket, contrato, proveedor, estado de mantenimiento, evidencia, notificación, usuario) y sus asociaciones, multiplicidades y operaciones clave.

Figura 4.

Diagrama de clases



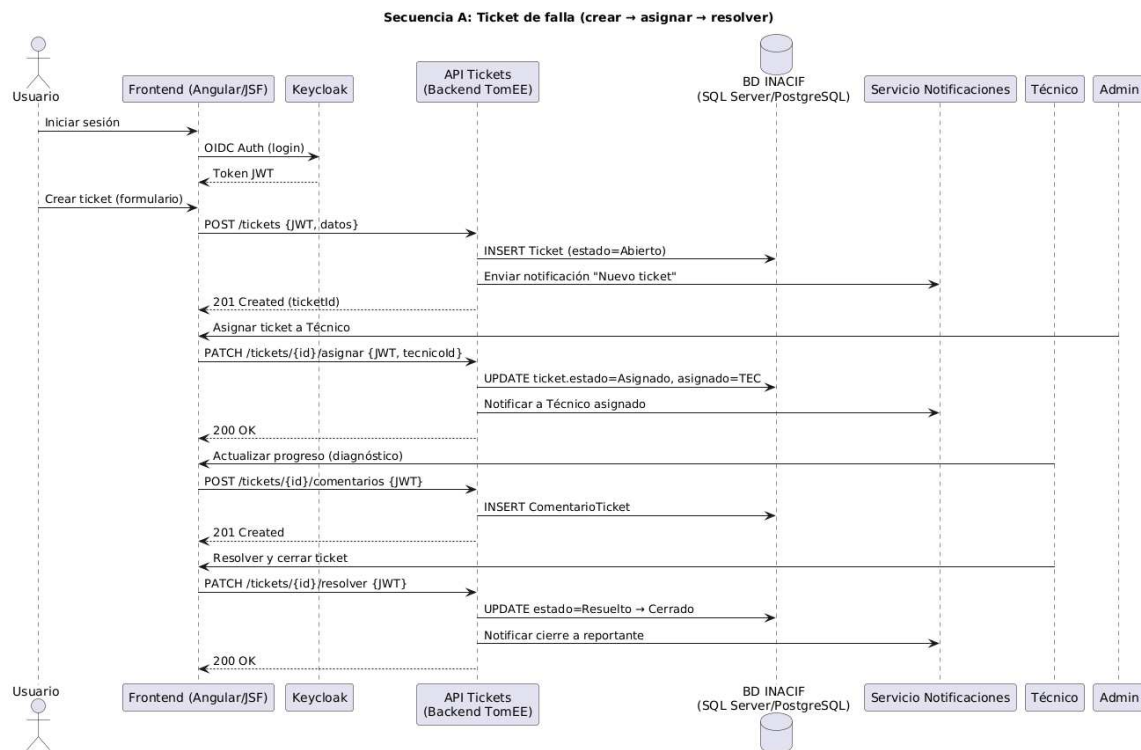
Nota. Diagrama de clases. Elaboración propia, realizado con PlantUML.

2.3.4.3. Diagramas de secuencia

Se incluyen dos secuencias representativas: (A) reporte y gestión de un ticket; (B) ciclo de mantenimiento preventivo con alerta y ejecución. Reflejan autenticación por *Keycloak*, servicios REST del *backend* y persistencia.

Figura 5.

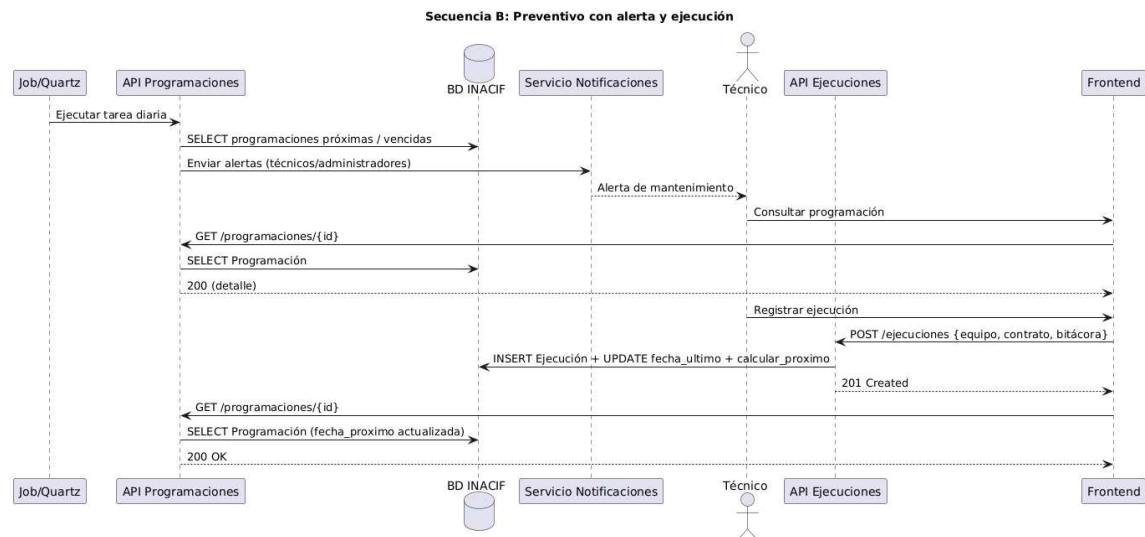
Diagrama de secuencia A



Nota. Diagrama de secuencia A. Elaboración propia, realizado con PlantUML.

Figura 6.

Diagrama de secuencia B

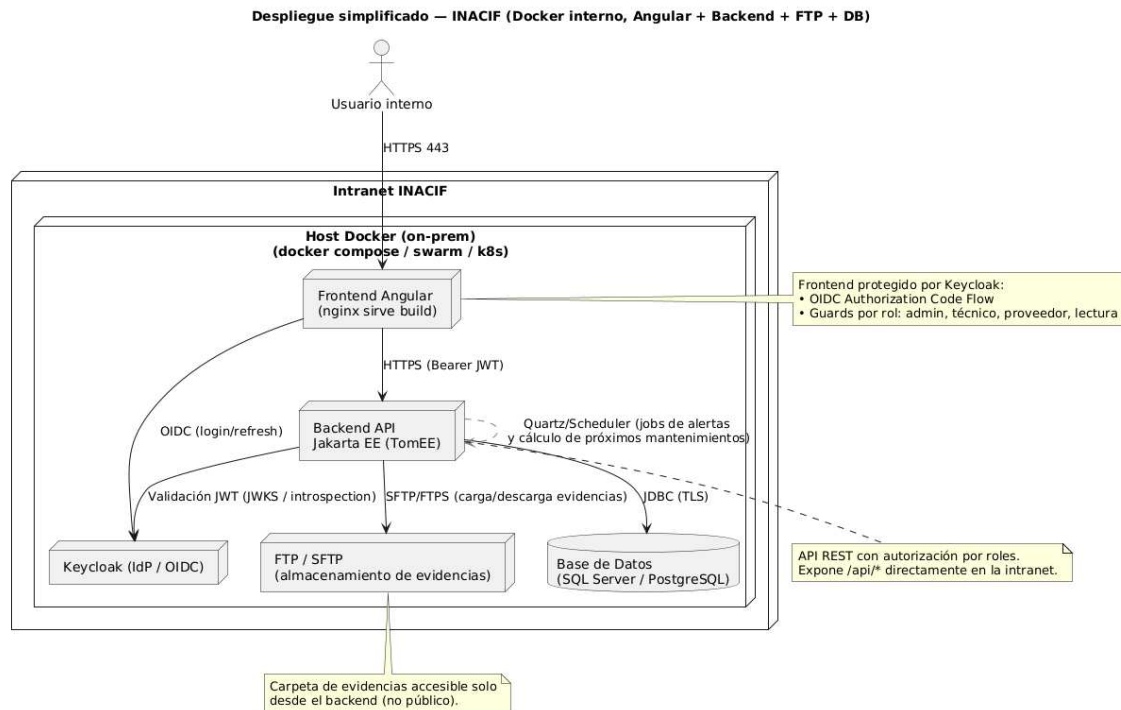


Nota. Diagrama de secuencia B. Elaboración propia, realizado con PlantUML.

2.3.4.4. Diagrama de despliegue

El despliegue muestra la distribución de componentes en la infraestructura del INACIF: *frontends* (Angular), *backend* Jakarta EE en *TomEE*, *Keycloak* como IdP, base de datos institucional, y redes (VPN). Se reflejan contenedores *Docker* para dev/prod y servicios expuestos por HTTPS.

Figura 7.
Diagrama de despliegue



Nota. Diagrama de despliegue. Elaboración propia, realizado con PlantUML.

2.3.5. Diseño de base de datos

En el siguiente apartado se presenta todo lo relacionado con el diseño de la base de datos, comenzando con lo atinente con el modelo entidad-relación, que se define y explica pormenorizadamente.

2.3.5.1. Modelo entidad–relación

El modelo entidad–relación (ER) constituye el eje central del diseño de la base de datos, ya que refleja de manera gráfica y conceptual las principales entidades involucradas en la gestión de mantenimientos, así como las relaciones existentes entre ellas. El objetivo del modelo fue garantizar integridad referencial, escalabilidad y trazabilidad, en cumplimiento con la norma ISO/IEC 17025, la cual demanda evidencias digitales, bitácoras y registros completos de cada acción de mantenimiento.

En el sistema desarrollado, la entidad equipos ocupa un lugar primordial, pues sobre ella se definen las programaciones de mantenimiento (preventivo, correctivo y calibraciones), las ejecuciones de mantenimiento realizadas, así como los tickets que registran fallas reportadas por usuarios internos. La trazabilidad se refuerza mediante entidades auxiliares como historial de equipos, evidencias y comentarios de ticket, las cuales documentan cada interacción del ciclo de vida de un equipo.

Los contratos constituyen el puente entre proveedores y equipos, delimitando el alcance y vigencia de los servicios de mantenimiento. A su vez, la relación de contratos con tipos de mantenimiento se normaliza a través de tablas intermedias, permitiendo así registrar mantenimientos preventivos, correctivos y calibraciones según la naturaleza de cada contrato.

De manera complementaria, se incluyen catálogos normalizados como tipos de mantenimiento, estados de mantenimiento y tipos de comentario, que permiten estandarizar la información y garantizar consistencia en los registros. Asimismo, el módulo de notificaciones facilita la gestión de alertas y avisos automáticos, mientras que configuración de alertas permite parametrizar los

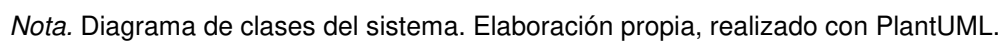
días de anticipación con los que el sistema debe advertir vencimientos o mantenimientos próximos.

El modelo también considera la integración con un sistema de gestión de identidades (*Keycloak*), por lo que la entidad usuarios está vinculada a un identificador externo (*keycloak_id*), evitando redundancia en credenciales y centralizando la autenticación/autorización.

En resumen, el diseño ER responde a cuatro principios fundamentales:

- Centralización de la información en torno a equipos, mantenimientos y proveedores.
- Normalización de catálogos y relaciones para evitar redundancia y asegurar consistencia.
- Escalabilidad mediante tablas puente y programación flexible.
- Trazabilidad mediante bitácoras, evidencias y seguimiento de estados.

Diagrama de entidad-relación



- Usuarios integrados con *Keycloak* vía *keycloak_id*.

- 31

- Evidencias polimórficas, asociables tanto a tickets como a ejecuciones de mantenimiento.
- Notificaciones automáticas soportadas por procedimientos almacenados y vistas (VW_AlertasMantenimiento, SP_DashboardAlertas).

2.3.6. Diseño de interfaz de usuario

El diseño de la interfaz de usuario (UI) constituye un aspecto esencial del sistema, ya que representa el medio de interacción entre los usuarios internos del Inacif y la plataforma de gestión de mantenimientos. Durante esta etapa se elaboraron prototipos de pantallas (*mockups*) que sirvieron como base para la construcción del *frontend* en Angular, con autenticación centralizada mediante *Keycloak*.

El enfoque adoptado se basó en los principios de simplicidad, accesibilidad y consistencia, garantizando que los usuarios puedan realizar sus tareas de forma intuitiva y con el menor número de pasos posibles. Además, se consideró la diversidad de perfiles que acceden al sistema –administradores, técnicos, proveedores y usuarios de consulta–, de manera que cada uno tuviera acceso únicamente a las funcionalidades que le correspondieran según su rol.

2.3.6.1. Mockups principales

Con el fin de validar el diseño de la interfaz antes de su implementación, se construyeron *mockups* de las pantallas principales. Estos prototipos permitieron simular la interacción del usuario con el sistema, asegurando que la distribución de elementos, los flujos de navegación y la disposición de la información fueran adecuados.

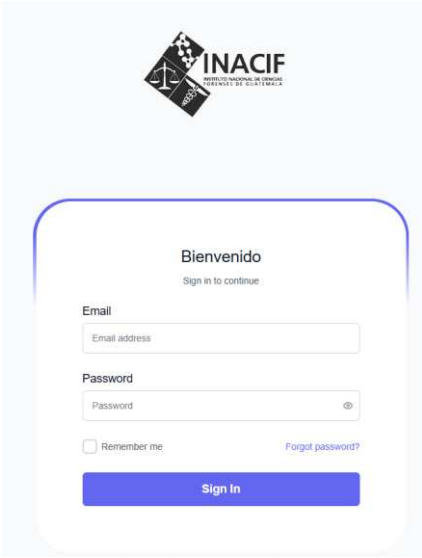
Los *mockups* elaborados corresponden a:

- Pantalla de inicio de sesión

Integrada con *Keycloak*, permite a los usuarios autenticarse mediante credenciales institucionales. Incluye logo institucional, formulario de ingreso y mensajes de error claros en caso de credenciales inválidas.

Figura 9.

Mockup de pantalla de inicio de sesión



The mockup shows a clean, modern login interface. At the top center is the INACIF logo, which includes a stylized diamond shape with a scale of justice and the text 'INACIF INSTITUCIÓN NACIONAL DE FISCOS FORTALEZCA SU ALIADO'. Below the logo, the text 'Bienvenido' is centered, followed by 'Sign in to continue:'. The form contains two input fields: 'Email' with a placeholder 'Email address' and 'Password' with a placeholder 'Password' and a small eye icon for toggling visibility. Below the password field is a 'Remember me' checkbox and a 'Forgot password?' link. A prominent blue 'Sign In' button is at the bottom of the form.

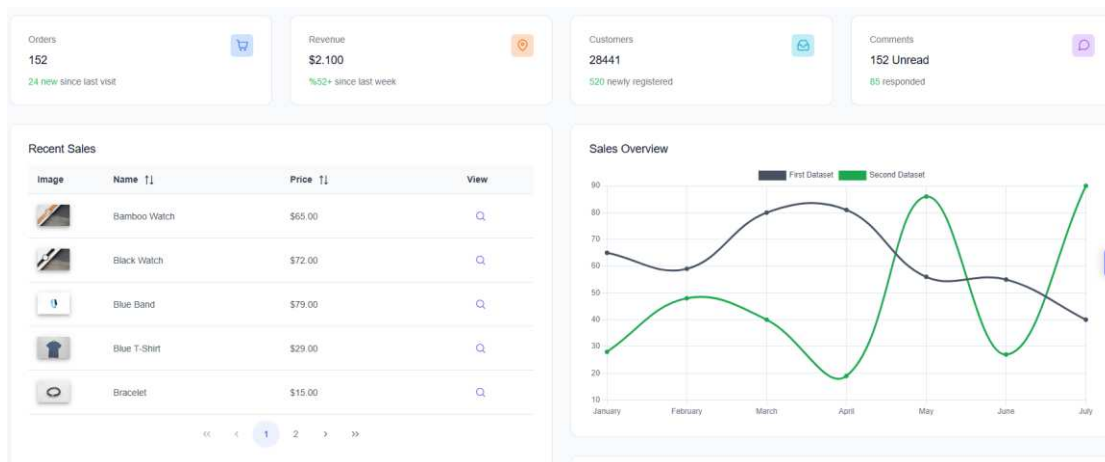
Nota. *Mockup* de la pantalla de inicio de sesión, diseñado en Angular como parte de la propuesta de interfaz. Elaboración propia.

- *Dashboard principal*

Presenta un panel de control con indicadores clave (mantenimientos próximos, tickets abiertos, contratos por vencer). El diseño privilegia la visualización rápida de alertas, así como accesos directos a los módulos de equipos, mantenimientos, tickets y reportes.

Figura 10.

Mockup de dashboard principal



Nota. Mockup del *dashboard* principal, diseñado en Angular como parte de la propuesta de interfaz. Elaboración propia.

- **Gestión de equipos**

Incluye una tabla con filtros por laboratorio, estado operativo y tipo de equipo. Se muestra información relevante como nombre, código Inacif, ubicación y estado actual. Desde esta vista se puede acceder al detalle de cada equipo, su historial y las evidencias asociadas.

Figura 11.

Mockup de gestión de equipos

Gestión de Equipos

+ Nuevo

Participantes

Q Buscar...

☐	Razón social ↑↓	NIT ↑↓	Telefono ↑↓	Estado ↑↓	
☐	Moore-Mahoney	90750143-0	(907)865-1729x59700	true	
☐	Mcclain, Williams and Lynch	90736179-8	(597)440-0091x0173	false	
☐	Ingram, Ramirez and Diaz	90799167-4	001-160-793-0460x38089	false	
☐	Brown Ltd	38210028-3	001-966-180-4065	false	
☐	Good-Montoya	73475964-1	0391404476	false	
☐	Stevenson-Savage	50931112-4	(251)978-0174x63339	false	

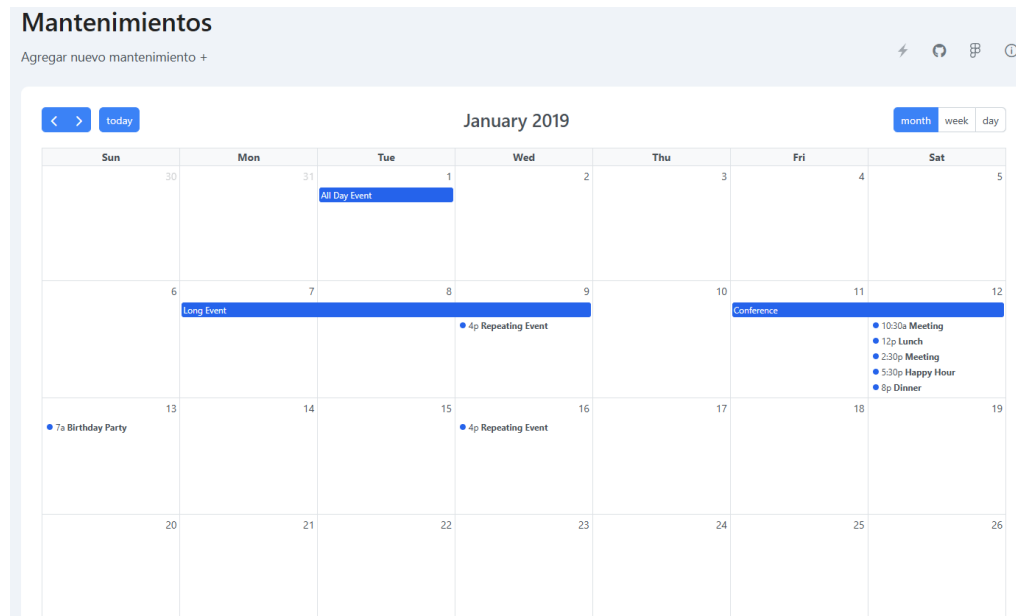
Nota. Mockup de la pantalla la gestión de equipos, diseñado en Angular como parte de la propuesta de interfaz. Elaboración propia.

- Calendario de mantenimientos

Permite visualizar, en un calendario interactivo, las programaciones de mantenimientos preventivos y correctivos. Cada evento muestra el equipo relacionado, la fecha de ejecución y el responsable asignado.

Figura 12.

Mockup de calendario de mantenimientos



Nota. Mockup de la pantalla de calendario de mantenimientos, diseñado en Angular como parte de la propuesta de interfaz. Elaboración propia.

- Gestión de tickets de falla

Presenta un formulario para registrar fallas de equipos, así como un flujo visual del estado del ticket (abierto, asignado, en proceso, resuelto, cerrado). Los usuarios pueden adjuntar comentarios y evidencias (documentos o fotografías).

- Módulo de reportes

Ofrece la generación de reportes personalizables en formatos PDF y XLS. El usuario puede aplicar filtros por rango de fechas, laboratorio, estado de equipos o tipo de mantenimiento.

2.3.6.2. Criterios de usabilidad

Los criterios de usabilidad aplicados en el diseño de las interfaces se basaron en estándares internacionales de interacción humano-computadora y en las necesidades particulares del Inacif. Entre ellos se destacan:

- Simplicidad: las pantallas muestran únicamente la información necesaria para cada operación, reduciendo la sobrecarga cognitiva del usuario.
- Consistencia: se mantuvo un estilo gráfico uniforme en colores, tipografías y disposición de botones. Esto permite que el usuario se familiarice rápidamente con el sistema y reduzca la curva de aprendizaje.
- Accesibilidad: las interfaces cumplen con principios básicos de accesibilidad, como contraste suficiente de colores, etiquetas descriptivas en formularios y soporte para navegadores modernos.
- Navegación intuitiva: los menús y accesos directos siguen una jerarquía lógica, priorizando el acceso a las funciones más utilizadas como equipos, tickets y mantenimientos.

- Retroalimentación inmediata: el sistema proporciona mensajes claros tras cada acción (confirmaciones, errores o alertas), evitando ambigüedades y facilitando la corrección de errores por parte del usuario.
- Compatibilidad: las interfaces fueron diseñadas con enfoque responsive, permitiendo su uso tanto en computadoras de escritorio como en dispositivos móviles y tabletas.
- Seguridad integrada: las rutas sensibles están protegidas mediante *guards* en Angular, que verifican el rol asignado en el token JWT de *Keycloak* antes de permitir el acceso.

2.3.7. Tecnologías utilizadas

La selección tecnológica para el desarrollo del sistema respondió a criterios de robustez, compatibilidad con la infraestructura institucional y alineación con estándares de la industria. Las herramientas elegidas permiten garantizar escalabilidad, seguridad y facilidad de mantenimiento.

2.3.7.1. Definición

- Java EE (Jakarta EE): plataforma de desarrollo orientada a aplicaciones empresariales distribuidas, soportada en componentes reutilizables y estándares abiertos. Facilita la creación de servicios web, la persistencia de datos mediante JPA y la exposición de APIs RESTful.
- Apache TomEE: servidor de aplicaciones compatible con Jakarta EE que combina Apache Tomcat con librerías Java EE, permitiendo desplegar aplicaciones empresariales de manera ligera y flexible.

- *Angular: framework frontend* basado en *TypeScript* que permite la construcción de aplicaciones web de una sola página (*Single Page Applications*, SPA), con alto rendimiento, modularidad y soporte para componentes reutilizables.
- *Keycloak*: sistema de gestión de identidades y accesos (IdP), que implementa estándares de autenticación como OAuth2.0 y *OpenID Connect* (OIDC). Permite administrar usuarios, roles y sesiones de forma centralizada.
- *SQL Server / PostgreSQL*: sistemas de gestión de bases de datos relacionales (RDBMS) que soportan integridad referencial, transacciones ACID y escalabilidad en ambientes empresariales. *PostgreSQL* es de código abierto y *SQL Server* es una alternativa ampliamente utilizada en instituciones gubernamentales.
- *Docker*: plataforma de contenedores que permite empaquetar aplicaciones junto con sus dependencias, garantizando portabilidad y replicabilidad en ambientes de desarrollo, pruebas y producción.
- *Maven*: herramienta de automatización de construcción para proyectos Java, que gestiona dependencias, compilaciones y empaquetado.
- *Visual Studio Code*: entorno de desarrollo integrado (IDE) ligero, multiplataforma y extensible, con soporte para múltiples lenguajes y contenedores *Docker*.

2.3.7.2. Justificación de selección

El conjunto de tecnologías fue seleccionado por las siguientes razones:

- Compatibilidad institucional: tanto *SQL Server* como *PostgreSQL* son soportados en el Centro de Datos del Inacif, lo cual asegura viabilidad operativa.
- Escalabilidad y sostenibilidad: *Angular* y *Jakarta EE* permiten el desarrollo modular y escalable, con posibilidad de añadir nuevos módulos en el futuro sin comprometer la arquitectura actual.
- Seguridad y cumplimiento: *Keycloak* facilita la integración con *Single Sign-On* y la gestión de roles, lo cual asegura el cumplimiento de políticas internas y normativas internacionales de seguridad de la información.
- Estandarización: el uso de *frameworks* y servidores ampliamente adoptados (*Angular*, *TomEE*, *Docker*) reduce la dependencia de soluciones propietarias y asegura soporte a largo plazo.
- Eficiencia en desarrollo: *Maven* versus *Code* optimizan el ciclo de desarrollo, integrándose fácilmente con contenedores *Docker* y control de versiones.

2.3.8. Plan de implementación

El plan de implementación se estructuró siguiendo la metodología ágil *Scrum*, organizando las actividades en *sprints* de dos semanas. Cada *sprint* produjo incrementos funcionales verificables y validados con usuarios clave.

2.3.8.1. Cronograma de actividades

El cronograma se extendió por 6 meses, desde el 3 de marzo hasta el 3 de septiembre de 2025, abarcando 8 *sprints* de tres semanas. El proyecto formal concluyó en esa fecha con la entrega técnica final.

Las actividades de capacitación, despliegue productivo y elaboración de documentación técnica y manuales de usuario se programaron posteriormente al 3 de septiembre, como actividades complementarias de transición hacia la operación institucional.

Resumen de fases:

- *Sprint 1* (3–23 de marzo 2025): configuración del ambiente y módulo de usuarios.
- *Sprint 2* (24 de marzo – 13 de abril 2025): gestión de equipos.
- *Sprint 3* (14 de abril – 4 de mayo 2025): programación de mantenimientos preventivos.
- *Sprint 4* (5 – 25 de mayo 2025): tickets de falla y evidencias.

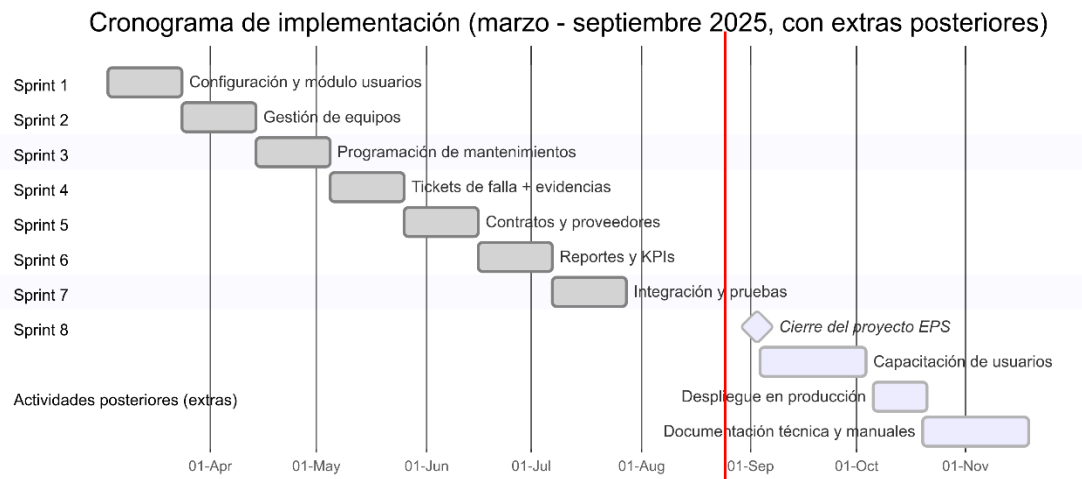
- *Sprint 5* (26 de mayo – 15 de junio 2025): contratos y proveedores.
- *Sprint 6* (16 de junio – 6 de julio 2025): reportes y KPIs.
- *Sprint 7* (7 – 27 de julio 2025): integración y pruebas de sistema.
- *Sprint 8* (28 de julio – 3 de septiembre 2025): cierre del proyecto EPS.

Actividades posteriores (extras):

- Septiembre – octubre 2025: capacitación de usuarios finales.
- Octubre 2025: despliegue oficial en producción.
- Octubre – noviembre 2025: elaboración y entrega de documentación técnica y manuales de usuario.

Figura 13.

Cronograma de actividades



Nota. Representación esquemática del cronograma de actividades, desarrollada en Mermaid como parte de la planificación del proyecto. Elaboración propia, realizado con Mermaid.

2.3.8.2. Estrategia de pruebas

Las pruebas se planificaron en distintos niveles:

- Pruebas unitarias: validación de métodos y componentes individuales.
- Pruebas de integración: validación de la interacción entre módulos, como *frontend-backend* y *backend-base de datos*.
- Pruebas funcionales: verificación del cumplimiento de los casos de uso definidos.

- Pruebas de aceptación: realizadas con usuarios finales para confirmar que el sistema responde a las necesidades planteadas.
- Pruebas de seguridad: validación del flujo de autenticación, autorización por roles y cifrado de comunicaciones.

2.3.8.3. Despliegue y capacitación

El despliegue se llevó a cabo de forma progresiva:

- Desarrollo y pruebas locales mediante contenedores *Docker*.
- Preproducción en el centro de datos institucional, simulando la infraestructura final.
- Producción en contenedores *Docker* bajo el entorno institucional, con respaldo automático de la base de datos.

Adicionalmente, se impartirán talleres de capacitación al personal administrativo y técnico, explicando el uso del sistema, la interpretación de reportes y el flujo de tickets y mantenimientos.

2.3.9. Seguridad y confiabilidad

Dada la naturaleza crítica de la información gestionada por el Inacif, la seguridad fue un eje transversal en el diseño del sistema. Se implementaron medidas tanto a nivel de aplicación como de infraestructura.

2.3.9.1. Autenticación y roles con *Keycloak*

El control de accesos se centralizó en *Keycloak*, configurado con:

- Roles principales: administrador, técnico, proveedor y usuario de consulta.
- Flujos de autenticación: mediante OAuth 2.0 y OIDC (*Authorization Code Flow*).
- Autorización basada en roles: validada en el *backend* mediante *tokens* JWT.
- Gestión centralizada de usuarios: evitando duplicidad de credenciales y permitiendo la trazabilidad de accesos.

2.3.9.2. Medidas de seguridad (VPN, TLS, *backups*)

Se establecieron las siguientes medidas adicionales:

- Acceso mediante VPN institucional: el sistema solo es accesible desde la red interna o a través de túneles seguros, restringiendo intentos externos no autorizados.
- Cifrado de comunicaciones (TLS 1.2+): todo intercambio de datos entre *frontend*, *backend* y base de datos se realiza bajo protocolos cifrados, garantizando confidencialidad e integridad.

- *Backups* automáticos: la base de datos cuenta con políticas de respaldos periódicos (diarios y semanales), almacenados en servidores redundantes.
- Control de integridad de evidencias: los archivos subidos (fotografías, certificados de calibración, reportes) incluyen metadatos de auditoría y son validados contra registros en la base de datos.
- Plan de recuperación ante desastres (DRP): contempla restauración de base de datos y servicios críticos en caso de fallos del hardware o corrupción de datos.

2.3.9.3. Evaluación y mitigación de Vulnerabilidades

Vulnerabilidades técnicas:

- Inyección de SQL: riesgo por falta de validación de entradas que permite ejecutar consultas maliciosas.
 - Mitigación: aplicar validación y sanitización rigurosa en formularios y usar consultas preparadas u ORM.
- Exposición de datos sensibles: riesgo de acceso a información confidencial sin cifrado ni control de accesos.
 - Mitigación: emplear cifrado fuerte (TLS en tránsito, AES en reposo) y controles de acceso basados en roles.

- Configuraciones incorrectas: riesgo por errores en la configuración de servidores o servicios.
 - Mitigación: aplicar configuraciones seguras, realizar auditorías periódicas y *hardening* de servidores.
- Falta de actualizaciones y parches: riesgo de explotación de vulnerabilidades conocidas en librerías no actualizadas.
 - Mitigación: establecer un proceso de actualización continua y gestión de vulnerabilidades (*CVE monitoring*).
- Autenticación y autorización inadecuadas: riesgo de accesos no autorizados por mecanismos débiles.
 - Mitigación: integrar autenticación robusta con *Keycloak*, usar OAuth2/JWT y políticas de contraseñas seguras.

Vulnerabilidades operativas:

- Errores humanos: riesgo de fallos en configuración, operación o mantenimiento del sistema.
 - Mitigación: definir procedimientos estandarizados y capacitar al personal en operaciones críticas.
- Falta de capacitación: riesgo de uso incorrecto del sistema y malas prácticas.

- Mitigación: impartir talleres periódicos, manuales de usuario y guías de buenas prácticas.
- Deficiencias en respaldos: riesgo de pérdida de datos por ausencia de procedimientos adecuados.
 - Mitigación: implementar un plan de respaldo y recuperación con copias periódicas y verificación de integridad.
- Incumplimiento de políticas de seguridad: riesgo de exposición por no cumplir lineamientos internos.
 - Mitigación: desarrollar políticas claras, realizar auditorías regulares y monitorear el cumplimiento.
- Respuesta insuficiente a incidentes: riesgo de demora en la detección y atención de incidentes.
 - Mitigación: establecer un plan de monitoreo y protocolos de respuesta rápida ante incidentes de seguridad.

2.4. Costos del proyecto

El proyecto fue desarrollado utilizando principalmente tecnologías libres y de código abierto, lo que permitió minimizar los gastos de licenciamiento. Sin embargo, se incurrió en costos asociados a infraestructura de apoyo, horas de trabajo del equipo desarrollador, recursos de hardware y servicios complementarios.

Tabla 3.*Costos del proyecto*

Categoría	Descripción	Cantidad	Costo unitario (Q)	Subtotal (Q)
Recursos humanos	Horas de trabajo de desarrollo, pruebas y documentación (480 h)	1	125.00 / hora	60,000.00
Equipo de cómputo	Laptop de desarrollo (16 GB RAM, SSD, Intel i7/AMD Ryzen)	1	9,000.00	9,000.00
Pantalla auxiliar	Monitor de alta resolución para programación y pruebas	1	2,400.00	2,400.00
Dispositivo de prueba	Tablet/smartphone para pruebas responsivas	1	1,200.00	1,200.00
Conectividad	Internet dedicado (6 meses x Q225/mes)	6	225.00	1,350.00
Gastos administrativos	Material de oficina, transporte y logística	-	-	2,000.00
Total, estimado del proyecto				75,950.00

Nota. Detalle del costo estimado para la realización del proyecto. Elaboración propia, realizado con Microsoft Excel.

- **Notas:**

El costo humano se calculó en función de un promedio de Q125 por hora, considerando análisis, desarrollo, pruebas y documentación.

- El equipo de cómputo y periféricos se consideraron como inversión necesaria para la ejecución.
- Al emplear tecnologías libres (Angular, *TomEE*, *Keycloak*, *SQLServer Express*, *Docker*), no se incurrió en gastos de licencias.

2.5. Beneficios del proyecto

El sistema desarrollado ofrece beneficios tangibles tanto a nivel operativo como institucional. En lo operativo, permite centralizar la gestión de equipos y mantenimientos, eliminar la duplicidad de registros, reducir fallas inesperadas y asegurar que cada acción quede trazada en bitácoras digitales con evidencias documentales. Esto se traduce en procesos más ágiles, reportes automáticos y una mayor disponibilidad de los equipos de laboratorio.

Desde la perspectiva normativa, el sistema contribuye directamente al cumplimiento de la ISO/IEC 17025, ya que proporciona la documentación y trazabilidad exigida por las auditorías y acreditaciones internacionales. Esto fortalece la confiabilidad de los procesos técnicos y simplifica la preparación de auditorías, al contar con reportes verificables y evidencia digital organizada.

A nivel institucional, el Inacif se beneficia de una modernización tecnológica significativa al migrar de hojas de cálculo a una plataforma web robusta, lo que incrementa la transparencia de sus procesos internos. El uso de software libre asegura sostenibilidad y reduce la dependencia de licencias costosas. Además, la capacitación impartida al personal permite garantizar la adopción de la herramienta y mejora sus competencias tecnológicas, fortaleciendo así la cultura de innovación en la institución.

En términos económicos, aunque el costo total del proyecto asciende a Q75,950.00, se espera una rápida recuperación de la inversión mediante el ahorro de tiempo administrativo, la reducción de mantenimientos reactivos y la prolongación de la vida útil de los equipos gracias al control preventivo.

3. FASE DE ENSEÑANZA-APRENDIZAJE

La fase de enseñanza-aprendizaje tuvo como propósito asegurar que el sistema desarrollado no solo fuera funcional en términos técnicos, sino también utilizable y sostenible en la práctica. Para ello, se planteó una capacitación general dirigida al personal del Inacif y la elaboración de manuales que sirven como material de apoyo permanente.

3.1. Capacitación propuesta

La capacitación fue diseñada como una sesión general única, posterior al cierre formal del proyecto el 3 de septiembre de 2025, con el fin de que todo el personal designado recibiera la misma inducción.

- Duración: 4 horas.
- Modalidad: presencial, con práctica directa en el sistema.
- Participantes: personal administrativo y técnico del Inacif designado para operar la plataforma.
- Contenidos tratados:
 - Introducción general al sistema y su importancia para la trazabilidad de mantenimientos.

- Explicación del flujo de trabajo: registro de equipos, creación de mantenimientos, gestión de tickets y generación de reportes.
- Buenas prácticas en el registro de información y resguardo de evidencias.
- Lineamientos básicos de seguridad en el uso de VPN y autenticación mediante *Keycloak*.

El enfoque fue práctico, con ejercicios guiados que permitieron a los participantes experimentar las funcionalidades clave del sistema.

3.2. Material elaborado

Para complementar la capacitación se elaborarán dos manuales principales, diseñados en formato digital (PDF) y accesibles en la intranet institucional:

3.2.1. Manual de usuario

Documento dirigido a los usuarios generales del sistema. Incluye instrucciones paso a paso para iniciar sesión, navegar en los distintos módulos, consultar equipos, generar reportes y realizar búsquedas rápidas. Está orientado a la operación cotidiana, con ejemplos visuales y explicaciones claras.

3.2.2. Manual técnico

Dirigido al personal con responsabilidades avanzadas de gestión y soporte. Contiene la descripción de procesos como la programación de mantenimientos, la gestión de tickets, la carga de evidencias, así como la administración de contratos y proveedores. También incluye notas sobre la resolución de incidencias comunes y recomendaciones de seguridad.

Ambos manuales se estructuraron con capturas de pantalla, diagramas de flujo simples y ejemplos prácticos, lo cual facilita su uso como guía de consulta rápida ante dudas en la operación diaria.

CONCLUSIONES

1. La implementación del sistema de gestión de mantenimientos para el Inacif permitió superar las limitaciones de los registros manuales y hojas de cálculo dispersas, consolidando toda la información en una plataforma digital segura y trazable.
2. El uso de tecnologías modernas como *Angular*, *Jakarta EE*, *Keycloak* y *Docker* garantizó la construcción de una solución escalable, portable y con altos estándares de seguridad, alineada con la infraestructura institucional.
3. La base de datos diseñada bajo un modelo entidad–relación normalizado contribuyó a garantizar integridad y consistencia en la información, facilitando la generación de reportes confiables para auditorías internas y externas.
4. La metodología ágil *Scrum* permitió estructurar el desarrollo en *sprints* iterativos, entregando valor de manera temprana y permitiendo retroalimentación continua de los usuarios clave.
5. El sistema aporta beneficios normativos y operativos directos: asegura cumplimiento de la norma ISO/IEC 17025, mejora la planificación de mantenimientos preventivos y fortalece la trazabilidad de evidencias en los laboratorios del Inacif.

6. El componente de enseñanza-aprendizaje con manuales y capacitación general posterior al 3 de septiembre de 2025 asegura la apropiación del sistema por parte del personal y su sostenibilidad a largo plazo.

RECOMENDACIONES

1. Mantener un proceso de mejora continua, incorporando módulos adicionales en función de las necesidades institucionales, como gestión de inventarios o integración con sistemas de compras.
2. Establecer un equipo de soporte interno que dé seguimiento a incidencias y brinde apoyo a los usuarios, garantizando continuidad operativa.
3. Programar respaldos automáticos diarios y semanales de la base de datos y almacenamiento de evidencias, validando periódicamente los procedimientos de recuperación ante desastres.
4. Reforzar la capacitación anual del personal, con actualizaciones de manuales y sesiones prácticas que permitan recordar flujos críticos y buenas prácticas de seguridad digital.
5. Integrar el sistema con servicios de auditoría digital y firma electrónica avanzada, a fin de fortalecer aún más el cumplimiento de normativas internacionales.
6. Documentar formalmente cada actualización del sistema mediante control de versiones y bitácoras de cambios, asegurando trazabilidad en el ciclo de vida del software.

REFERENCIAS

Angular Team. (2023). *Angular documentation*. Angular. <https://angular.io/docs>

Inacif. (2025). *Información de la institución*. Inacif.

Pressman, R. y Maxim, B. (2020). *Ingeniería de software: un enfoque práctico*. McGraw-Hill.

Red Hat. (2023). *Keycloak documentation*. Red Hat. <https://www.keycloak.org/documentation>

