

**Escuela Superior Politécnica del Litoral**  
**Facultad de Ingeniería en Electricidad y Computación**

Desarrollo de una Solución Tecnológica para la Emisión y Validación de  
Certificados Digitales

TECH-409

**Proyecto Integrador**

Previo la obtención del Título de:

**Ingeniero en Ciencias de la Computación**

Presentado por:

Alan Fernando Villavicencio Villacis  
Nicolas Mauricio Coronel Mendoza

Guayaquil - Ecuador

Año: 2025

## **Dedicatoria**

---

Dedico este proyecto a mis padres,  
quienes con su amor, esfuerzo y apoyo  
incondicional me han dado la fortaleza  
para culminar esta etapa académica.  
Gracias por enseñarme el valor de la  
perseverancia y la disciplina.

A mi familia, que siempre ha sido un pilar  
fundamental en mi vida, acompañándome  
en los momentos difíciles y compartiendo  
conmigo cada logro alcanzado.

A mis amigos y compañeros de carrera,  
quienes con su compañía y colaboración  
hicieron más llevadero este camino  
universitario.

Nicolás Coronel

## Dedicatoria

---

Le dedico este proyecto a mis padres,  
Fernando e Inés, quienes han sido un  
pilar importante a lo largo de toda mi  
vida y me han apoyado en todos los  
momentos que los he necesitado.

Siempre que he buscado consejo o  
ayuda, ellos han estado ahí para mí,  
dándome sus ánimos para que pueda  
seguir adelante ante las dificultades que  
se me han presentado.

También quiero dedicársela a mi  
hermana, Miluska, quien siempre a  
estado a mi lado para mantenerme  
positivo y alegre, con ella siempre paso  
momentos divertidos los cuales han sido  
fundamentales durante mi tiempo en la  
Universidad para mantenerme alegre y  
positivo.

Por último, a todos mis amigos que he  
hecho a lo largo de mi vida, ya que ellos  
han sido un gran apoyo a lo largo de  
distintas etapas de mi vida.

Alan Villavicencio

## Agradecimientos

---

Quiero expresar mi más sincero agradecimiento a todas las personas que contribuyeron al desarrollo y culminación de este proyecto.

En primer lugar, al Ing. Ronald Criollo, por su guía y orientación académica, siempre dispuesto a aportar sus conocimientos y a aclarar dudas en cada etapa del trabajo.

Al Msc. Milton Iván Alfonzo, por su valiosa colaboración como cliente, cuya retroalimentación permitió alinear la solución a las necesidades reales de la institución.

A la Escuela Superior Politécnica del Litoral (ESPOL), por brindarme los recursos, conocimientos y un espacio académico propicio para mi formación profesional.

Finalmente, a mi familia, por su apoyo constante, paciencia y motivación, que fueron esenciales para alcanzar este objetivo.

Nicolás Coronel

## Agradecimientos

---

Quiero agradecer a toda mi familia que siempre ha velado por mi felicidad y siempre ha estado allí para apoyarme cuando mas los he necesitado.

Al Ing. Ronald Criollo, por compartirnos su guía y conocimientos a lo largo del proyecto, los cuales fueron esenciales para lograr nuestro objetivo

A mis profesores, ya que ellos me dieron los conocimientos para poder enfrentar los retos que se han presentado a lo largo de mi carrera universitaria.

Al Msc. Milton Iván Alfonso, por su colaboración en este proyecto, ya que con su ayuda pudimos lograr la solución deseada.

Por último, a mis amigos, ya que ellos han hecho que pase grandes momentos a lo largo de mi vida y permitieron que haga buenos recuerdos.

Alan Villavicencio

## **Declaración Expresa**

---

Nosotros Alan Fernando Villavicencio Villacis y Nicolas Mauricio Coronel Mendoza

acordamos y reconocemos que:

La titularidad de los derechos patrimoniales de autor (derechos de autor) del proyecto de graduación corresponderá al autor o autores, sin perjuicio de lo cual la ESPOL recibe en este acto una licencia gratuita de plazo indefinido para el uso no comercial y comercial de la obra con facultad de sublicenciar, incluyendo la autorización para su divulgación, así como para la creación y uso de obras derivadas. En el caso de usos comerciales se respetará el porcentaje de participación en beneficios que corresponda a favor del autor o autores.

La titularidad total y exclusiva sobre los derechos patrimoniales de patente de invención, modelo de utilidad, diseño industrial, secreto industrial, software o información no divulgada que corresponda o pueda corresponder respecto de cualquier investigación, desarrollo tecnológico o invención realizada por mí/nosotros durante el desarrollo del proyecto de graduación, pertenecerán de forma total, exclusiva e indivisible a la ESPOL, sin perjuicio del porcentaje que me/nos corresponda de los beneficios económicos que la ESPOL reciba por la explotación de mi/nuestra innovación, de ser el caso.

En los casos donde la Oficina de Transferencia de Resultados de Investigación (OTRI) de la ESPOL comunique a los autores que existe una innovación potencialmente patentable sobre los resultados del proyecto de graduación, no se realizará publicación o divulgación alguna, sin la autorización expresa y previa de la ESPOL.

Guayaquil, 29 de Mayo del 2025.

---

Alan Villavicencio

---

Nicolas Coronel

## **Evaluadores**

---

**Ing. Ronald Raúl Criollo Bonilla**

Profesor de Materia

---

**Ing. Ronald Raúl Criollo Bonilla**

Tutor de proyecto

## **Resumen**

El presente proyecto propone el desarrollo de una solución tecnológica para la emisión y validación de certificados digitales en organizaciones que actualmente dependen de procesos manuales o poco integrados. La problemática identificada radica en la pérdida de tiempo, duplicidad de esfuerzos y baja trazabilidad en la gestión documental tradicional.

La propuesta consiste en una aplicación web con dos perfiles de usuario: administrador y usuario interno. El sistema permite la generación, aprobación, firma digital y descarga de certificados, además de notificaciones automáticas por correo y validación mediante código QR. Durante el proceso de implementación se empleó una metodología iterativa con reuniones periódicas con el cliente y pruebas de usuario. Los resultados obtenidos demuestran una reducción significativa en el tiempo de emisión de certificados, mayor seguridad en la validación y mejor trazabilidad institucional.

La solución representa un avance en la modernización de procesos administrativos, incrementa la transparencia y eficiencia, y sienta las bases para futuras mejoras como la firma masiva de documentos o la integración con otros sistemas de gestión.

**Palabras Clave:** Firma electrónica, Trazabilidad, Optimización, Transformación digital



## **Abstract**

*This project presents the development of a technological solution for the issuance and validation of digital certificates in organizations that still rely on manual or poorly integrated processes. The main problem identified lies in inefficiencies such as information loss, duplication of efforts, and low traceability in document management. The proposed solution is a web application with two user roles: administrator and internal user. The system enables certificate requests, approvals, electronic signatures, downloads, email notifications, and QR-based validation.*

*An iterative methodology was followed, including regular client meetings and user testing. Results show a significant reduction in certificate issuance time, enhanced security, and improved process traceability. This solution contributes to the digital transformation of institutional processes, increasing efficiency and transparency while providing a scalable foundation for future improvements such as bulk signing of documents and integration with external systems.*

*Keywords: Electronic signature, Traceability, Optimization, Digital transformation*

# Índice General

<i>Resumen</i> .....	1
<i>Abstract</i> .....	2
<i>Índice General</i> .....	3
<i>Abreviaturas</i> .....	5
<i>Índice de figuras</i> .....	6
<i>Índice de tablas</i> .....	6
<i>Capítulo 1</i> .....	1
1. Introducción.....	2
1.1 Descripción del Problema.....	2
1.2 Justificación del Problema.....	3
1.3 Objetivos .....	5
1.4 Marco teórico .....	5
<i>Capítulo 2</i> .....	8
2. Metodología.....	9
2.1. Análisis.....	9
2.2 Requerimientos.....	10
2.3 Alcance y Limitaciones de la Solución .....	13
2.4 Riesgos y Beneficios de la Solución.....	14
2.5 Usuarios.....	15
2.6 Diseño de la Solución .....	15
2.7 Prototipo .....	24
<i>Capítulo 3</i> .....	36
3. Resultados y Análisis .....	37
3.1 Plan de Implementación .....	37
3.2 Pruebas .....	42
3.3 Resultados.....	46
3.4 Análisis de costos .....	47
<i>Capítulo 4</i> .....	48
4. Conclusiones y Recomendaciones .....	49
4.1 Conclusiones.....	49
4.2 Recomendaciones .....	50
<i>Referencias</i> .....	51
<i>Apéndices</i> .....	53
Apéndice A .....	53

Manual de implementación de FirmaEC .....	53
Apéndice B.....	57
Formularios de Evaluación.....	57
Formulario de observación (llenado por Nicolás Coronel) .....	57
Apéndice C.....	58
Historias de Usuario .....	58

## Abreviaturas

API    Application Programming Interface

BD    Database

HTTPS    Hypertext Transfer Protocol Secure

PEM    Privacy Enhanced Mail

QR    Quick response

URL    Uniform Resource Locator

## Índice de figuras

Figura 1 Propuesta de Arquitectura en modelo 4+1 .....	16
Figura 2 Diagrama de casos de uso del sistema.....	17
Figura 3 Vista lógica del sistema.....	18
Figura 4 Diagrama de componentes del sistema.....	20
Figura 5 Vista física del sistema .....	21
Figura 6 Vista física del sistema.....	23
Figura 7 Prototipo de baja fidelidad (escoger certificados).....	25
Figura 8 Prototipo baja fidelidad (Ver solicitudes).....	25
Figura 9 Prototipo baja fidelidad (crear solicitud).....	26
Figura 10 Primer prototipo en Figma (Login) .....	27
Figura 11 Primer prototipo en Figma (ver solicitudes).....	27
Figura 12 Primer prototipo en Figma (ver solicitudes Admin).....	28
Figura 13 Primer prototipo en Figma (Ventana solicitud).....	29
Figura 14 Primer prototipo en Figma (crear solicitud) .....	29
Figura 15 Primer prototipo en Figma (Creación solicitud).....	30
Figura 16 Primer prototipo en Figma (Vista detalles Aprobado) .....	31
Figura 17 Primer prototipo en Figma (Vista detalles Rechazo) .....	31
Figura 18 Prototipo final en Figma (ver solicitudes).....	33
Figura 19 Prototipo final en Figma (validación QR).....	33
Figura 20 Prototipo final en Figma (vista admin aprobar/rechazar solicitud).....	34
Figura 21 Prototipo final en Figma (ingresar firma).....	34
Figura 22 Diagrama de gantt del sprint 0 (parte 1).....	38
Figura 23 Diagrama de gantt del sprint 0 (parte 2).....	39
Figura 24 Diagrama de gantt del sprint 1(parte 1).....	40

Figura 25 Diagrama de gantt del sprint 1 (parte 2).....	40
Figura 26 Diagrama de gantt del sprint 2 (parte 1).....	41
Figura 27 Diagrama de gantt del sprint 2 (parte 2).....	42
Figura 28 Resultados del formulario post pruebas parte 1 .....	44
Figura 29 Resultados del formulario post pruebas parte 2 .....	44
Figura 30 Resultados del formulario post pruebas parte 3 .....	45
Figura 31 Resultados del formulario post pruebas parte 4 .....	45

## Índice de tablas

Tabla 1 Historias de Usuario.....	58
-----------------------------------	----

# Capítulo 1



# **1. Introducción**

En un entorno cada vez más digitalizado, la gestión eficiente de la información se ha convertido en un factor clave para el funcionamiento transparente y ágil de las organizaciones. Sin embargo, muchas instituciones aún dependen de procesos manuales y herramientas no integradas para la emisión de documentos, lo que genera múltiples limitaciones operativas. Esta situación evidencia la necesidad de adoptar soluciones tecnológicas que permitan optimizar la gestión documental, mejorar la trazabilidad de los procesos y fortalecer la confianza institucional tanto interna como externamente.

## **1.1 Descripción del Problema**

En muchas organizaciones, especialmente aquellas con recursos limitados o estructuras operativas tradicionales, los procesos relacionados con la gestión documental; como la emisión de certificados y reportes, la recolección de firmas y el archivo de documentos, continúan realizándose de forma manual y dispersa. La dependencia de formatos físicos o herramientas no integradas genera múltiples ineficiencias operativas, como la pérdida de información, la duplicación de esfuerzos y retrasos significativos en la entrega de documentos clave. Esta situación se agrava ante la falta de una plataforma digital centralizada que permita automatizar flujos, rastrear el estado de cada documento en tiempo real y garantizar la integridad del proceso desde su creación hasta su validación final. La dependencia de formatos impresos o de soluciones tecnológicas aisladas provoca ineficiencias estructurales, como la pérdida o extravío de documentos importantes, la duplicación innecesaria de tareas, y retrasos considerables en la entrega o validación de información clave. Tales deficiencias no solo obstaculizan el trabajo diario del personal administrativo, sino que además comprometen la capacidad de la organización para

responder con agilidad y transparencia ante auditorías, requerimientos legales o solicitudes externas. La inexistencia de un sistema estructurado limita la trazabilidad de los documentos, impide el control efectivo de cada etapa y dificulta la auditoría oportuna de los procesos internos

Adicionalmente, la falta de herramientas digitales adecuadas para la autenticación, verificación y seguimiento de los documentos emitidos afecta de manera directa la confianza institucional, tanto hacia adentro como hacia el exterior. Los usuarios internos se ven obligados a implementar controles manuales paralelos que incrementan la carga laboral y aumentan el margen de error, mientras que los usuarios externos (como ciudadanos, instituciones aliadas o entes reguladores) perciben una imagen de desorganización o falta de fiabilidad documental.

Esto puede disminuir la confianza tanto de los usuarios internos como de los receptores externos de los certificados u otros reportes emitidos. En consecuencia, esta problemática impacta directamente en la productividad del personal administrativo, en la calidad del servicio ofrecido y en la capacidad de respuesta institucional ante auditorías, solicitudes ciudadanas o requerimientos legales. Frente a este contexto, se vuelve necesario diseñar e implementar una solución tecnológica que permita centralizar, automatizar y asegurar la gestión documental, optimizando así los recursos y garantizando mejores estándares de control y trazabilidad.

## **1.2 Justificación del Problema**

La justificación de este problema radica en que la gestión documental es una función crítica en cualquier organización, ya que permite conservar evidencia formal de procesos, certificar hechos y asegurar la trazabilidad de la información. En cualquier organización o

institución, la correcta emisión y control de documentos como certificados, constancias y reportes es esencial para mantener la credibilidad, la eficiencia operativa y el cumplimiento normativo. En este sentido, la falta de un sistema estructurado y automatizado no solo representa un obstáculo técnico, sino también un riesgo institucional, pues compromete la integridad, la autenticidad y la disponibilidad de la información. Procesos manuales, herramientas desconectadas o controles informales pueden dar lugar a errores, manipulaciones involuntarias, demoras y pérdida de documentos, afectando negativamente la calidad del servicio ofrecido y deteriorando la confianza de los usuarios internos y externos. Además, esta situación puede generar un impacto económico significativo, ya que la duplicación de esfuerzos y la resolución de errores implican una sobrecarga operativa y administrativa.

Desde esta perspectiva, implementar un módulo de emisión y validación de certificados digitales representa una solución estratégica que aporta múltiples beneficios: permite reducir tiempos de procesamiento, incrementar la seguridad y autenticidad de los documentos, mejorar la transparencia de los procesos administrativos, reducir la carga de trabajo de varios departamentos. Además, un sistema digital bien diseñado facilita la colaboración interdepartamental, agiliza la toma de decisiones basada en datos documentales y permite responder con mayor rapidez y precisión a auditorías, solicitudes ciudadanas o requerimientos normativos. Asimismo, al integrar funcionalidades como la generación automática de certificados, validación mediante códigos QR y reportería, se proporciona una herramienta de alto valor tanto para usuarios internos como externos. La transformación digital de la gestión documental debe entenderse como una inversión estratégica que promueve la modernización institucional, optimiza el uso de recursos, y contribuye significativamente a la construcción de una cultura organizacional basada en la eficiencia, la transparencia y la rendición de cuentas.

## 1.3 Objetivos

### 1.3.1 Objetivo general

Desarrollar una aplicación web para la emisión de certificados digitales, que automatice la generación de documentos personalizados, con el fin de optimizar los procesos documentales y mejorar la trazabilidad del proceso de emisión de certificados digitales.

### 1.3.2 Objetivos específicos

1. Diseñar una interfaz de gestión para la generación automatizada de certificados digitales con campos personalizables.
2. Desarrollar una solución tecnológica, donde los usuarios puedan buscar y generar sus certificados de forma segura, con trazabilidad y control de accesos básicos.
3. Reducir tiempos y errores en la emisión de certificados digitales a través de procesos automatizados y eficientes.
4. Evaluar las funcionalidades del sistema mediante pruebas de los usuarios involucrados.

## 1.4 Marco teórico

### 1.4.1 Gestión documental en organizaciones

La gestión documental se refiere al conjunto de normas y procedimientos técnicos que se emplean para manejar documentos de cualquier tipo dentro de una entidad. Su propósito es promover la recuperación de información, establecer el periodo durante el cual los documentos deben ser conservados y garantizar que permanezcan íntegros y accesibles con el paso del tiempo. [1]. En el contexto de las organizaciones sin fines de lucro, la implementación de sistemas de información ha demostrado ser un factor diferenciador, permitiendo una mejor organización y eficiencia en sus operaciones [2].

### **1.4.2 Certificados Digitales y su Infraestructura**

Los certificados digitales son documentos electrónicos que utilizan criptografía para garantizar la autenticidad e integridad de la información. Estos certificados permiten verificar la identidad de las partes involucradas en una transacción electrónica y asegurar que los datos no han sido alterados. La infraestructura de clave pública (PKI) es fundamental en este contexto, ya que proporciona un marco para la emisión, gestión y revocación de certificados digitales [3]. Además, estándares como X.509 definen el formato de los certificados y los procedimientos para su validación [4].

### **1.4.3 Tecnologías Web para la Emisión de Certificados**

El desarrollo de sistemas para la emisión de certificados digitales se apoya en tecnologías web que permiten construir aplicaciones accesibles desde navegadores, escalables ante un número creciente de usuarios y seguras en el tratamiento de información sensible. Estas tecnologías facilitan la creación de interfaces interactivas, así como la implementación de la lógica del sistema tanto en el cliente como en el servidor. Además, fomentan el diseño modular, la reutilización de componentes y la integración con servicios externos mediante interfaces de programación de aplicaciones (APIs). Este enfoque contribuye al desarrollo de soluciones eficientes, mantenibles y alineadas con las buenas prácticas del desarrollo web.[5]

### **1.4.4 Usabilidad en Sistemas de Información**

La usabilidad es un aspecto crítico en el diseño de sistemas de información, ya que influye directamente en la eficiencia y satisfacción del usuario. Un sistema usable debe ser fácil de aprender, eficiente de utilizar, fácil de recordar, con pocos errores y satisfactorio en su uso [6]. En el contexto de la emisión de certificados digitales, una interfaz intuitiva y procesos simplificados son esenciales para garantizar que los usuarios puedan obtener sus

certificados sin dificultades.

#### **1.4.5 Seguridad en la Emisión de Certificados Digitales**

La seguridad en los sistemas de emisión de certificados digitales es primordial para proteger la confidencialidad, integridad y disponibilidad de la información. Esto implica la implementación de medidas como el cifrado de datos, autenticación de usuarios, control de accesos y auditorías de seguridad. Además, es fundamental cumplir con estándares y normativas internacionales que regulan la protección de datos y la seguridad de la información [7]. La integración de mecanismos de seguridad robustos no solo protege la información, sino que también genera confianza en los usuarios del sistema.

#### **1.4.6 Casos de Implementación en Organizaciones sin Fines de Lucro**

A nivel internacional, diversas organizaciones sin fines de lucro han adoptado sistemas de emisión de certificados digitales para mejorar sus procesos. Por ejemplo, la plataforma Sertifier ha permitido a instituciones educativas emitir certificados digitales de manera eficiente, mejorando la visibilidad y reconocimiento de sus programas [8]. En el contexto latinoamericano, iniciativas como la de Chile, con su plataforma ChileAtiende, han implementado certificados digitales para facilitar trámites ciudadanos de forma segura y eficiente [9].

## **Capítulo 2**

## **2. Metodología**

En el siguiente capítulo se proporcionan más detalles sobre el desarrollo de la solución tecnológica propuesta. Primero, se describen los requerimientos funcionales y no funcionales, donde se describen las distintas características y funcionalidades que debe tener la solución para cumplir los objetivos que se propusieron. Posteriormente, se limita el alcance de la solución, incluyendo las limitaciones que se encontraron, además, se detallan los riesgos y beneficios de la solución propuesta y los distintos usuarios que formarán parte de esta.

### **2.1. Análisis**

Durante la etapa de análisis, se realizaron varias reuniones con nuestro tutor, el Ingeniero Ronald Criollo y con nuestro cliente, el Máster Milton Iván Alfonzo estas reuniones nos fueron de ayuda para obtener una mejor idea sobre cómo debería funcionar la solución, para de esta forma definir de forma asertiva a los usuarios y los requerimientos que debe cumplir nuestra solución.

La funcionalidad principal de nuestra solución debía ser la de emisión de certificados digitales, ya que, al realizar esta tarde de forma manual, se consume mucho tiempo y recursos, lo cual lleva a retrasos y a falta de comunicación entre distintos departamentos. En base a lo discutido en las distintas reuniones, se optó por desarrollar una aplicación web la cual permitiera que los usuarios internos de una empresa puedan realizar una solicitud de un certificado digital y de esta forma el encargado de dicho certificado apruebe o niegue la solicitud, en caso de aprobarse, la aplicación web generará el certificado solicitado firmado electrónicamente por el encargado.

Además, se discutieron sobre varias funcionalidades adicionales que facilitan el uso de la aplicación y mejora la experiencia tanto al usuario interno como al



encargado/administrador. Por esta razón, se plantearon funcionalidades como el uso de notificaciones por correo electrónico para que los usuarios puedan tener conocimiento de cuando haya un avance en el proceso de solicitud de un certificado digital, así mismo se planteó añadir un código QR al certificado para poder realizar una validación de autenticidad de este, lo cual añade una capa de seguridad para evitar copias o modificaciones a certificados ya emitidos.

## **2.2 Requerimientos**

### **2.2.1 Requerimientos funcionales**

- **Usuario interno inicia sesión con sus credenciales**

Un usuario interno debe tener la capacidad de usar sus credenciales de inicio de sesión para poder ingresar a la aplicación, haciendo uso de su usuario y contraseña podrá validarlos para así hacer uso de las funcionalidades disponibles.

- **Usuario interno solicita un certificado**

Un usuario interno debe tener la capacidad de realizar una solicitud de un certificado, para lo cual deberá primero escoger el certificado a solicitar para que se genere su solicitud, por ejemplo, un certificado de empleabilidad, donde podrá elegir si desea el certificado con sueldo o sin sueldo.

- **Usuario interno descarga un certificado**

Un usuario interno debe poder descargar un certificado de una solicitud aprobada, cuando el encargado de la aprobación del certificado aprueba dicho certificado, el usuario podrá ingresar a la aplicación para descargar el certificado generado.

- **Usuario interno visualiza todas las solicitudes que ha realizado**

Un usuario interno debe poder visualizar todas las solicitudes generadas dentro de la plataforma, de esta forma podrá revisar solicitudes antiguas y tener en un solo lugar todos los

certificados solicitados, además el usuario podrá ordenar dichas solicitudes para poder realizar una mejor búsqueda de alguna solicitud.

- **Usuario interno recibe notificaciones sobre el proceso de su solicitud**

Un usuario interno deberá recibir notificaciones a su correo electrónico para poder llevar un control del proceso de su solicitud, la aplicación enviará una notificación cuando se haya generado una solicitud correctamente y cuando una solicitud sea aprobada o negada.

- **Usuario interno valida el certificado con el código QR**

Un usuario interno deberá poder escanear el código QR incluido en el certificado digital para poder confirmar su autenticidad, dicho código QR enviará al usuario a una pestaña donde se mostrará si el certificado es válido y auténtico, además de la información incluida en el certificado.

- **Administrador recibe una notificación cuando se genera una solicitud**

Un administrador deberá recibir una notificación a su correo electrónico cuando se genera una solicitud pendiente de aprobación, de esta forma podrá llevar un control de las solicitudes e ingresar a la aplicación cuando sea necesario.

- **Administrador aprueba o niega una solicitud**

Un administrador debe ser capaz de poder aprobar o negar una solicitud, en caso de aprobarse se genera el certificado solicitado y se permitirá al solicitante descargarlo en formato PDF, además de enviarle una notificación al solicitante, en caso de negarse, el administrador podrá añadir una razón para el rechazo en caso de ser necesario.

- **Administrador visualiza las solicitudes que se han generado**

Un administrador debe ser capaz de visualizar todas las solicitudes generadas por los usuarios para poder decidir cuales aprobar o negar y así llevar un mejor control de estas y evitar la pérdida de información, además será capaz de ordenarlas para visualizarlas de forma más clara.

- **Administrador agrega más certificados a la aplicación**

Un administrador debe poder agregar más certificados a la aplicación, esto en base a las necesidades de la organización que use la aplicación, para que los usuarios internos tengan más opciones de certificados digitales a generar.

- **Administrador gestiona los roles de los usuarios**

Un administrador debe tener la capacidad de gestionar los roles de los distintos usuarios, para poder definir qué usuarios son usuarios internos o administradores, para de esta forma poder limitar las funcionalidades de cada uno de los tipos de usuario.

## **2.2.2 Requerimientos no funcionales**

- **Usabilidad**

La interfaz de la solución tecnológica debe ser intuitiva y accesible para que usuarios que no tengan mucho conocimiento técnico puedan usarla fácilmente y sin problemas. De esta forma será fácil de comprender y los usuarios podrán navegar y hacer uso de las funcionalidades que ofrece sin dificultad.

- **Rendimiento**

La solución debe contar con tiempo de carga y tiempos de respuesta rápidos a las acciones que realice el usuario para asegurar la satisfacción de este, ya que la presencia de fallas o de lentitud por parte de la solución pueden provocar una sensación de disconformidad al usuario.

- **Trazabilidad**

La solución deberá registrar todas las solicitudes y emisiones de certificados digitales para poder llevar un control de estos y tenerlos disponibles en caso de una auditoría interna o externa.

- **Accesibilidad**

La solución debe ser accesible desde distintos dispositivos, tales como computadoras o dispositivos móviles, de esta forma se asegura que los usuarios puedan hacer uso de las funcionalidades que ofrece en el lugar y momento que lo necesiten.

- **Seguridad**

La solución debe asegurarse de mantener la integridad de los datos de los distintos usuarios que la usen, además se debe mantener las restricciones a los distintos roles establecidos. Además, deberá tener medidas de seguridad contra accesos no autorizados y debe mantener la confidencialidad de la información.

## **2.3 Alcance y limitaciones de la solución**

### **2.3.1 Alcance**

La solución tecnológica desarrollada consiste en una aplicación web para la emisión de certificados y documentos digitales. Esta aplicación está diseñada para cubrir las siguientes funcionalidades clave:

- Permitir a los usuarios internos solicitar certificados digitales mediante una interfaz sencilla.
- Facilitar la aprobación o rechazo de solicitudes por parte de un administrador autorizado.
- Generar certificados digitales con firma electrónica integrada.
- Gestionar usuarios y roles dentro del sistema para controlar el acceso.
- Notificar automáticamente por correo electrónico a los usuarios sobre el estado de sus solicitudes.

Esta solución está orientada a mejorar la trazabilidad, eficiencia y seguridad de los

procesos documentales en instituciones u organizaciones que requieren emitir certificados formales.

### **2.3.2 Limitaciones**

- Dependencia de conexión a Internet: Al ser una aplicación web, requiere conexión estable para su funcionamiento.
- Firma electrónica básica: La solución implementa una firma digital sencilla; no incluye integración con servicios de firma electrónica avanzada o biométrica o mediante QR.

## **2.4 Riesgos y Beneficios de la Solución**

### **2.4.1 Riesgos**

- Seguridad de datos: Si no se implementan protocolos robustos de ciberseguridad, existe el riesgo de manipulación o acceso no autorizado a los certificados.
- Errores en la generación de certificados: Fallos en la lógica de generación podrían producir documentos incorrectos, afectando la confianza institucional.

### **2.4.2 Beneficios**

- Reducción del tiempo de emisión: La automatización de procesos reduce significativamente los tiempos para generar y entregar certificados.
- Mejora de la trazabilidad: Cada solicitud y emisión queda registrada, facilitando auditorías y consultas posteriores.
- Aumento de la transparencia institucional: La trazabilidad y validación digital fortalecen la confianza en los documentos emitidos.
- Ahorro de recursos: Disminuye la dependencia de papel, impresoras y tiempo humano, lo que representa un ahorro administrativo.

## **2.5 Usuarios**

En base a las reuniones realizadas y a la información obtenida, se ha decidido tener dos tipos de usuarios para la solución tecnológica propuesta:

- Administrador

El administrador tiene la capacidad de visualizar, aprobar y denegar las solicitudes generadas por los usuarios internos, además tiene la capacidad de gestionar los roles de los distintos usuarios en la aplicación. Así mismo, es capaz de agregar nuevos certificados a la plataforma en base a las necesidades de la organización y de validar los certificados a través de un código QR.

- Usuario interno

El usuario interno tiene la capacidad de generar solicitudes de certificados digitales para posteriormente descargarlos para su uso en caso de que la solicitud sea aprobada, además es capaz de ver las solicitudes que ha generado y de validar los certificados a través de un código QR.

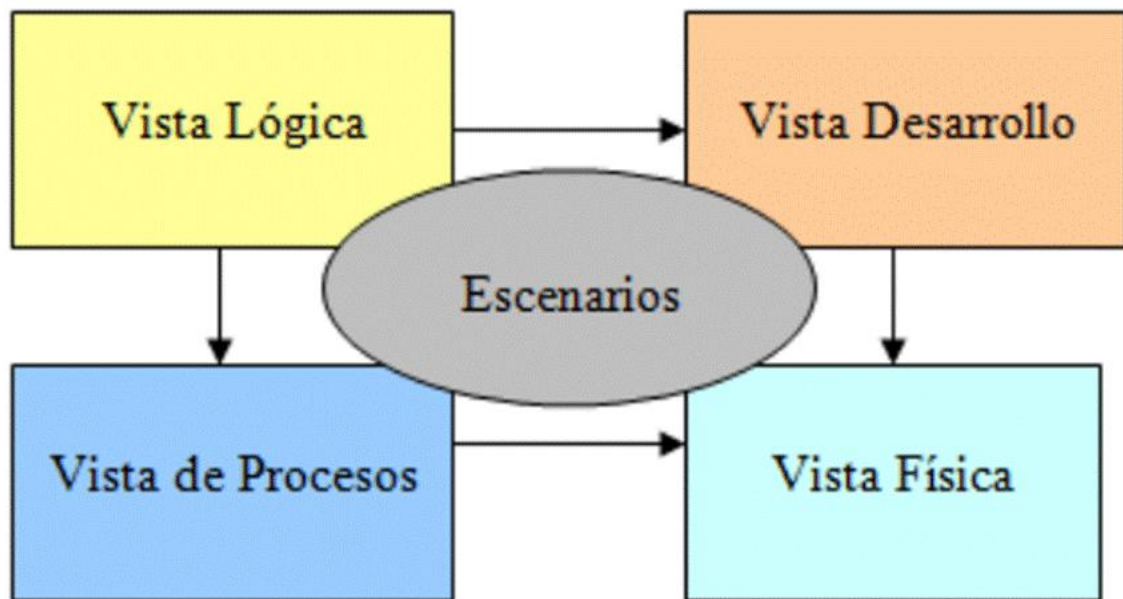
## **2.6 Diseño de la Solución**

### **2.6.1 Propuesta de Arquitectura**

La propuesta de la solución se basa en el modelo “4+1” vistas de la arquitectura de software propuesta por Philippe Kruchten [10], el cual plantea el uso de vistas concurrentes para abordar diferentes aspectos de un sistema. Este modelo permite hacer mas simple el diseño de la solución mediante 5 perspectivas, asegurando una cobertura integral y estructurada del diseño como se ilustra en la Figura 1.

**Figura 1**

*Propuesta de Arquitectura en modelo 4+1 [12]*



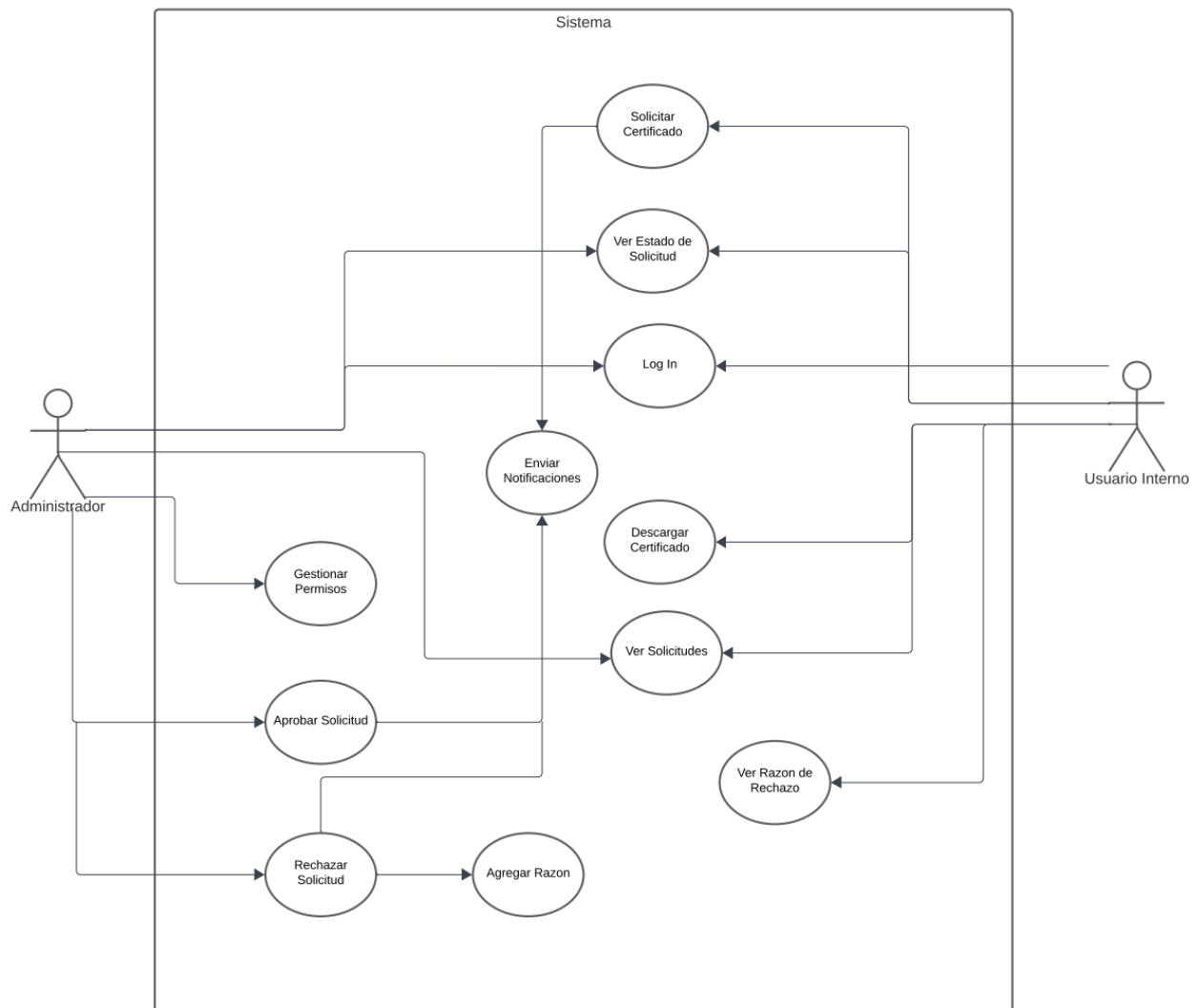
Esta arquitectura ofrece un marco estructurado para la creación de software sólido y escalable [10], asegurando que se traten todas las inquietudes pertinentes desde el diseño hasta la implementación.

### **2.6.2 Escenario**

Se presenta el siguiente diagrama para entender lo que la solución tecnológica propone, el cual muestra los principales casos de uso del sistema de emisión de certificados digitales. Se identificaron dos actores principales, usuario interno y administrador. Se puede observar las principales funciones que podrá realizar los usuarios y el administrador. Los dos actores se comunican usando un sistema que centraliza la comunicación a través del envío de notificaciones, las cuales notifican a los usuarios acerca de las modificaciones en el estado de las solicitudes.

**Figura 2**

*Diagrama de casos de uso del sistema*



Estos escenarios propuestos validan que la arquitectura soporte todos los requisitos funcionales necesarios.

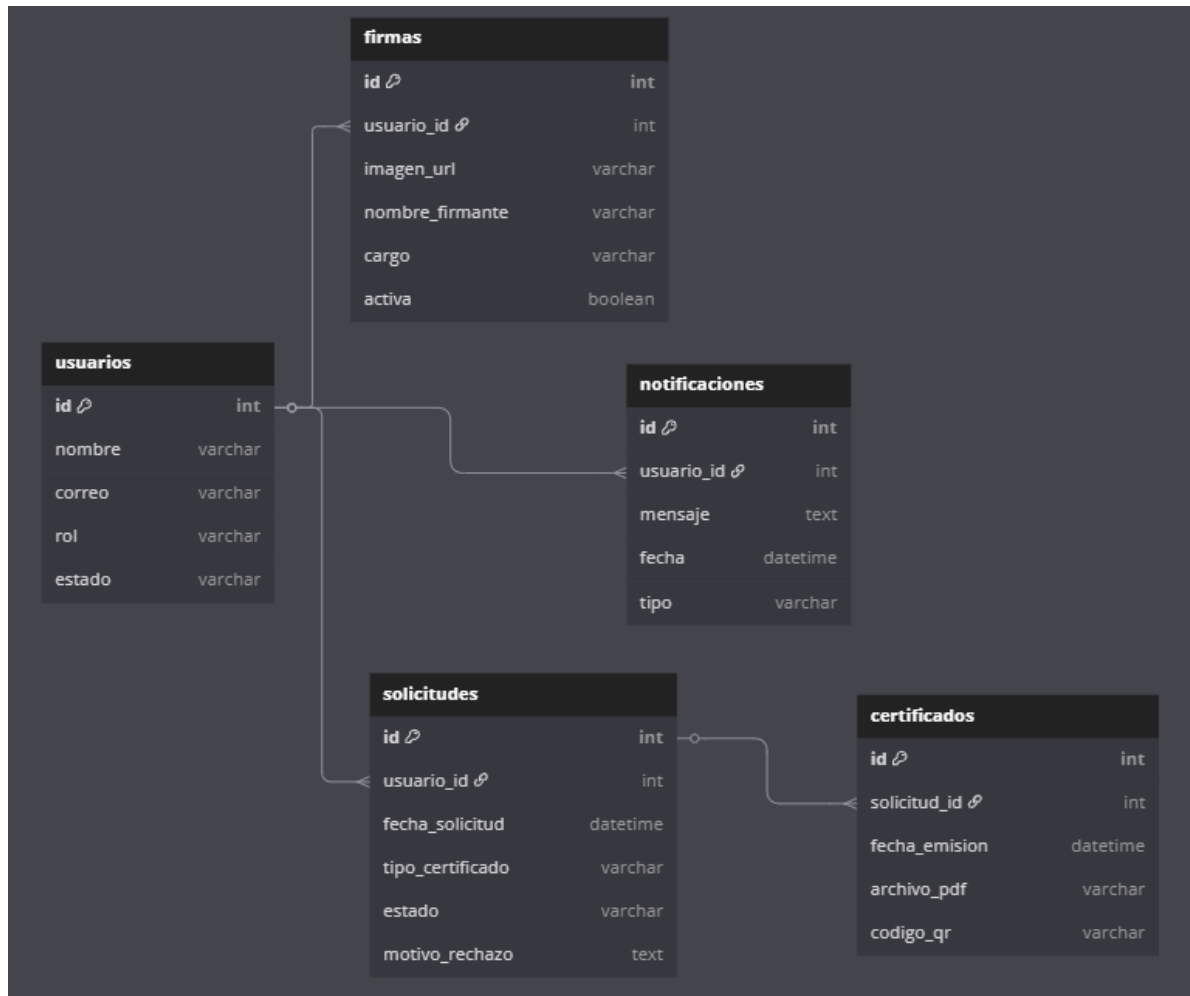
### 2.6.3 Vista Lógica

En la vista lógica se modelan las principales entidades del sistema y sus relaciones funcionales. Las entidades: usuario, solicitud, certificado y notificaciones corresponden tanto a componentes lógicos del backend como a tablas persistentes en la base de datos.



**Figura 3**

*Vista lógica del sistema*



Esta vista permite organizar de forma efectiva la lógica de negocio del sistema y garantizar integridad de almacenamiento, permitiendo mantener el historial completo de cada solicitud y su correspondiente validación.

**Entidades principales:**

- Usuarios: representa a los actores del sistema (usuarios internos y administradores). Contiene información como nombre, correo, rol y estado de la cuenta.
- Solicitudes: almacena cada solicitud de certificado realizada por un usuario. Incluye atributos como tipo de certificado, estado (pendiente, aprobado, rechazado).

- **Certificados:** contiene los certificados emitidos por el sistema. Cada certificado está vinculado a una solicitud aprobada y almacena datos como la fecha de emisión, el archivo generado y el código QR asociado.
- **Notificaciones:** registra los mensajes enviados al usuario, ya sea para confirmar la creación, aprobación o rechazo de una solicitud. Se almacena el contenido, la fecha de envío y el tipo de notificación.
- **Firmas:** representa las firmas digitales o imágenes asociadas a los administradores autorizados para emitir certificados. Incluye datos como el nombre del firmante, cargo, imagen (como URL o base64) y estado (activa o no).

#### **Relaciones clave entre entidades:**

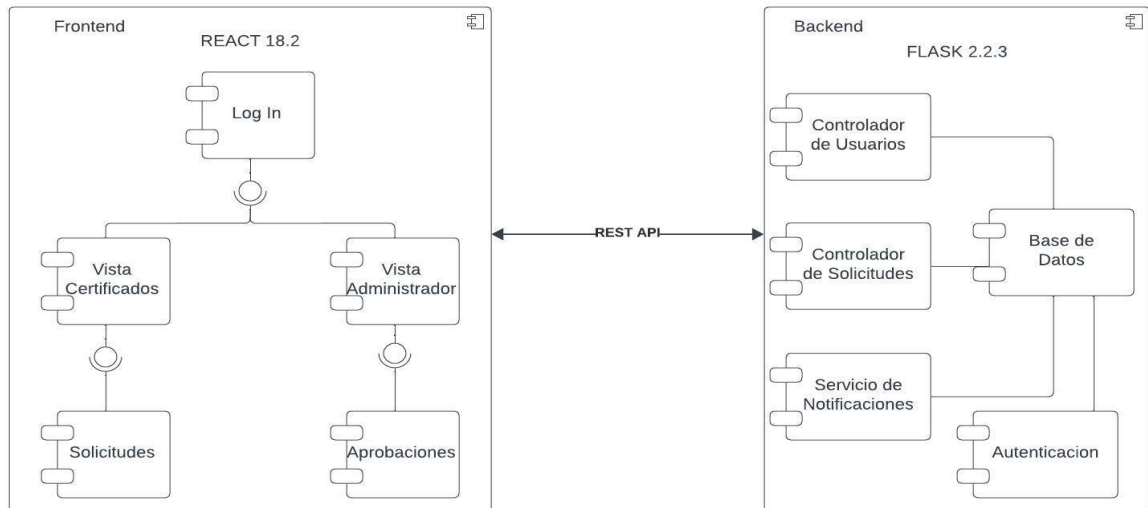
- Un usuario puede realizar múltiples solicitudes y recibir múltiples notificaciones.
- Cada solicitud está relacionada con un único usuario, y puede generar un único certificado.
- Cada certificado está asociado exactamente a una solicitud.
- Cada firma pertenece a un único usuario, generalmente con rol de administrador.

#### **2.6.4 Vista Desarrollo**

El diagrama de componentes permite visualizar el modularidad, fomentar la reutilización de código y mantener la mantenibilidad del sistema a largo plazo [12].

**Figura 4**

*Diagrama de componentes del sistema*



### Frontend (React 18.2)

- **Log In:** manejo de autenticación del usuario.
- **Vista Certificados y Solicitudes:** funcionalidades para los usuarios internos.
- **Vista Administrador y Aprobaciones:** gestión de solicitudes por parte del administrador.
- Todos estos componentes se comunican con el backend a través de una API REST.

### Backend (Flask 2.2.3)

- **Controlador de Usuarios y Controlador de Solicitudes:** gestionan peticiones entrantes desde el frontend.
- **Servicio de Notificaciones:** envía correos sobre el estado de las solicitudes.
- **Autenticación:** módulo de seguridad y validación.
- **Base de Datos:** persistencia de información.

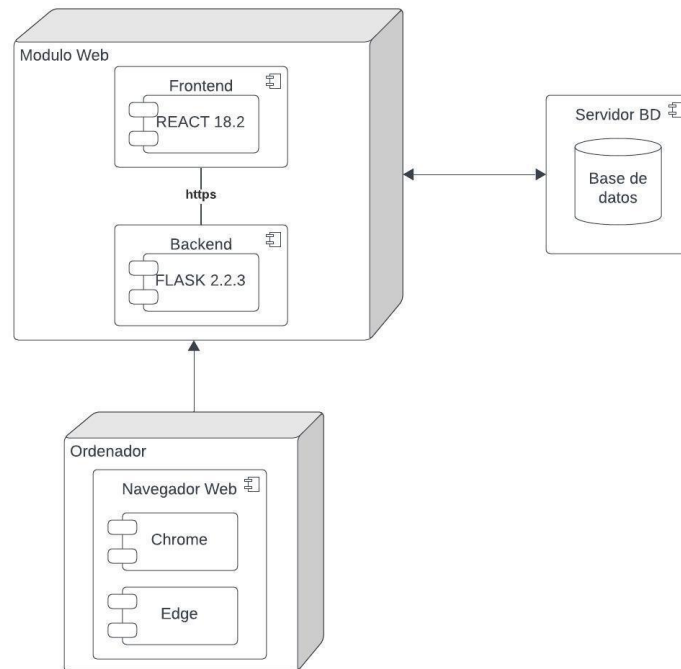
Este diseño ofrece una visión clara y precisa de la arquitectura de implementación del sistema, mostrando las dependencias entre módulos, facilitando la escalabilidad y mantenimiento del proyecto.

### 2.6.5 Vista Física

La vista física del sistema muestra la infraestructura de despliegue y los canales de comunicación entre los diferentes componentes de la solución tecnológica.

**Figura 5**

*Vista física del sistema*



Los módulos del sistema son los siguientes:

- El módulo web está compuesto por dos componentes: el Frontend y el Backend.
- El componente del Backend se desarrolló utilizando Flask 2.2.3, encargado de procesar la lógica del servidor, gestionar las solicitudes de los usuarios, y conectarse con la base de datos para registrar o recuperar información. Este componente se comunica a través del protocolo HTTPS, garantizando la seguridad en la transmisión

de la información.

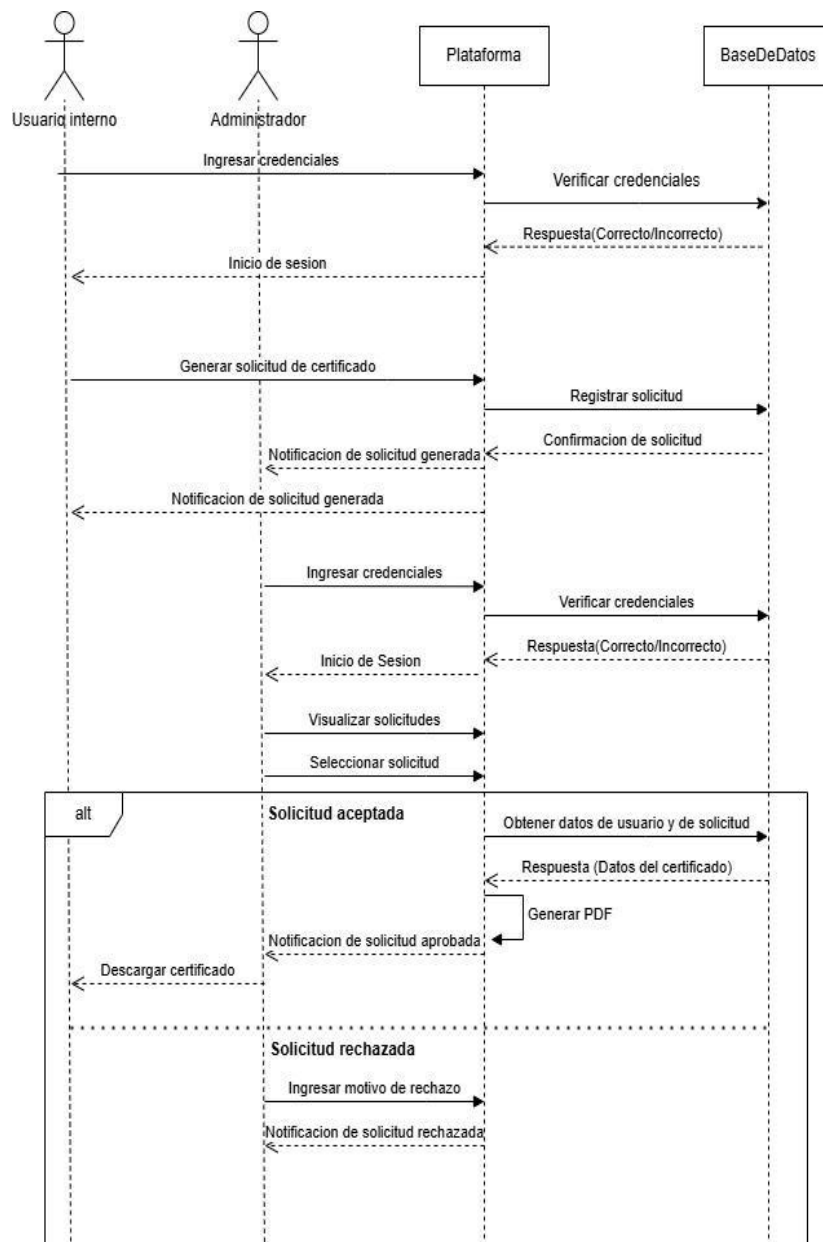
- Se utilizó React 18.2 para implementar el componente del Frontend, que ofrece una interfaz de usuario dinámica e interactiva.. Este módulo permite a los usuarios internos y administradores acceder a funcionalidades como la solicitud, consulta, aprobación y descarga de certificados digitales. La comunicación entre los componentes se realiza mediante HTTPS, asegurando la integridad y confidencialidad de la información.
- El servidor de base de datos guarda todos los datos requeridos para que el sistema funcione, incluyendo los datos de usuarios, solicitudes, certificados generados, estados de aprobación y trazabilidad del proceso.  
  
Esta base de datos se encuentra alojada en un entorno seguro y es accedida exclusivamente por el Backend a través de consultas controladas.

#### **2.6.6 Vista Procesos**

Esta vista se encarga de mostrar el comportamiento dinámico del sistema, especialmente en cuanto la comunicación entre componentes concurrentes, flujo de mensajes y tiempo de respuesta entre ellos.[11]

**Figura 6**

*Vista física del sistema*



En la figura 6 se puede observar el diagrama de secuencia de las principales acciones que realizan el usuario interno y el administrador. El diagrama inicia con el ingreso de credenciales por parte del usuario interno, los cuales son ingresados en la plataforma para luego ser confirmado en la base de datos.

Posteriormente, el usuario interno selecciona la opción de generar solicitud en la plataforma, luego procede a escoger qué certificado necesita y la plataforma registra la

solicitud en la base de datos. Además, en caso de que se haya generado correctamente la solicitud, la plataforma enviará una notificación al correo electrónico del usuario interno para confirmar la creación exitosa de la solicitud.

Por parte del administrador, el también deberá ingresar sus credenciales en la plataforma para que sean verificadas en base de datos y de esta forma hacer uso de las funcionalidades de esta. Como siguiente paso, procederá a visualizar las solicitudes pendientes en forma de lista y escoge la solicitud que desea revisar en la plataforma para aprobar o rechazar; en caso de aprobarse, la plataforma obtendrá los datos necesarios del solicitante a través de la base de datos para luego generar el certificado correspondiente, luego enviará una notificación al solicitante que su solicitud ha sido aprobada y así el usuario interno podrá ingresar y descargar su certificado digital; en caso de rechazar la solicitud, el administrador ingresa el motivo de rechazo en la plataforma dependiendo del caso y la plataforma envía una notificación al solicitante de que se solicitud ha sido rechazada.

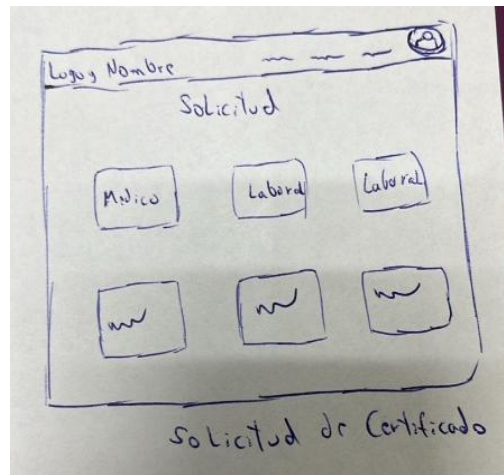
## **2.7 Prototipo**

### **2.7.1 Prototipos iniciales**

Se realizó un primer prototipo de baja fidelidad en hojas de papel, para mostrar la idea del diseño inicial que se tenía, de esta forma; si era necesario hacer un cambio de forma más rápida. Una vez obtenida la retroalimentación por parte del cliente, se realizaron los cambios necesarios y se procedió a realizar un segundo prototipo en Figma.

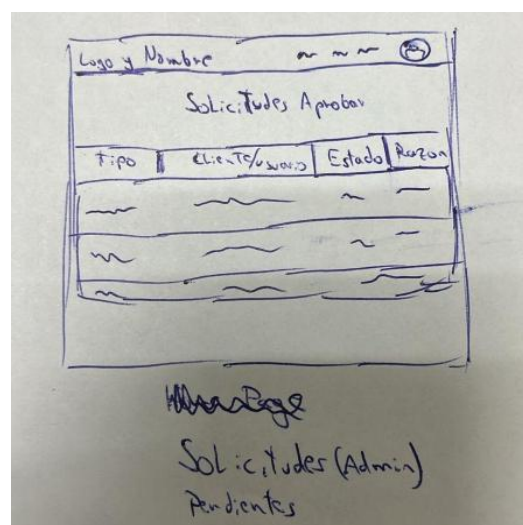
**Figura 7**

*Prototipo de baja fidelidad (escoger certificados)*



**Figura 8**

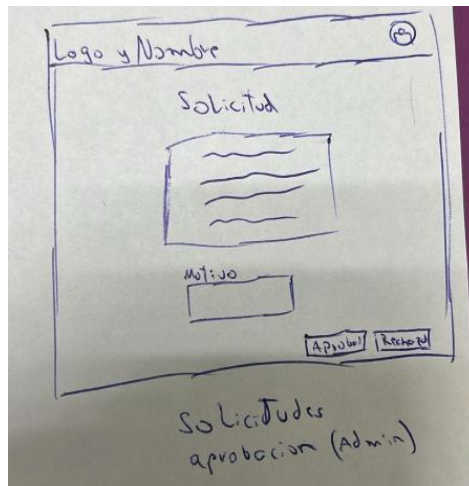
*Prototipo baja fidelidad (Ver solicitudes)*





## Figura 9

### Prototipo baja fidelidad (crear solicitud)



En las Figuras #7, 8 y 9 se pueden observar algunas de las ventanas principales de la aplicación, entre ellas la visualización de las solicitudes de certificados por parte del usuario y del administrador, así mismo como la ventana del administrador para aprobar o rechazar alguna solicitud, estas serían las dos funcionalidades principales con las que cuenta la solución, por ende, fueron a las que se les dio más prioridad.

En base a este primer prototipo, se tomaron en cuenta los distintos detalles que nos brindó el cliente, en base a ellos se modificaron varios aspectos, principalmente la información que mostraría cada ventana de la aplicación, en la ventana de solicitudes del usuario se vería el número de la solicitud creada, el tipo certificado solicitado, la fecha de emisión y el estado actual de dicha solicitud. En cuanto a la ventana de solicitudes del administrador, se vería el nombre y correo del solicitante, el tipo de certificado solicitado, su estado actual, una observación, y la fecha de emisión de la solicitud.

Adicionalmente, se decidió unir la pestaña de solicitudes y de certificados que inicialmente habíamos hecho por separado, esto para que sea más intuitivo y que el usuario no tenga que visitar varias ventanas para poder realizar el proceso de solicitar un certificado. También se conversó sobre la información que tendría la ventana de la validación Qr, para

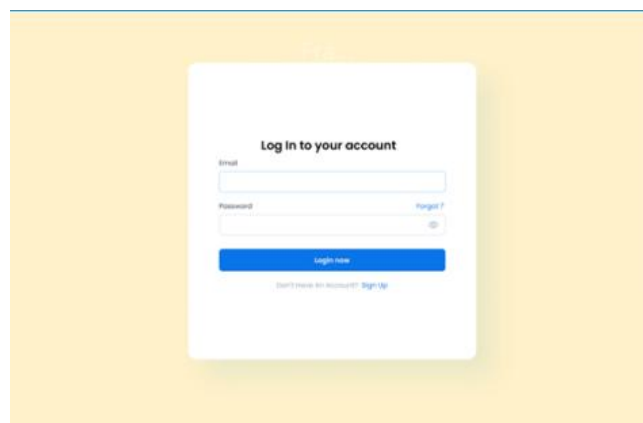
incluir los elementos necesarios para que se compruebe correctamente la autenticidad y validez de este.

### 2.7.2 Prototipo en Figma

Haciendo uso de las observaciones realizadas por el cliente, se procedió a realizar un primer prototipo en Figma, en el cual ya se podían experimentar el flujo de las distintas funcionalidades que ofrece la aplicación. Este prototipo ya incluía varias ventanas más, tales como la ventana de inicio de sesión, distintas ventanas de visualizaciones de los certificados y solicitudes en base a los distintos estados que tendría la solicitud de un certificado, la ventana para aprobar/rechazar un certificado y las ventanas para hacer la solicitud de estos.

**Figura 10**

*Primer prototipo en Figma (Login)*



**Figura 11**

*Primer prototipo en Figma (ver solicitudes)*

Mis CertificadosSolicitarInicio

Mis Certificados

Solicitar +

Solicitud N°	Tipo Certificado	FechaEmision ↑↓	Estado	
001	Empleabilidad	20-06-2025	Espero	Detalles...
002	Pasantias	10-06-2025	Aprobado	Detalles...
003	Miembro	17-05-2025	Rechazado	Detalles...

«

<

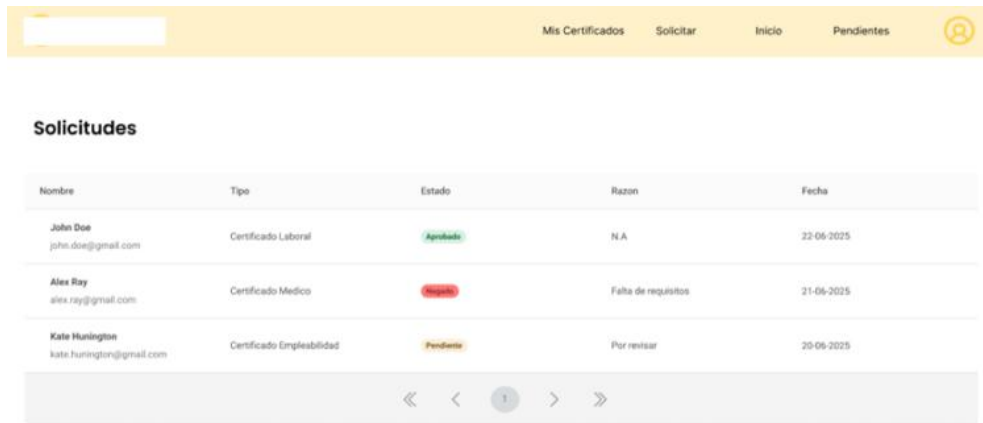
1

>

»

**Figura 12**

*Primer prototipo en Figma (ver solicitudes Admin)*



Nombre	Tipo	Estado	Razon	Fecha
John Doe john.doe@gmail.com	Certificado Laboral	Aprobado	N.A	22-06-2025
Alex Ray alex.ray@gmail.com	Certificado Medico	Rechazado	Falta de requisitos	21-06-2025
Kate Huntington kate.huntington@gmail.com	Certificado Empleabilidad	Pendiente	Por revisar	20-06-2025

En las Figuras #10, 11 y 12 se pueden observar las primeras ventanas de nuestro prototipo, donde se incluye la ventana de inicio de sesión, donde los usuarios deberán ingresar sus credenciales y en base al rol que tengan asignado los llevará a la ventana inicial ya sea de un usuario interno o de un administrador. Una vez que un usuario interno haya ingresado lo primero que se mostrarán serán las solicitudes que haya creado en forma de lista con los datos establecidos por el cliente anteriormente, en esta pestaña también tendrán la opción de realizar una nueva solicitud o ver más detalles de solicitudes ya creadas. De forma similar, el administrador verá las solicitudes pendientes en forma de lista y podrá seleccionar la que desee para observar más detalles sobre la misma.

**Figura 13**

*Primer prototipo en Figma (Ventana solicitud)*



**Figura 14**

*Primer prototipo en Figma (crear solicitud)*



En las Figuras #13 y 14 se puede visualizar las ventanas correspondientes a la solicitud de un certificado, como primera ventana se mostrarán los distintos tipos de certificados que el usuario pueda seleccionar y una vez escogidos pasará a la siguiente ventana donde deberá incluir el motivo por el cual hace dicha solicitud y también podrá confirmar el tipo de certificado a solicitar. En caso de que el administrador deba hacer una

solicitud, observará las mismas ventanas.

## Figura 15

### Primer prototipo en Figma (Creación solicitud)

El prototipo muestra una interfaz de usuario para la gestión de solicitudes. En la parte superior, hay una barra de navegación amarilla con los enlaces: 'Mis Certificados', 'Solicitar', 'Inicio' y 'Pendientes' (destacado con un icono de usuario). El título principal de la sección es 'Solicitud Pendiente'. A la izquierda, se muestra un 'CERTIFICADO DE TRABAJO' con un campo 'A QUERER INTERESADO' y un texto de ejemplo. A la derecha, un recuadro 'Motivo Solicitante' contiene el texto: 'Necesito un certificado que demuestre mi estado de empleabilidad con sueldo'. Debajo de este, hay un botón 'Escoger firma...'. En el centro, un campo 'Razon' para comentarios está precedido por un recuadro de texto. Al final, hay dos botones: 'Aprobar' (amarillo) y 'Rechazar' (gris).

En la figura #15 se puede observar la ventana de aprobación/rechazo de un certificado desde la vista de un administrador, aquí podrá observar un avance sobre cómo se verá el certificado con los distintos campos ya rellenados, también podrá observar el motivo ingresado por el solicitante y tendrá la opción de escoger el archivo p12 que incluye la firma a poner en el certificado. Finalmente, tendrá un recuadro donde ingresar una observación en caso de rechazar la solicitud y al final se encuentran los botones para aprobar o rechazar dicha solicitud.

**Figura 16**

*Primer prototipo en Figma (Vista detalles Aprobado)*



**Figura 17**

*Primer prototipo en Figma (Vista detalles Rechazo)*



En las figuras #16 y 17, se puede observar las ventanas de detalles sobre una solicitud por parte de un usuario, aquí se mostrará información que ira en el certificado, la cual dependerá del certificado solicitado, así como que tipo de certificado es y también se puede observar el motivo ingresado por el solicitante. También se incluye el estado actual de una solicitud y en caso de que esté aprobada se habilitará un botón para descargar el certificado en PDF, caso contrario, si fue rechazada, se incluirá la observación ingresada por el administrador sobre el motivo del rechazo.

### **2.7.3 Pruebas de Usuario**

Una vez realizado el primer prototipo en Figma, se procedió a hacer una prueba de

este con nuestro cliente, el cual procedió a hacer uso de las funcionalidades del prototipo y navego por todas las ventanas que se realizaron. Una vez revisado todo el prototipo, el cliente nos comentó sus observaciones y los cambios que debíamos hacer para mejorarlo y así tener el prototipo final. Las principales observaciones fueron:

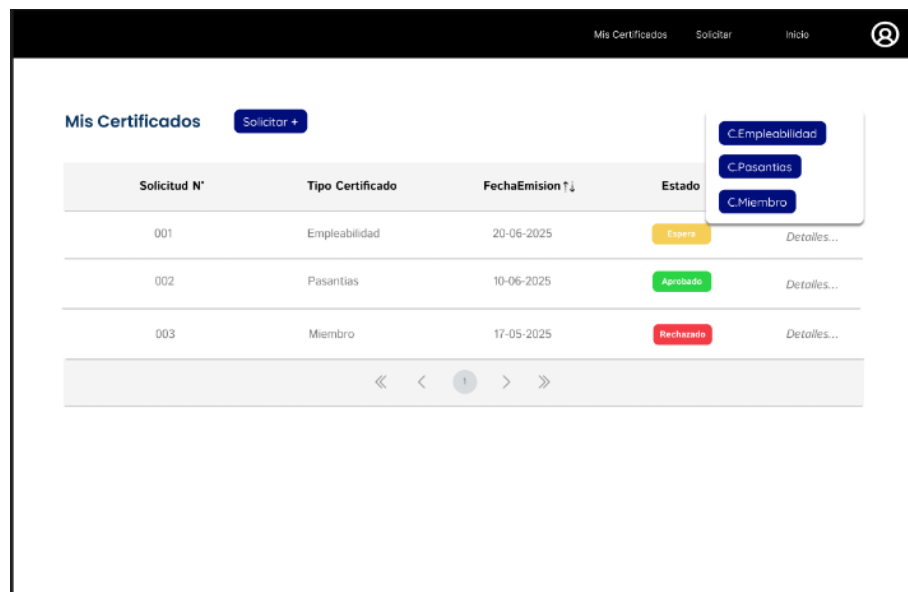
- Cambio en el diseño: El cliente decidió cambiar el esquema de color y la fuente del texto a utilizar, en cuanto al color, se decidió usar un color negro para la barra de navegación y en gris en algunas secciones de las tabla y recuadros.
- Información para mostrar: En la pestaña de aceptar o rechazar se decide cambiar la ubicación de la información a mostrar, además se decidió mostrar el botón de seleccionar la firma solo cuando se apruebe un certificado, también una opción para agrandar la vista previa del certificado a emitir. Finalmente, se decidió agregar el número de teléfono y el email del solicitante a la pestaña de aceptar o rechazar.
- Mayor cantidad de filtros: Inicialmente solo se había previsto ordenar las solicitudes por fecha, pero además se optó por agregar un filtro por tipo de certificado para mejorar la experiencia de usuario.
- Información de validación Qr: Por último, se decidió la información que mostraría la pestaña al validar un certificado a través del Qr, está cambiaría en base el certificado, pero tendría una plantilla base similar, de esta forma se asegura la correcta autenticación del certificado.

#### **2.7.4 Prototipo final**

En base a las observaciones del cliente se realizaron los cambios dichos anteriormente, y se terminó de diseñar las ventanas que faltaban. Además, se cambió la gama de colores de la aplicación y la fuente del texto que forma parte de esta.

**Figura 18**

*Prototipo final en Figma (ver solicitudes)*



**Figura 19**

*Prototipo final en Figma (validación QR)*



Como se observa en las figuras #18 y 19, en cuanto a las ventanas de usuario se agregó un filtro a la ventana de visualización de las solicitudes para filtrar por tipo de



[illegible]

Finalmente, como se ve en las figuras 20 y 21, para las ventanas del administrador, se agregó el mismo filtro de certificado a la ventana de visualización de las solicitudes pendientes del administrador. Además, se agregó una sección con la información de contacto del solicitante al momento de aprobar o rechazar una solicitud, de esta forma si el administrador tiene alguna duda u observación puede intentar contactar al solicitante directamente. También se cambió la disposición de las secciones en la misma ventana para que se muestre la información relevante primero.

Por último, se hizo que el botón de agregar firma solo aparezca cuando se vaya a aceptar una solicitud y se dio la funcionalidad de incrementar el tamaño de la vista previa del certificado para leerlo más detenidamente.

## Capítulo 3

## **3. Resultados y Análisis**

### **3.1 Plan de Implementación**

Para nuestro plan de implementación se realizó un Diagrama de Gantt, donde se fueron registrando las distintas actividades como reuniones, avances y tareas que se fueron realizando a lo largo del proyecto, además se incluye información como la fecha de inicio y fin, la carga de la actividad y los participantes de esta. El diagrama registró:

- Fecha de inicio y fin de cada tarea.
- Carga de trabajo estimada.
- Participantes responsables.

A continuación, se adjuntan capturas de las distintas secciones del diagrama de Gantt realizado:

#### **Sprint 0:**

Durante las primeras semanas se realizó lo que fue el Sprint 0, durante este periodo se realizó la descripción del problema, objetivos y necesidades del cliente, para definir estos puntos se realizaron varias reuniones tanto con el cliente como con nuestro tutor. Finalmente se realizó el capítulo uno del documento final donde se recopiló la información de este Sprint.

**Figura 22****Diagrama de gantt del sprint 0 (parte 1)**

<b>1 Sprint 0</b>					
1.1	Reunión con cliente 1 (Conocer al cliente, lo que esperan del proyecto y su punto de vista)	Nicolas Coronel, Alan Villavicencio	11/05/25	12/05/25	100 %
1.2	Firma de Acuerdo de Confidencialidad	Nicolas Coronel, Alan Villavicencio	13/05/25	15/05/25	100 %
1.3	Modificación de Ficha de Proyecto (Según las correcciones del tutor)	Alan Villavicencio	19/05/25	22/05/25	100 %
1.4	Planificación de Sprint 0	Nicolas Coronel	19/05/25	22/05/25	100 %
1.5	Reunión con el tutor 1 (revisión de las correcciones de la ficha)	Alan Villavicencio	20/05/25	20/05/25	100 %
1.6	Realización de portafolio en Noción	Nicolas Coronel	20/05/25	22/05/25	100 %
1.7	Objetivos, Descripción del Problema, Justificación del Borrador del Capítulo 1	Alan Villavicencio	20/05/25	22/05/25	100 %
1.8	Marco Teórico del Borrador del Capítulo 1	Nicolas Coronel	21/05/25	22/05/25	100 %
1.9	Reunión con el Cliente 2 (realización de preguntas y discusión de ideas)	Alan Villavicencio	22/05/25	22/05/25	100 %
1.10	Corrección del Capítulo 1 (mejorar marco teórico, objetivos) post reunion 2	Nicolas Coronel	26/05/25	29/05/25	100 %
1.11	Corrección del Capítulo 1 (mejorar descripción del problema y justificación) post reunion 2	Alan Villavicencio	26/05/25	29/05/25	100 %
1.12	Documentación de alcance y resultados esperados del sistema al finalizar el semestre	Nicolas Coronel	27/05/25	28/05/25	100 %
1.13	Reunion 3 con tutor	Nicolas Coronel	27/05/25	27/05/25	100 %
1.14	Correccion de la descripcion y justificacion el problema post reunion 3	Alan Villavicencio	23/05/25	27/05/25	100 %

**Figura 23**

**Diagrama de gantt del sprint 0 (parte 2)**

1.15	Corrección de objetivos y marco teorico del capítulo post reunion 3	Nicolas Coronel	23/05/25	27/05/25	100 %
1.16	Reunión con cliente 3	Alan Villavicencio	26/05/25	26/05/25	100 %
1.17	Corrección despues de retroalimentacion obtenida en clase	Nicolas Coronel, Alan Villavicencio	28/05/25	02/06/25	100%
1.18	Finalización del Capitulo 1	Nicolas Coronel, Alan Villavicencio	30/05/25	03/06/25	100 %
1.19	Reunion 4 con tutor	Nicolas Coronel, Alan Villavicencio	02/06/25	02/06/25	100 %
1.20	Realizacion de diapositivas para presentacion de capitulo 1	Nicolas Coronel, Alan Villavicencio	03/06/25	03/06/25	100 %
1.21	Grabacion de presentacion y edicion de video por parte de Alan Villavicencio	Nicolas Coronel, Alan Villavicencio	03/06/25	03/06/25	100 %
1.22	Elaboracion de planificacion del Sprint 1	Nicolas Coronel	04/06/25	06/06/25	100 %

**Sprint 1:**

Para el Sprint 1, como se observa en la figura #22 y #23 se realizaron las historias de usuario a trabajar para que el cliente las apruebe y paralelo a ello también se realizó el capítulo 2 del documento, el cual se basa en la metodología usada para el proyecto, aquí se incluyen los requerimientos, diagramas y toda información relacionada a cómo realizamos nuestra solución tecnológica.

**Figura 24***Diagrama de gantt del sprint 1(parte 1)*

2	Sprint 1				
2,2	Elaboracion de historias de usuario	Nicolas Coronel, Alan Villavicencio	06/06/25	10/06/25	100 %
2,3	Reunion con el cliente (Historias)	Nicolas Coronel, Alan Villavicencio	09/06/25	09/06/25	100 %
2,4	Correccion de las historias de usuario	Nicolas Coronel, alan Villavicencio	10/06/25	10/06/25	100 %
2,5	Elaboracion del primer borrador del capitulo 2	Nicolas Coronel, Alan Villavicencio	10/06/25	13/06/25	100 %
2,6	Definicion de reunion para pruebas de usuario y acceso a la base de datos	Nicolas Coronel, Alan Villavicencio	10/06/25	10/06/25	100 %
2,8	Elaboracion de primer prototipo de baja fidelidad	Nicolas Coronel, Alan Villavicencio	12/06/25	13/06/25	100 %
2,9	Reunion con cliente primer prototipo	Nicolas Coronel, Alan Villavicencio	16/06/25	16/06/25	100 %
210	Elaboracion de prototipo en figma	Nicolas Coronel, Alan Villavicencio	17/06/25	20/06/25	100 %

**Figura 25***Diagrama de gantt del sprint 1 (parte 2)*

2,11	Elaboracion del segundo borrador del capitulo 2	Nicolas Coronel, Alan Villavicencio	19/06/25	23/06/25	100 %
2,12	Pruebas de usuario	Nicolas Coronel, Alan Villavicencio	23/06/25	23/06/25	100 %
2,1	Correcciones del prototipo y finalizacion del capitulo 2	Nicolas Coronel, Alan Villavicencio	24/06/25	30/06/25	100 %
2,11	Preparacion de la presentacion del sprint 1, capitulo 2	Nicolas Coronel, Alan Villavicencio	27/06/25	30/06/25	100 %
2,12	Planificacion del Sprint 2	Nicolas Coronel	30/06/25	01/07/25	100 %
2,13	Reunion con cliente para visualizar cambio al prototipo	Nicolas Coronel, Alan Villavicencio	02/07/25	02/07/25	100 %

**Sprint 2:**

Para el Sprint 2, el cual se puede observar en la figuras #26 y #27 se realizó principalmente la implementación de la solución, primero se desarrolló el prototipo de la solución a realizara para que lo apruebe el cliente, luego se procedió a la implementación de la solución donde se realizó el proyecto en React para el frontend, Python/Flask para el

backend y se usó un servidor Wildfly para la implementación de las funcionalidades de FirmaEC, adicionalmente, se realizaron los capítulos 3 y 4 del documento.

**Figura 26**

*Diagrama de gantt del sprint 2 (parte 1)*

<b>3 Sprint 2</b>					
3.1	Obtener firma del capitulo 2 por parte del client	Nicolas Coronel, Alan Villavicencio	30/06/25	04/07/25	100 %
3.2	Avance del prototipo(Frontend Usuario)	Nicolas Coronel, Alan Villavicencio	03/07/25	08/07/25	100 %
3,3	Obtencion de acceso a la base de datos	Nicolas Coronel, Alan Villavicencio	09/07/25	09/07/25	100 %
3,4	Reunion para rubrica de calificacion de capitulo 2	Nicolas Coronel, Alan Villavicencio	09/07/25	09/07/25	100 %
3.3	Realizar el primer borrador del plan de evaluacion	Nicolas Coronel	09/07/25	15/07/25	100 %
3.4	Avance del prototipo 2 (Frontend Admin/Backend sistema de firma)	Nicolas Coronel, Alan Villavicencio	11/07/25	15/07/25	100 %
3.5	Realizar correcciones del plan de evaluacion	Nicolas Coronel	16/07/25	18/07/25	100 %
3.6	Avance del prototipo 3 (App del cliente)	Nicolas Coronel, Alan Villavicencio	16/07/25	22/07/25	100 %
3.7	Reunion con Tutor y Ingeniero de GTSI para discutir posibles soluciones para la firma electronica	Nicolas Coronel, Alan Villavicencio	18/07/25	18/07/25	100 %
3.8	Avance del borrador plan de evaluacion	Alan Villavicencio	23/07/25	24/07/25	100 %



**Figura 27**

**Diagrama de gantt del sprint 2 (parte 2)**

3.9	Elaboracion del primer borrador del capitulo 3	Nicolas Coronel, Alan Villavicencio	24/07/25	26/07/25	100 %
3.10	Avance del prototipo 4	Nicolas Coronel, Alan Villavicencio	24/07/25	28/07/25	100 %
3.11	Video de presentacion para el 5min speech	Nicolas Coronel, Alan Villavicencio	29/07/25	29/07/25	100 %
3.12	Video de historias de usuario realizadas y por realizar	Nicolas Coronel, Alan Villavicencio	30/07/25	30/07/25	100 %
3.13	Finalizacion del Capitulo 3 y primer borrador del capitulo 4	Nicolas Coronel, Alan Villavicencio	31/07/25	05/08/25	100 %
3.14	Finalizacion del capitulo 4	Alan Villavicencio	06/08/25	06/08/25	100 %
3.15	Elaboracion del poster	Nicolas Coronel	06/08/25	08/08/25	100 %
3.16	Finalizacion del documento y entrega de poster academico	Nicolas Coronel, Alan Villavicencio	08/08/25	19/08/25	100 %
3.17	Video de la presentacion de la solucion terminada	Nicolas Coronel, Alan Villavicencio	19/08/25	25/08/25	100 %
3.18	Video de la segunda version del 5 min pitch	Nicolas Coronel, Alan Villavicencio	25/08/25	25/08/25	100 %
3.19	Correccion del documento final	Nicolas Coronel, Alan Villavicencio	24/08/25	26/08/25	100 %

## 3.2 Pruebas

### 3.2.1 Pruebas de Usuario

Se realizaron pruebas con cinco usuarios divididos en tres roles clave (empleado, administrador, talento humano). Cada participante interactuó con el sistema en escenarios reales de uso y los hallazgos obtenidos fueron:

- Claridad en la navegación: los usuarios comprendieron rápidamente cómo solicitar, aprobar certificados.
- Seguridad: el acceso a funcionalidades restringidas se mantuvo protegido según el rol del usuario.
- Validación QR: todos los usuarios confirmaron que el proceso de verificación de autenticidad era rápido y confiable.

- La velocidad en la que se encuentra listo el certificado con el sistema es mucho mayor que la del proceso manual que se tenía. Esto con un promedio de 4 minutos por el proceso completo.

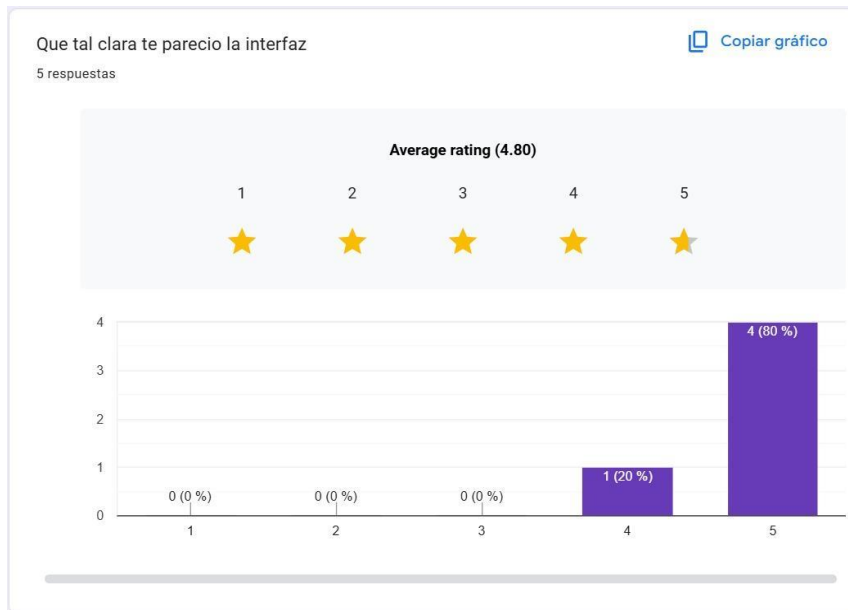
Los participantes navegaron a través de la aplicación, haciendo el proceso de:

- Generar una solicitud de certificado a través de una cuenta tipo usuario internos.
- Ver el estado de la solicitud creada en la solución.
- Verificar la notificación de la creación de la solicitud en el correo electrónico del solicitante y del administrador.
- Ingresar como usuario administrador y aceptar la solicitud generada.
- Firmar el certificado con la implementación de FirmaEC, ingresando el pem de la firma deseada junto a la contraseña.
- Descargar el certificado generado el cual fue enviado por correo electrónico junto a la notificación de que se aprobó la solicitud.

Finalmente, una vez completadas las pruebas, se les dio a los usuarios el acceso a un formulario en google forms para obtener retroalimentación sobre la experiencia de uso de la solución presentada.

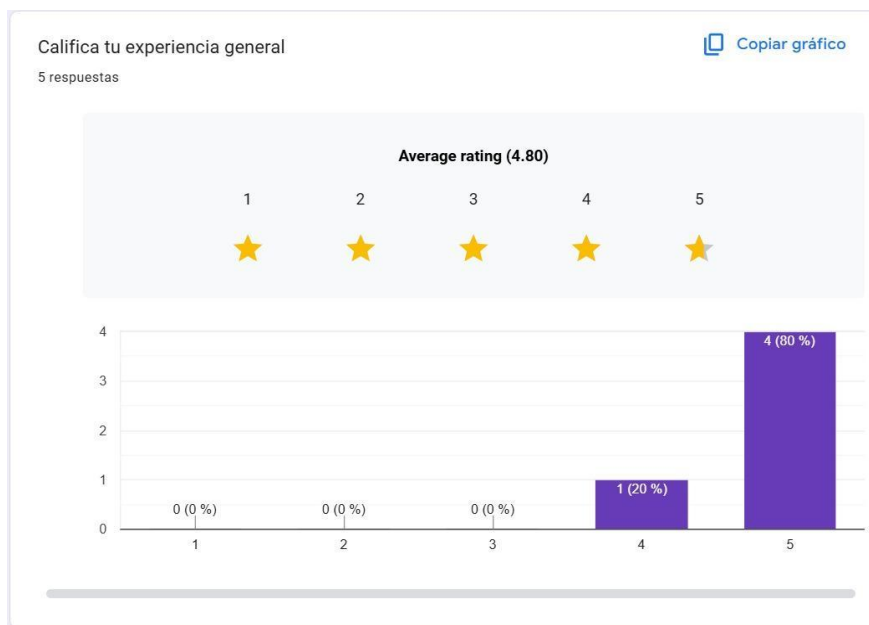
**Figura 28**

*Resultados del formulario post pruebas parte 1*



**Figura 29**

*Resultados del formulario post pruebas parte 2*



**Figura 30**

**Resultados del formulario post pruebas parte 3**

Que parte del proceso fue confusa o poco intuitiva?  
4 respuestas

- Ninguna
- No hubo ninguna
- Pude entender bien todo el proceso

Hay algo que mejorarías?  
5 respuestas

- No en realidad
- Nada
- Varios temas, se mencionaron en la demostración: Colores descriptivos, ajuste de aprobador delegado, cambios en temas de forma, entre otros
- No
- Me gustaría que se puedan firmar varios documentos a la vez, ya que ir de uno en uno es un proceso largo

**Figura 31**

**Resultados del formulario post pruebas parte 4**

Comentarios adicionales  
3 respuestas

- Excelente trabajo, tuvieron un buen nivel de abstracción para captar lo que se buscaba.
- Realizar lo sugerido
- Poder agregar que se firme la solicitud con una firma distinta a la del usuario logueado

**3.2.2 Aceptación del Proyecto**

Se realizó una reunión de validación funcional con el cliente y las personas que administrarán el sistema, en la cual se presentó el sistema funcional. Se destacaron los siguientes puntos:

- Reducción significativa del tiempo en la emisión de certificados
- Flujo de aprobación claro y seguro.

- Documentación clara y mantenible.

La solución fue aceptada como viable para la implementación en producción con cambios mínimos de color y diseño. el cliente y las personas del área de talento humano destacaron que la solución reduce significativamente el tiempo de la creación de una solicitud y del firmado de un certificado, según los tiempos tomados el día de las pruebas, todo el proceso tomaba en promedio 4 minutos de realizar, siendo 1 minuto y 30 segundos el promedio en crear y visualizar una solicitud y 2 minutos y medio el tiempo para firmar el certificado. También, se habló sobre posibles mejoras, tales como la firma masiva de documentos y la creación de solicitudes para personas fuera de la empresa. Finalmente, se hablaron de mejoras básicas en diseño y forma, las cuales se realizaron después de las pruebas.

### **3.3 Resultados**

#### **3.3.1 Interfaz de Usuario**

Las principales vistas implementadas fueron:

- Vista de Solicitud

Formulario con selección del tipo de certificado, motivo y campos autocompletados del usuario autenticado.

- Vista del Administrador

Listado de solicitudes pendientes, con opciones para revisar datos y aprobar o rechazar la generación del certificado, con integración de FirmaEC, donde se ingresa el archivo pem y su contraseña para realizar la firma del certificado.

- Vista de Certificados Emitidos

El empleado visualiza sus certificados en estado de pendiente, rechazado y aprobados, además de razones por las que el certificado fue rechazado o aprobado.

- Vista de Opciones

En esta vista se puede escoger las opciones de ver certificados, aprobar certificados y solicitar certificados. Estas interfaces fueron evaluadas con usuarios reales bajo criterios de claridad, navegación intuitiva y tiempos de respuesta.

### **3.2.2 Seguridad**

Se implementó autenticación basada en JWT para proteger los endpoints, garantizando que solo usuarios autorizados puedan:

- Registrar solicitudes (empleados y administradores)
- Ver y aprobar solicitudes (administradores)
- Descargar certificados emitidos (usuarios autenticados)

Además, al haber implementado FirmaEC en un servidor de forma descentralizada, la firma es hecha en un servidor propio, por ende, los datos sensibles como los archivos pem de las firmas y las contraseñas de estos están seguros.

## **3.4 Análisis de costos**

El equipo estuvo compuesto por 2 desarrolladores trabajando durante 14 semanas a 20 horas/semana, con un costo estimado de USD 700 mensuales por recurso.

- Costo por hora:  $\text{USD } 700 / 160 \text{ horas} = \text{USD } 4,38$ .
- Horas por recurso:  $14 \times 20 = 280 \text{ horas}$ .
- Costo por recurso:  $280 \times 4,38 = \text{USD } 1,226$ .
- Costo total:  $\text{USD } 2,452$ .

## **Capítulo 4**

## 4. Conclusiones y Recomendaciones

### 4.1 Conclusiones

- La solución tecnológica cumplió con el objetivo general propuesto, ya que cumplió con reducir el tiempo de emisión de certificados, logrando optimizar los procesos de creación y de firma, de esta forma, ayudando a mejorar la trazabilidad de estos. Esto se demuestra con los tiempos obtenidos en las pruebas realizadas y con la satisfacción de los usuarios al hacer uso de la solución.
- En base a la arquitectura adoptada para el desarrollo de la solución, se permite la integración de nuevas funcionalidades para mejorar aún más la solución a futuro, por ejemplo, la firma masiva de documentos para poder reducir aún más el tiempo de firma de los certificados.
- Se logró una automatización del proceso de firma de certificados, anteriormente, la firma de estos documentos se hacía a través de un proceso manual, donde los usuarios debían ir personalmente o por correo a solicitar el certificado deseado, para luego esperar días a que este sea tramitado. Ahora, gracias a la solución y a su sistema de notificaciones, los certificados se tramitan de forma más rápida y los usuarios tienen un mejor seguimiento del estado de su solicitud.
- Aunque la solución logró con el objetivo propuesto, se notó la limitación de usar firmaEC para el firmado de documentos, ya que se necesita tener instalada la aplicación de firmaEC para un correcto funcionamiento de la solución. También se destaca la falta de documentación para la implementación de firmaEC, lo cual complica el uso de esta.



## 4.2 Recomendaciones

- Se recomienda explorar otros métodos para realizar la firma de documentos, ya que, si estos son seguros y son más fáciles de implementar, pueden ayudar a hacer la solución más práctica y quitar la dependencia a la aplicación de firmaEC.
- Se recomienda también agregar más funcionalidades, el sistema de firmaEC permite implementar la firma masiva de documentos, lo cual ayudaría a reducir el tiempo que se usa para firmar los certificados al encargado correspondiente.
- Se recomienda realizar pruebas automatizadas para garantizar la estabilidad del sistema ante futuras actualizaciones, principalmente por parte del sistema de firmaEC. Así mismo, incluir un historial detallado de acciones (auditoría) para cada certificado emitido, con fecha, hora y usuario responsable, para a través de los datos obtenidos observar en que sector se puede optimizar más la solución.

## Referencias

- [1] ISO 15489-1:2001, "Information and documentation — Records management — Part 1: General," International Organization for Standardization, 2001.
- [2] S. K. Nielsen, "The implementation of an information system in a non-profit organization in a developing country," ResearchGate, 2009. [En línea]. Disponible en: <https://www.researchgate.net/publication/236953021>
- [3] M. Myers et al., "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP," IETF RFC 2560, 1999.
- [4] ITU-T Recommendation X.509, "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks," International Telecommunication Union, 2019.
- [5] E. Freeman and E. Robson, "Head First JavaScript Programming," O'Reilly Media, 2014.
- [6] J. Nielsen, "Usability Engineering," Morgan Kaufmann, 1993.
- [7] ISO/IEC 27001:2013, "Information technology — Security techniques — Information security management systems — Requirements," International Organization for Standardization, 2013.
- [8] Sertifier, "Case Study: The Power Business School," Sertifier Blog, 2022. [En línea]. Disponible en: <https://sertifier.com/blog/case-study-the-power-business-school/>
- [9] ChileAtiende, "Certificados - ChileAtiende," [En línea]. Disponible en: <https://www.chileatiende.gob.cl/temas/certificados>.
- [10] P. Kruchten, *The Rational Unified Process: An Introduction*, 3rd ed. Boston, MA, USA:

Addison-Wesley, 2004.

[11] I. Sommerville, *Software Engineering*, 10th ed. Boston, MA, USA: Pearson, 2015.

[12] P. Kruchten, “Architectural Blueprints—The ‘4+1’ View Model of Software Architecture,”

# Apéndices

## Apéndice A

### Manual de implementación de FirmaEC

A continuación, se mostrará una serie de pasos a realizar para lograr la implementación de FirmaEC de manera mas fácil, ya que uno de los problemas que encontramos al momento de desarrollar la solución, fue que la implementación de FirmaEC fue confusa y el manual ya existente en la web no da mucha información sobre la implementación. Aun así se considera que el manual ya existente es bueno para comprender como funcionan los métodos y proceso que se implementan.

#### Requisitos previos

- Descargar o clonar los repositorios de firmadigital-servicio, firmadigital-librería y firmadigital-api en su versión más reciente.
- Tener instalado Maven 3.8.9 o versiones similares, JDK 17, Wildfly en su versión más reciente y PostgreSQL 17

#### Pasos que seguir:

- En los repositorios de firmadigital hay pasos a seguir en el readme para compilar los elementos necesarios, en base a nuestra experiencia previa es mejor seguirlo de esta forma:
  1. Realizar pasos del readme de la librería, haciendo uso “mvn clean install” en una consola de comandos donde se esté en la dirección del repositorio descargado/clonado.
  2. Realizar los pasos del readme del servicio: “mvn clean package”
  3. Finalmente seguir los pasos del readme del api: “mvn clean package”

- Una vez logrado que tanto la librería, el api y el servicio estén compilados correctamente, en la carpeta “target” de tanto el servicio como el api se va a encontrar un archivo .war, por ejemplo: servicio.war y api.war. Estos archivos hay que separarlos ya que los usaremos después para levantar el servidor Wildfly
- Hay que localizar en la carpeta donde tenemos instalado los archivos de Wildfly el archivo “standalone.xml”, tendremos que ir a la carpeta “\standalone\configuration” y ahí encontraremos el archivo standalone.xml. En este archivo se encontrará la configuración del servidor.
- Este archivo se puede abrir con cualquier editor de código, aquí se debe agregar en la sección de “system-properties” debemos agregar una etiqueta “property” como variable global de esta forma:

```
<property name="firmadigital-servicio.url" value="ip-de-donde-se-levanta-el-servidor/servicio"/>.
```

- Antes de seguir es importante descargar un archivo .jar de Postgres, este puede ser el mas reciente, este archivo se lo ingresara en la carpeta de Wildfly dentro de “\modules\org\postgresql\main”. En el caso que las carpetas no existan hay que crearlas.
- Además del archivo .jar de postgres, hay que crear un archivo llamado “module.xml”, el cual debe tener dentro el siguiente código:

```
<?xml version="1.0" encoding="UTF-8"?>
<module xmlns="urn:jboss:module:1.1" name="org.postgresql">
  <resources>
    <resource-root path="postgresql-42.7.7.jar"/>
  </resources>
  <dependencies>
    <module name="javax.api"/>
    <module name="javax.transaction.api"/>
  </dependencies>
</module>
```

Nota: Cambiar la versión del .jar a la que haya sido instalada.

- Después, es necesario crear una base de datos en postgres la cual se comunicará con el api, esta puede llamarse de cualquier forma, una vez creada hay que agregar en la sección de “datasources” del archivo standalone.xml el siguiente código:

```
<datasource jndi-name="java:/FirmaDigitalDS" pool-name="FirmaDigitalDS">
    <connection-url>jdbc:postgresql://ip-bd-postgres/nombre-bd-
postgres</connection-url>
    <driver>postgresql</driver>
    <security user-name="user-de-bd-postgres" password="contraseña-bd-
postgres"/>
    <validation>
        <valid-connection-checker class-
name="org.jboss.jca.adapters.jdbc.extensions.postgres.PostgreSQLValidConnectionC
hecker"/>
        <exception-sorter class-
name="org.jboss.jca.adapters.jdbc.extensions.postgres.PostgreSQLExceptionSorter"/
>
    </validation>
</datasource>
<drivers>
    <driver name="postgresql" module="org.postgresql">
        <xa-datasource-class>org.postgresql.xa.PGXADatasource</xa-
datasource-class>
    </driver>
</drivers>
```

- Como siguiente paso, hay que agregar el archivo servicio.war y api.war a la ruta: “\standalone\deployments”.
- Luego, hay que abrir una consola de comandos donde este ubicado la carpeta “bin” de wildfly y usar el comando: “standalone.bat” para Windows y “standalone.sh” para Linux. Este comando levantará el servidor de Wildfly y se podrá usar los servicios de FirmaEC.
- Finalmente, en la base de datos creada en postgres, hay que insertar lo siguiente:  
INSERT INTO sistema(nombre,url,apikey,descripción) values ('nombre',

'http://ip/nombre', '\$API\_KEY\_HASH', 'nombre'), para esto hay que crear un apikey y luego encriptarlo con hash256.

El funcionamiento de los métodos de FirmaEC están descritos de forma entendible en el manual de implementación del propio FirmaEC.

## **Apéndice B**

### **Formularios de Evaluación**

- ¿Qué tan clara te pareció la interfaz? (1–5)
- ¿Qué parte del proceso fue confusa o poco intuitiva? (Respuesta abierta)
- ¿Hay algo que mejorarías? (Respuesta abierta)
- ¿Calificarías tu experiencia general? (1-5)
- Comentarios adicionales: (Respuesta abierta/opcional)

### **Formulario de observación (llenado por Nicolás Coronel)**

**Nombre del participante:**

**Rol:**

☐ Cliente      ☐ Empleado      ☐ Administrador

**Fecha:**

**Evaluador:** Nicolás Coronel

**¿El usuario comprendió fácilmente lo que debía hacer?**

☐ Sí      ☐ Parcialmente      ☐ No

**¿Se completó exitosamente la tarea?**

**Tiempo en que se completó la tarea asignada:**

Comentarios:

**¿El usuario pidió ayuda para completar alguna tarea?**

☐ Sí      ☐ No

Si respondió “sí”, ¿en qué parte?:

**Errores técnicos o de validación detectados durante la prueba:**

**Sugerencias del evaluador tras la observación:**



## Apéndice C

### Historias de Usuario

Tabla 1 Historias de Usuario

Identificador de la Historia	Rol	Característica	Razón	Criterio de Aceptación	Contexto	Evento	Resultado
Doc-user-001	Como un usuario interno	Necesito solicitar un certificado de empleabilidad	Con la finalidad de contar con la documentación oficial	Certificado de empleabilidad con sueldo	En caso de que el certificado requerido necesite incluir el valor del sueldo	Cuando seleccione la opción de solicitar certificado	El sistema generará una solicitud del certificado la cual se enviará al encargado correspondiente
				Certificado de empleabilidad sin sueldo	En caso de que el certificado requerido no necesite incluir el valor del sueldo	Cuando seleccione la opción de solicitar certificado	El sistema generará una solicitud del certificado la cual se enviará al encargado correspondiente
Doc-user-002	Como un usuario interno	Necesito validar la autenticidad del certificado	Con la finalidad de asegurarme que el certificado es legítimo	Validación <u>gr</u>	En caso de que se necesite validar la autenticidad y validez del certificado	Cuando se escanee el código <u>gr</u> del certificado	El sistema enviara al usuario a una página donde se muestre si el certificado es legítimo o no
Doc-user-003	Como un usuario interno	Necesito poder ver todos los documentos que he generado en forma de lista	Con la finalidad de evitar la pérdida de información	Lista de todos los certificados	En caso de que se requiera ver una lista de todos los certificados generados	Cuando se seleccione la opción de ver todos los certificados	El sistema desplegará en forma de lista todos los certificados generados
Doc-user-004	Como un usuario interno	Necesito poder ordenar la lista de los documentos que he generado	Con la finalidad de ver de una forma más ordenada los documentos	Ordenar por fecha de emisión	En caso de que se requiera ordenar los certificados por fecha de emisión para ver de forma	Cuando se seleccione la opción de ordenar por fecha	El sistema ordenará la lista de certificados por fecha de emisión

Doc-user-005	Como un usuario interno	Necesito poder descargar un certificado	Con la finalidad de poder tener el archivo para hacer uso del mismo	Descargar certificado	En caso de que se requiera descargar el archivo del certificado	Cuando se seleccione la opción de descargar el certificado	El sistema realizara una descarga del archivo en formato pdf
Doc-user-006	Como un usuario interno	Necesito poder visualizar el estado de mi solicitud	Con la finalidad de obtener información sobre una solicitud	Ver estado de solicitud	En caso de que se requiera visualizar si mi solicitud fue aprobada o no	Cuando se seleccione una solicitud	El sistema mostrara una ventana con más información de la solicitud, incluyendo su estado de aprobación, fecha emisión y que departament o está encargado de su aprobación.
Doc-admin-001	Como un administrador del sistema	Necesito poder aprobar o negar una solicitud	Con la finalidad de permitir o no que se genera un certificado	Aprobar un certificado	En caso de que se vaya a aprobar la solicitud	Cuando seleccione la opción de aprobar solicitud	El sistema generara el certificado solicitado con los datos del solicitante y permite su descarga
				Negar un certificado	En caso de que la solicitud tenga algún problema y no se pueda aceptar	Cuando seleccione la opción de negar solicitud	El sistema mostrara una caja de texto para ingresar la razón por la cual se negó el certificado
Doc-admin-002	Como un administrador del sistema	Necesito poder gestionar los roles de los usuarios	Con la finalidad de controlar el acceso y las funciones de cada rol	Asignar rol	En caso de que se registre un nuevo usuario	Cuando seleccione la opción de asignar rol	El sistema desplegara una lista con los roles para que el administrador seleccione uno de ellos

				Cambiar rol	En caso de que se requiera cambiar el rol a un usuario	Cuando seleccione la opción de cambiar rol	El sistema desplegará una lista para seleccionar el nuevo rol
Doc-user-007	Como un usuario interno	Necesito poder iniciar sesión con mis credenciales	Con la finalidad de poder acceder a las funciones del sistema	Login exitoso	En caso de que las credenciales de inicio de sesión sean correctas	Cuando seleccione la opción de iniciar sesión	El sistema permitirá al usuario ingresar al portal del sistema y usar sus funciones
				Login fallido	En caso de que las credenciales de inicio de sesión sean incorrectas	Cuando seleccione la opción de iniciar sesión	El sistema mostrará un mensaje de error y requerirá al usuario que revise sus credenciales
Doc-admin-003	Como administrador del sistema	Necesito poder visualizar todas las solicitudes que se han generado en el sistema	Con la finalidad de evitar la pérdida de información	Visualizar solicitudes	En caso de que se requiera ver todas las solicitudes	Cuando se seleccione la acción de visualizar todas las solicitudes	El sistema mostrará una lista con todas las solicitudes pendientes de aprobación
Doc-admin-004	Como administrador del sistema	Debo poder escribir en caso de que lo desee, por qué se negó la solicitud	Con la finalidad de dar una retroalimentación a la persona y dejar en constancia por qué se tomó esa decisión	Visualizar el motivo de negación	En caso de que quiera escribir por qué se negó la solicitud	Cuando se niegue una solicitud	El sistema mostrará una sección donde se pueda escribir la razón de porque se niega
Doc-user-008	Como un usuario interno	Necesito recibir una notificación por correo cuando se apruebe o rechace una solicitud	Con la finalidad de estar informado sin necesidad de revisar el sistema constantemente	Notificación por correo	En caso de que el encargado de la solicitud apruebe o rechace una solicitud	Cuando se actualice el estado de la solicitud	El sistema enviará una notificación por correo al solicitante
Doc-user-009	Como un usuario interno	Necesito recibir una notificación por correo	Con la finalidad de estar informado sin necesidad	Notificación por correo	En caso de que la solicitud se genere	Cuando se genere la solicitud	El sistema enviará una notificación por correo

		cuando se genere la solicitud	de revisar el sistema constantemente		correctamente		al solicitante
Doc-user-010	Como un usuario interno	Debo poder ver el motivo de la negación de mi solicitud en caso de ser necesario	Con la finalidad de saber por qué se negó la solicitud	Visualización en el sistema	En caso de que nieguen la solicitud	Cuando se niegue la solicitud	El sistema mostrara una sección con el motivo de la negación de la solicitud
Doc-admin-005	Como administrador del sistema	Necesito que me llegue un correo de que se generó una solicitud de certificado por aprobar	Con la finalidad de estar informado cuando se genera una solicitud pendiente de aprobación	Notificación por correo	En caso de que algún usuario interno genere una solicitud de certificado	Cuando se genera una solicitud de certificado	El sistema enviara una notificación por correo al administrador del sistema
Doc-admin-006	Como administrador del sistema	Necesito poder agregar más tipos de certificados	Con la finalidad de cumplir con diferentes requerimientos de entidades externas	Ampliación de tipos de certificados	En caso de que se necesite agregar otro tipo de <del>certificado</del>	Cuando seleccione la opción de "agregar certificado"	El sistema permite al administrador agregar la plantilla de otro certificado