Desarrollo e implementación de un sistema de gestión y verificación de historial laboral digital basado en Blockchain para la optimización del reclutamiento empresarial

Ricardo Muñoz Hoyos

Ing. Handry Orozco

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Ingeniería de Sistemas

Mayo 2026

CCAV Pitalito

Exclusión de responsabilidad

El contenido y el título de este documento han sido elaborados bajo criterios académicos y técnicos del programa de Ingeniería de Sistemas de la Universidad Nacional Abierta y a Distancia (UNAD). Los conceptos, ideas y opiniones expresados corresponden exclusivamente al autor, quien asume la responsabilidad por ellos.

La institución no se hace responsable por el uso indebido de la información presentada; cualquier implementación tecnológica o consecuencias derivadas recaerán exclusivamente sobre los ejecutores.

Ricardo Muñoz Hoyos

Autor

Programa de Ingeniería de Sistemas ECBTI – UNAD

Nota de Aceptación

Presidente del Jurado

Jurado

Dedicatoria

Quiero dedicar este proyecto con especial gratitud a mi familia. A mi madre, mi padre y mis hermanos. Su amor, apoyo incondicional y aliento constante han sido el eje fundamental que me ha permitido llevar a cabo este proyecto.

Agradecimientos

Quiero expresar mi más sincero agradecimiento a mi familia, especialmente a mis padres, por su apoyo incondicional y motivación constante durante el desarrollo de este proyecto. Asimismo, a la Universidad Nacional Abierta y a Distancia (UNAD) por proporcionar los recursos académicos, la formación y el entorno necesario para llevar a cabo esta investigación y contribuir al avance en tecnologías emergentes. Finalmente, a la música en especial al Rock, que siempre me acompañó durante las sesiones de trabajo, proporcionando la energía y el ritmo necesarios para mantener la concentración y la creatividad en cada línea de código.

Tabla de contenido

Lista de tablas

Lista de imágenes

Lista de diagramas

Resumen

En el entorno laboral actual, la verificación de historiales laborales representa un desafío crítico en los procesos de contratación, donde la falta de transparencia y eficiencia genera costos significativos para las organizaciones. El proyecto (RIMU) surge como una solución innovadora que aprovecha los principios de la tecnología criptográfica para transformar radicalmente la gestión de historiales laborales, ofreciendo un sistema seguro, verificable y resistente a manipulaciones.

La plataforma propuesta no solo optimiza los procesos de comprobación, sino que también establece un nuevo estándar de confiabilidad en la gestión de información profesional. Al implementar lógica de validación automatizada y segura junto a criptografía avanzada, RIMU garantiza la autenticidad de los registros laborales, reduciendo drásticamente el riesgo de fraude y manipulaciones.

La investigación se basa en un enfoque metodológico mixto que combina análisis cualitativos con profesionales de Recursos Humanos y evaluaciones cuantitativas del rendimiento del sistema. Los resultados preliminares indican mejoras significativas en términos de eficiencia operativa, reducción de costos de verificación y mayor transparencia en los procesos de contratación.

Este proyecto adquiere especial relevancia en el contexto de la transformación digital del sector de Recursos Humanos, donde la necesidad de soluciones confiables para la gestión de talento se ha vuelto prioritaria, por lo tanto, este no solo resuelve problemas inmediatos de verificación, sino que también sienta las bases para un ecosistema más justo y eficiente en la gestión de la información laboral, beneficiando tanto a empleadores como a profesionales en su trayectoria laboral.

Palabras clave: historial laboral, verificación de empleo, criptografía, gestión digital, contratación eficiente, transparencia.

Abstract

In today's work environment, verifying work histories presents a critical challenge in hiring processes, where a lack of transparency and efficiency incurs significant costs for organizations. The project (RIMU) emerges as an innovative solution that leverages the principles of cryptographic technology to radically transform the management of work histories, offering a secure, verifiable, and manipulation-resistant system.

The proposed platform not only optimizes verification processes but also establishes a new standard of reliability in managing professional information. By implementing automated and secure validation logic alongside advanced cryptography, RIMU ensures the authenticity of work records, drastically reducing the risk of fraud and manipulation.

The research is based on a mixed methodological approach that combines qualitative analysis with Human Resources professionals and quantitative assessments of system performance. Preliminary results indicate significant improvements in terms of operational efficiency, reduced verification costs, and increased transparency in hiring processes.

This project is particularly relevant in the context of the digital transformation of the Human Resources sector, where the need for reliable talent management solutions has become a priority. Therefore, it not only addresses immediate verification issues but also lays the groundwork for a fairer and more efficient ecosystem in managing labor information, benefiting both employers and professionals in their career paths.

Keywords: employment history, employment verification, cryptography, digital management, efficient hiring, transparency.

Introducción

Actualmente, el proceso de selección en el entorno laboral enfrenta retos considerables, especialmente en lo que respecta a la verificación del historial de los candidatos. Este proyecto se basa en la creación de un sistema innovador que utiliza la tecnología criptográfica para abordar las ineficiencias, imprecisiones y falta de transparencia de los métodos tradicionales de comprobación. Estas deficiencias pueden acarrear consecuencias negativas tanto para empleadores como para postulantes.

La verificación del historial laboral es esencial para establecer procesos de contratación que sean justos, ágiles y confiables. La creciente globalización de las organizaciones demanda métodos estandarizados que faciliten la interoperabilidad entre plataformas y aseguren el cumplimiento normativo en diversas jurisdicciones.

La adopción de un sistema de registro inmutable inspirado en la arquitectura blockchain tiene el potencial de revolucionar los procesos de contratación al mejorar la eficiencia, la transparencia y la seguridad. Esta tecnología permite la creación de un sistema de alta integridad e interoperable que facilita el intercambio seguro de datos laborales verificados entre diferentes plataformas y jurisdicciones.

Implementar este sistema en los procedimientos de verificación laboral no solo optimiza la eficiencia y la fiabilidad de los procesos de selección, sino que también establece las bases para sistemas más innovadores, sostenibles y centrados en el usuario. Un enfoque integral en el diseño e implementación de sistemas basados en blockchain es crucial para abordar los aspectos técnicos, sociales y legales involucrados, así como para prepararse ante los desafíos futuros del mercado laboral digital.

Planteamiento del Problema

El proceso de verificación del historial laboral es esencial en el reclutamiento, pero los métodos actuales carecen de transparencia y fiabilidad. Los enfoques tradicionales son manuales, lentos y propensos a errores humanos, lo que puede generar desconfianza entre empleadores y candidatos.

Esta falta de transparencia puede llevar a decisiones de contratación inadecuadas, mayor rotación de personal y costos adicionales para las empresas. Además, los departamentos de RR. HH. deben invertir tiempo y recursos significativos en la verificación manual.

Descripción del Problema

La problemática actual en la gestión de historiales laborales se manifiesta a través de múltiples dimensiones interconectadas que afectan la eficiencia, confiabilidad y seguridad de los procesos de validación. Estas dimensiones reflejan las limitaciones estructurales de los sistemas actuales y los desafíos que enfrentan las organizaciones al intentar verificar la experiencia laboral de manera efectiva. La complejidad de este escenario se ve agravada por la creciente movilidad laboral y la necesidad de validar experiencias profesionales adquiridas en diferentes contextos geográficos y organizacionales.

La problemática actual se manifiesta en tres dimensiones principales:

Dimensión Técnica.

- Falta de interoperabilidad entre los sistemas de gestión de recursos humanos de diferentes organizaciones.Arquitecturas obsoletas que no aprovechan las ventajas de las tecnologías modernas.
- Escalabilidad limitada para manejar volúmenes crecientes de verificaciones.

Dimensión Operativa

- Tiempos de respuesta prolongados en los procesos de verificación.
- Altos costos operativos asociados a la validación manual de documentos.
- Dificultad para auditar el historial de verificaciones realizadas.

Dimensión de Seguridad

- Riesgo de manipulación de la información laboral.
- Exposición de datos sensibles durante los procesos de verificación.
- Ausencia de trazabilidad en las modificaciones a los registros.

Antecedentes en la Gestión de Historiales Laborales

La evolución de los sistemas de gestión de historiales laborales ha estado marcada por una transición lenta desde formatos físicos hacia soluciones digitales parciales. A pesar de los avances tecnológicos, la mayoría de las organizaciones aún dependen de procesos manuales para validar la experiencia laboral. Esta situación se ha mantenido debido a la falta de estándares universales, la resistencia al cambio en las prácticas de recursos humanos y la ausencia de soluciones tecnológicas integrales que aborden las necesidades específicas de este ámbito. (Cambarieri M. V., 2024)

- **Antecedente 1:**

  Autor: (Nieto Ripoll, 2021)

  Año: 2021

  Lugar: Medellin, Colombia (Universidad EAFIT)

  Objetivo: Proponer un modelo de mejora para los procesos de selección y contratación de personal mediante el uso de la tecnología blockchain.

  Tecnología: Tecnología blockchain aplicada a recursos humanos.

Resultado: El estudio determinó que la implementación de blockchain permite optimizar el reclutamiento al aumentar la seguridad y la veracidad de la información suministrada por los candidatos.

- **Antecedente 2**

  Autor: (Cuello Velásquez, 2020)

  Año: 2020

  Lugar: Bogotá, Colombia (Universidad de los Andes)

  Objetivo: Analizar el uso de blockchain para optimizar la transparencia dentro de los procesos de contratación estatal.

  Tecnología: Blockchain.

  Resultado: Se concluyó que el uso de registros distribuidos previene de manera efectiva la manipulación de datos en las etapas de licitación y contratación pública.

- **Antecedente 3**

  Autor: (Gómez Almeyda, 2023)

  Año: 2023

  Lugar: Bogotá, Colombia (Universidad Distrital Francisco José de Caldas)

  Objetivo: Diseñar e implementar un prototipo basado en blockchain para la verificación automática de requisitos de grado.

  Tecnología: Prototipo basado en tecnología Blockchain.

  Resultado: Logró automatizar la validación de documentos académicos, asegurando la integridad de los certificados emitidos y reduciendo los tiempos de respuesta institucional.

- **Antecedente 4**

Autor: (Parada Gonzales, 2023)

Año: 2023

Lugar: Bucaramanga, Colombia (Unidades Tecnológicas de Santander - UTS)

Objetivo: Optimizar los procesos de contratación en instituciones públicas mediante el uso de contratos inteligentes.

Tecnología: Contratos inteligentes (Smart Contracts) basados en tecnología Blockchain.

Resultado: Demostró que la automatización de las cláusulas contractuales mediante código reduce significativamente los tiempos administrativos y mejora el cumplimiento legal de los acuerdos.

- **Antecedente 5**

  Autor: (Ligarreto Avendaño, 2024)

  Año: 2024

  Lugar: Bogotá, Colombia (Politécnico Grancolombiano)

  Objetivo: Estudiar el proceso de reclutamiento y selección implementando herramientas de inteligencia artificial en el sector retail.

  Tecnología: Inteligencia Artificial (herramienta Aira).

  Resultado: Se identificó una mejora notable en la eficiencia del filtrado de candidatos, aunque se recalca la importancia de la validación de datos para evitar sesgos en la contratación.

Antecedentes Internacionales

- **Antecedente 6**

  Autor: (Cambarieri M. V., 2024)

Año: 2024

Lugar: Viedma, Argentina (Universidad Nacional de Río Negro)

Objetivo: Explorar el potencial de las microcredenciales y blockchain para la transformación digital en la educación superior y la gestión de identidad en entidades públicas.

Tecnología: Tecnología Blockchain para la emisión y verificación de Microcredenciales.

Resultado: Se validó que blockchain facilita una gestión de identidad soberana y descentralizada, permitiendo que los certificados sean portables y verificables de forma global.

- **Antecedente 7**

  Autor: (Barrenechea L., 2020)

  Año: 2020

  Lugar: Lima, Perú (ESAN Business School)

  Objetivo: Desarrollar un modelo de negocio para un sistema de seguridad, respaldo y verificación digital para la gestión documental de notarías.

  Tecnología: Blockchain aplicado a la gestión documental.

  Resultado: El modelo propuesto garantizó el respaldo inmutable de documentos notariales, eliminando el riesgo de falsificación en trámites legales y administrativos.

- **Antecedente 8**

  Autor: (Fernández Gonzalvo, 2019)

  Año: 2019

  Lugar: Barcelona, España (Universitat Oberta de Catalunya - UOC)

Objetivo: Analizar la gestión soberana de identidades descentralizadas mediante el uso de blockchain.

Tecnología: Blockchain para la gestión de identidades descentralizadas.

Resultado: Propuso un marco donde el usuario tiene control total sobre sus atributos de identidad, permitiendo compartir información verificada de manera segura sin intermediarios.

- **Antecedente 9**

  Autor: (Gutiérrez Martínez, 2024)

  Año: 2024

  Lugar: Valladolid, España (Universidad de Valladolid)

  Objetivo: Crear ContractMe, una aplicación móvil basada en blockchain que simplifica la contratación y verificación mediante contratos inteligentes.

  Tecnología: Aplicación móvil basada en Blockchain y Smart Contracts.

  Resultado: La herramienta simplificó drásticamente el proceso de verificación de cumplimiento de contratos, permitiendo interacciones seguras y directas entre los actores involucrados.

- **Antecedente 10**

  Autor: (Vicente Valle, 2022)

  Año: 2022

  Lugar: Salamanca, España (Universidad de Salamanca - USAL)

  Objetivo: Desarrollar un sistema de verificación de certificados académicos basado en blockchain.

  Tecnología: Blockchain.

Resultado: El sistema permitió la validación automática de la autenticidad de títulos universitarios en tiempo real, eliminando la necesidad de procesos de verificación manuales lentos.

Análisis del Problema en la Gestión de Historiales Laborales

Estado Actual y Limitaciones

El actual manejo de historiales laborales presenta una desconexión entre la tecnología y la validación de experiencias. Las organizaciones dependen de documentos no estandarizados, lo que genera ineficiencias y largos tiempos de verificación, especialmente para empresas desaparecidas. La falta de estandarización dificulta la comparación y exposición a fraudes, además de que la gestión de consentimientos y protección de datos se convierte en un reto. La necesidad de un sistema centralizado es urgente para liberar recursos y mejorar la efectividad en Recursos Humanos. (Alvarracín Toledo, 2025)

Necesidades del Mercado Laboral

Debido a lo anterior, el mercado laboral actual exige soluciones rápidas para validar experiencias profesionales debido a la movilidad laboral. Las organizaciones deben verificar credenciales con eficiencia, especialmente en sectores regulados como salud y educación. La tendencia al trabajo remoto ha intensificado la necesidad de sistemas de verificación efectivos a nivel internacional. Las empresas buscan reducir costos en procesos de contratación y mitigar riesgos de información falsa, mientras que los profesionales demandan privacidad y control sobre sus datos. Este contexto presenta un desafío para los sistemas tradicionales, que deben adaptarse a una mayor diversidad e inclusión. (Cuevas Olarte, 2023)

Oportunidades de Mejora Mediante Principios de Inmutabilidad Blockchain

En contextos tecnológicos, la criptografía implementada con blockchain ofrece una solución innovadora para gestionar historiales laborales, permitiendo un registro inmutable y seguro. Su implementación elimina el riesgo de fraude documental mediante registros verificados y seguidos criptográficamente. Además, estas firmas criptográficas automatizan la verificación, reduciendo tiempos de respuesta de días a minutos y minimizando errores humanos. También permite generar credenciales verificables por medio de un identificador único, protegiendo datos personales y cumpliendo con normativas de protección de datos, como el GDPR en Europa y la LGPD en Brasil. (Fernández Gonzalvo, 2019)

Alcance del Problema

La problemática afecta a diversos actores y requiere soluciones flexibles que se adapten a las necesidades de organizaciones, desde pymes hasta grandes corporaciones, manteniendo consistencia y confiabilidad. (Cuello Velásquez, 2020)

Esta problemática afecta directamente a:

- Empresas y organizaciones que requieren validar el historial laboral de sus candidatos.
- Profesionales que necesitan demostrar su experiencia laboral de manera confiable.
- Instituciones educativas que deben verificar la experiencia profesional de sus egresados.

Impacto del Problema

El problema afecta la economía al incrementar costos, obstaculizar la movilidad laboral y generar desconfianza en contrataciones, acentuado por la globalización y la necesidad de verificación internacional. (Cambarieri M. V., 2024)

La persistencia de estos problemas genera consecuencias significativas:

Para las empresas:

- Mayores costos operativos en procesos de contratación.
- Riesgo de contrataciones inadecuadas por información laboral no verificable.
- Pérdida de productividad en los departamentos de RR. HH.

Para los profesionales:

- Dificultad para demostrar su experiencia laboral de manera confiable.
- Procesos de contratación más lentos y engorrosos.
- Exposición innecesaria de datos personales sensibles.

Para el mercado laboral:

- Ineficiencias sistémicas en la movilidad laboral.
- Desconfianza generalizada en los procesos de selección.
- Barreras para la validación transfronteriza de experiencias laborales.

Formulación del Problema

La formulación del problema surge de la necesidad de superar las limitaciones de los sistemas actuales mediante soluciones tecnológicas innovadoras. El desafío radica en desarrollar una plataforma que no solo resuelva las deficiencias existentes, sino que también establezca un nuevo estándar en la gestión de historiales laborales. Esta solución debe ser capaz de integrarse con los sistemas existentes, garantizar la máxima seguridad de la información y ofrecer una experiencia de usuario intuitiva para todos los actores involucrados. (Gómez Almeyda, 2023)

De esta manera, se plantea una gran incógnita, ¿De qué manera se puede optimizar la confiabilidad y los tiempos de respuesta en procesos de selección?

Solución Propuesta

La solución propuesta utiliza tecnologías de criptográficas y frameworks modernos, creando un ecosistema que mejora la gestión de historiales laborales, destacando por su transparencia, eficiencia y seguridad, sentando un nuevo estándar en el sector.

La implementación de RIMU aborda estas problemáticas mediante una solución integral que combina una variedad de tecnologías para garantizar la inmutabilidad y trazabilidad de los registros laborales.

- API RESTful con Django para un back-end robusto y escalable.
- Interfaz moderna con React/Next.js para una experiencia de usuario óptima.
- Arquitectura de microservicios para garantizar escalabilidad y mantenibilidad.
- Mecanismos de seguridad avanzados para la protección de datos sensibles.

Objetivos de la Investigación

General

Desarrollar un sistema de gestión y verificación de historial laboral digital mediante tecnologías web y criptográficas para optimizar la eficiencia y seguridad en los procesos de selección y/o contratación empresarial.

Específicos

Analizar los requerimientos técnicos y funcionales.

Identificar las necesidades críticas de los departamentos de Recursos Humanos y candidatos mediante el análisis de los datos recolectados en la fase diagnóstica, estableciendo las bases para el diseño del sistema.

Diseñar la arquitectura de seguridad y datos.

Definir la estructura de microservicios y el modelo de integridad documental basado en firmas digitales (Ed25519) y sellado de tiempo (RFC 3161) para asegurar registros únicos y verificables.

Desarrollar los módulos operativos de sistema.

Implementar las funcionalidades de gestión de empresas, perfiles de usuario y verificación criptográfica utilizando el stack tecnológico seleccionado (Django, React, PostgreSQL).

Validar la eficiencia y seguridad del sistema.

Evaluar el rendimiento técnico y la experiencia de usuario (UX) mediante pruebas controladas, comparando la reducción de tiempos y costos frente a los métodos tradicionales de verificación identificados en la investigación.

Justificación

La presente investigación se justifica por la necesidad de transformar la gestión de talento humano mediante tecnología que garantice la confianza y la eficiencia. El proyecto RIMU aborda esta problemática desde tres dimensiones fundamentales:

Justificación Teórica

Desde una perspectiva académica, este proyecto utiliza la criptografía para resolver el problema de la "información asimétrica" en la verificación laboral. Al implementar registros inmutables, se crea un sistema de reputación profesional basado en algoritmos seguros que eliminan la necesidad de depender de métodos tradicionales para validar la trayectoria laboral de un empleado.

Justificación Metodológica

La metodología utilizada en el desarrollo se centra en el diseño orientado al usuario, basado en metodologías ágiles lo que permite que la herramienta se adapte constantemente a las exigencias del mercado, esto tratando de garantizar un enfoque principal de "seguridad por defecto", que asegura la privacidad y protección de los datos personales y que estos no sean un dato extra, sino una parte esencial de la arquitectura del software. (Cambarieri M. V., 2024)

Justificación Práctica

La implementación de una solución para la verificación de antecedentes laborales ofrece beneficios tanto para empresas como para empleados. Para las empresas, disminuye significativamente los costos operativos asociados al reclutamiento, reduciendo el tiempo de contratación de días a horas. Esto les proporciona una ventaja competitiva en la captación de talento, especialmente en mercados laborales ajustados. (Fernández Infanzón, 2021)

Para los empleados, la solución les otorga más control sobre su información laboral, permitiéndoles compartir credenciales verificables de manera selectiva y segura. Esto es fundamental en un contexto de creciente movilidad laboral, ya que necesitan demostrar su experiencia en diferentes entornos. Además, reduce la duplicación en los procesos de verificación, ahorrando tiempo y recursos. (Bartolomeo, 2020)

En el ámbito del mercado laboral, la implementación de esta solución ayuda a reducir las asimetrías de información, mejorando el emparejamiento entre habilidades y necesidades de las empresas. Esto potencialmente incrementa la productividad, disminuye la rotación de personal y favorece la transparencia en la contratación. (Estrada Rivera, 2024)

Delimitación

De acuerdo con (Tamayo, 2004), la delimitación de la investigación permite establecer con claridad los límites temporales, espaciales, conceptuales y poblacionales del estudio para garantizar su viabilidad técnica y académica.

Delimitación especial

La investigación se centra en el contexto empresarial de Colombia, con un enfoque particular en las dinámicas de contratación del sector administrativo y tecnológico vinculadas al entorno del CCAV Pitalito de la UNAD. El desarrollo y las pruebas del sistema se realizan en entornos de infraestructura en la nube (Azure Cloud) accesibles de forma remota.

Delimitación temporal

El estudio y la recolección de datos primarios (fase diagnóstica) se llevaron a cabo en el periodo comprendido entre enero y marzo de 2025. El ciclo completo de desarrollo, implementación y validación técnica del sistema RIMU se extiende hasta octubre de 2025.

Delimitación conceptual

El proyecto se delimita teóricamente en el área de la Ingeniería de Software. Se centra específicamente en la aplicación de criptografía asimétrica (Ed25519), hashes de integridad (SHA-256 - SHA-512) y el estándar de sellado de tiempo (RFC 3161) para garantizar la inmutabilidad de registros laborales, sin incurrir en los costos de latencia de una red blockchain pública distribuida.

Delimitación poblacional

La población objeto de estudio para la validación de requisitos y pruebas de usuario está conformada profesionales activos y reclutadores. La muestra específica consta de 55 sujetos,

distribuidos en 50 postulantes a empleo y 5 reclutadores senior con experiencia en departamentos de Recursos Humanos.

Marco referencial

Marco Teórico

Fundamentos de Criptografía y Tecnologías de Registro Distribuido (DLT)

La seguridad de la información ha evolucionado de manera abrupta, ya no se trata solo de proteger los accesos externos, sino de garantizar que los propios datos sean confiables por diseño. RIMU se establece como una solución innovadora en la gestión de información, fundamentada en principios de descentralización, transparencia, inmutabilidad y seguridad criptográfica. Su arquitectura basada en la inmutabilidad y trazabilidad criptográfica permite la creación de registros permanentes y verificables sin la necesidad de una autoridad central, lo que la hace particularmente adecuada para aplicaciones que requieren altos niveles de confianza y trazabilidad. En el contexto laboral, la criptografía facilita la creación de un ecosistema donde múltiples actores pueden interactuar de manera segura, con la garantía de que la información registrada no puede ser alterada. (Barrenechea L., 2020)

Gestión Documental Digital

En la actualidad, la gestión documental ha evolucionado de ser un simple repositorio digital a sistemas avanzados que garantizan la autenticidad y disponibilidad de la información. En el entorno laboral, se enfrenta al reto de asegurar registros precisos a lo largo del tiempo, superando las limitaciones de los métodos tradicionales basados en papel o en formatos digitales no estandarizados. Por esta razón, el desafío actual en el entorno laboral no es solo almacenar el documento, sino demostrar matemáticamente que este no ha sido alterado desde su emisión. La convergencia entre la gestión documental tradicional y los estándares de sellado de tiempo (como RFC 3161) permite vincular un documento a un instante temporal exacto. (Fiaño Rodríguez, 2022)

Seguridad de Datos y Criptografía

La protección de la información sensible en RIMU se sustenta en el uso de criptografía asimétrica de alto rendimiento, específicamente mediante el uso de curvas elípticas (Ed25519). Este mecanismo permite establecer una autoría innegable: solo la empresa empleadora, poseedora de la clave privada, puede generar un certificado válido. Complementariamente, se utilizan funciones de resumen criptográfico (Hash SHA-512) para asegurar la integridad; cualquier cambio, por mínimo que sea en el documento, altera radicalmente su hash, evidenciando la manipulación de inmediato. Este enfoque garantiza confidencialidad, integridad y autenticidad sin la sobrecarga operativa de redes públicas. (Bartolomeo, 2020)

Marco Conceptual

Términos Clave

El marco conceptual del proyecto se articula en torno a conceptos fundamentales que definen su alcance y funcionalidad. La verificación de historiales laborales se refiere al proceso de confirmar la autenticidad y precisión de la experiencia profesional declarada por un candidato. La descentralización, principio rector de la tecnología blockchain, implica la distribución del control y la validación entre múltiples nodos independientes, eliminando la dependencia de una única entidad central. La inmutabilidad garantiza que, una vez registrada, la información no puede ser alterada sin dejar rastro, proporcionando así un nivel de confiabilidad en los registros. Asimismo, se ofrecerá a los usuarios soberanía sobre sus datos, lo que se refiere al derecho y la capacidad de los individuos para controlar el acceso y uso de su información personal, mientras que la transparencia verificable permite que las partes interesadas confirmen la autenticidad de la información sin comprometer la privacidad subyacente.

Modelos de Referencia

El proyecto se alinea con modelos de referencia establecidos en el ámbito de la gestión de Identidades Descentralizadas (DID) y las credenciales verificables. El modelo de confianza **basado** en blockchain permite la creación de un ecosistema donde empleadores, empleados e instituciones pueden interactuar con mayor eficiencia y seguridad. La arquitectura propuesta sigue un enfoque por capas, separando la infraestructura blockchain de las aplicaciones y servicios que interactúan con los usuarios finales. De esta manera, el modelo facilita la escalabilidad y adaptabilidad del sistema, permitiendo su integración con plataformas existentes de gestión de recursos humanos. Así, el enfoque de gobernanza distribuida asegura que ninguna entidad única tenga control absoluto sobre el sistema, fomentando la adopción generalizada y la confianza entre los participantes. (Cambarieri M. V., 2024)

Estándares Aplicables

La implementación del sistema se rige por un conjunto de estándares y normativas que garantizan su interoperabilidad, seguridad y cumplimiento legal. A nivel técnico, se adoptan estándares abiertos para la gestión de identidades descentralizadas (DID) y credenciales verificables del World Wide Web Consortium (W3C), asegurando la compatibilidad con otros sistemas en el ecosistema digital. En materia de seguridad, se siguen las mejores prácticas definidas por organizaciones como el Instituto Nacional de Estándares y Tecnología (NIST) y la Organización Internacional de Normalización (ISO), particularmente en lo relacionado con la gestión de riesgos de seguridad de la información y la protección de datos personales. El cumplimiento de regulaciones como el Reglamento General de Protección de Datos (GDPR) en Europa, la California Consumer Privacy Act (CCPA) en Estados Unidos y leyes locales de protección de datos en América Latina asegura que el sistema respete los derechos

fundamentales de privacidad y protección de datos de los usuarios. (Ver el capítulo 1: marco jurídico)

Marco Jurídico

Norma Internacional y Europea

Una de las referencias más sólidas a nivel mundial en protección de datos es el Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés), aplicable en todos los países de la Unión Europea desde mayo de 2018. Este reglamento establece principios fundamentales como:

- Licitud, lealtad y transparencia.
- Limitación de la finalidad del tratamiento.
- Minimización de datos.
- Exactitud y actualización.
- Limitación del plazo de conservación.
- Integridad y confidencialidad.
- Responsabilidad proactiva.

El GDPR también otorga a los ciudadanos derechos como el derecho al olvido, el derecho de acceso, portabilidad, rectificación y oposición al tratamiento de datos. Esta tecnología con su inmutabilidad plantea retos técnicos frente a algunos de estos derechos, especialmente el de supresión, por lo que el sistema deberá incorporar mecanismos técnicos como hashes no reversibles, enlaces off-chain y segmentación de datos que permitan un cumplimiento regulatorio aceptable.

Normativa en Estados Unidos

En Estados Unidos no existe una ley federal única de protección de datos equivalente al GDPR. Sin embargo, existen normativas sectoriales y estatales relevantes:

- **California Consumer Privacy Act (CCPA):** Otorga a los residentes de California derechos similares al GDPR, como el acceso, eliminación y control del uso de sus datos personales.
- **Health Insurance Portability and Accountability Act (HIPAA):** Protege la información médica en entornos laborales vinculados al sector salud.
- **Fair Credit Reporting Act (FCRA):** Regula el uso de información de antecedentes laborales y crediticios para fines de contratación.
- **Children's Online Privacy Protection Act (COPPA):** Protege los datos de menores en plataformas digitales.

Estas leyes enfatizan la necesidad de consentimiento informado, el derecho a conocer qué datos se recopilan, y la posibilidad de restringir o eliminar su uso. Estas se aplicarían al proyecto exceptuando inicialmente (COPPA) pues no se estarían almacenando datos de menores, puesto que en la mayoría de los países sería ilegal el uso de menores en empresas con finalidades laborales.

Normativas en América Latina

En América Latina, varios países han adoptado leyes similares al GDPR, consolidando el derecho a la privacidad y el uso responsable de datos personales. Puesto a que nos ubicamos en esta zona, debemos aplicar y acatar las leyes y directivas de cada uno de estos países en los que se podría desplegar el sistema:

- **Colombia:** Ley 1581 de 2012 y Decreto 1377 de 2013. Regulan el tratamiento de datos personales e imponen obligaciones claras sobre la autorización, finalidad y seguridad.
- **México:** Ley Federal de Protección de Datos Personales en Posesión de los Particulares (2010). Establece los principios de consentimiento, información, calidad, seguridad y responsabilidad.
- **Perú:** Ley N.º 29733 de Protección de Datos Personales. Incluye el consentimiento expreso y derechos ARCO (Acceso, Rectificación, Cancelación y Oposición).
- **Argentina:** Ley 25.326 de Protección de los Datos Personales. Reconocida por la UE como "adecuada" para transferencias de datos.
- **Chile:** Ley 19.628 sobre la Protección de la Vida Privada, actualmente en proceso de modernización para alinearse con estándares internacionales.

Normas Sobre Firma Electrónica y Evidencia Digital

Dado que el sistema propuesto incluye contratos inteligentes, es esencial considerar las regulaciones que dan validez legal a transacciones electrónicas:

- Ley Modelo de la CNUDMI sobre Comercio Electrónico y su versión sobre Firmas Electrónicas (2001).
- Reglamento eIDAS (UE): Define el marco de identificación y firma digital en la Unión Europea.
- ESIGN Act (Estados Unidos): Otorga validez legal a las firmas electrónicas y contratos digitales.
- Leyes nacionales de firma digital, como la Ley 527 de 1999 en Colombia o la Ley N.º 27269 en Perú.

Consideraciones Éticas y de Empleabilidad

Además del cumplimiento legal, el sistema debe considerar los principios de ética digital, garantizando que los datos laborales sean utilizados exclusivamente con fines legítimos, con consentimiento informado y bajo estándares de equidad, evitando su uso discriminatorio o indebido.

También deben respetarse las normas laborales vigentes en cada jurisdicción, que otorgan a los trabajadores el derecho de acceder, corregir y controlar la información que forma parte de su historial profesional, incluyendo leyes como:

- Código Sustantivo del Trabajo (CO). (Senado, 2025)
- Título III de la Ley Federal del Trabajo (mx). (Diputados, 2024)
- Código del Trabajo (cl). (Chile, 2002)
- Código del Trabajo (pe) (Perú, 2024)
- Ley de contrato del Trabajo (ar) (Argentina, 1974)

Metodología

El proyecto se desarrolla bajo un marco de Ingeniería de Software Aplicada, utilizando un ciclo de vida de desarrollo ágil. En este contexto, la investigación (de enfoque mixto) no se presenta como un estudio social independiente, sino como la fase de Elicitación de Requisitos y Diagnóstico Técnico. El objetivo de recolectar datos es fundamentar con rigor estadístico las decisiones de arquitectura del sistema RIMU, asegurando que cada funcionalidad responda a una falla técnica o de proceso identificada en el mercado. (Hernández-Sampieri, 2018) *Véase el campo Fases de Implementación*

Investigación Cualitativa

La investigación cualitativa, realizada entre enero y marzo de 2025, involucró entrevistas a 5 profesionales del sector de recursos humanos y reclutamiento. El 87% consideró ineficientes los métodos de verificación, con un promedio de 0.33 días para completarlos eso quiere decir que toma 8 horas en promedio diarios. Además, el 73% detectó casos de información laboral falsificada. Este tiempo podría ser redirigido hacia actividades más estratégicas, dada la dedicación del 30% del tiempo a la verificación manual.

Ficha Técnica

Para el componente cuantitativo, se definió un diseño no probabilístico por conveniencia, enfocado en actores clave del mercado laboral. A continuación, se detalla la ficha técnica del instrumento aplicado:

Tabla 1

Ficha Técnica de la Investigación

Concepto	Descripción
Universo	Profesionales activos y reclutadores en el sector tecnológico y administrativo.
Muestra (n)	55 sujetos (50 postulantes, 5 reclutadores senior).

Nivel de Confianza	95% ($\boldsymbol{Z = 1.96}$).
Margen de Error	$\pm$8% (Calculado bajo el supuesto de máxima indeterminación $\boldsymbol{p = q = 0.5}$).
Fecha de Campo	Enero - marzo 2025.
Instrumento	Encuesta estructurada de 10 preguntas cerradas (Véase, Anexo 1).

Hipótesis

El estudio se guio bajo las siguientes hipótesis de trabajo para validar la necesidad del sistema RIMU:

- **Hipótesis 1 (H_1):** Se acepta, dado que los resultados muestran que el 87% de los reclutadores tarda 8 horas o más, lo cual correlaciona ($r = 0.68$) con la pérdida de talento. Esto justifica técnicamente la implementación de una arquitectura de consulta en tiempo real.
- **Hipótesis 2 (H_2):** Se acepta, ya que la percepción de inseguridad y la detección de fraude (78%) superan el umbral planteado. Esto valida la necesidad de abandonar el formato PDF simple en favor de firmas criptográficas Ed25519.

Investigación Cuantitativa

El componente cuantitativo del estudio se basó en una encuesta aplicada a 5 profesionales de recursos humanos y 50 postulantes a empleo, realizada durante el primer trimestre de 2025. Los resultados cuantificaron el impacto de las ineficiencias en los procesos de verificación:

Tabla 2

Resultados Cuantitativos Consolidados

Indicador Evaluado	Resultado Promedio / Frecuencia	Impacto en el Negocio
Tiempo Promedio de Verificación	8 horas hábiles	Retraso crítico en contratación (Time-to-Fill).
Costo Unitario	$1.5 USD	Gasto operativo recurrente no recuperable.
Integridad de la Información	15% de CVs con discrepancias	Alto riesgo de contratación fallida.

Correlación (Demora vs Abandono)	$r = 0.68$ (Correlación Fuerte)	Evidencia estadística de que la lentitud hace perder posibles talentos.

El análisis estadístico mostró una correlación significativa ($r = 0.68,\ p < 0.01$) entre la duración del proceso de verificación y la tasa de abandono de candidatos. Además, se identificó que las empresas que implementaron soluciones tecnológicas parciales redujeron su tiempo de contratación en un 35% en comparación con aquellas que dependen completamente de procesos manuales.

Los datos obtenidos no solo evidenciaron las falencias del modelo actual, sino que dictaron los requerimientos funcionales específicos del sistema RIMU. La siguiente tabla detalla cómo cada hallazgo estadístico se tradujo en una característica del software:

Tabla 3

Hallazgo Estadístico y Solución Tecnológica

Hallazgo Cuantitativo	Dato Clave	Característica Implementada en RIMU	Justificación del Diseño
Lentitud en procesos	El 87% reporta demoras de cerca de un día hábil.	Verificación Instantánea (Real-time)	Se eliminó el flujo de revisión manual. El sistema valida hashes en milisegundos, reduciendo el tiempo de días a segundos.
Fraude Documental	El 78% ha encontrado discrepancias o documentos falsos.	Criptografía y Firma Digital (Ed25519)	Se implementó inmutabilidad. Ya no se confía en el PDF, sino en la firma criptográfica que garantiza que el documento no fue alterado.
Abandono de Candidatos	Tasa de abandono del 20% por demora.	Dashboard de Autogestión	Se diseñó una interfaz donde el candidato ya tiene sus documentos verificados *antes* de aplicar, eliminando el tiempo de espera durante la contratación.
Costos Operativos	Costo promedio de $1.5 USD por verificación manual.	Automatización de Consultas	Al usar una base de datos centralizada con acceso vía API, el costo marginal por verificación tiende a cero tras la implementación.

La conexión entre los hallazgos y la ingeniería del sistema no es solo funcional, sino de integridad de datos. El costo operativo de $1.5 USD detectado no se reduce simplemente por "ser digital", sino porque la arquitectura de RIMU elimina la necesidad de terceros validadores mediante el uso de hashes SHA-512. La solución responde directamente a la desconfianza del usuario: se sustituye la validación humana (lenta y falible) por verificación matemática inmutable, garantizando que el sistema sea una herramienta de ingeniería de alta confiabilidad y no solo una base de datos de consulta.

Análisis de Entrevistas

Tabla 4

Análisis de Entrevistas

Entrevistado	Cargo	Experiencia (año)	Promedio de Verificación (días)	Tasa de Discrepancias en CV	Nivel de Satisfacción (1-10)	Inversión en Verificación (USD/año)
1	Directora de Talento	7	3	20%	4	2100
2	Gerente de Reclutamiento	4	2	15%	6	2200
3	Especialista en Verificación	3	2	25%	3	2000
4	Jefe de RR. HH.	5	3	10%	6	1800
5	Reclutador	3	2	18%	5	1300
TOTAL		22	12	88,00%	4,8	9400

Nota. Resumen cuantitativo de las entrevistas realizadas.

Análisis de los Datos

Los datos recopilados muestran que los profesionales experimentados reportan menores tiempos de verificación, pero el sistema actual recibe una calificación promedio de 4.8/10. La inversión anual en estos procesos oscila entre $1,800 y $2,000 USD, y las tasas de discrepancia en CV son del 12%.

Ingeniería de software

La elección de esta línea de investigación, centrada en la ingeniería de software dentro de la rama de la Cadena de Formación en Sistemas, se aplica en este proyecto y sirve para abordar de manera sistemática los complejos desafíos asociados con la verificación de historiales laborales. Este enfoque disciplinado permite desarrollar una solución robusta, escalable y segura que integra tecnologías emergentes con sistemas empresariales existentes. La aplicación de principios de ingeniería de software asegura que el sistema cumpla con los más altos estándares de calidad, seguridad y usabilidad, al mismo tiempo que se mantiene dentro de los plazos y presupuestos establecidos.

Fases de Implementación

1. **Fase de análisis**

En la fase de análisis, se definirán objetivos, alcance y especificaciones del sistema. Se analizará la información de entrevistas, partes interesadas y se revisará la literatura existente para identificar soluciones y deficiencias que el nuevo sistema pueda abordar.

2. **Fase de diseño**

Durante la fase de diseño, se desarrollará la arquitectura del sistema y los flujos de trabajo. Se crearán especificaciones detalladas y se diseñarán interfaces de usuario intuitivas para

facilitar la navegación. También se elaborarán diagramas de flujo de datos para asegurar la captura, almacenamiento y verificación de información, garantizando transparencia y seguridad.

3. Fase de Implementación

La fase de implementación se centra en la codificación y el desarrollo del sistema, convirtiendo el diseño en una aplicación funcional. Se usarán metodologías ágiles que permiten pruebas iterativas y retroalimentación continua. Además de esto, análisis periódicos que ayudarán a resolver problemas rápidamente. También, se integrarán funciones críticas como la verificación de identidad, cifrado de datos y control de acceso, asegurando la protección de información confidencial contra accesos no autorizados y fraudes.

4. Fase de prueba

Una vez construido el sistema, se comenzará la fase de prueba, que incluye:

- Pruebas de control de calidad
- Pruebas unitarias
- Pruebas de integración
- Pruebas de aceptación del usuario (UAT)

Además, se realizarán pruebas de seguridad utilizando técnicas de penetración para identificar vulnerabilidades y asegurar la protección de los datos del usuario en el sistema.

5. Fase de evaluación

Finalmente, en la fase de evaluación, se recopilará la opinión de usuarios mediante encuestas y entrevistas para medir su satisfacción. Además, se analizarán métricas de rendimiento, como el tiempo utilizado en procesos antes y después de la implementación. Esta evaluación no solo medirá el éxito, sino que también proporcionará información valiosa para

futuras mejoras, garantizando así la relevancia y eficacia del sistema en un mercado laboral en constante evolución.

Stack Tecnológico

Back-end

- **Lenguaje:** Python 3.11
- **Framework:** Django 4.2
- **Base de datos:** PostgreSQL 15
- **Caché:** Redis 7.0

Front-end

- **Aplicación web:** React 18 con TypeScript
- **Framework UI:** Material-UI v5
- **SSR:** Next.js

Infraestructura

- **Contenedores:** Docker 23.0
- **Orquestación:** Kubernetes 1.27
- **CI/CD:** GitHub Actions

Seguridad

- **Autenticación:** OAuth 2.0 + OpenID Connect
- **Cifrado:** AES-256 para datos en reposo, TLS 1.3 para datos en tránsito

Fundamentación Teórica

Análisis de la Tecnología Blockchain y su Adaptación Arquitectónica

Para comprender el proceso y la arquitectura adaptada en RIMU, es necesario desglosar la tecnología Blockchain no como un bloque monolítico, sino como un conjunto de herramientas criptográficas y de red, que en si en el conjunto es cómo funciona esta tecnología. A continuación, se explanan los elementos fundamentales que componen este ecosistema tecnológico y se especifica la selección arquitectónica y de herramientas propias aplicadas en este proyecto.

Elementos y Herramientas del Ecosistema Blockchain

La tecnología Blockchain integra múltiples disciplinas (criptografía, redes, teoría de juegos) a través de las siguientes herramientas:

- **Distribución Descentralizada (P2P):** Red de nodos pares donde la información se replica globalmente, eliminando el punto único de fallo.
- **Inmutabilidad:** Característica garantizada por funciones hash que impide la modificación de registros históricos.
- **Criptografía Asimétrica:** Uso de pares de claves (Pública/Privada) para firmar transacciones y validar identidades sin revelar secretos.
- **Protocolos de Consenso:** Mecanismos (PoW, PoS, Raft) para que nodos desconectados acuerden una "verdad única" sin un administrador central.
- **Transparencia y Trazabilidad:** Capacidad de auditar el historial completo de un activo desde su origen.
- **Contratos Inteligentes (Smart Contracts):** Código autoejecutable que automatiza acuerdos entre partes sin intermediarios.

- **Tokenización:** Representación digital de valor o utilidad (fungibles o no fungibles).
- **Árboles de Merkle (Merkle Trees):** Estructura de datos que permite verificar la integridad de grandes volúmenes de información de manera eficiente mediante hashes.
- **Sellado de Tiempo (Timestamping):** Registro cronológico inalterable que prueba la existencia de un dato en un momento específico.
- **Interoperabilidad y Oráculos:** Puentes que permiten a la cadena comunicarse con el mundo exterior u otras cadenas.

Justificación de la Arquitectura de Integridad Selectiva Para RIMU

De acuerdo con las anteriores herramientas o elementos propios que integran el ecosistema de Blockchain se realiza la siguiente selección de herramientas a usar en el sistema propuesto.

El proyecto adopta una arquitectura de integridad selectiva. En lugar de replicar una blockchain completa (con sus costos de "gas" y latencia), extraemos las herramientas de seguridad críticas y las implementamos sobre una infraestructura de alta eficiencia.

Tabla 5

Selección de Elementos y Tecnologías Para la Construcción de RIMU

Herramienta Blockchain	Estado en RIMU	Justificación Técnica
Criptografía (Firmas)	ACTIVO	Se implementa el estándar Ed25519 (PyNaCl) para firmas digitales, garantizando que solo el dueño de los datos (empresa/empleado) pueda autorizar registros.
Inmutabilidad	ACTIVO	Se utilizan cadenas de Hashes (SHA-512) para vincular registros; cualquier alteración en un historial rompe la cadena de verificación matemática.
Sellado de Tiempo	ACTIVO	Implementación del estándar RFC 3161, actuando como un notario digital que certifica el "cuándo" de cada verificación.

Trazabilidad	ACTIVO	Registro de auditoría criptográfica que permite seguir el ciclo de vida completo de un documento.
Árboles de Merkle	ACTIVO	Se utiliza una estructura simplificada de hash-linking para verificar la integridad del historial laboral completo de un usuario.
Distribución (Nodos)	DESCARTADO	Se opta por una arquitectura centralizada para garantizar respuestas en milisegundos y costo cero por transacción para el usuario.
Consenso / Minería	DESCARTADO	No se requiere minería (Proof of Work) ya que la confianza recae en la criptografía y la autoridad de la plataforma, no en mineros anónimos.

Requisitos y Viabilidad

Requisitos Funcionales

Módulo de Empresas

El módulo de empresas está diseñado para permitir a las organizaciones gestionar eficientemente la verificación de historiales laborales. Este componente permite a los empleadores registrar su organización en la plataforma, proporcionando información corporativa verificable y documentación legal que valide su existencia y operatividad. Una vez autenticadas, las empresas pueden emitir certificados laborales digitales para sus empleados actuales o anteriores, los cuales se registran de forma inmutable en el sistema. Además de esto, la plataforma ofrece herramientas para gestionar solicitudes de verificación, donde los empleadores pueden aprobar o rechazar peticiones de acceso a la información laboral de sus exempleados, manteniendo un registro transparente de todas las interacciones.

Módulo de Empleados

Este módulo está centrado en el trabajador y cualquier persona del común, proporcionándole control total sobre su información profesional, en este los usuarios pueden crear un perfil personal que incluye su historial laboral, habilidades, certificaciones y logros profesionales. La plataforma permite a los empleados solicitar a sus empleadores actuales o anteriores que emitan certificados laborales digitales, los cuales se visualizan de forma segura en su perfil. Un aspecto clave es el sistema de consentimiento, donde los empleados pueden otorgar o revocar permisos para que empleadores específicos accedan a su información, con la posibilidad de establecer límites de tiempo para dichos accesos. Los usuarios reciben notificaciones en tiempo real sobre cualquier acción relacionada con sus datos, incluyendo intentos de verificación, emisión de nuevos certificados o actualizaciones de información. La

interfaz intuitiva permite a los empleados mediante un dashboard visualizar su trayectoria profesional de manera cronológica, con la capacidad de exportar su historial en formatos estandarizados para su presentación a empleadores potenciales.

Gestión de Documentos

El sistema de gestión documental proporciona un back-end seguro para almacenar y administrar documentos relacionados con el historial laboral. La plataforma soporta diferentes formatos de archivo, entre los que se destaca el formato PDF y DOCX, además utiliza algoritmos de búsqueda aplicada en los dashboards, especialmente en el módulo de empresas que sirven para la extracción automática de datos relevantes. Los documentos se almacenan de forma cifrada en la plataforma, garantizando su integridad y disponibilidad permanente. Además de esto, el sistema mantiene un registro detallado de auditoría que documenta todas las interacciones con cada documento, incluyendo visualizaciones, descargas y modificaciones.

Requisitos no Funcionales

Rendimiento y Escalabilidad

La plataforma está diseñada para manejar un alto volumen de transacciones simultáneas sin comprometer el rendimiento. El tiempo de respuesta promedio para las operaciones críticas no excederá los dos segundos, incluso durante períodos de carga máxima. La arquitectura distribuida del sistema permite escalar horizontalmente para adaptarse a un crecimiento en el número de usuarios y documentos gestionados. Se implementarán mecanismos de caché (Redis Cache) y balanceo de carga para optimizar el rendimiento en diferentes condiciones de uso. También, la base de datos está optimizada para realizar consultas complejas de manera eficiente, garantizando tiempos de respuesta rápidos en todas las funcionalidades.

Seguridad y Privacidad

Como todo requisito en una plataforma distribuida digitalmente, la seguridad de la información de la que se provee es una prioridad fundamental en el diseño y mantenimiento del sistema. Se implementa cifrado de extremo a extremo para proteger los datos tanto en tránsito como en reposo. La autenticación de usuarios se realiza mediante múltiples factores, incluyendo la verificación tradicional, además de la verificación de email. Esto complementado con los controles de acceso basados en roles garantizan que cada usuario solo pueda acceder a la información estrictamente necesaria para sus funciones, además, la plataforma cumple con los principales estándares de protección de datos, incluyendo GDPR, CCPA y normativas locales aplicables.

Experiencia de Usuario

Algo tan importante como la seguridad de la plataforma también es la interfaz de usuario con la que el individuo autenticado podrá navegar por las distintas herramientas creadas y ofrecidas. En este caso, la UI ha sido diseñada siguiendo principios de diseño centrado en el usuario para garantizar una experiencia intuitiva y satisfactoria. La interfaz se adapta automáticamente a diferentes tamaños de pantalla, ofreciendo una experiencia óptima tanto en dispositivos móviles como de escritorio. Los flujos de trabajo están optimizados para minimizar el número de pasos necesarios para completar las tareas más comunes y también el sistema proporciona retroalimentación clara y oportuna al usuario sobre el resultado de sus acciones. Además de esto, La plataforma está disponible en múltiples idiomas y se adapta automáticamente a las preferencias regionales del usuario.

Requerimientos de Hardware y Software

Estos requerimientos están adaptados para entornos de alta productividad y disponibilidad.

Hardware

1. **Servidores de Producción**

- **Procesador:** Mínimo 8 núcleos físicos (16 hilos) por nodo, arquitectura 64 bits
- **Memoria RAM:** Mínimo 32 GB por nodo, preferiblemente 64 GB para entornos de alta disponibilidad

Almacenamiento:

- SSD NVMe de 500 GB para el sistema operativo y aplicaciones
- Almacenamiento distribuido de al menos 500 GB
- Sistema de respaldo en frío con capacidad para 1 TB

Red:

- Conexión de red dedicada de 1 Gbps (10 Gbps recomendado)
- Ancho de banda mínimo de 100 Mbps simétrico por nodo
- Red redundante con balanceo de carga

2. **Nodos de Validación**

- **Procesador:** 4 núcleos físicos (8 hilos) por nodo
- **Memoria RAM:** 16 GB por nodo
- **Almacenamiento:** SSD de 500 GB
- **Red:** Conexión estable con ancho de banda mínimo de 100 Mbps

3. **Estaciones de Trabajo para Administradores**

- **Procesador:** 4 núcleos (8 hilos) o superior

- **Memoria RAM:** 16 GB mínimo
- **Almacenamiento:** SSD de 512 GB
- **Monitores:** 1 monitor Full HD (1920x1080)

4. **Dispositivos Móviles (para acceso de usuarios)**
    - **Smartphones:** Android 10+ o iOS 14+ con al menos 4 GB de RAM
    - **Tablets:** Android 10+ o iPadOS 14+ con al menos 4 GB de RAM

Software

1. **Sistema Operativo de Servidores**
    - **Sistema Base:** Ubuntu Server LTS (última versión estable) o Red Hat Enterprise Linux 8+
    - **Contenedores:** Docker 28.3+ con Docker Compose 2.38+
    - **Orquestación:** Kubernetes 1.22+ para entornos de producción
2. **Back-end**
    - **Lenguaje:** Python 3.13+
    - **Framework:** Django 5.2+
    - **Bases de datos:**
        - PostgreSQL 17+ (base de datos relacional)
        - Redis 5.2+ (caché y colas)
    - **Servidor Web:** Nginx 1.18+ con uWSGI o Gunicorn
3. **Front-end**
    - **Engine:** Node.js 22.18+
    - **Framework:** React 18+ con TypeScript
    - **React framework:** Next.js 15.4+

- **Estilos:** Tailwind CSS 4.0+ con diseño responsivo
- **Navegadores:** Chrome, Edge, Brave Etc.

4. **Seguridad**
    - **Firewall:** Configuración de reglas de red restrictivas
    - **WAF:** Protección contra ataques web (ModSecurity)
    - **Cifrado:** TLS 1.3 para todas las comunicaciones
    - **Autenticación:** OAuth 2.0, soporte para MFA
    - **Monitoreo:** Herramientas de monitoreo de seguridad en tiempo real
5. **Herramientas de Desarrollo**
    - **Control de Versiones:** Git 2.50+
    - **Pruebas:** Jest

Estudio de Viabilidad

Económica

La implementación de la plataforma RIMU representa una inversión significativa con un retorno atractivo a mediano y largo plazo. El análisis de costos iniciales incluye el desarrollo del software, infraestructura tecnológica y gastos de implementación. Los costos operativos recurrentes abarcan el mantenimiento de la plataforma, actualizaciones de seguridad, soporte técnico y gastos de alojamiento en la nube que se requieran. El modelo de negocio propuesto se basa en una estructura de suscripción estable, donde las empresas pagan mensualmente en función del número de verificaciones realizadas, mientras que los trabajadores acceden de forma gratuita a las funcionalidades básicas, asimismo, el análisis de retorno de inversión (ROI) proyecta un período de recuperación de capital de 24 a 36 meses, considerando la reducción en costos operativos para las empresas usuarias, que podrían ahorrar hasta un 70% en procesos de

verificación manual. La escalabilidad de la solución permite un crecimiento sostenido sin incrementos proporcionales en los costos operativos, mejorando significativamente los márgenes con el aumento de la base de usuarios.

Técnica

Como se ha descrito a lo largo de esta lectura, la plataforma RIMU utiliza mecanismos criptográficos avanzados para garantizar la integridad, autenticidad y confidencialidad de los datos, abordando así los desafíos de seguridad y trazabilidad en entornos digitales. En lugar de depender de una arquitectura blockchain tradicional (que conlleva latencia y costos operativos altos), RIMU implementa una cadena de bloques lógica (Logical Blockchain). Esta arquitectura se fundamenta en primitivas criptográficas robustas basadas en PyNaCl, una biblioteca criptográfica moderna y segura derivada del proyecto NaCl (Networking and Cryptography Library, 2016).

PyNaCl proporciona un conjunto completo de herramientas criptográficas esenciales: permite la generación y verificación de firmas digitales mediante criptografía de curva elíptica (Ed25519), el cifrado simétrico de alta velocidad (como XSalsa20-Poly1305), y el cifrado asimétrico (por ejemplo, con Curve 25519 para intercambio de claves). Además, soporta funciones de hash criptográfico (SHA-512), autenticación de mensajes (HMAC), y mecanismos seguros de derivación de claves a partir de contraseñas (como scrypt), así como el hash seguro de contraseñas para proteger credenciales de acceso.

Complementariamente, RIMU incorpora timestamps criptográficos conforme al estándar RFC 3161, que permite sellar digitalmente la fecha y hora de creación o modificación de un documento, vinculando inequívocamente un hash del contenido a un instante temporal verificable. Este mecanismo, emitido por autoridades de tiempo confiables, aporta una prueba

irrefutable de integridad y cronología, esencial en escenarios de auditoría, cumplimiento regulatorio y resolución de disputas (Adams, C., Cain, P., Pinkas, D., & Zuccherato, R, 2001).

La combinación de PyNaCl y el protocolo RFC 3161 permite a RIMU asegurar los datos en reposo y en tránsito, sin necesidad de una cadena de bloques distribuida, logrando un alto nivel de seguridad con menor complejidad operativa. La integración con sistemas externos se realiza mediante API RESTful protegidas criptográficamente, y una capa de orquestación garantiza la interoperabilidad con estándares del sector. Además, la plataforma implementa identidades descentralizadas (DID), permitiendo a los usuarios mantener el control total sobre su información personal y decidir cuándo y cómo compartirla, reforzando así la privacidad y la soberanía digital.

Operacional

La implementación de RIMU seguirá una metodología ágil con lanzamientos incrementales para permitir la retroalimentación de los usuarios. Se prevé una fase piloto con un grupo específico de empresas y empleados para comprobar la usabilidad y el rendimiento. También ofrecerá soporte técnico, que estará disponible en horarios prolongados y a través de canales prioritarios para las empresas. La plataforma incluirá herramientas de monitoreo en tiempo real para gestionar incidencias; además, la migración de datos está planificada para provocar la menor interrupción posible, y el modelo de gobernanza establece roles, responsabilidades y la gestión de disputas.

Legal

La plataforma RIMU se fundamenta en el cumplimiento de normativas de protección de datos como el GDPR y la CCPA. Algunas de sus características incluyen:

- **Privacidad por diseño:** Incorporación de principios de privacidad en todas las capas del sistema.
- **Control de datos:** Los usuarios pueden gestionar sus consentimientos de manera detallada.
- **Contratos inteligentes:** Incluyen cláusulas que aseguran el cumplimiento automático de plazos de conservación y derechos de supresión.
- **Anonimización:** Implementa mecanismos para reducir riesgos en el tratamiento de datos.
- **Acuerdos de procesamiento:** Clarifican responsabilidades en el tratamiento de la información.
- **Gestión de derechos:** Herramientas eficientes para manejar solicitudes de acceso y otros derechos de los interesados.

Análisis Económico

Inversión Inicial

El desarrollo de RIMU requiere una inversión inicial significativa distribuida en:

- **Software:** 35% del presupuesto (diseño, programación e integración).
- **Infraestructura tecnológica:** 50% (servidores y servicios en la nube).
- **Implementación:** 10% (migración de datos y pruebas).
- **Capacitación y lanzamiento:** 5%.

Costos Operativos

Los costos operativos recurrentes se categorizan de la siguiente manera:

- **Infraestructura en la nube:** 40% del total.
- **Mantenimiento y actualizaciones de software:** 25%.

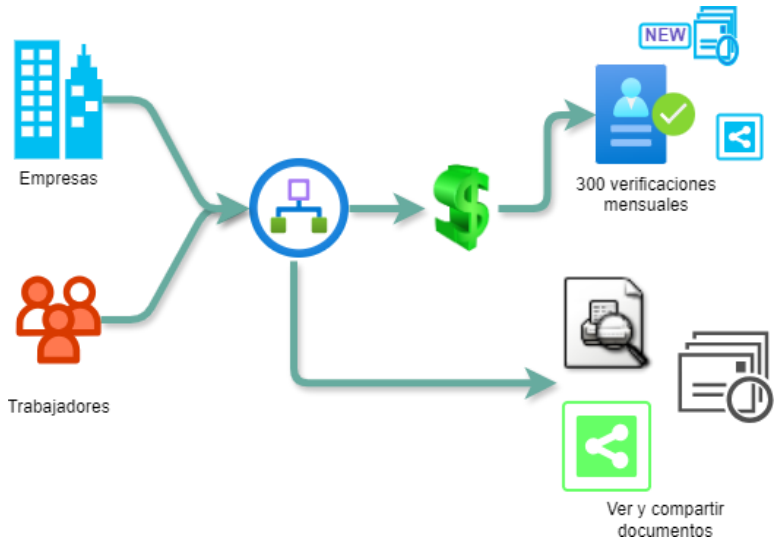
- **Soporte técnico y atención al cliente:** 20%.
- **Gastos administrativos y legales:** 15%.

Modelo de Ingresos

El modelo de ingresos se estructura en precios escalables, permitiendo a las empresas pagar una cuota mensual con límites de verificaciones y tarifas adicionales por excedentes. Se ofrecen descuentos por volumen para fomentar la adopción masiva. Los planes de suscripción mensual se adaptan a organizaciones con diversas necesidades, para lo cual requieren una suscripción premium, mientras que los trabajadores pueden acceder gratuitamente a funciones básicas de gestión de su perfil.

Imagen 1

Modelo de Ingresos



Nota: Imagen del modelo de ingresos de la plataforma RIMU. Fuente: autoría propia.

Análisis Técnico

Arquitectura del Sistema

La arquitectura de RIMU se fundamenta en microservicios, lo que garantiza escalabilidad y un mantenimiento autónomo de sus componentes.

Capas Principales

- **Capa de Presentación:** Aplicación web en React y React Native, asegurando una experiencia uniforme en dispositivos.
- **Capa de API:** Desarrollada en Python, gestiona y dirige solicitudes a microservicios.
- **Capa de Servicios de Negocio:** Implementa la lógica de la aplicación, incluyendo gestión de perfiles y reportes.
- **Capa de Almacenamiento:** Combina bases de datos relacionales y sistemas de archivos distribuidos.

Tecnología

La implementación, como se ha dicho anteriormente, es basada en blockchain, pero se fundamenta en un modelo de seguridad criptográfica moderna y verificación temporal confiable. En lugar de utilizar nodos distribuidos para alcanzar consenso, RIMU emplea primitivas criptográficas de alta seguridad proporcionadas por PyNaCl para garantizar la autenticidad, integridad y confidencialidad de todas las operaciones. Cada transacción o emisión de credencial se protege mediante firmas digitales Ed25519, asegurando que solo las entidades autorizadas puedan emitir o modificar datos.

La lógica de negocio como la emisión y comprobación de credenciales digitales se ejecuta a través de servicios back-end seguros, donde las operaciones críticas están protegidas con cifrado de clave pública y secreta. Los datos sensibles se cifran en reposo y en tránsito utilizando algoritmos como XSalsa20-Poly1305, mientras que los hashes criptográficos (SHA-512) generados con PyNaCl permiten verificar la integridad de cualquier documento en cualquier momento.

Para reforzar la trazabilidad y el respaldo temporal, RIMU integra timestamps criptográficos conforme al estándar RFC 3161. Cada documento o credencial importante es sellado por una Autoridad de Tiempo (TSA) certificada, vinculando su hash a un instante exacto y verificable. Este sello no solo prueba que el contenido existía en ese momento, sino que también es irrefutable frente a modificaciones posteriores, lo que lo convierte en un mecanismo esencial para auditorías, cumplimiento normativo y pruebas legales.

El sistema gestiona la identidad digital mediante claves criptográficas basadas en Curve 25519, utilizando pares de claves pública/privada que garantizan autenticación segura y eficiente, sin depender de infraestructuras pesadas como X.509. Los documentos (diplomas, certificados, etc.) se almacenan fuera del sistema (off-chain), mientras que sus hashes firmados digitalmente se registran en un índice seguro, asegurando integridad y detectando cualquier manipulación. Para esto se emplea verificación criptográfica atómica en lugar de consenso distribuido, cada operación incluye firma digital, hash y sello de tiempo, lo que permite su validación independiente por terceros, eliminando la necesidad de coordinación entre nodos, reduciendo latencia y complejidad, y manteniendo alta confianza, escalabilidad y audibilidad.

Seguridad y Privacidad

La seguridad es un pilar fundamental en el diseño de cualquier sistema, en particular en esta, se ha implementado múltiples capas de protección. Una capa de autenticación de usuarios se realiza mediante OAuth 2.0, lo que permite y a la vez soporta múltiples factores de autenticación. Los datos sensibles se cifran en tránsito (SHA256 o SHA512) y en reposo (AES-256), con gestión centralizada de claves mediante un HSM (Hardware Security Module). La privacidad se garantiza mediante técnicas de conocimiento cero (zero-knowledge proofs) que permiten verificar la validez de las credenciales sin revelar la información subyacente. El control

de acceso basado en atributos (ABAC) asegura que los usuarios solo puedan acceder a los recursos estrictamente necesarios para sus funciones. El sistema implementa técnicas avanzadas de detección de amenazas, incluyendo análisis de comportamiento para identificar actividades sospechosas.

Rendimiento y Escalabilidad

El rendimiento del sistema ha sido optimizado para manejar grandes volúmenes de operaciones simultáneas con una eficiencia superior a las soluciones blockchain tradicionales. La arquitectura basada en PyNaCl permite un procesamiento de operaciones significativamente más rápido, con pruebas de carga que demuestran capacidades que superan ampliamente los 10,000 TPS, gracias a la eliminación de la sobrecarga de consenso distribuido.

La arquitectura modular del sistema está diseñada para escalar de manera elástica según la demanda. A diferencia de las redes blockchain convencionales que requieren múltiples nodos para validar transacciones, RIMU utiliza firmas digitales de PyNaCl que permiten una verificación casi instantánea de la autenticidad de los datos. Este enfoque elimina los cuellos de botella asociados con el consenso distribuido, permitiendo un rendimiento lineal al aumentar la capacidad de procesamiento.

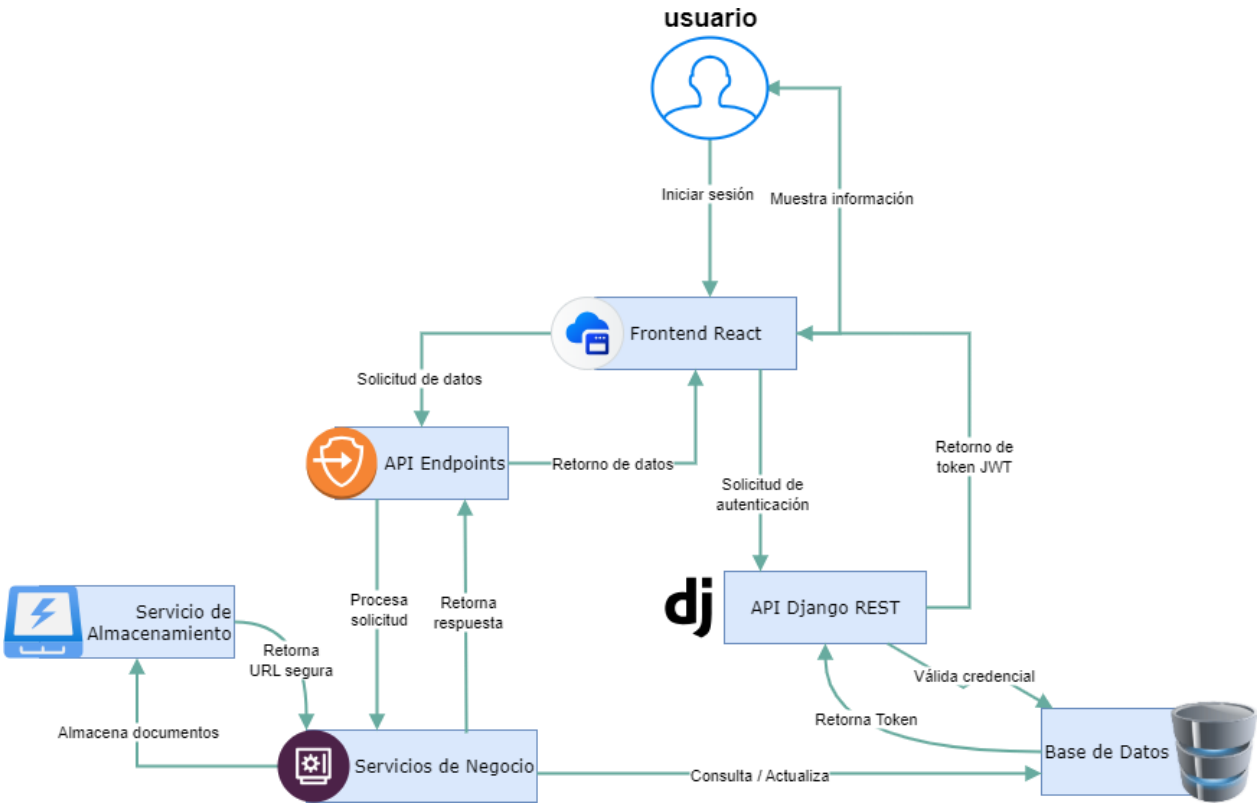
El sistema implementa una capa de caché en memoria optimizada para acelerar el acceso a los datos más frecuentemente consultados, incluyendo los hashes de comprobación y los metadatos de las credenciales. Esta implementación reduce significativamente la latencia en operaciones de lectura, manteniendo tiempos de respuesta inferiores a 100 ms incluso bajo cargas elevadas.

Arquitectura de Sistema

Diagramas de Flujo de datos

Diagrama 1

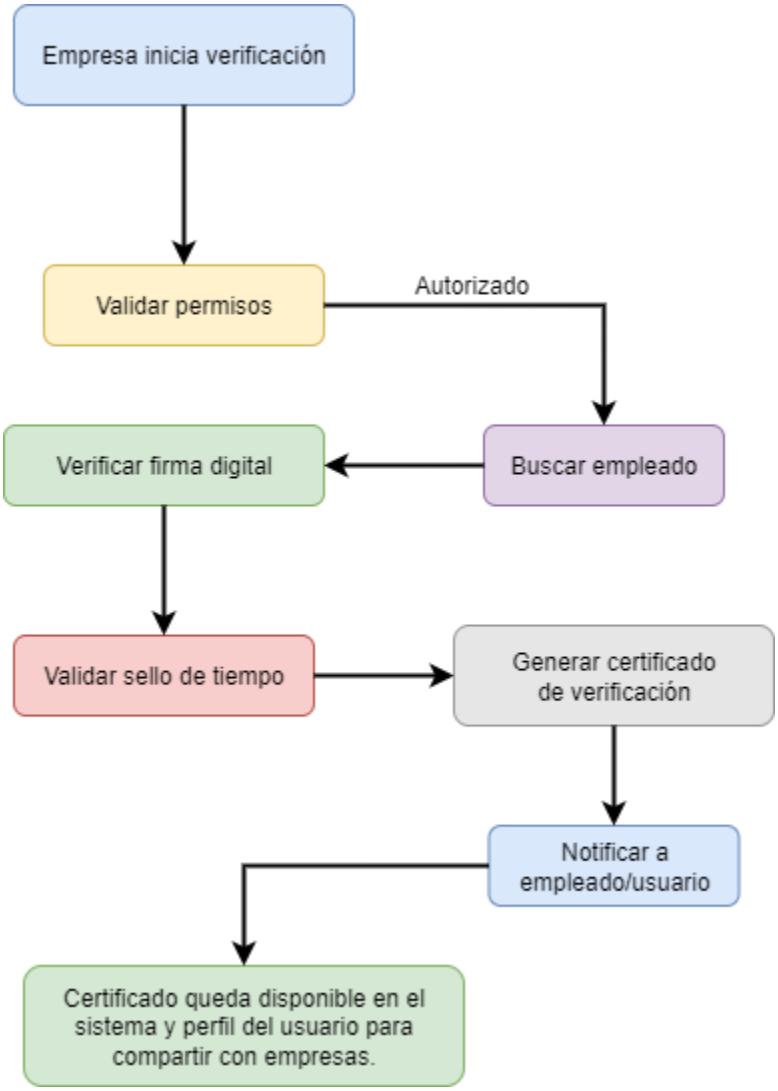
Flujo de datos del sistema



Nota: Ilustración gráfica del flujo del sistema. Fuente. autoría propia

Diagrama 2

Flujo de verificación de documentos

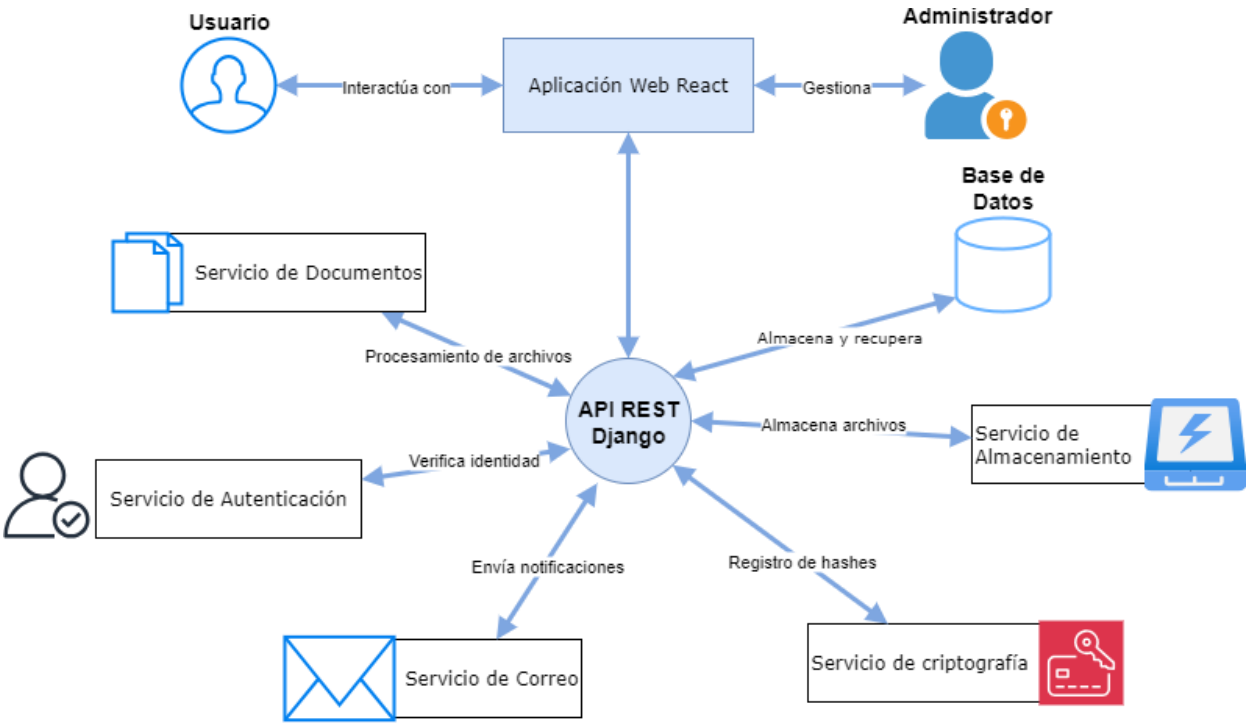


Nota: Flujo del sistema por medio de las empresas para la realización de la verificación de experiencias y documentos para cada empleado o usuario del sistema. Fuente: autoría propia,

Diagramas de Contexto

Diagrama 3

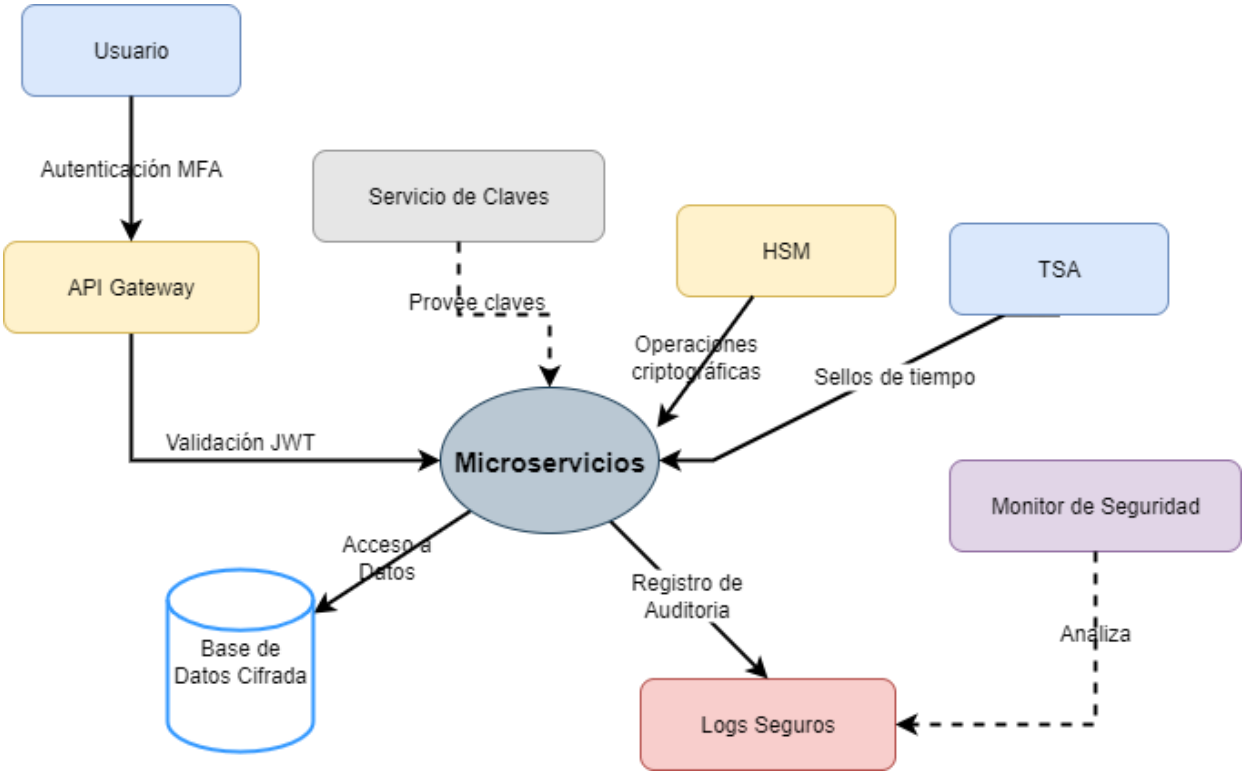
Diagrama de contexto



Nota: El presente diagrama ilustra los servicios disponibles administrados por un back-end de Django. Fuente. autoría propia.

Diagrama 4

Contexto de seguridad y microservicios

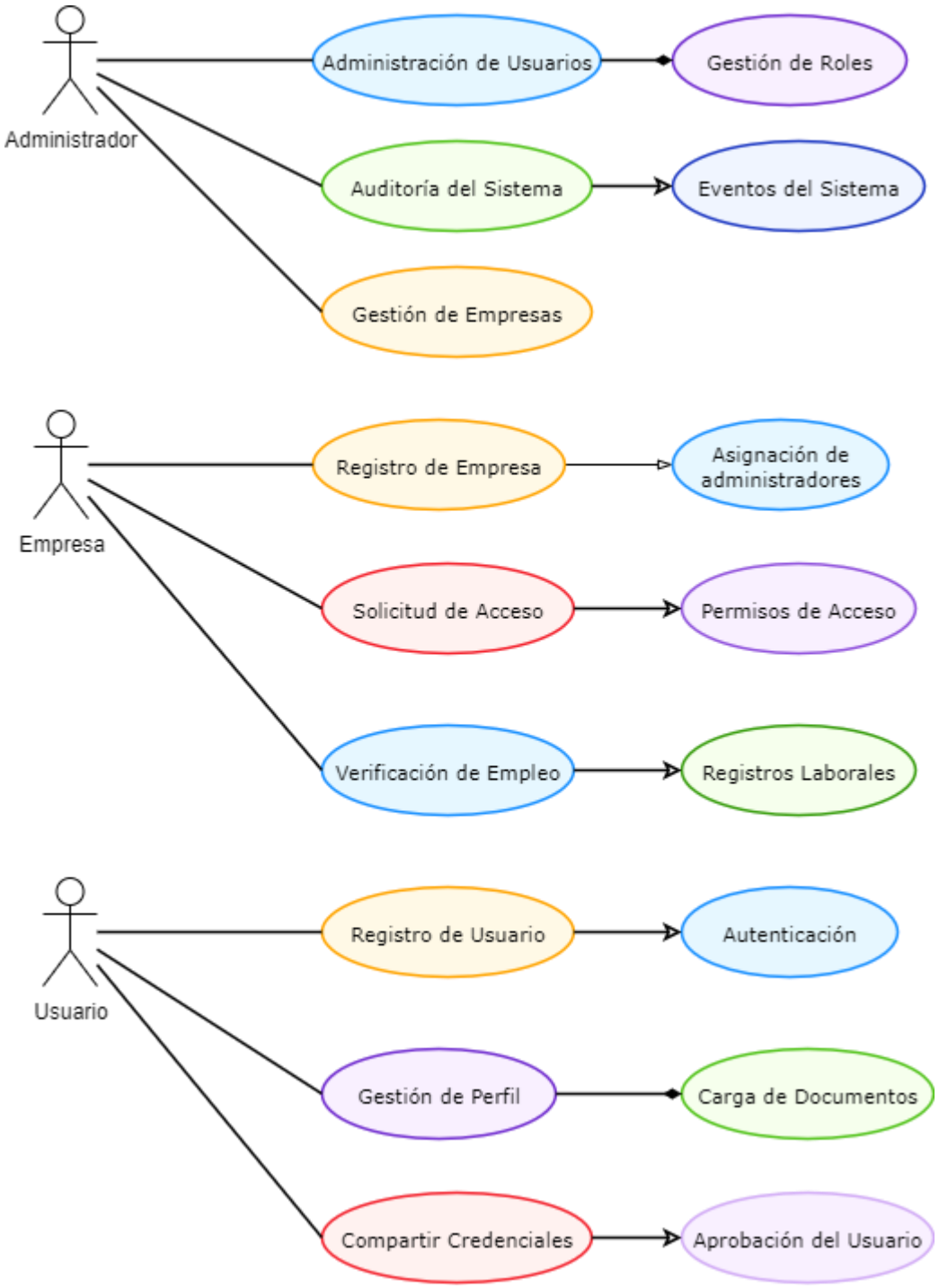


Nota: En la siguiente gráfica se pueden diferenciar los siguientes microservicios de la aplicación y sus respectivas normas de seguridad que cada una de ellas posee. Fuente: autoría propia.

Casos de Uso

Diagrama 5

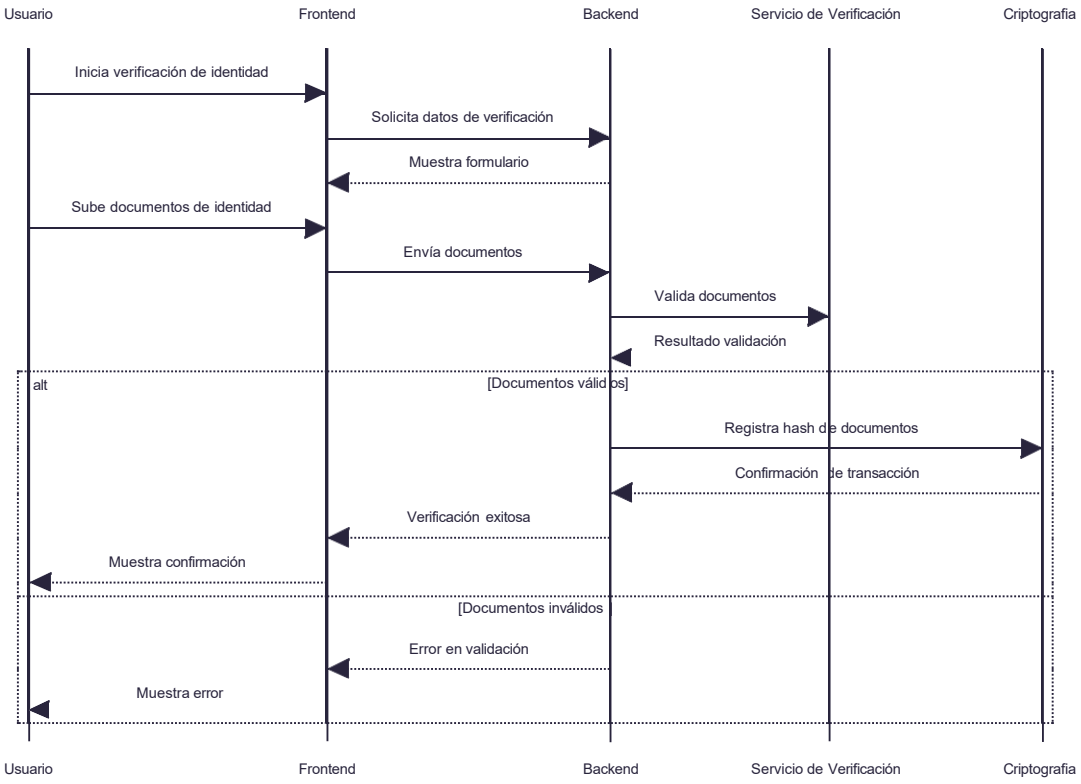
Diagrama de casos de uso del sistema



Nota: Actores y casos de usos para el sistema. Fuente. autoría propia.

Diagrama 6

Flujo de Verificación de Identidad



Nota: El diagrama muestra el flujo del sistema para la comprobación de identidad y validación de documentos, previamente pedidos por el usuario o automáticamente generados por la empresa a la que pertenece el usuario. Fuente: autoría propia.

Diagrama 7

Flujo de Compartición de Credenciales

Nota: El diagrama muestra el flujo de verificación de documentos, el cual ha sido pedido por el usuario a una empresa de la cual hace o ha hecho parte, después de esto la verificación y el documento quedará disponible en el perfil del usuario del cual podrá compartir. Fuente: autoría propia.

Implementación del Sistema Propuesto

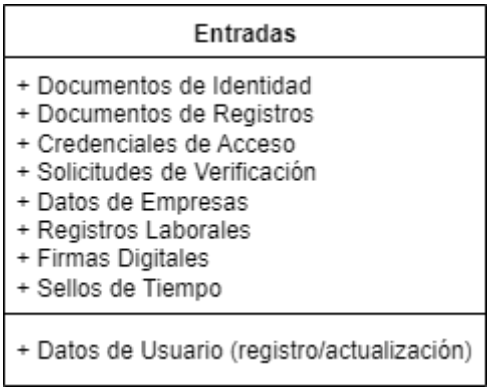
Para el cumplimiento de los requerimientos de RIMU se han diseñado y aplicado los siguientes diagramas para el funcionamiento del sistema.

Requerimientos de Entrada/Salida

Entradas del Sistema

Diagrama 8

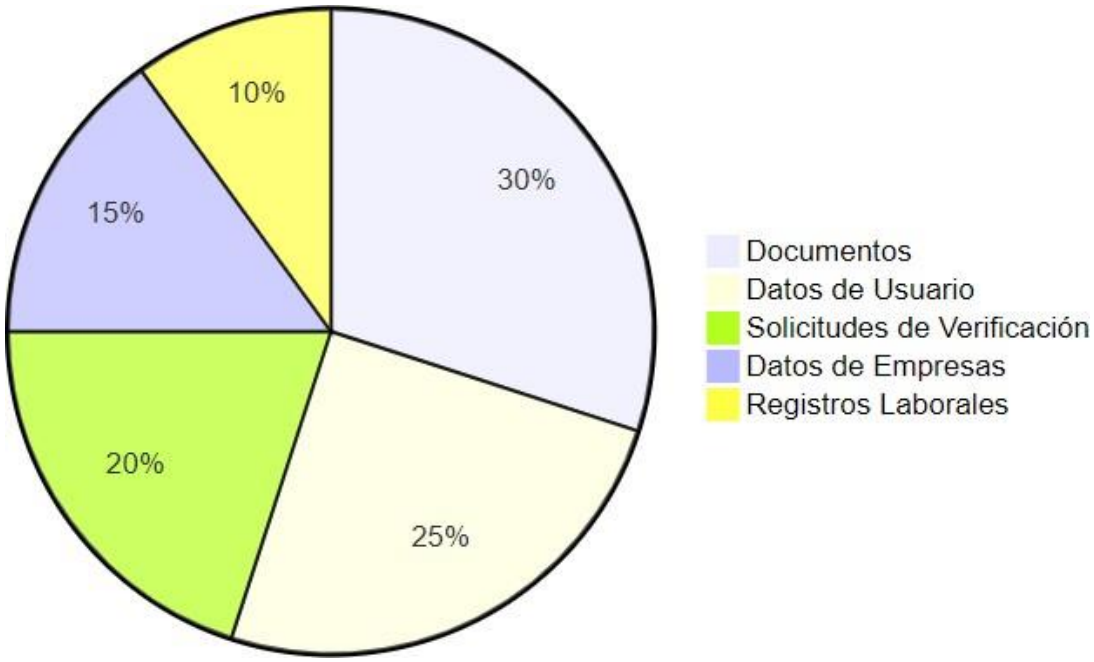
Entradas de datos principales del sistema



Nota: El gráfico muestra todas las entradas disponibles en el sistema que se generan por medio de funcionalidades de este, arrojando una salida útil dependiendo el caso usado. Fuente: autoría propia.

Imagen 2

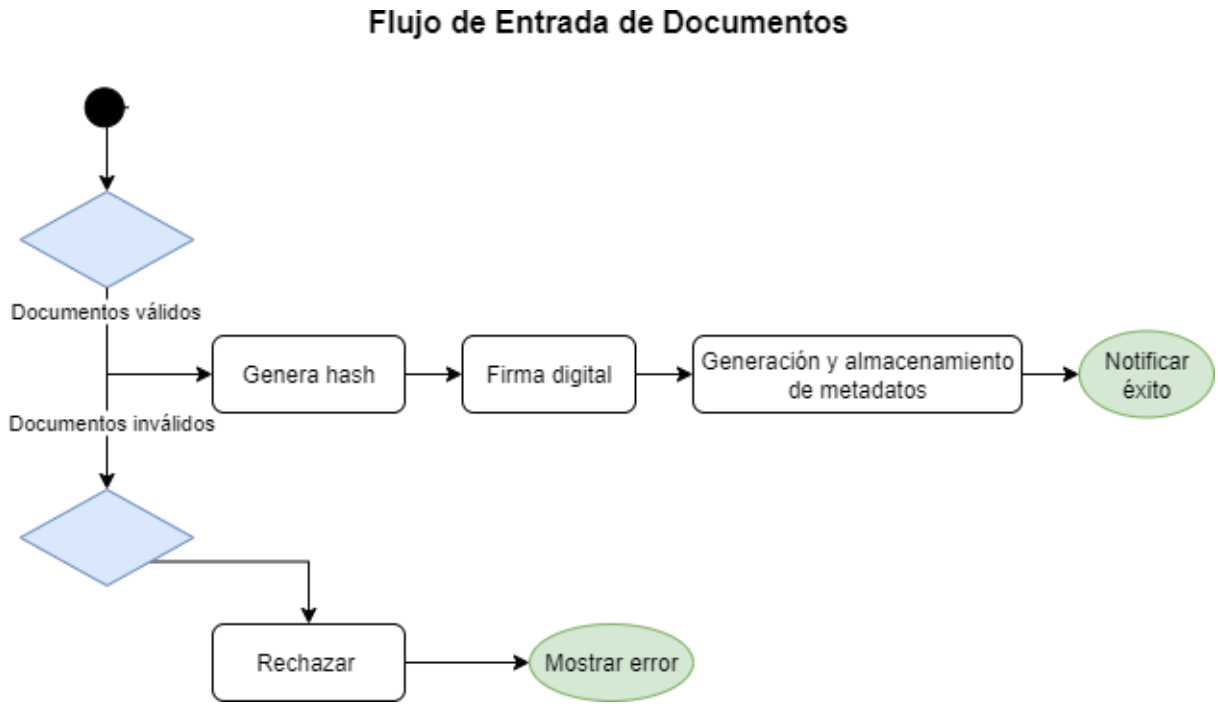
Distribución de Entradas al Sistema



Nota: El gráfico muestra el flujo total promedio de la cantidad de funciones que se usaran en el sistema para su respectivo funcionamiento y generación de firmas y validaciones de documentos y registro de datos correspondientes a datos de empresas, registros laborales u otros. Fuente: autoría propia.

Diagrama 9

Flujo de Entrada de Documentos



Nota: en el anterior diagrama podemos observar el flujo que se lleva a cabo por el sistema para la creación y firma de un documento. Fuente: autoría propia.

Salidas del Sistema

Diagrama 10

Salidas creadas por el sistema

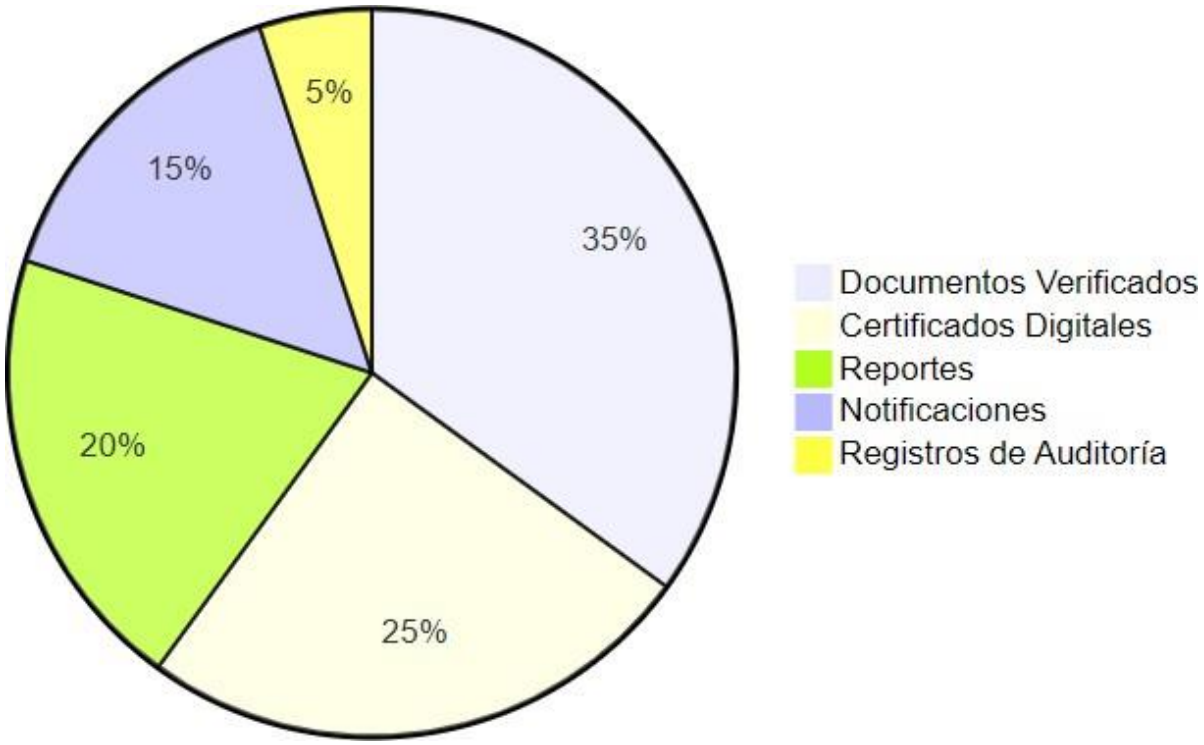
Salidas
+Perfiles de Usuario +Documentos Verificados +Certificados Digitales +Reportes de Actividad +Notificaciones +Registros de Auditoría +Estadísticas de Uso +Alertas de Seguridad

Nota: El diagrama muestra las salidas efectuadas del sistema que van de la mano con las entradas del sistema, estas funcionalidades son las principales para el correcto desempeño de RIMU.

Fuente: autoría propia.

Imagen 3

Tipos de Salidas Generadas



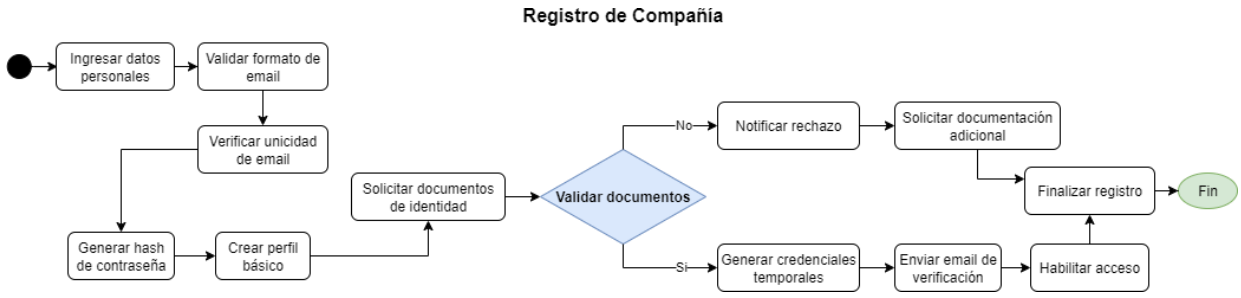
Nota: la imagen muestra el total de salidas que se generaría en cuestión de documentación.

Fuente: autoría propia.

Diagramas de Actividades

Diagrama 11

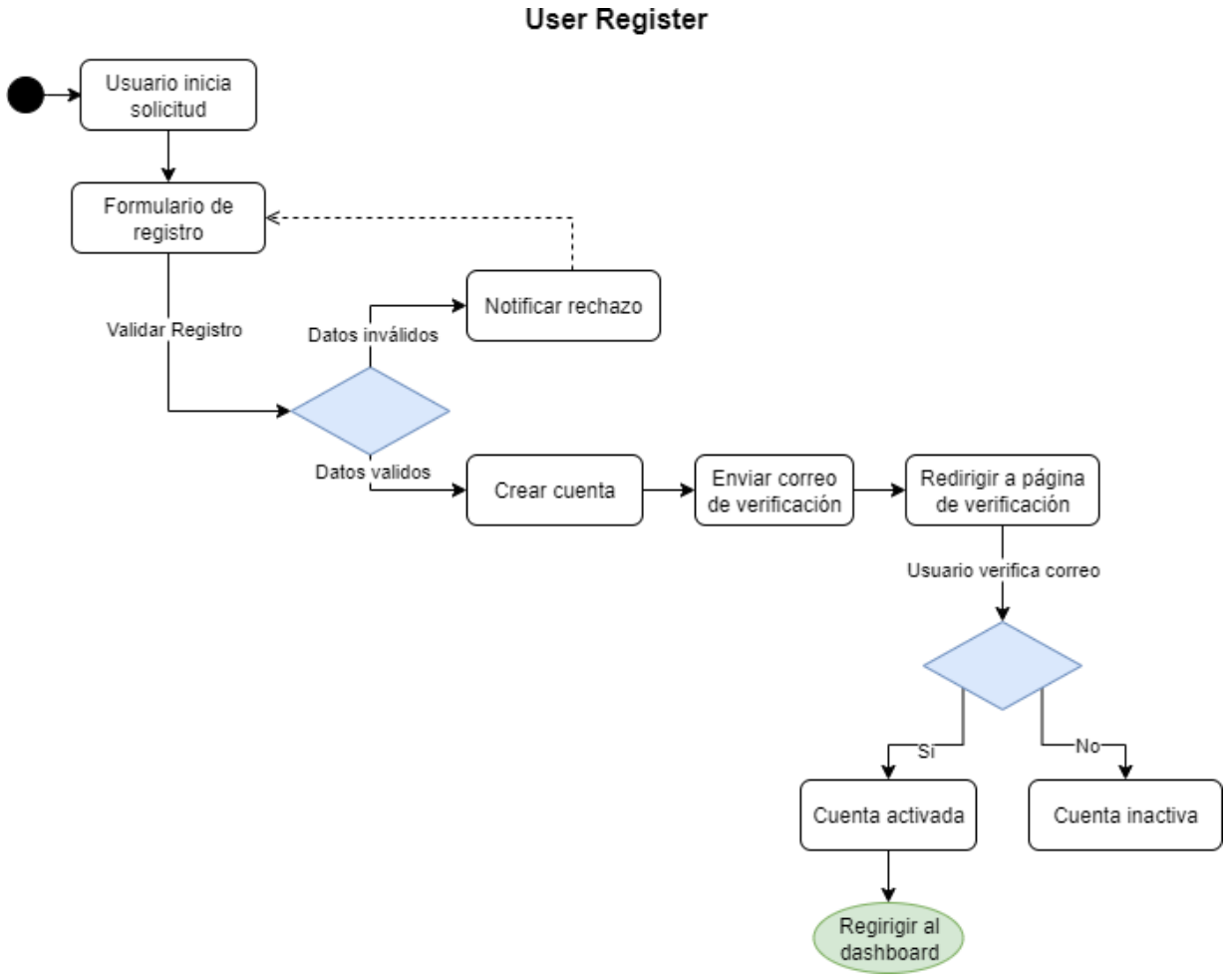
Flujo de registro para compañías



Nota: En el diagrama podemos ver el flujo de registro de una compañía en el sistema. El administrador encargado de registrar la compañía principalmente tiene que registrar su compañía en el sistema mediante un formulario el cual se validara por medio de los administradores del sistema y evaluaran el registro o no de la empresa, después de este paso se le notificara al administrador o encargado de la empresa el registro satisfactorio de la compañía en el sistema y se generaran automáticamente las credenciales de acceso temporales que este mismo usuario puede modificar en su primer inicio de sesión para efectos de control y seguridad. Fuente: autoría propia.

Diagrama 12

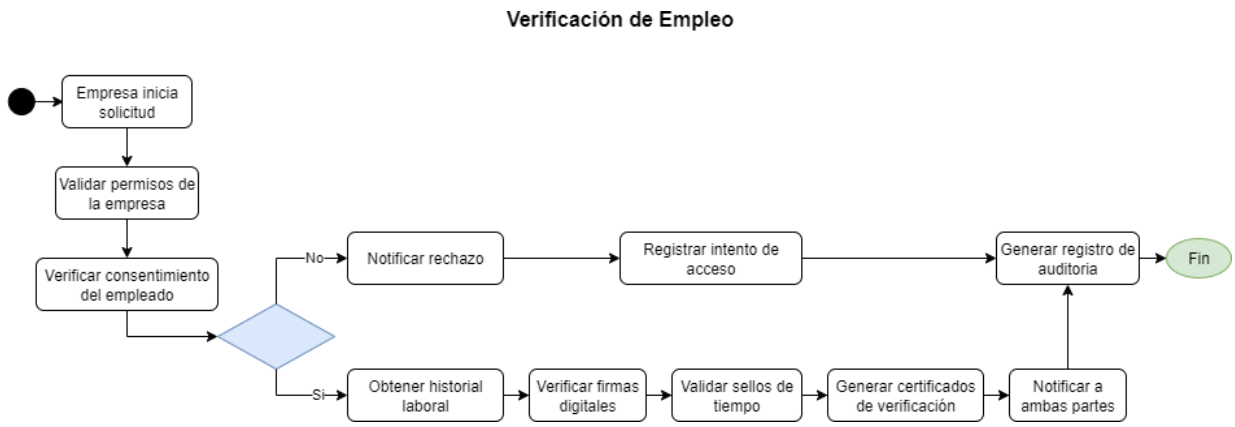
Flujo de registro para usuarios normales



Nota: En el diagrama se muestra el flujo de registro de un usuario normal que podría ser un empleado o cualquier persona del común que quiera usar el servicio. Este registro sería más simple que el de empresa siguiendo unas etapas donde se le pide al mismo usuario que llene sus datos personales y verificaciones de credenciales, seguidas de una verificación de email, para así, posteriormente mostrar el dashboard en el que se dispondrán las diferentes funcionalidades del sistema creadas para este tipo de usuarios. Fuente: autoría propia.

Diagrama 13

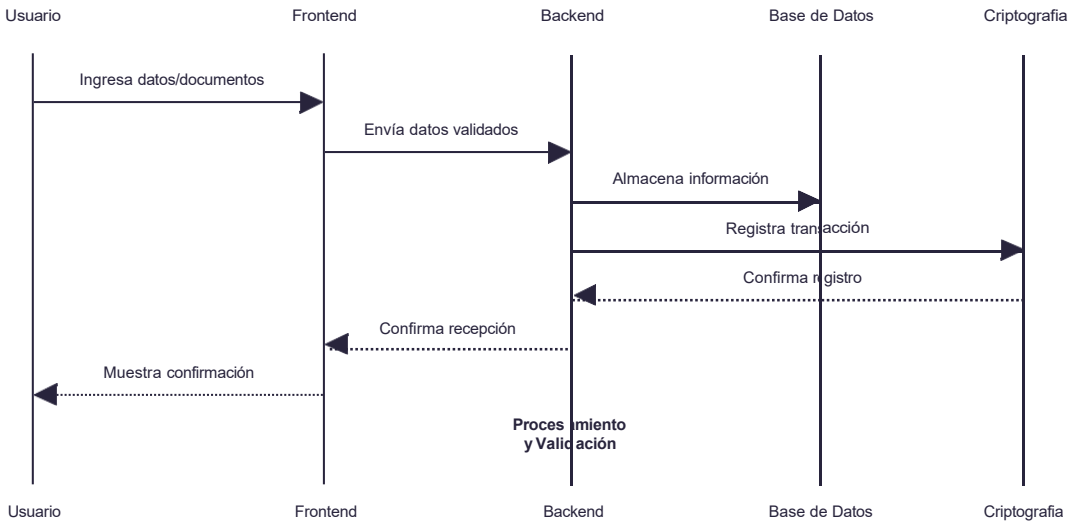
Flujo de verificación de documentos de empleados



Nota: En el diagrama anterior se presenta el flujo de verificación de documentos de empleados, esta es una herramienta que solo está disponible para usuarios tipo compañía (empresas), donde se dispone de las herramientas necesarias y relaciones de los empleados que se manejan en la misma para así poder manejar la verificación de documentos. Fuente: autoría propia.

Diagrama 14

Flujo de verificación de documentos

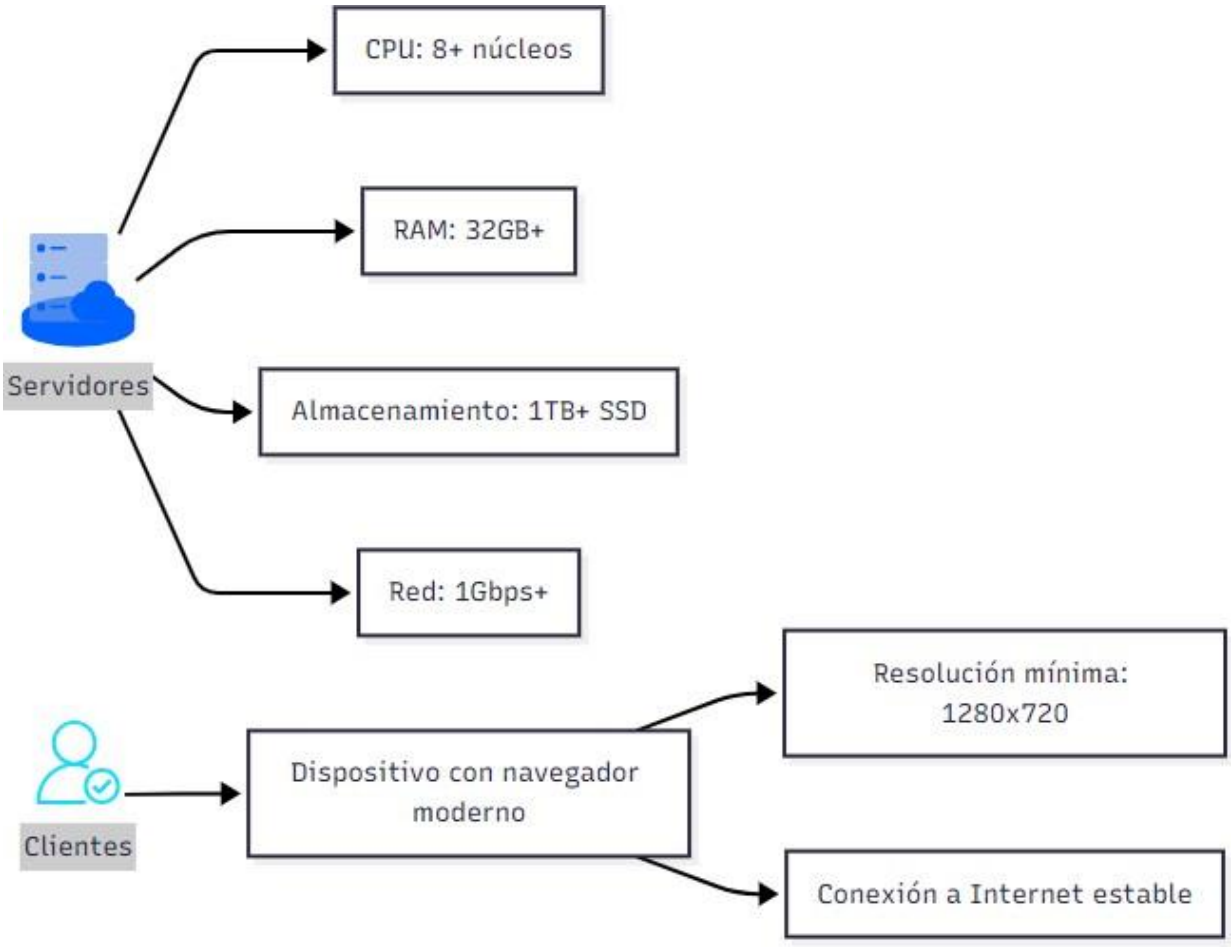


Nota: en el anterior diagrama se observa el flujo que lleva el sistema para la correcta verificación de los documentos. Fuente: autoría propia.

Requisitos de Hardware/Software

Diagrama 15

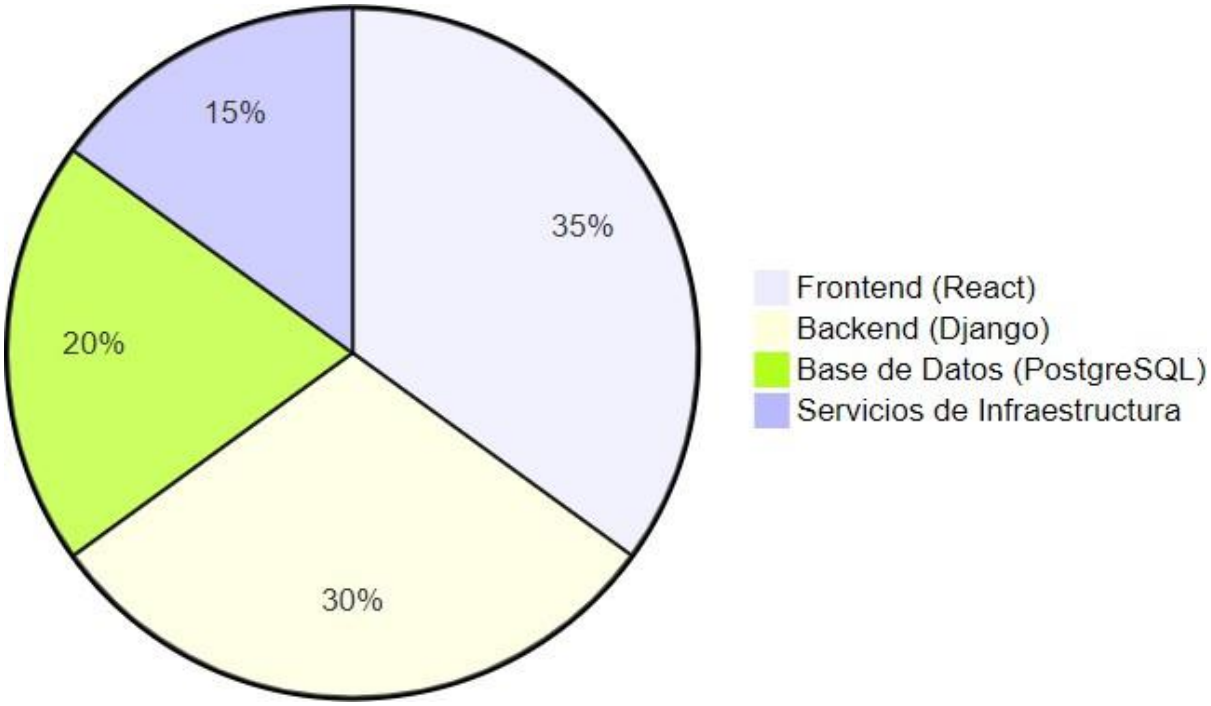
Requisitos principales de Hardware



Nota: Se pueden observar las principales recomendaciones que debe llevar el hardware donde se esté sirviendo el sistema (Deployment). Además de esto también se muestran las especificaciones recomendadas para uso del sistema por parte de los clientes o usuarios. Fuente: autoría propia.

Imagen 4

Requisitos de Software Principales Para el Sistema



Nota: En el gráfico se muestran los principales requisitos de software utilizados del sistema, además de esto su valor porcentual que debería aplicarse para cada caso. Fuente: autoría propia.

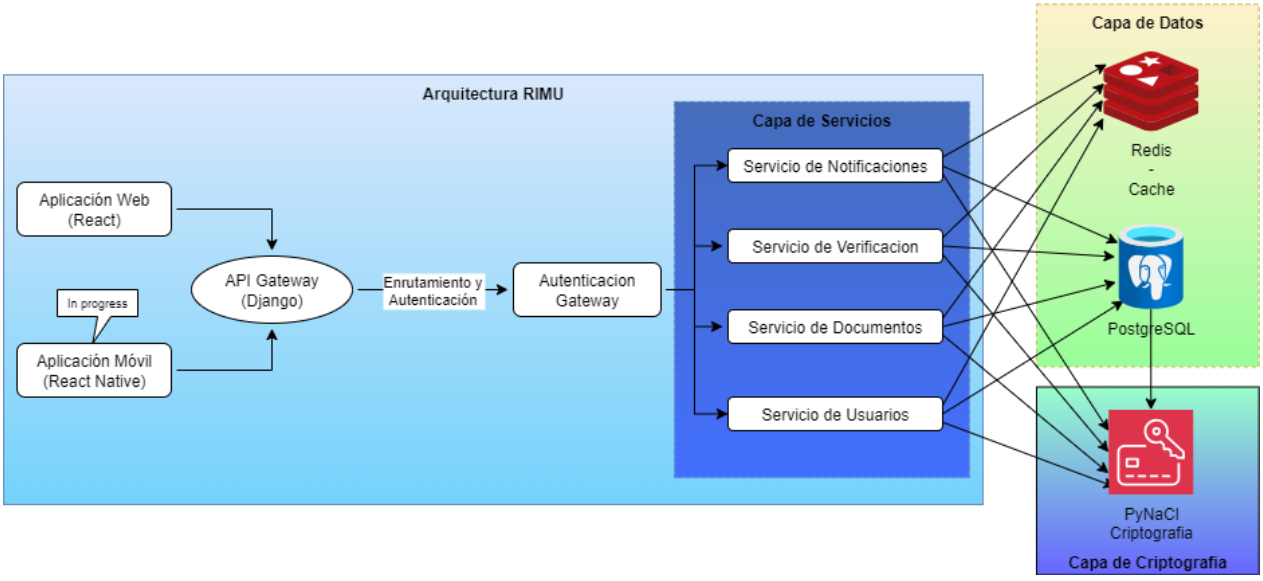
Diseño del Sistema

Arquitectura General

La siguiente imagen muestra la arquitectura general del sistema complementado por API de lado del back-end y servidores de bases de datos muy potentes e importantes como lo son, Redis, en este caso Redis Cache utilizado como un elemento de ayuda para cuando la carga de documentos se realice de forma recurrente y de esta forma tenerlos disponibles más eficazmente. Por otro lado, encontramos a PostgreSQL que llevaría toda la lógica de negocio y autenticación.

Imagen 5

Arquitectura del Sistema RIMU

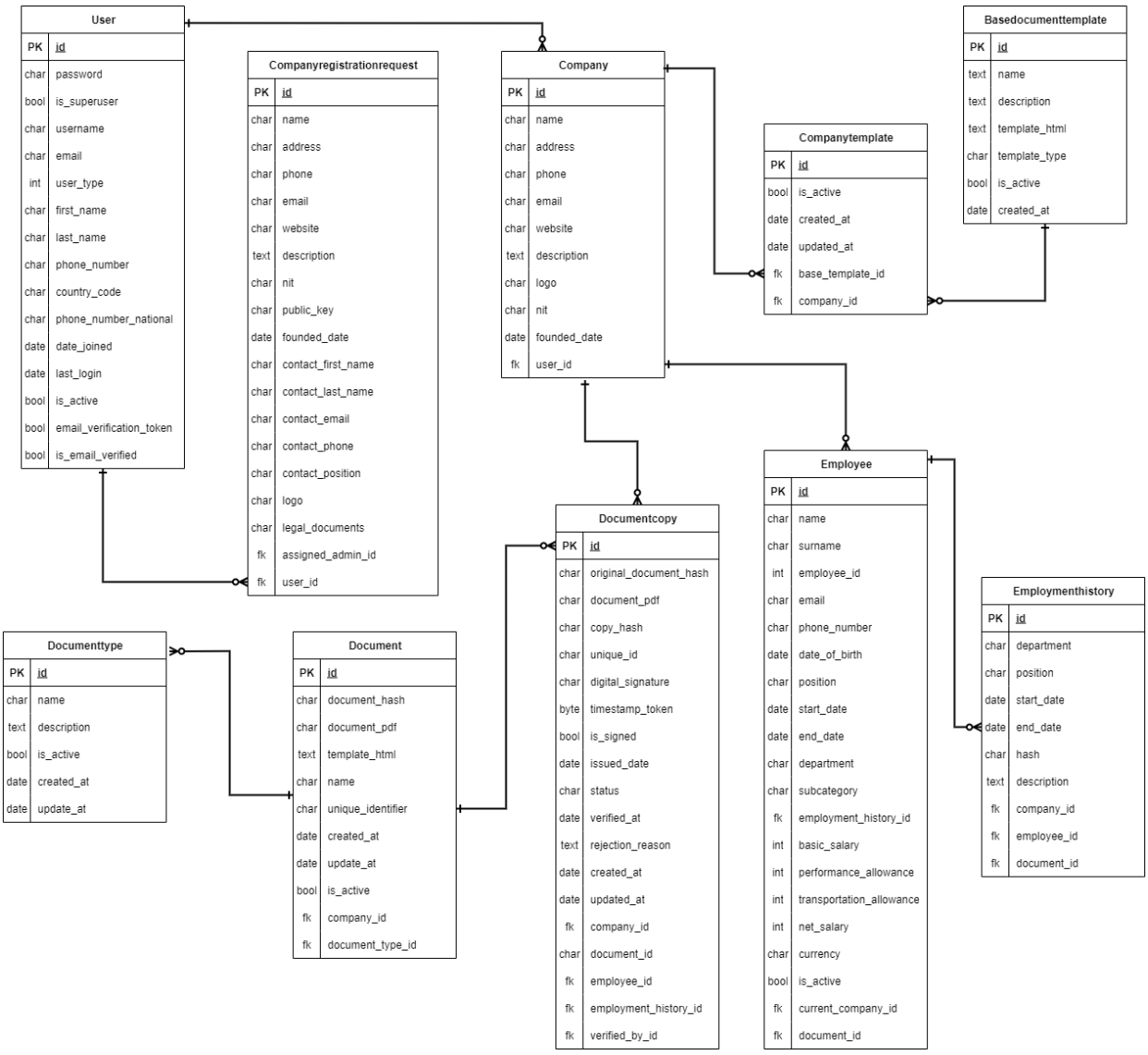


Nota: La anterior imagen ilustra de manera gráfica la arquitectura que se implementa en la construcción del sistema RIMU. En esta podemos apreciar algunas de sus herramientas principales también su lógica de datos que contemplan el uso de herramientas como PostgreSQL y Redis para un rendimiento óptimo. Fuente: autoría propia.

Diseño de Base de Datos (modelo entidad-relación)

Diagrama 16

Modelo de Datos (ER)



Nota: el modelo de datos representado en el anterior diagrama de entidad relación muestra la arquitectura y el diseño de la base de almacenamiento del sistema, recordemos que se usa el DBMS PostgreSQL, un modelo relacional de código abierto reconocido por su robustez y

utilizado mayoritariamente por grandes empresas reconocidas como Apple, Instagram, etc. Fuente: autoría propia.

Diseño de Controles (seguridad, permisos)

El control de seguridad del proyecto abarca diferentes etapas en las cuales podemos encontrar diferentes enfoques. El principal es el back-end, desarrollado en Django y Django REST Framework. Este implementa múltiples capas de seguridad que incluyen autenticación basada en tokens, autorización granular y protección contra ataques comunes.

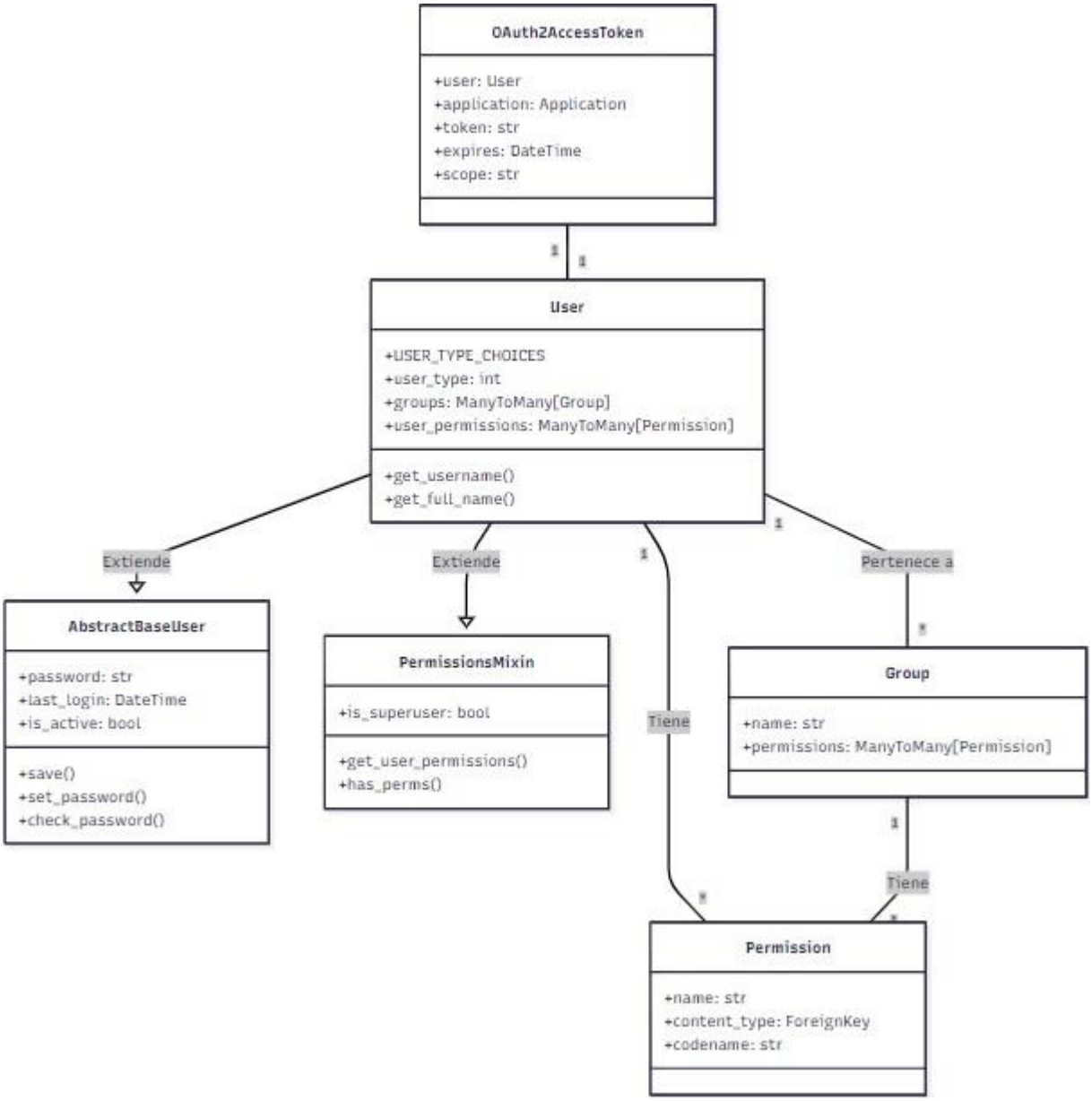
La otra capa que se busca proteger es la del front-end, desarrollado puramente con React, ya que es el principal punto en la conexión con el back-end. En este campo se implementan pasos de seguridad y protección contra Cross-Site Scripting (XSS), SQL Injection, Ataques de CSRF.

Autenticación Basada en Tokens (JWT y OAuth2)

El sistema cuenta con una combinación entre JWT y OAuth2 para la autenticación, lo cual permite que esta implementación siga las mejores prácticas de OAuth2, generando tokens únicos y configurando expiraciones apropiadas. Además de esta combinación también se genera un tipo de autorización basada en roles lo que permite a al sistema redirigir al usuario de acuerdo con los roles asignados al momento de creación del perfil de usuario.

Diagrama 17

Autenticación Basada en Tokens y RBAC



Nota: el diagrama representa el flujo del sistema al momento de asignar roles a usuarios. Fuente: autoría propia.

También, la encriptación de datos y el manejo de sesiones seguras son aspectos fundamentales en la arquitectura del sistema. Como ya vimos en el anterior diagrama, el sistema

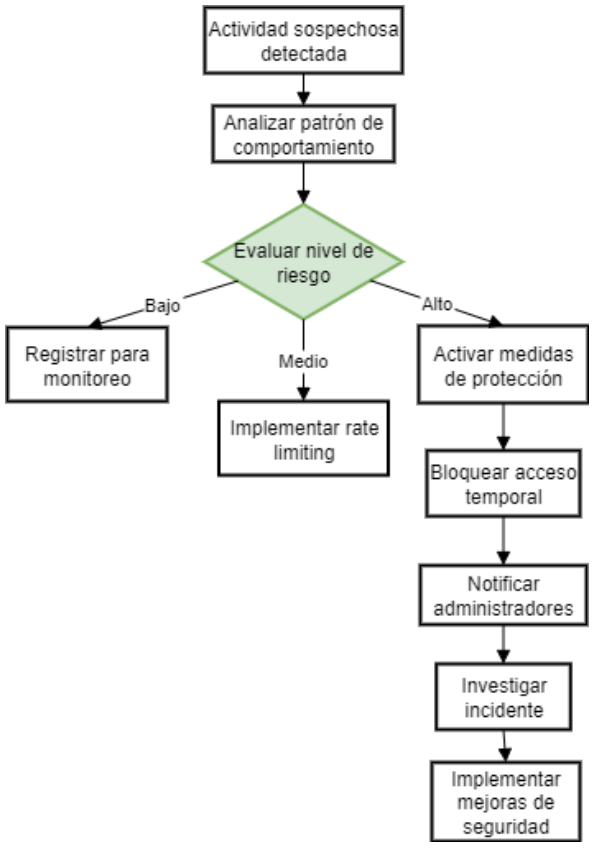
implementa encriptación de contraseñas mediante el método set_password() de Django y utiliza HTTPS para todas las comunicaciones. Las sesiones se manejan a través de tokens JWT con expiraciones configurables; esto permite la mitigación de vulnerabilidades comunes como las ya mencionadas, tales como SQL Injection, XSS, entre otras

Flujo de Prevención de Amenazas

El flujo de prevención de amenazas está siempre a la escucha y operativo para el análisis de las respuestas que ocurran como llamadas a la API. Este flujo asegura al sistema de una gran cantidad de amenazas, entre ellas y la principal es la de ataques de fuerza bruta. Este es un ataque que, por medio de prueba y error, en una manera escalonada y demasiado abrasiva, intenta descifrar contraseñas con el fin de obtener accesos no autorizados al sistema.

Diagrama 18

Flujo de Prevención de Amenazas



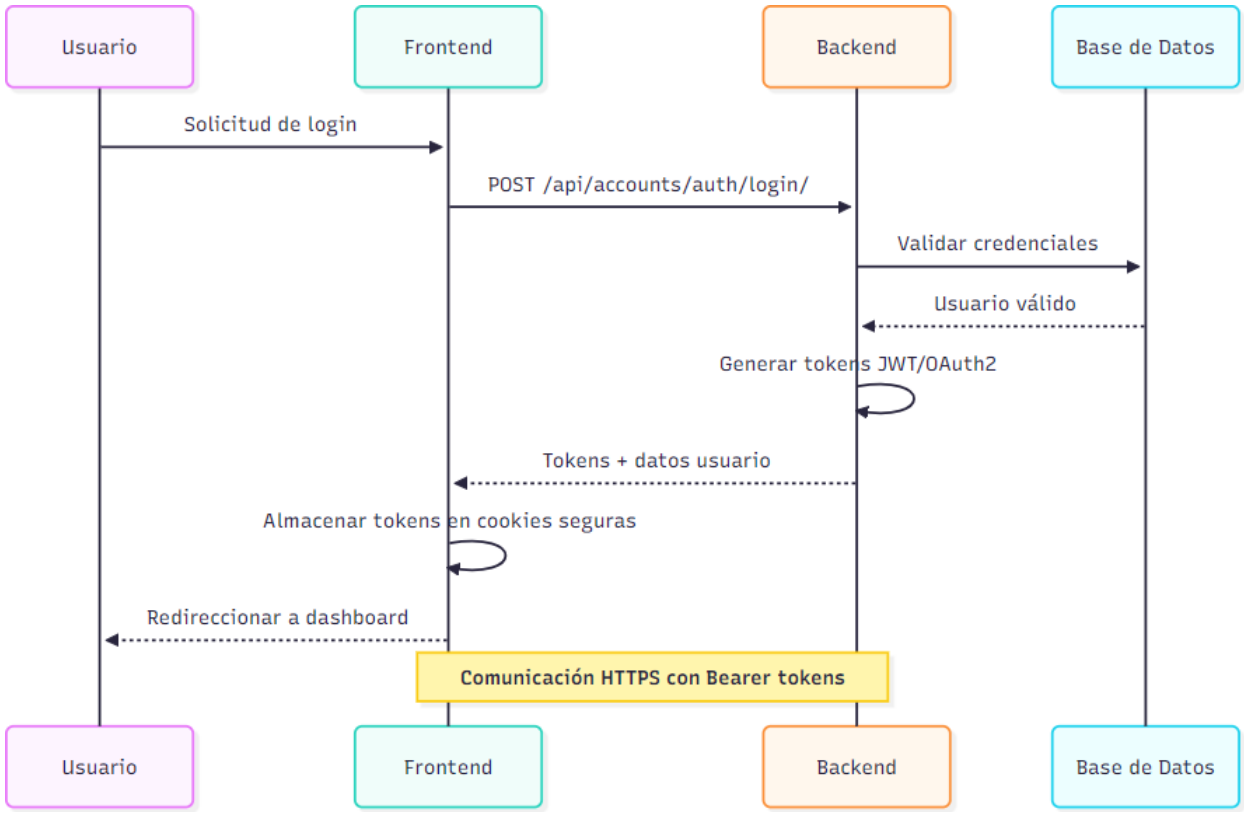
Integración Backend-Frontend

Como se dijo anteriormente, el principal elemento que se comunica con el back-end es el mismo front-end el cual debe contar con las mejores implementaciones de seguridad. Esto se realiza mediante diversos métodos que permiten el mejor control de la seguridad del proyecto.

El componente AuthContext del front-end gestiona el estado de autenticación, manteniéndolo sincronizado con el back-end. Usa una caché de datos de usuario para reducir llamadas a la API y actualiza automáticamente los refresh tokens. Al hacer logout, se realiza una limpieza completa de la sesión. De esta manera en cada nuevo inicio de sesión los permisos se sincronizan verificando en el back-end con decoradores como @permission_classes y validando tokens en el front-end mediante un middleware que protege las rutas.

Diagrama 19

Flujo de autenticación backend-frontend



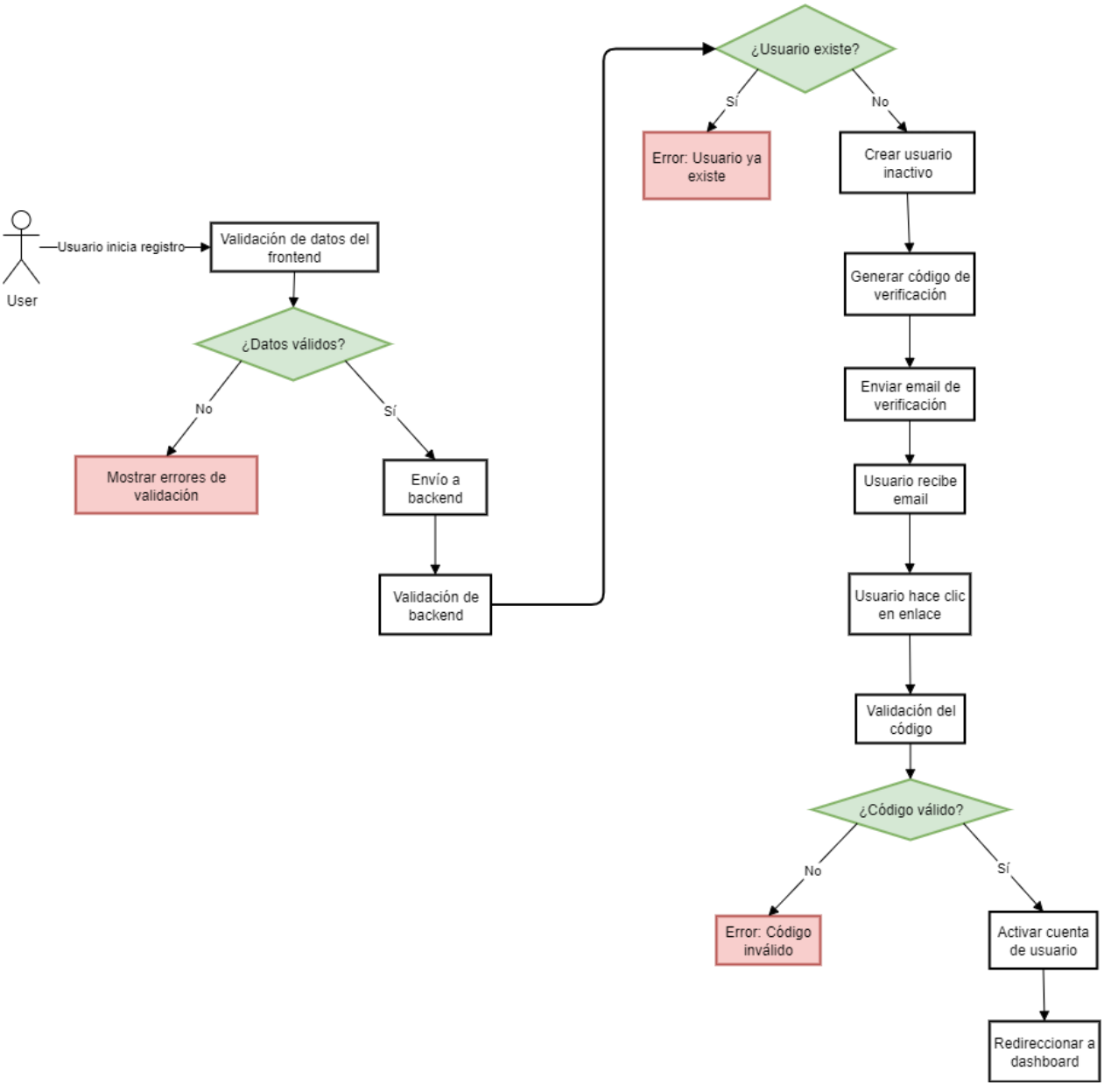
Nota: el diagrama muestra cómo se realiza el flujo seguro dentro del sistema, integrando comunicación back-end y front-end y generando automáticamente los tokens y credenciales de seguridad que validan al usuario y generan un registro seguro. Fuente: autoría propia.

Diseño de Procedimientos (flujos de trabajo)

El flujo de trabajo del proyecto RIMU representará gráficamente cómo los usuarios interactúan con el sistema y cómo se procesan las operaciones críticas, todo esto en el contexto del proyecto y su modo de autenticación, gestión de usuarios y registro de empresas, entre muchos otros procedimientos eficientes y fundamentales los cuales garantizan una experiencia de usuario fluida y segura.

Diagrama 20

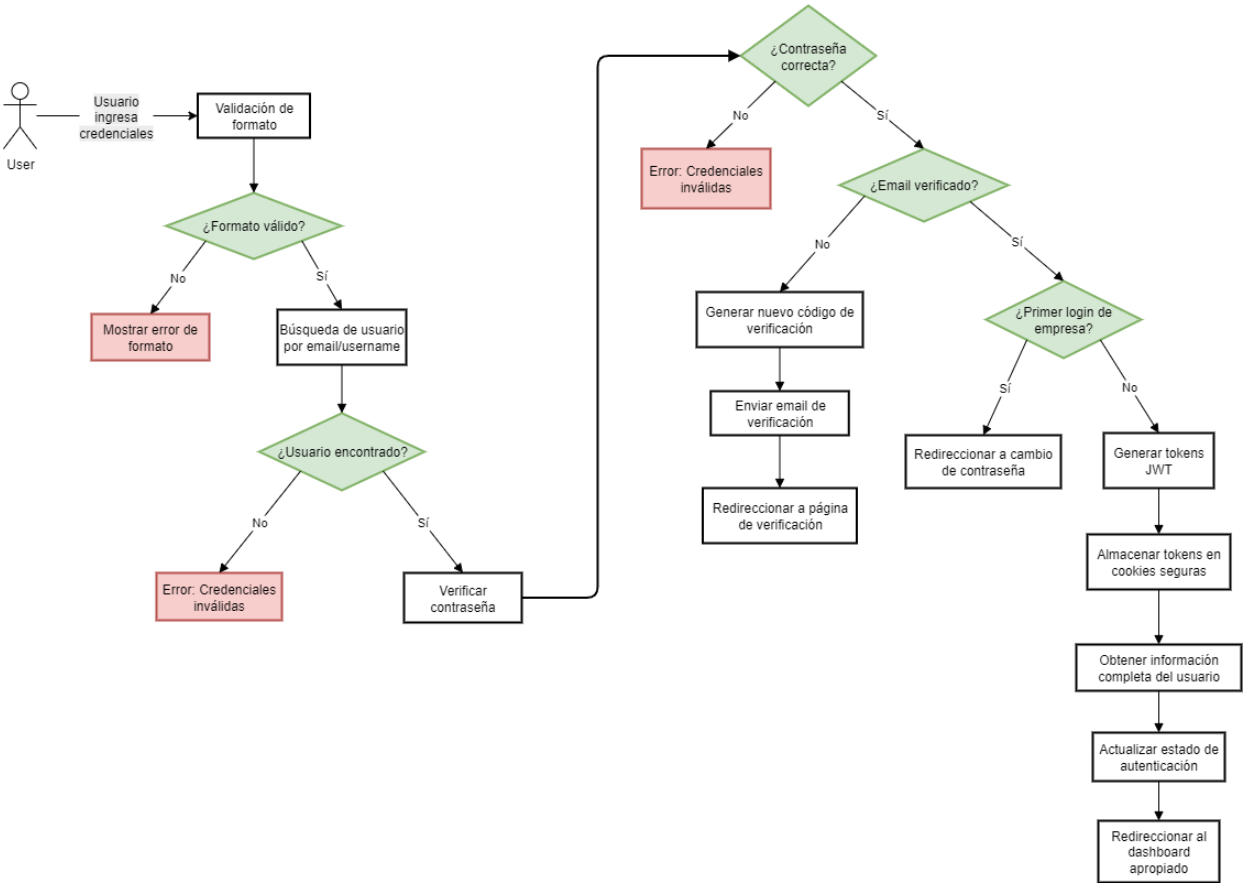
Flujo de Registro de Usuarios



Nota: este flujo incorpora múltiples capas de validación y seguridad, incluyendo verificación de reCAPTCHA y rate limiting para prevenir abusos. Fuente: autoría propia.

Diagrama 21

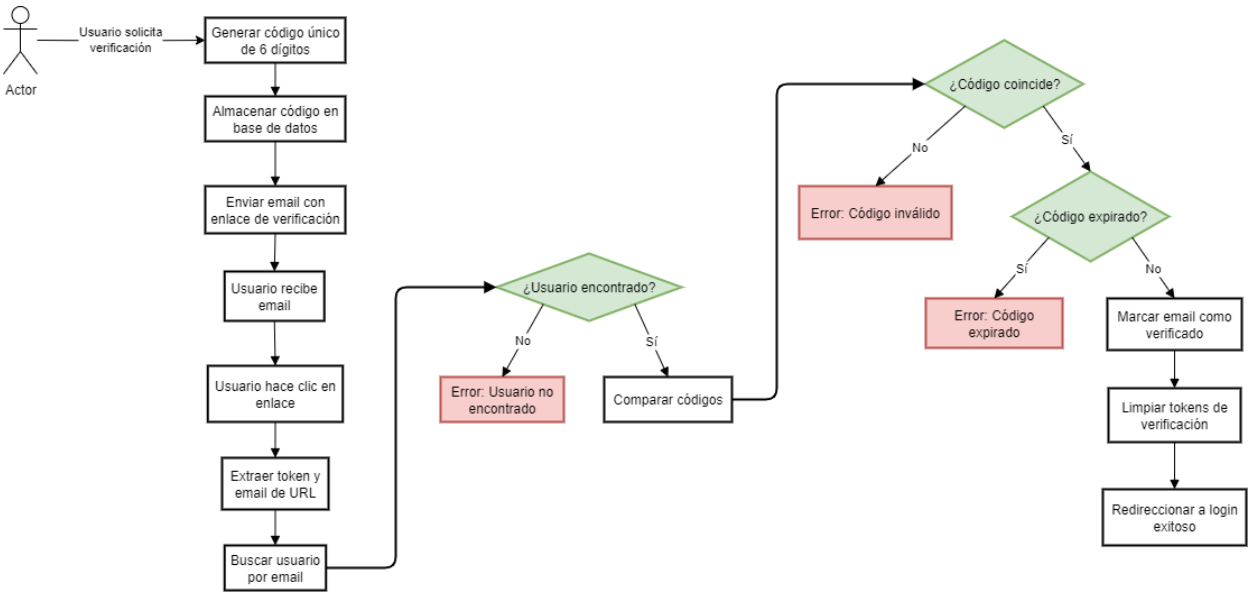
Flujo de Autenticación y Login



Nota: el proceso de login es un flujo complejo que maneja diferentes escenarios de usuario y estados de verificación. Fuente: autoría propia.

Diagrama 22

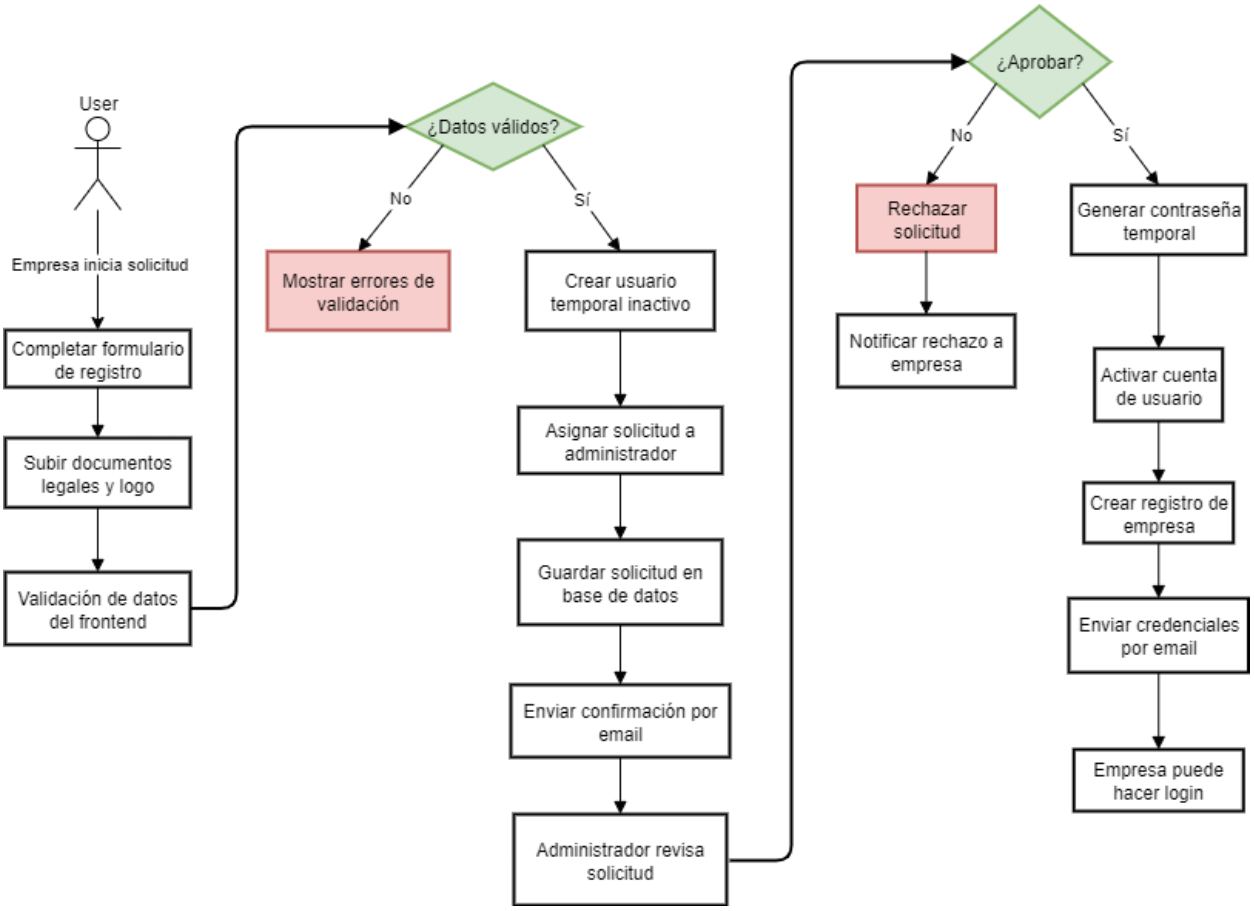
Flujo de Trabajo de Verificación de Email



Nota: la verificación de email es crucial para la seguridad y el cumplimiento normativo, especialmente bajo regulaciones como GDPR.

Diagrama 23

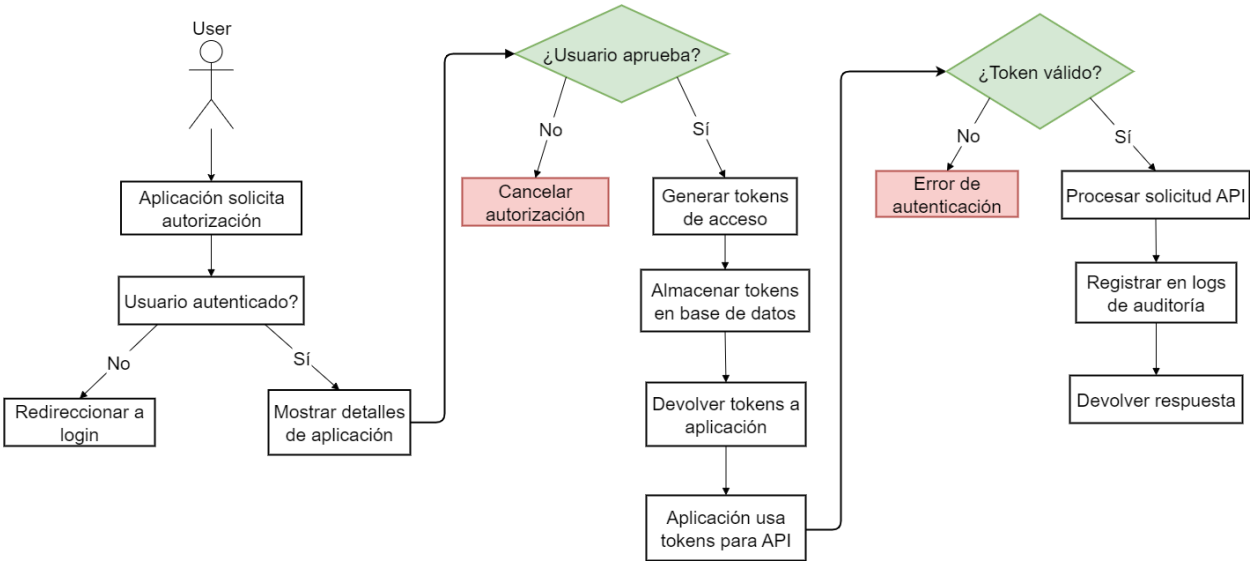
Flujo de Registro de Empresa



Nota: el registro de empresas es un proceso complejo que involucra múltiples pasos y revisiones administrativas. Fuente: autoría propia.

Diagrama 24

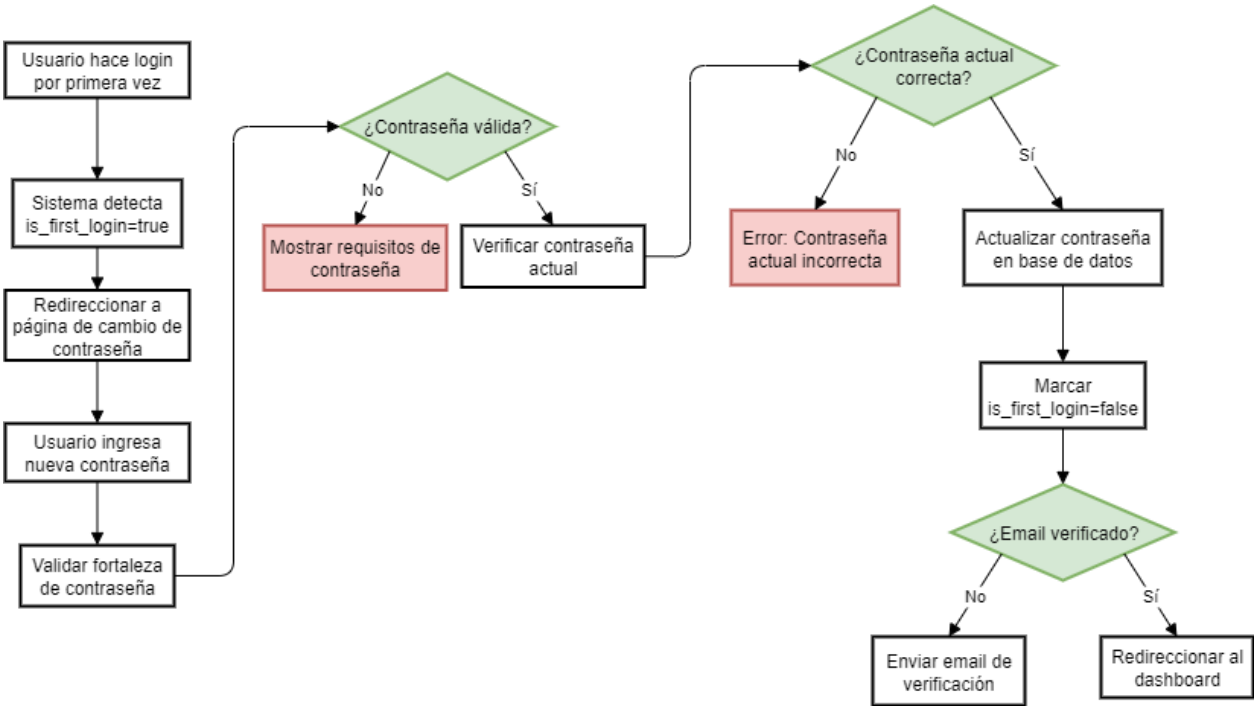
Flujo de Gestión de Tokens OAuth2



Nota: la gestión de tokens OAuth2 se implementó para la integración con aplicaciones de terceros y el mantenimiento de sesiones seguras. Fuente: autoría propia.

Diagrama 25

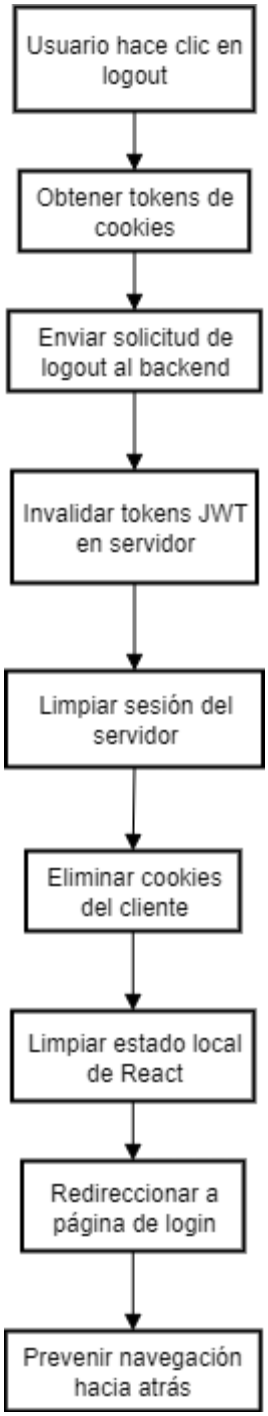
Flujo de Trabajo de Cambio de Contraseña Inicial



Nota: para usuarios de empresa es obligatorio la generación de contraseña, ya que la primera es una opción generada por el sistema y se fuerza el cambio en el primer login. Fuente: autoría propia.

Diagrama 26

Flujo de Logout Seguro



Nota: el logout asegura la limpieza completa de sesiones y tokens.

Diagramas de Secuencia

Diagrama 27

Diagrama de Secuencia - Flujo de Autenticación JWT

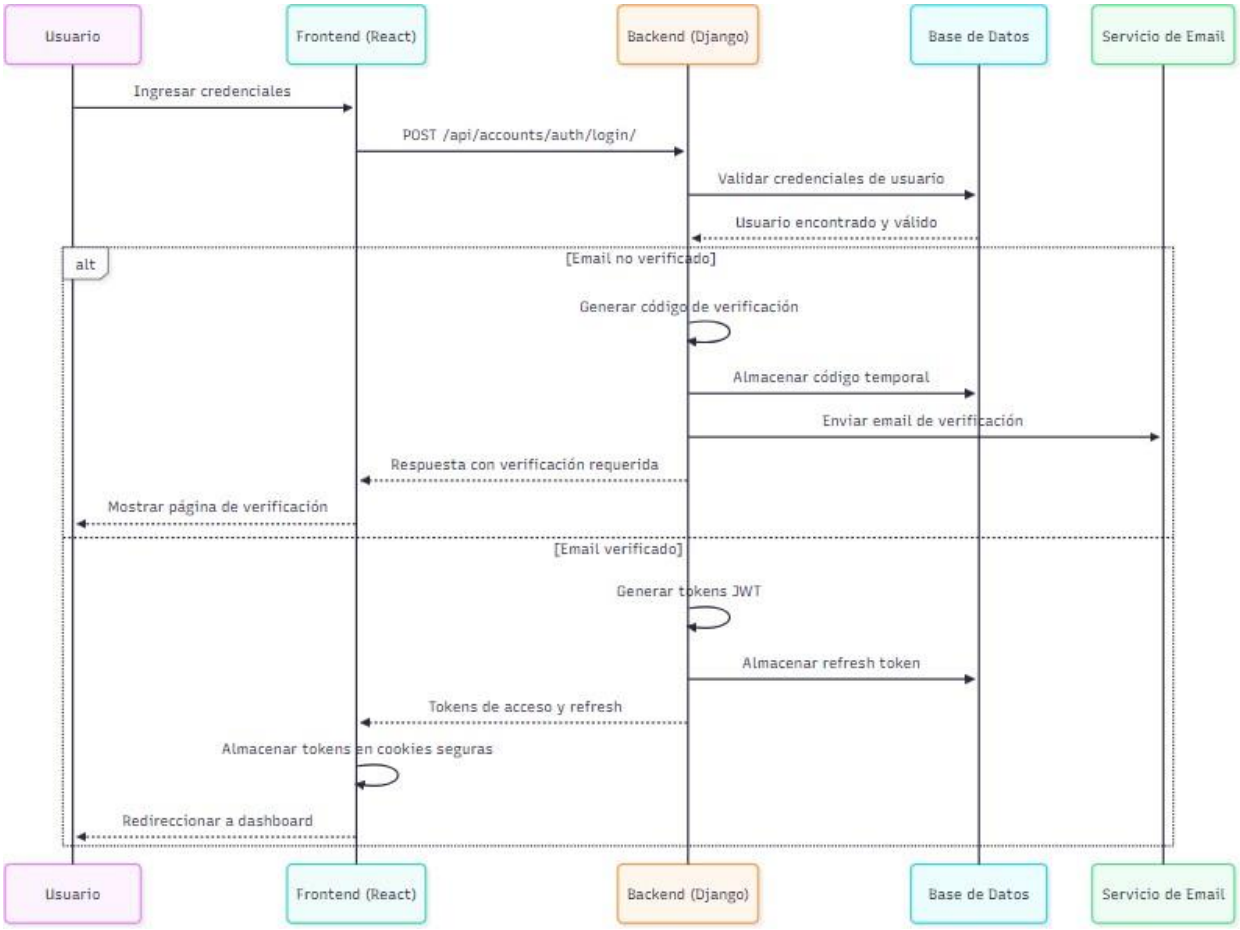


Diagrama 28

Diagrama de Secuencia - Flujo de Autorización Basada en Roles

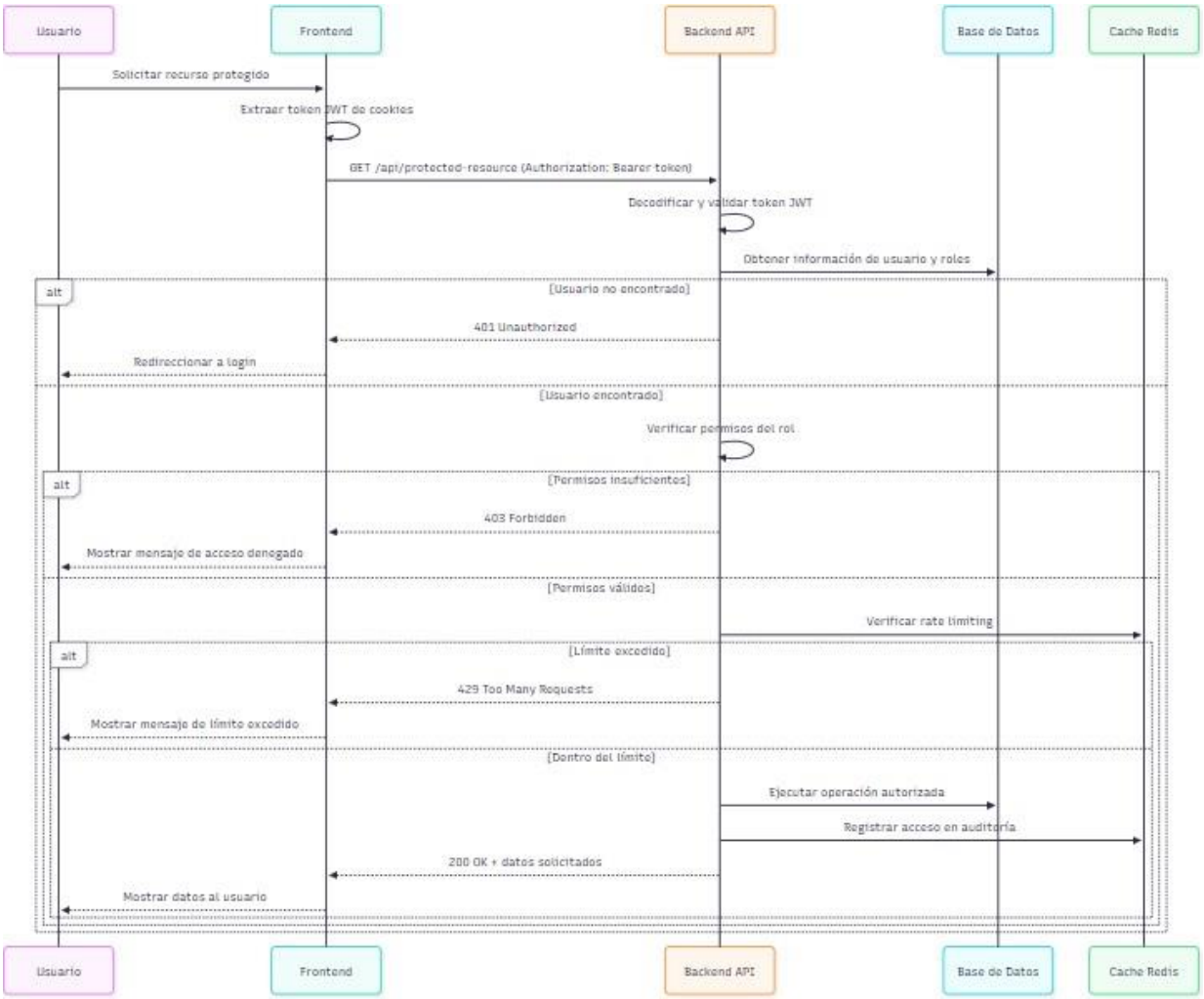


Diagrama 29

Diagrama de Secuencia - Gestión de Tokens OAuth2

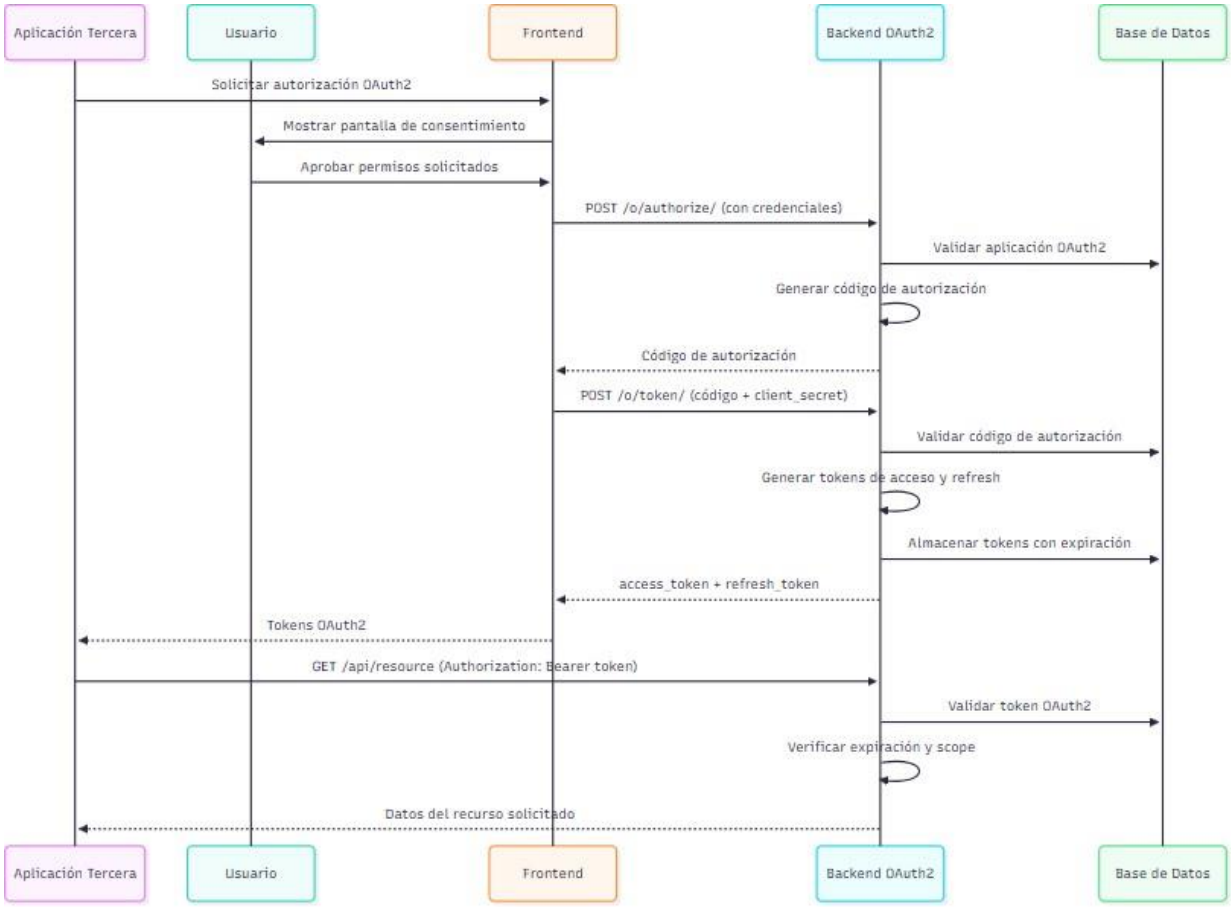


Diagrama 30

Diagrama de Secuencia - Prevención de Amenazas y Rate Limiting

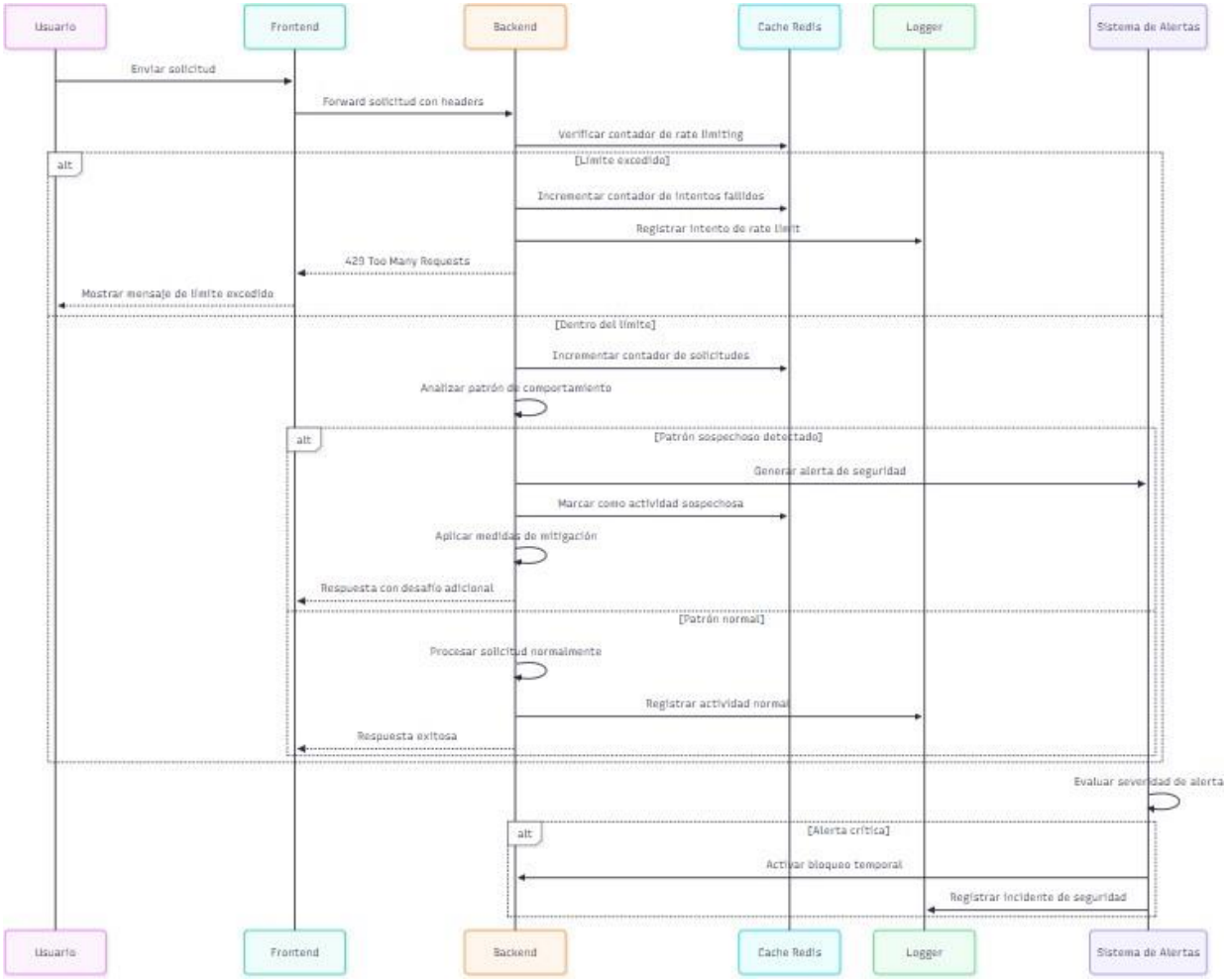


Diagrama 31

Diagrama de Secuencia - Respuesta a Incidentes de Seguridad

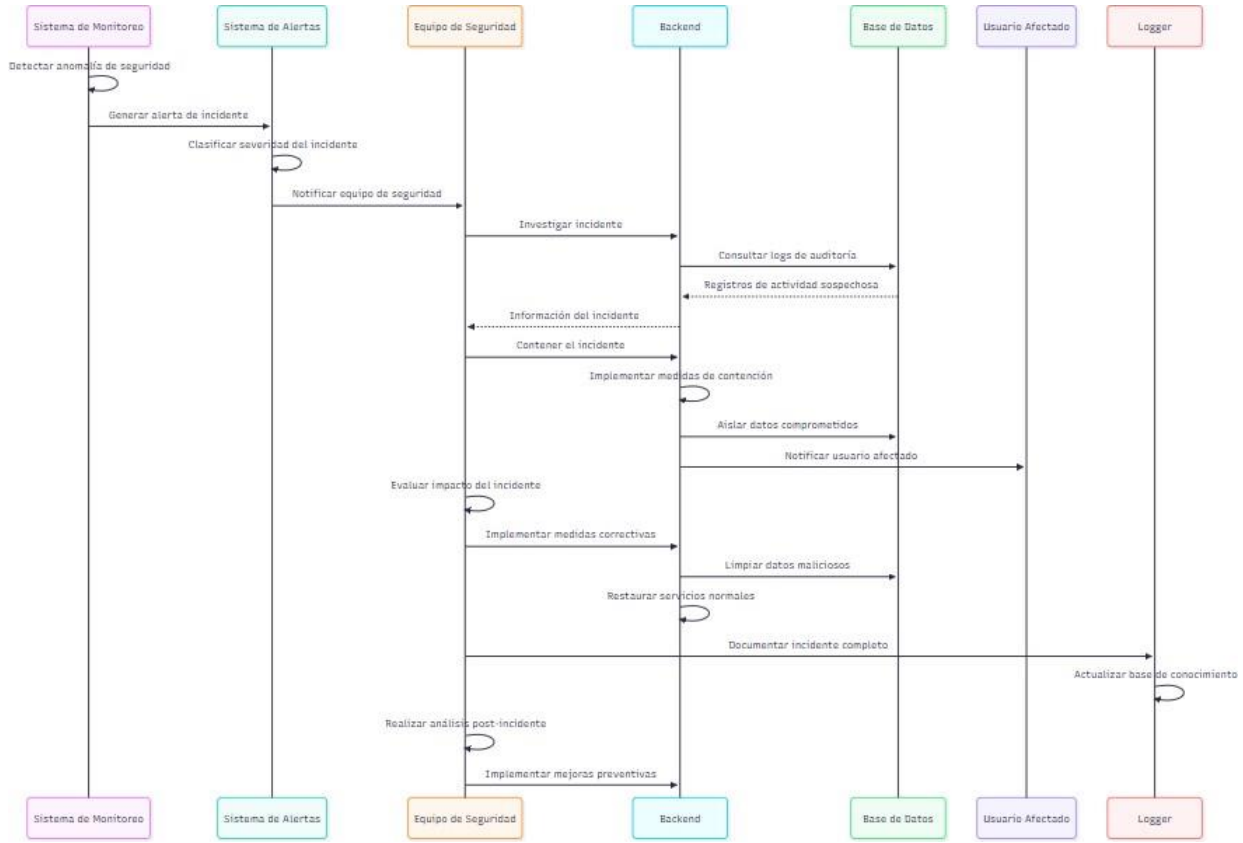


Diagrama 32

Diagrama de Secuencia - Verificación de Email y Recuperación de Cuenta

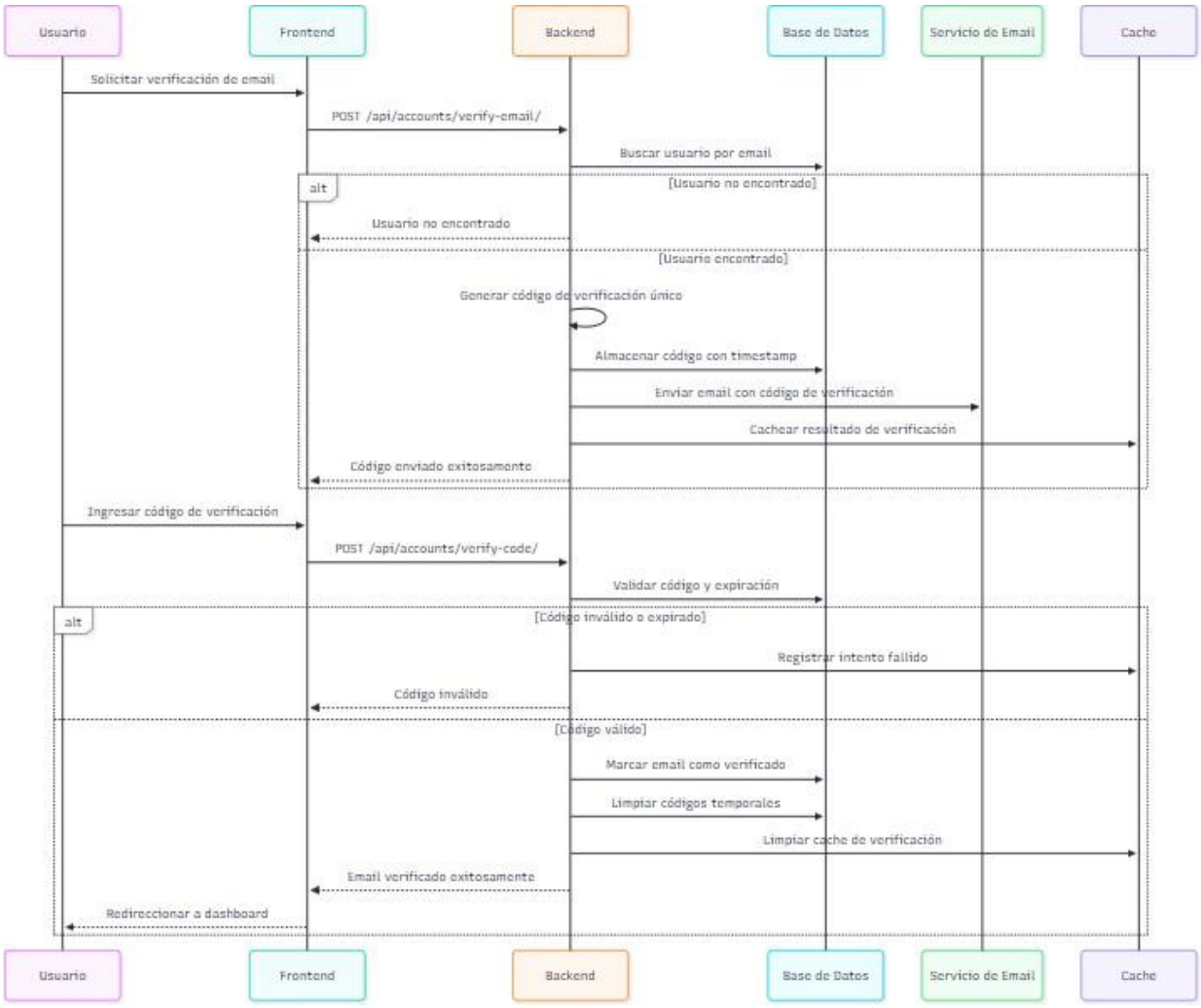


Diagrama 33

Diagrama de Secuencia - Gestión de Sesiones y Logout Seguro

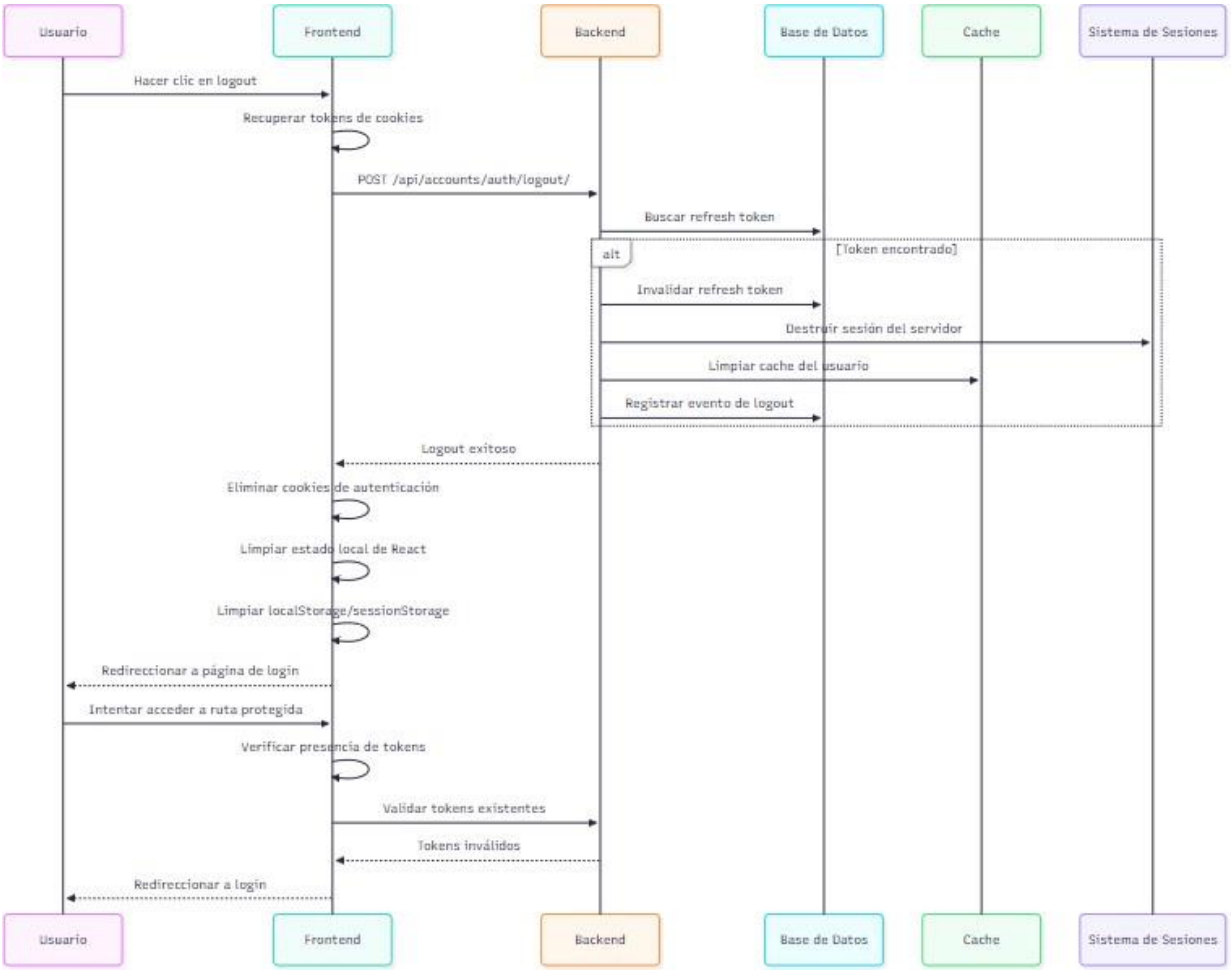
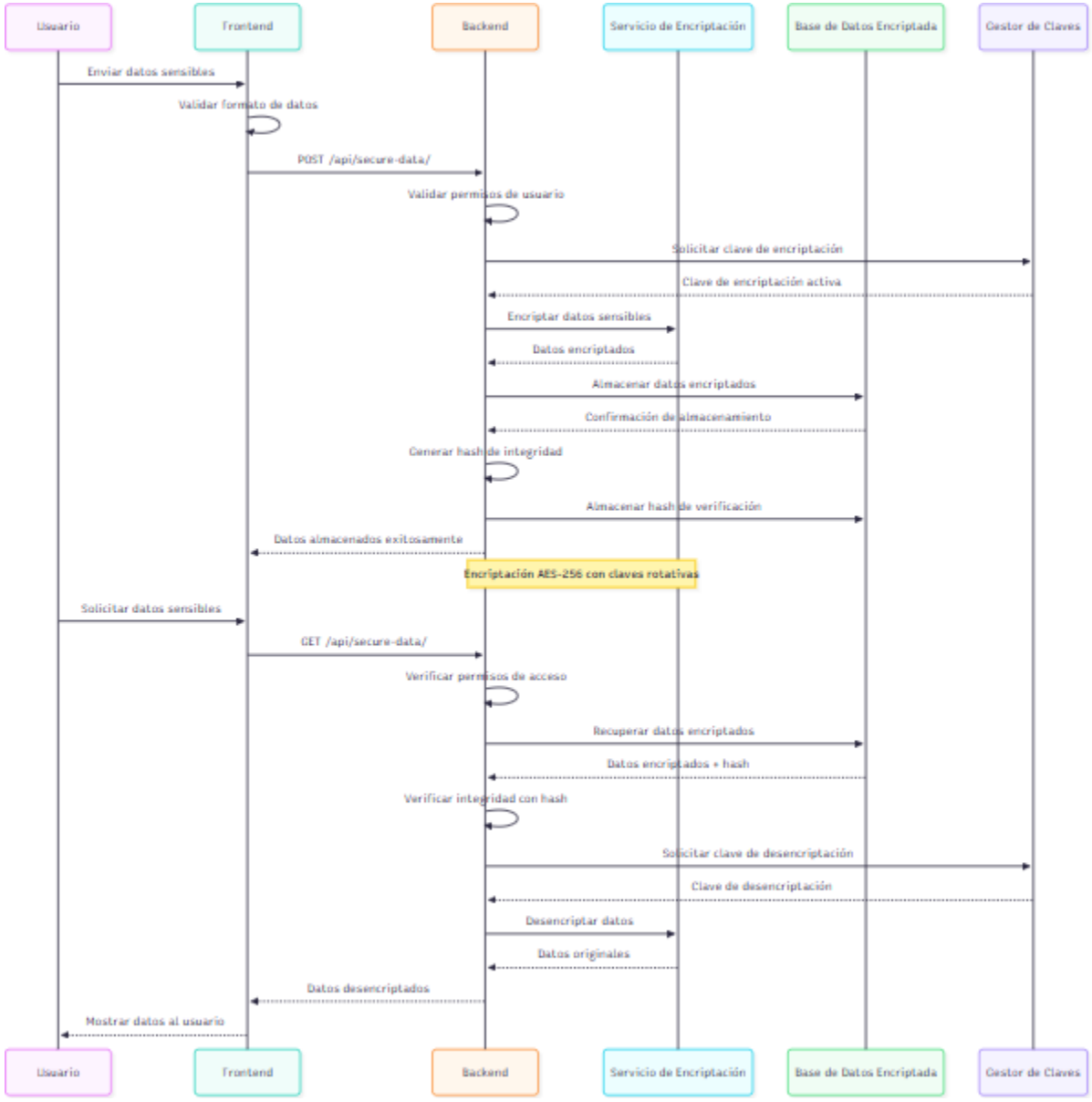


Diagrama 34

Diagrama de Secuencia - Encriptación y Protección de Datos



Diseño de Interfaz de Usuario (UI)

Para la fase de diseño, se empleó mayoritariamente el enfoque de metodologías ágiles, lo que implico el desarrollo de la interfaz de usuario de manera síncrona de acuerdo con las especificaciones de la recolección de información que requería el sistema. De acuerdo con esas especificaciones, y el análisis, se fue abordando el proyecto junto con su desarrollo y partiendo de una base primordial, que es la creación de componentes visuales e interfaces amigables con el usuario.

Para esto, se decidió que la aplicación debería de contar con componentes integrales de navegación, junto con formularios de registro tanto para empresas como para registros de usuarios, también, el sistema cuenta con servicios de notificaciones, las cuales se realizan por medio de correos directos al usuario.

Imagen 6

Componentes clave de los cuales parte el sistema

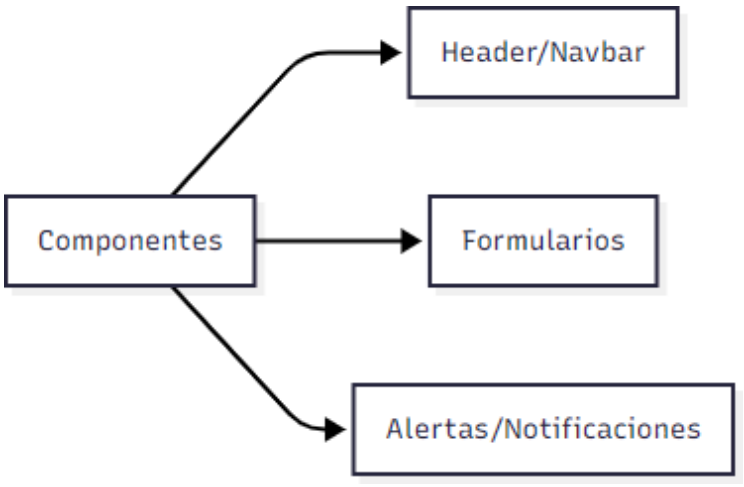
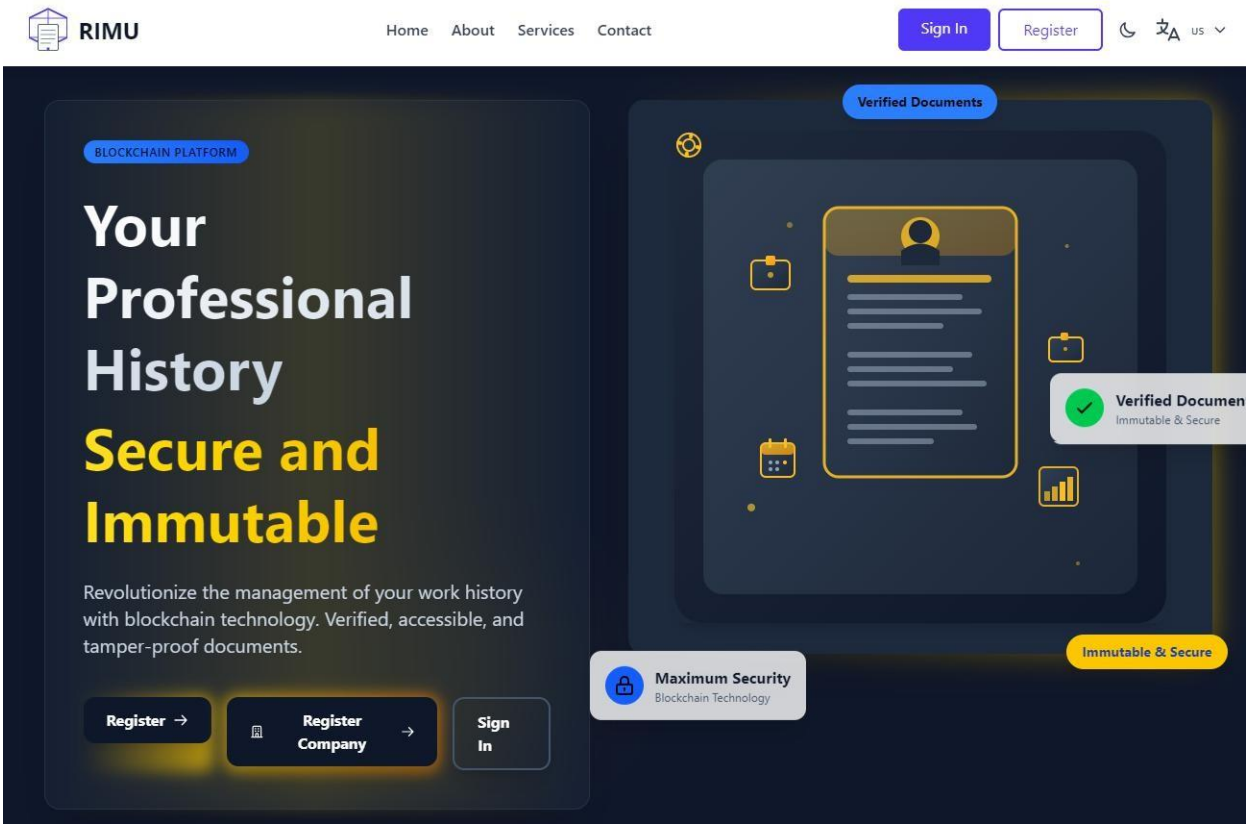


Imagen 7

Home inicial



Nota: en la imagen de *Home inicial* podemos ver la vista principal que recibe al usuario, con una interfaz llamativa y un *header* que lo lleva por varios componentes en los cuales el usuario se puede informar del funcionamiento y propósito del proyecto. Fuente: autoría propia.

Imagen 8

Formulario de registro de usuario normal

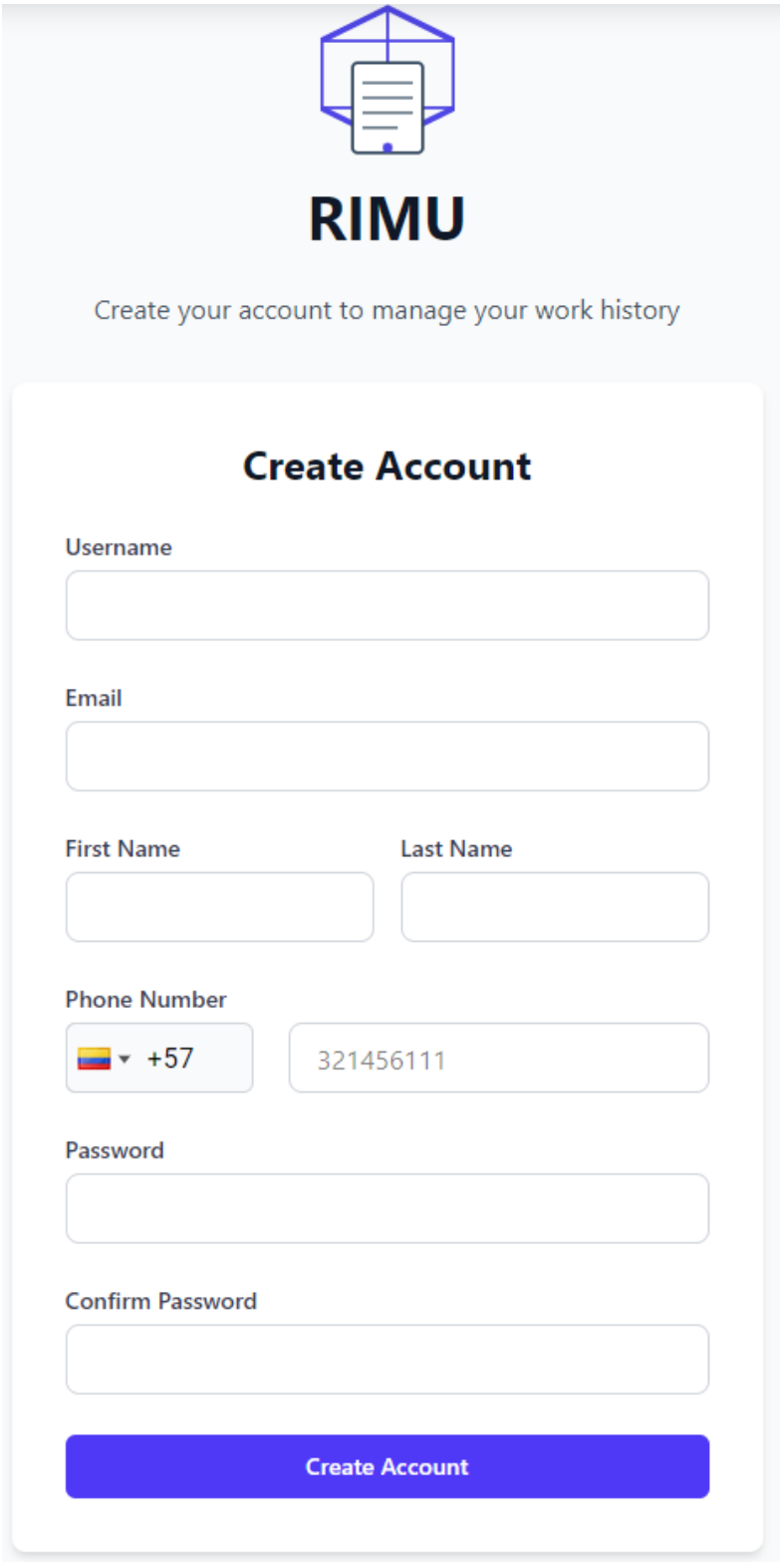


Imagen 9

Formulario de registro de usuario tipo compañía

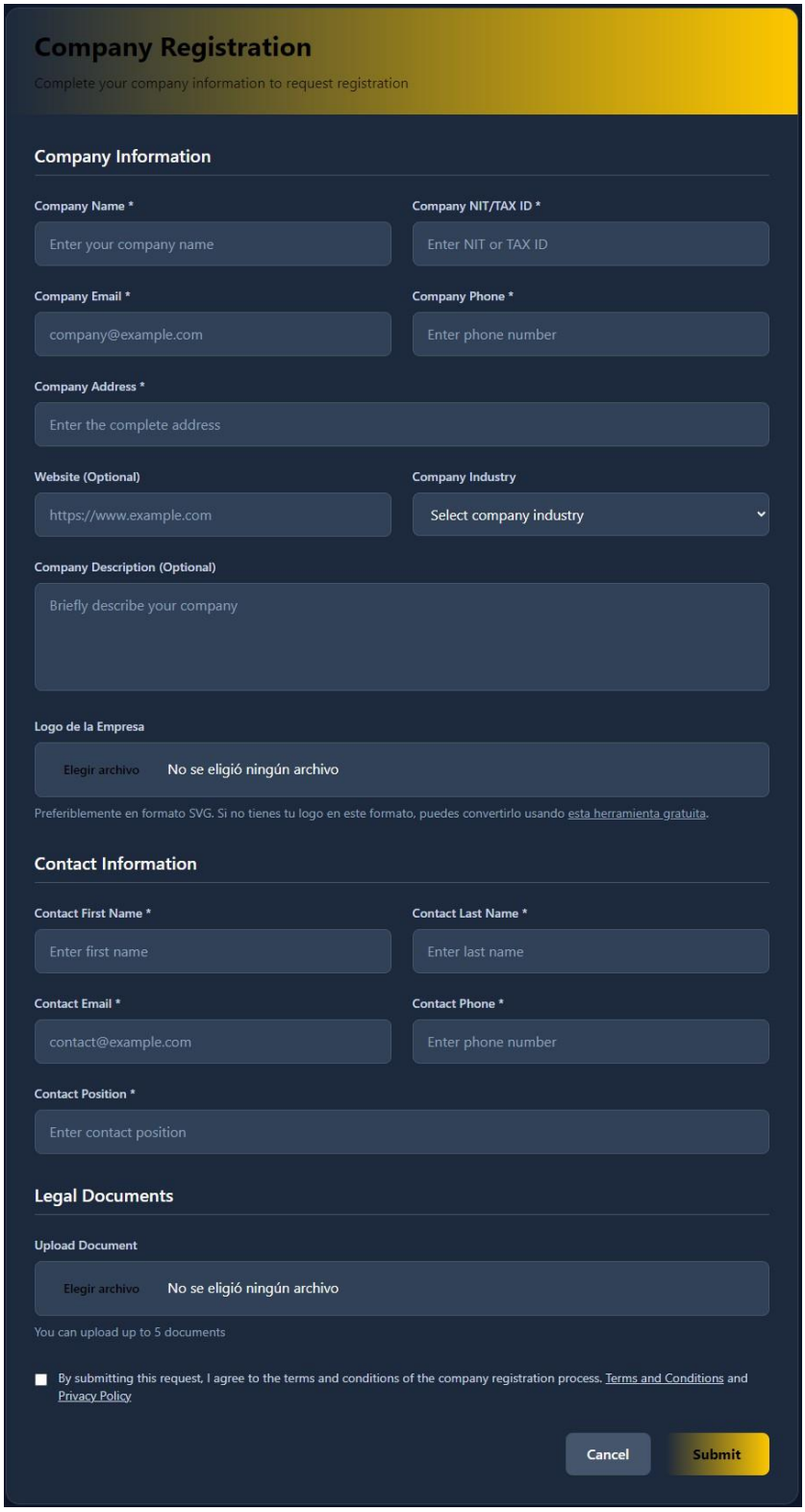
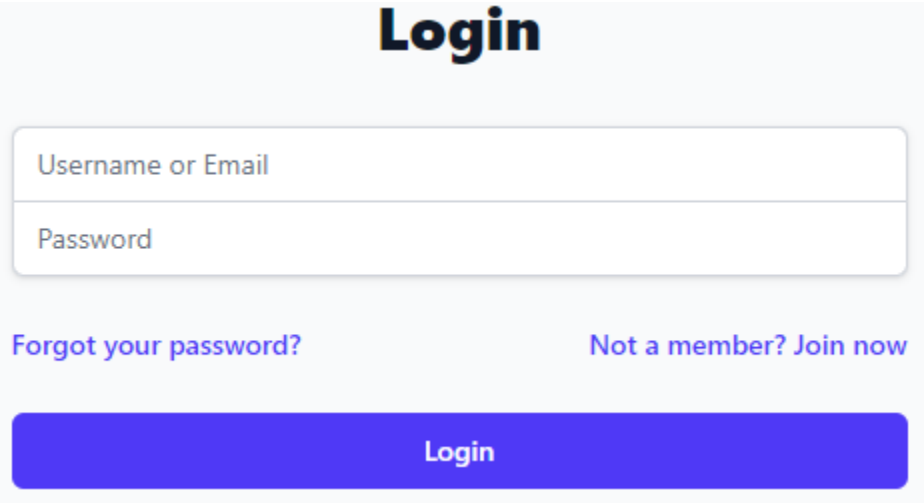


Imagen 10

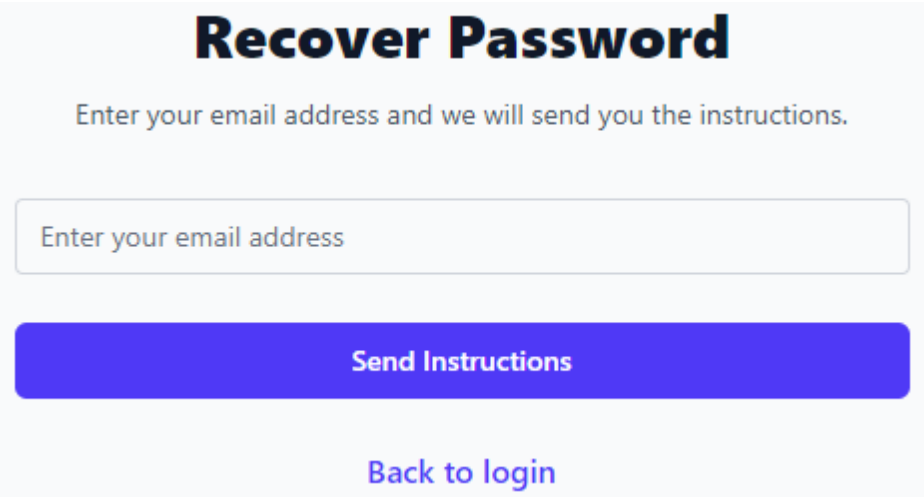
Formulario de login para cualquier tipo de usuario



Nota: El siguiente login implementa un patrón de diseño "Single Sign-On" (SSO) el cual permite que al momento de la autenticación el sistema detecte automáticamente el rol del usuario (Empresa o Persona) y este se redirige automáticamente a su respectivo dashboard. Esto mejora la UX y la seguridad del sistema.

Imagen 11

Formulario de recuperación de contraseña

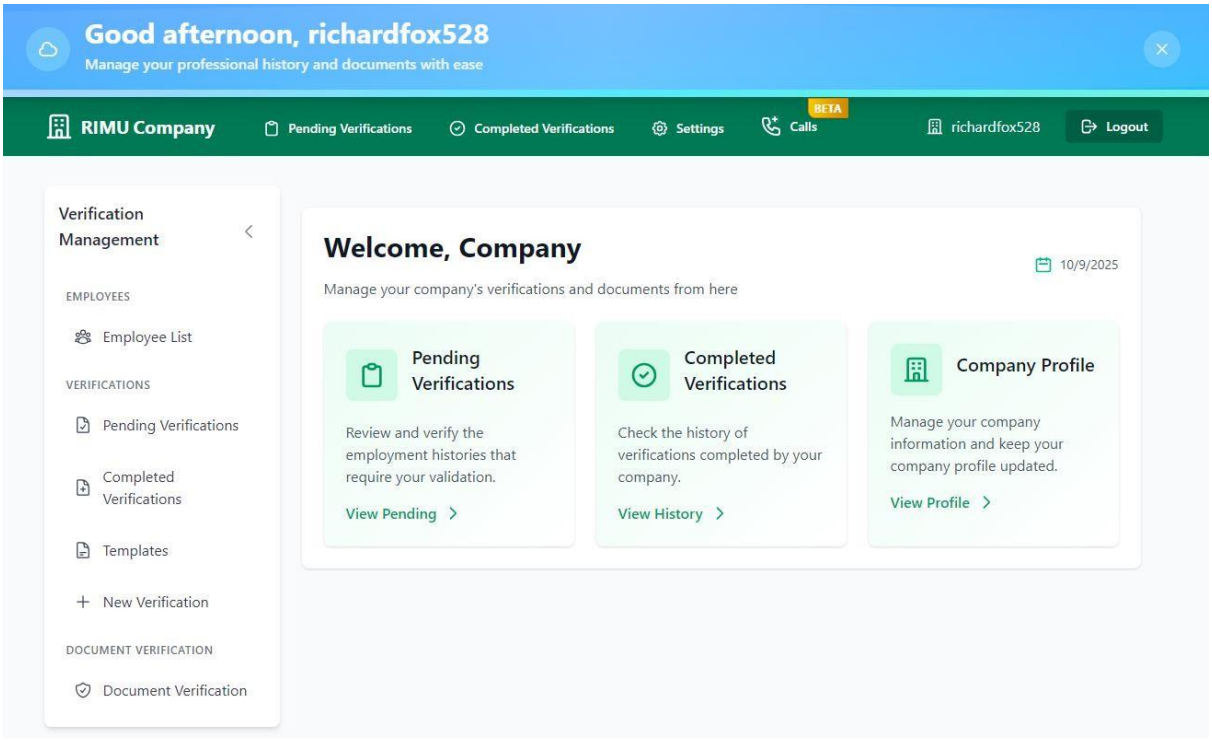


Hasta este punto hemos observado lo principalmente básico que es el punto de acceso para todos los usuarios al visitar el dominio principal del sitio, la página de home y sus demás componentes. Ahora, detallamos lo que cada usuario puede hacer con el sistema dependiendo del tipo de usuario que sea.

Cabe recordar que en el sistema se da prioridad a dos tipos de usuarios. Unos, son los usuarios “normales” que aquellos son los empleados o cualquier otra persona que se registre en el sistema, mientras que los usuarios tipo “Company” son los que obtendrán la mayoría de las herramientas del sistema, pudiendo agregar empleados, firmar y generar documentos etc.

Imagen 12

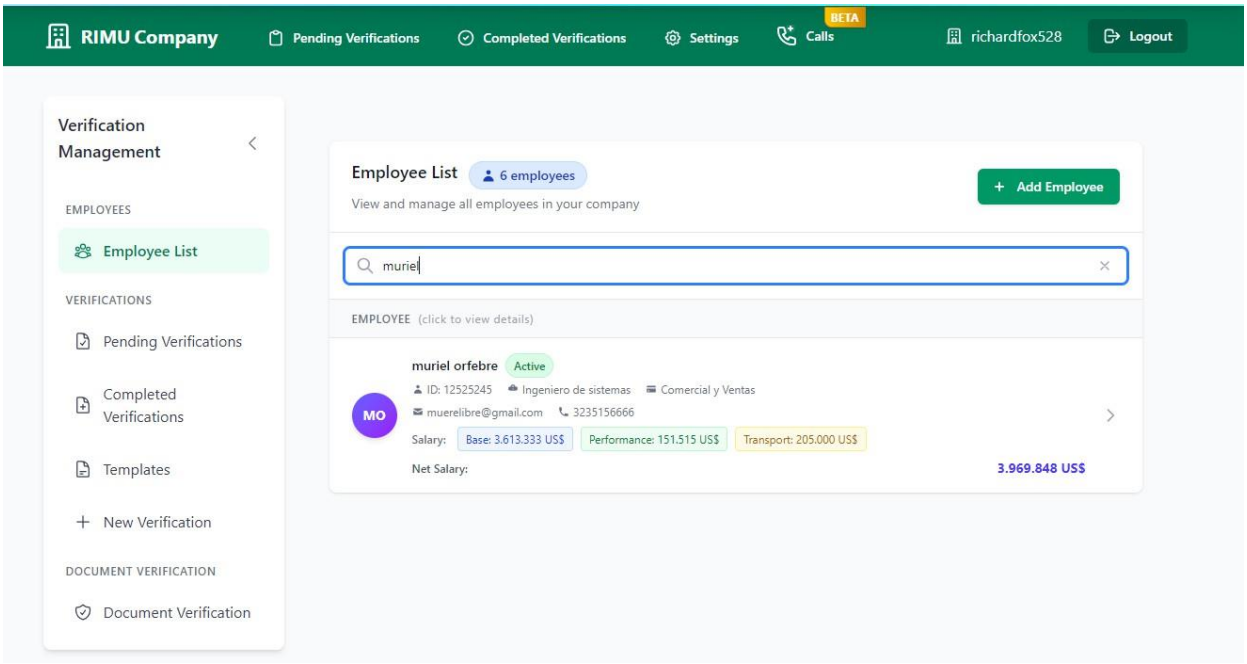
Dashboard de usuario Company



Nota: en la imagen podemos ver el dashboard principal que vería el usuario tipo compañía después de validar credenciales y su login al sistema. Fuente: autoría propia.

Imagen 13

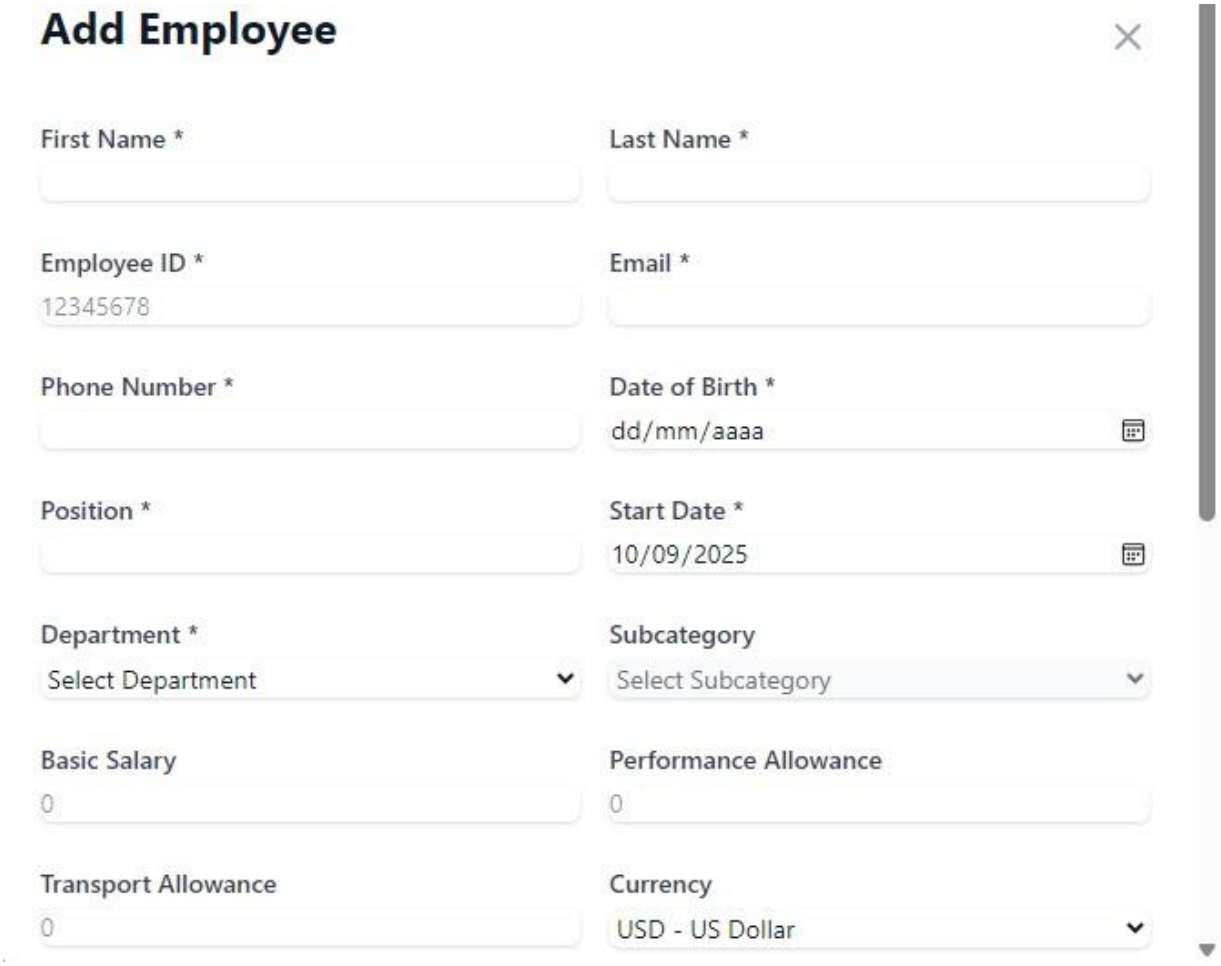
Lista de empleados de la empresa o Company



Nota: en la imagen podemos apreciar como el sistema permite listar todos los empleados y además, con un control de búsqueda hacer que el manejo de estos y la gestión sea mucho más asequible. Fuente: autoría propia.

Imagen 14

Formulario para añadir empleado



Nota: en el formulario para añadir empleado tenemos diferentes inputs para asegurar de tener la mayor información del mismo empleado y así mejorar las herramientas de las que podrá disfrutar después el empleado, se añaden campos como, salario básico de transporte y performance en diferentes tipos de divisas (COP, USD, MXN, EUR, GBP, CAD, ARS, CLP, BRL y PEN) además de esto la inserción del documento de identificación nacional del empleado que quedará directamente alojado en el sistema. Fuente: autoría propia.

Imagen 15

Listado de empleados con verificaciones pendientes

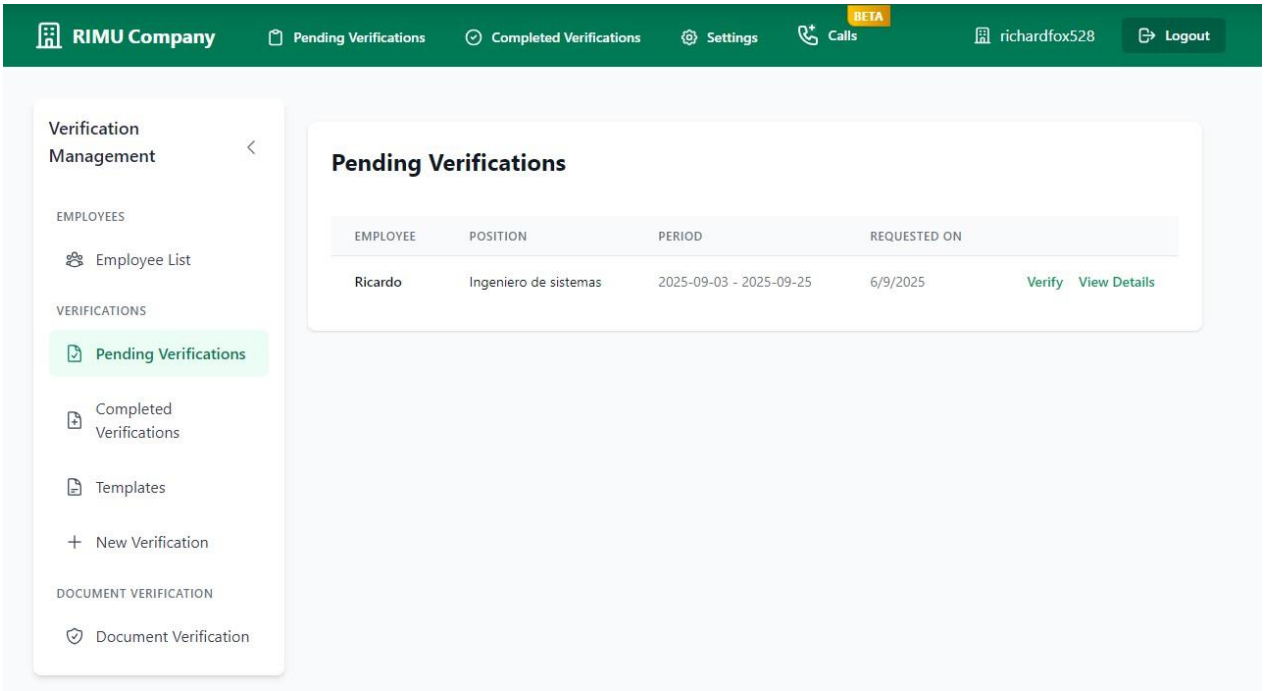
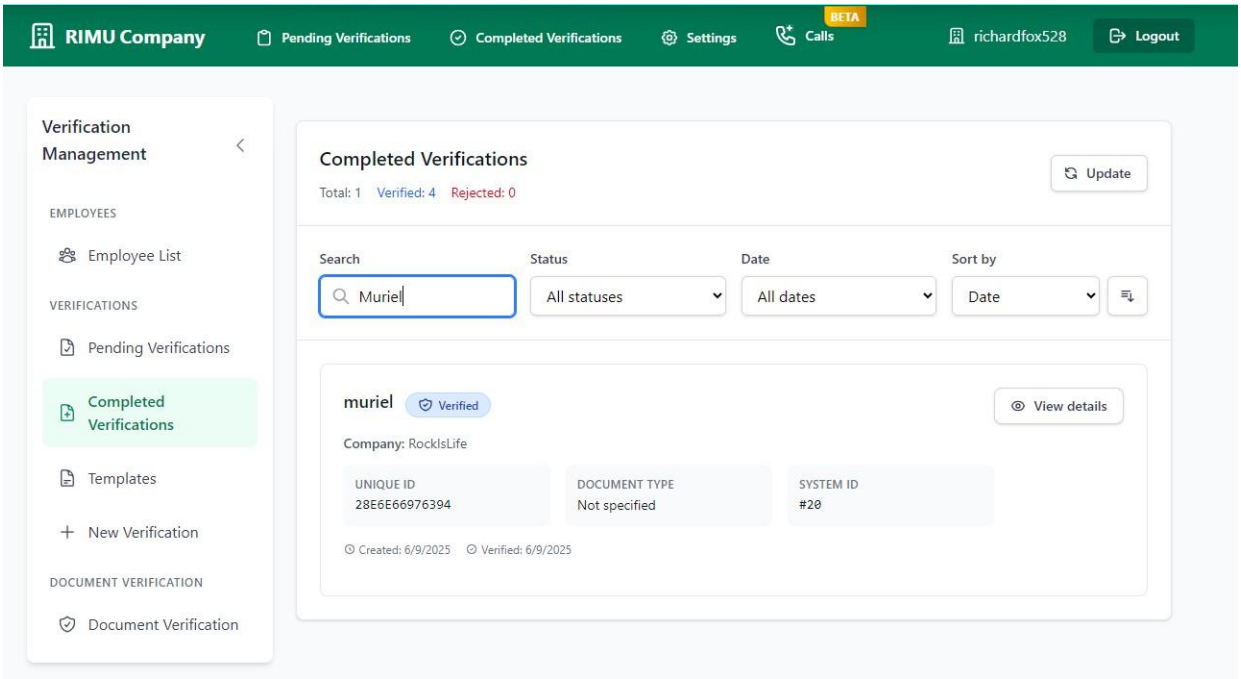


Imagen 16

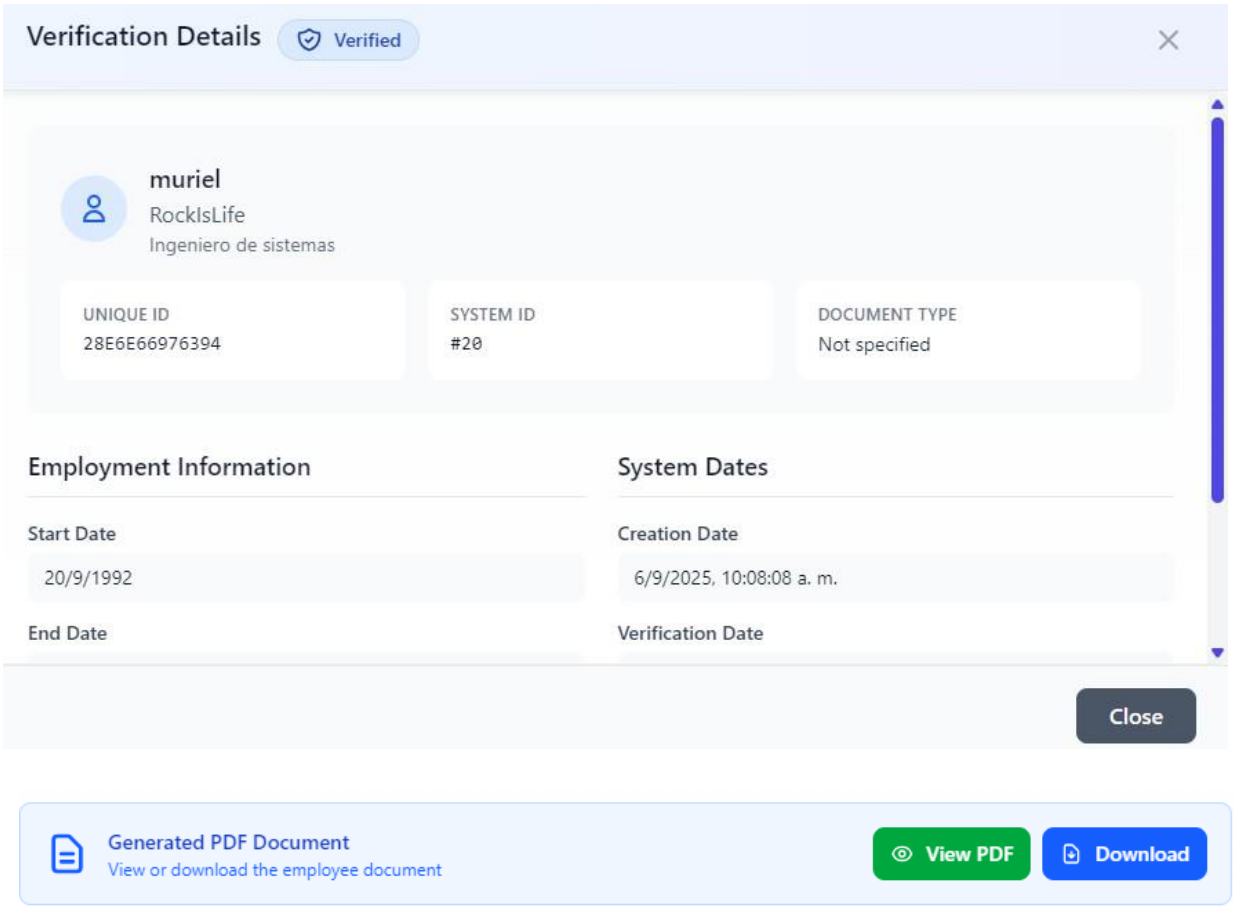
Componente que lista las verificaciones completas



Nota: en la imagen podemos observar como el componente lista todas las verificaciones que han sido completadas satisfactoriamente, ya sea en estado *verified* (completed) o *rejected*, también disponemos de un buscador integrado y múltiples opciones de filtrado para hacer la búsqueda mucho más efectiva y rápida. Fuente: autoría propia.

Imagen 17

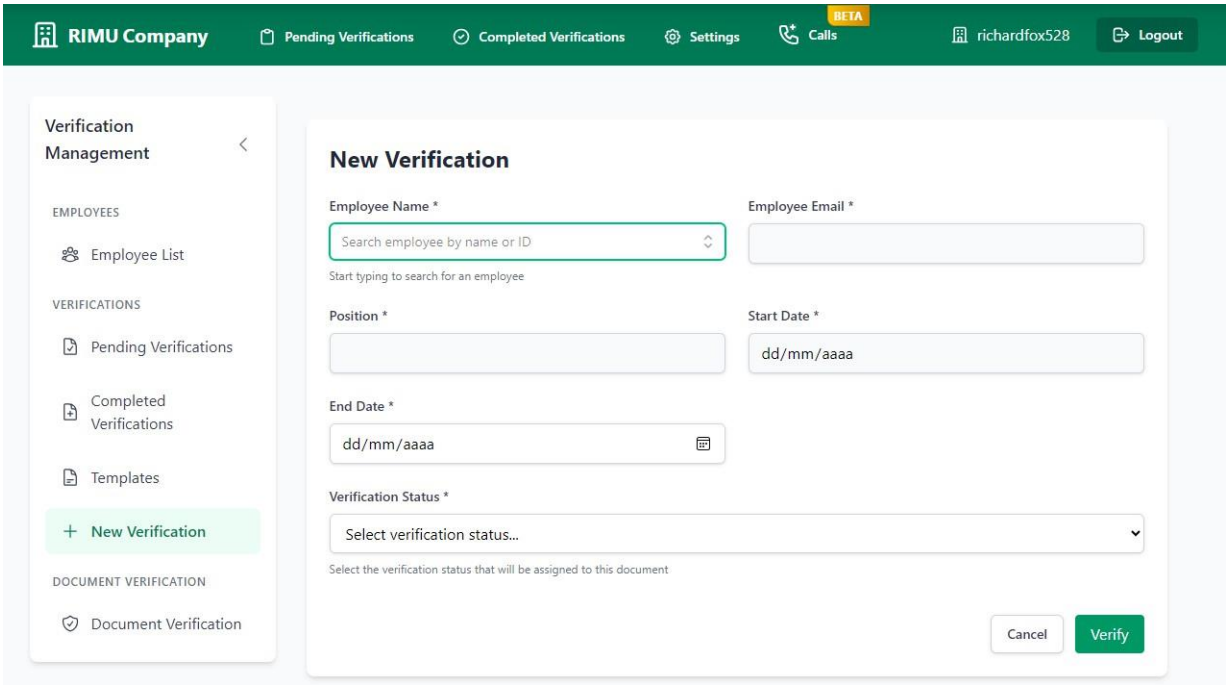
Modal con información detallada de la verificación realizada a dicho empleado



Nota: el modal de visualización de información de los datos de verificaciones nos muestra información principal del empleado verificado como también accedo a su historial laboral, lo que será en este caso la verificación en formato PDF.

Imagen 18

Vista de verificación de empleados



Nota: este componente es esencial para el sistema, pues es el encargado principal de la generación de verificaciones para los empleados de la empresa, en él se emplean diferentes herramientas dan versatilidad y permiten una mayor experiencia de usuario (UX). En el componente basta con buscar el nombre del empleado a verificar y este automáticamente trae los datos necesarios para la generación del documento. Fuente: autoría propia.

Una vez buscado el empleado a verificar el sistema integra automáticamente los datos y al dar clic en el botón de “Veirfy” se genera automáticamente la firma digital junto a los hashes criptográficos que se almacenan automáticamente en la base de datos, generando así un mayor control de esos mismos datos para los usuarios empleados a quienes se les originó el documento.

La generación de esta verificación también va acompañada por un código único de identificación de ese documento, el cual se puede consultar desde la misma plataforma. Principalmente, se dispone de un ID que es un identificador único de 13 caracteres que se añade

como metadatos al documento y también se almacena en la base de datos. Este identificador tiene un formato alfanumérico como el siguiente “EF3AAEEEAB364”. Además de esto, el documento viene acompañado con un hash criptográfico que también ayuda en la veracidad y unicidad de los documentos.

De esta manera al final del documento PDF generado tendríamos los datos tanto ID como HASH que son mediante el cual futuramente nos permitirá realizar la búsqueda exacta de estos mismos.

ID: 6A977F6E8F904 | Hash: d1f721d897fc028fcdf14b951b4dc3d9ea26f30bb30d48d87e3c6d585dd7966d

Una vez explicado la función y herramientas con la que cuenta el componente, visualizamos la estructura disponible para la búsqueda y comprobación de los documentos. Como dije anteriormente, las opciones de búsqueda admiten el ID de documento, pero además de este también se añade el campo de identificación del empleado, generando de esta forma una manera más simple de consultar y verificar estos documentos.

Imagen 19

Modal con detalles del documento verificado

Nota: el modal representa los datos de los empleados los cuales han sido verificados por alguna de las empresas relacionadas con el sistema. Este se encuentra en la barra lateral de navegación en la sección de *Document Verification* donde se dispone de un formulario donde se introducen los datos a buscar ya sea el Id Único del documento o Id del empleado. Fuente: autoría propia.

Especificación Técnica

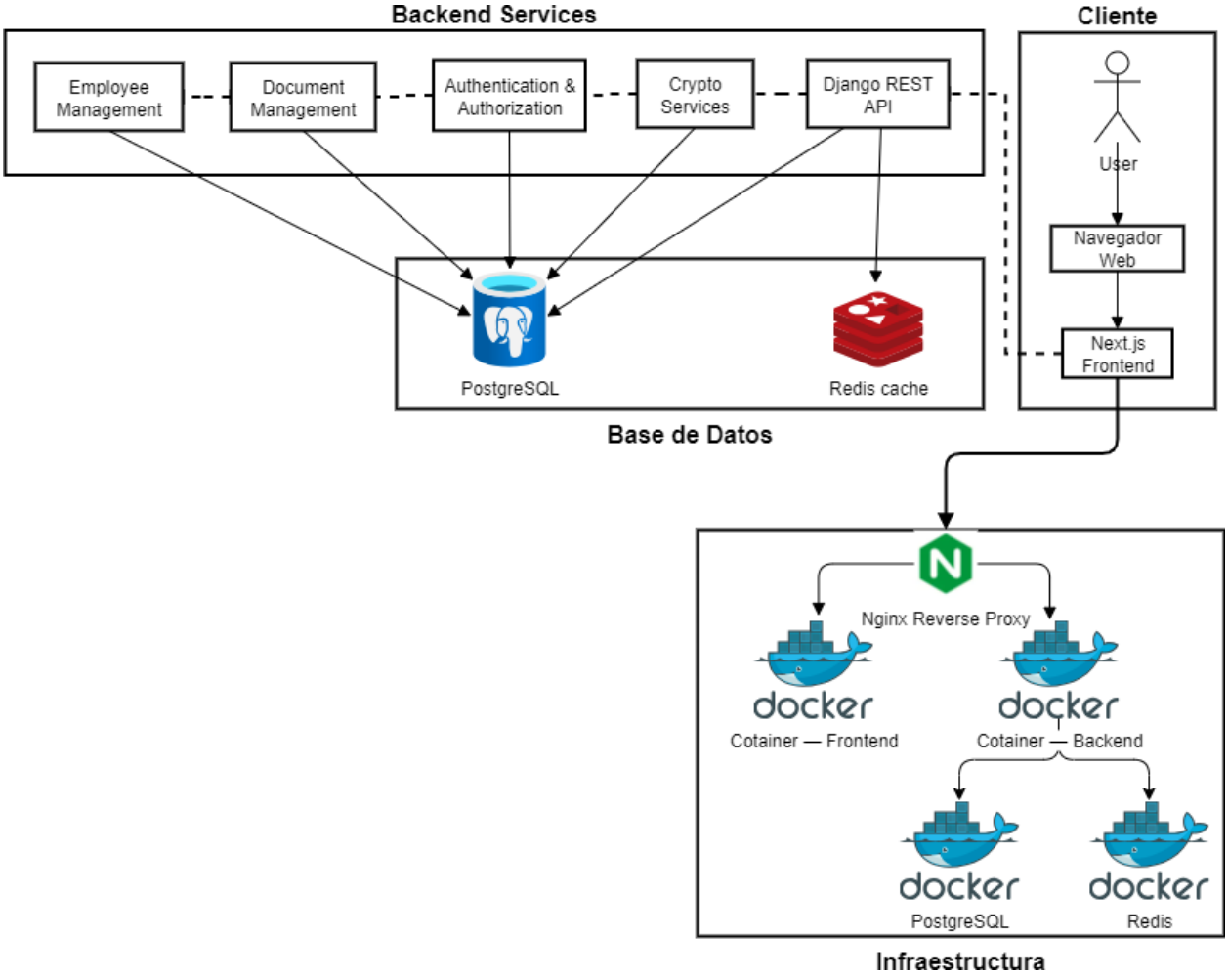
Infraestructura (Docker, entornos)

La implementación general consta de diversas tecnologías. Entre estas encontramos un administrador de aplicaciones dentro de contenedores llamado Docker, el cual nos permitirá instalar en un entorno aislado cada una de las funcionalidades y servicios de RIMU. Como segunda opción encontramos el servidor web que se encargara de la comunicación inversa entre los demás servicios (contenedores) de Docker, se utiliza Nginx una herramienta Open Source al igual que la primera que permite gestión web mediante protocolos TCP/UDP ofreciendo un gran desempeño en la comunicación de proxy inverso.

Cada uno de estos servicios estarán alojados en un entorno aislado como se pronunció anteriormente, permitiendo que cada servicio o herramienta tenga mayor control de recursos sin que interfiera entre las demás. Esto genera una mayor eficiencia dentro del sistema y sus servicios.

Diagrama 35

Arquitectura general del sistema



Desarrollo Back-end

La arquitectura back-end requiere una combinación estratégica de patrones de diseño, tecnologías escalables y prácticas de seguridad que garanticen la integridad, confidencialidad y disponibilidad de los servicios. En el contexto de los flujos de autenticación y autorización previamente diagramados, el back-end debe implementar una arquitectura de microservicios o monolítica modular que facilite la separación de responsabilidades y el mantenimiento del código.

Herramientas Back-end:

Tabla 6

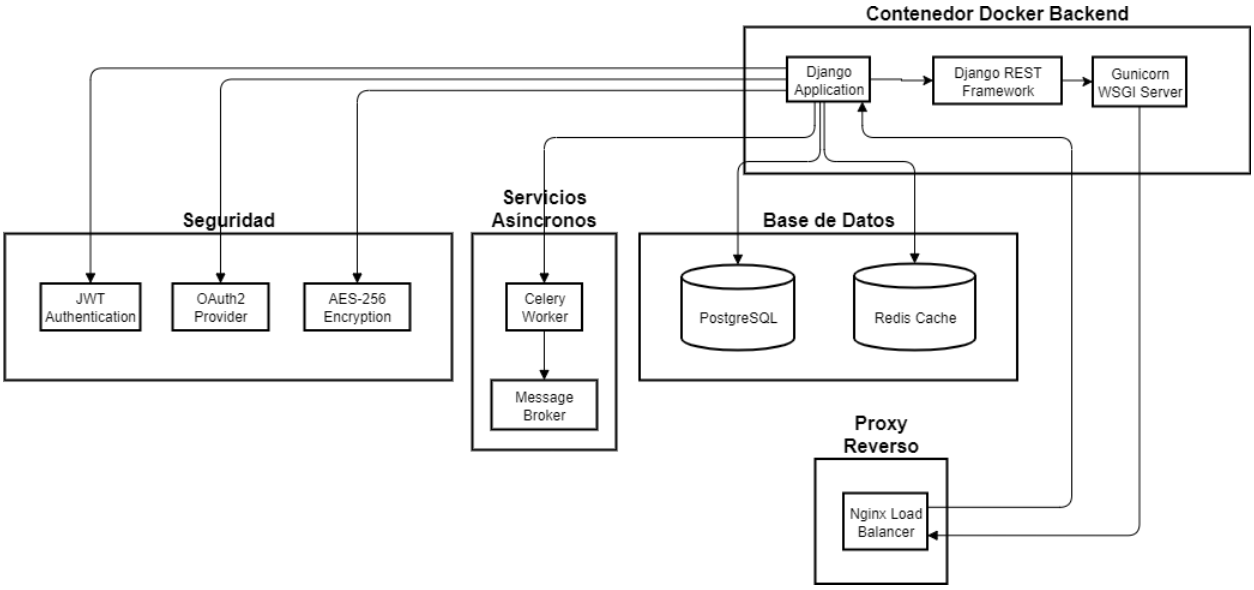
Lista de Herramientas Utilizadas en Back-end

Herramienta	Descripción
Django Application	Framework web de alto nivel para construir aplicaciones web rápidas y eficientes en Python.
Django REST Framework	Conjunto de herramientas para construir API RESTful de manera sencilla y rápida con Django.
Gunicorn WSGI Server	Servidor HTTP para aplicaciones Python que permite manejar múltiples solicitudes simultáneamente.
PostgreSQL	Sistema de gestión de bases de datos relacional y objeto, conocido por su robustez y flexibilidad.
Redis Cache	Almacenamiento en memoria que se utiliza como base de datos, caché y broker de mensajes.
Celery Worker	Herramienta para ejecutar tareas asíncronas en segundo plano, ideal para manejar trabajos en cola.
Message Broker	Sistema que permite la comunicación entre diferentes servicios, facilitando la mensajería asíncrona.
JWT Authentication	Método de autenticación que utiliza tokens JSON Web para verificar la identidad de los usuarios.
OAuth2 Provider	Protocolo de autorización que permite a las aplicaciones acceder a recursos en nombre de un usuario.
AES-256 Encryption	Algoritmo de cifrado simétrico que proporciona un alto nivel de seguridad para proteger datos.
Nginx Load Balancer	Servidor web que actúa como proxy inverso y balanceador de carga, distribuyendo el tráfico entre múltiples servidores.

Nota: la lista de herramientas son las principales que se usan en el proyecto, esto no indica que alguna de estas dependa de otra y no esté especificada. Fuente: autoría propia.

Diagrama 36

Implementación de Implementación Back-end



Desarrollo Front-end

En cuanto a la arquitectura front-end del proyecto, este permite desarrollar experiencias de usuario atractivas y eficientes. Frameworks como Next.js y React permiten la creación de aplicaciones basadas en componentes, lo que facilita la reutilización del código. Además, para lograr un estilo moderno, el proyecto incorpora Tailwind CSS y PostCSS, que permiten diseñar interfaces responsivas de manera ágil. También, al utilizar Next.js, se dispone de herramientas como Webpack y Terser, que optimizan el código y mejoran los tiempos de carga.

Tabla 7

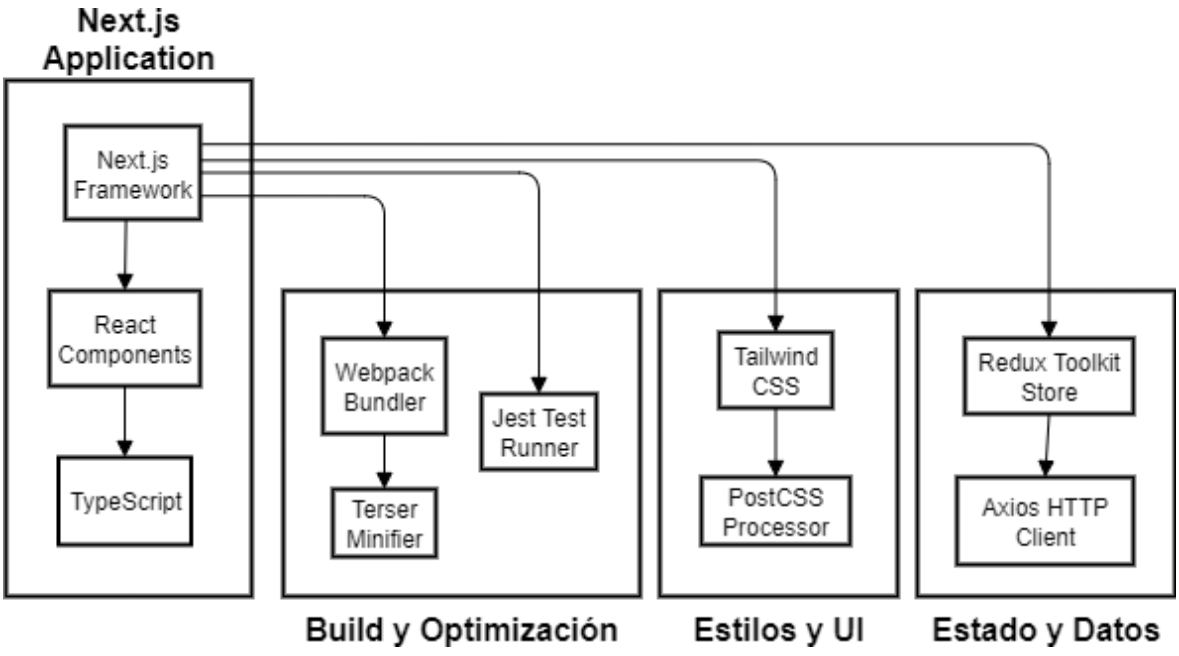
Lista de Herramientas Utilizadas en Front-end

Herramienta	Descripción
Next.js Framework	Framework de React para construir aplicaciones web y sitios estáticos con renderizado del lado del servidor (SSR).
React Components	Componentes reutilizables que permiten construir interfaces de usuario interactivas en aplicaciones React.
TypeScript	Superset de JavaScript que añade tipado estático, mejorando la calidad y mantenibilidad del código.

Redux Toolkit Store	Biblioteca para manejar el estado global de la aplicación de manera predecible y eficiente.
Axios HTTP Client	Cliente HTTP basado en promesas que facilita la realización de solicitudes a API.
Tailwind CSS	Framework de CSS utilitario que permite crear diseños personalizados de manera rápida y eficiente.
PostCSS Processor	Herramienta para transformar CSS con plugins, permitiendo la adición de características modernas.
Webpack Bundler	Herramienta de empaquetado de módulos que permite optimizar y gestionar recursos en aplicaciones web.
Terser Minifier	Herramienta para minimizar el código JavaScript, reduciendo su tamaño y mejorando el rendimiento.
Jest Test Runner	Framework de pruebas para JavaScript que permite realizar pruebas unitarias y de integración de manera sencilla.

Diagrama 37

Arquitectura de Implementación Front-end



Despliegue y Mantenimiento

Estrategia de Despliegue

La estrategia de despliegue adoptada para la plataforma se basa en principios de DevOps modernos, integrando prácticas de desarrollo continuo, automatización y monitoreo proactivo. Esta estrategia garantiza la entrega confiable de software mientras minimiza los riesgos asociados con los despliegues en producción.

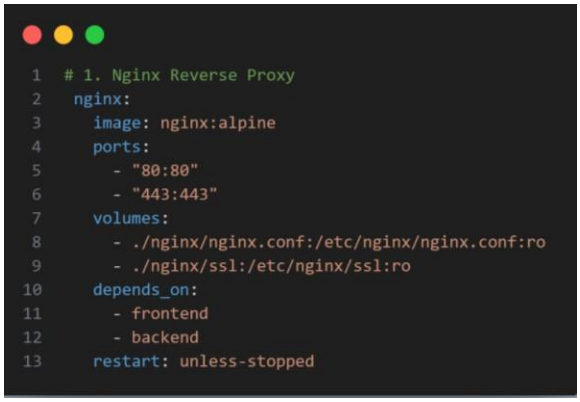
Entornos de Desarrollo (Local – Compartido)

La arquitectura de entornos se organiza en una jerarquía de dos niveles, cada uno diseñado para cumplir propósitos específicos en el ciclo de vida del proyecto. El entorno de desarrollo local ofrece a cada desarrollador un espacio de trabajo aislado. Este utiliza Docker y Docker Compose para orquestar los servicios, lo que permite la ejecución integral de la aplicación en la máquina del desarrollador y su visualización real en entornos de producción. Además, para el entorno compartido se emplea Git, Git Flow y otras herramientas para facilitar el desarrollo colaborativo.

- **Servicios:**

Imagen 20

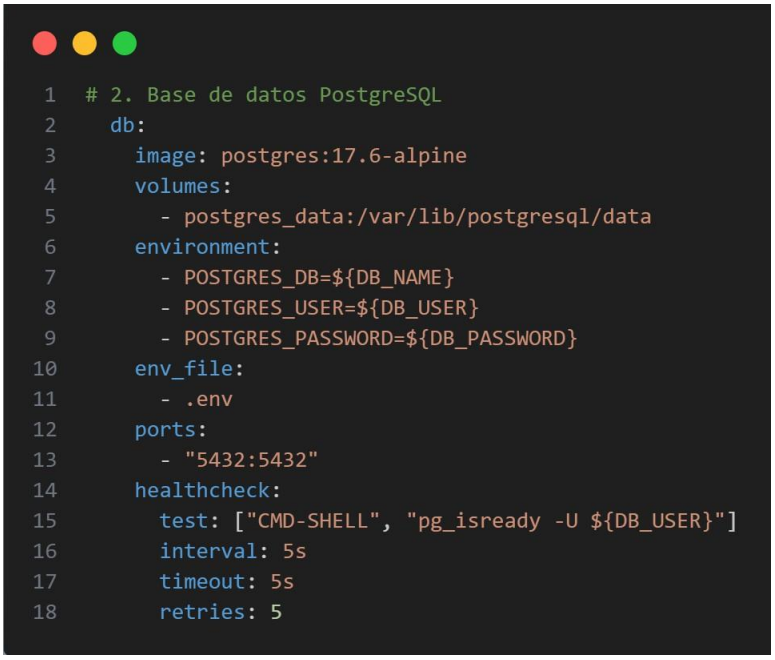
Servicio Nginx en Docker



```
# 1. Nginx Reverse Proxy
 nginx:
   image: nginx:alpine
   ports:
     - "80:80"
     - "443:443"
   volumes:
     - ./nginx/nginx.conf:/etc/nginx/nginx.conf:ro
     - ./nginx/ssl:/etc/nginx/ssl:ro
   depends_on:
     - frontend
     - backend
   restart: unless-stopped
```

Imagen 21

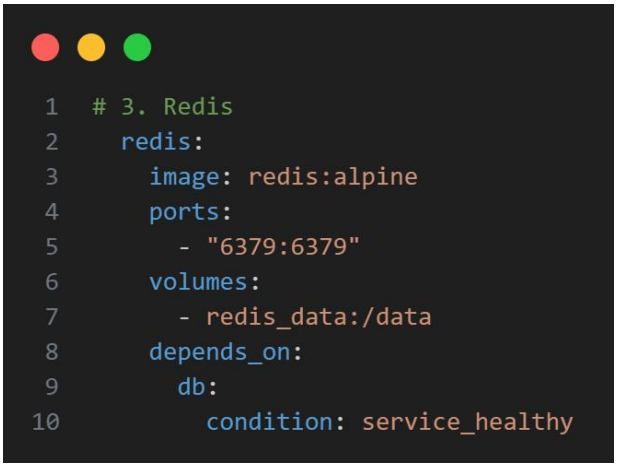
Servicio de PostgreSQL en Docker



```yaml
# 2. Base de datos PostgreSQL
  db:
    image: postgres:17.6-alpine
    volumes:
      - postgres_data:/var/lib/postgresql/data
    environment:
      - POSTGRES_DB=${DB_NAME}
      - POSTGRES_USER=${DB_USER}
      - POSTGRES_PASSWORD=${DB_PASSWORD}
    env_file:
      - .env
    ports:
      - "5432:5432"
    healthcheck:
      test: ["CMD-SHELL", "pg_isready -U ${DB_USER}"]
      interval: 5s
      timeout: 5s
      retries: 5
```

Imagen 22

Servicio de Redis en Docker



```yaml
# 3. Redis
  redis:
    image: redis:alpine
    ports:
      - "6379:6379"
    volumes:
      - redis_data:/data
    depends_on:
      db:
        condition: service_healthy
```

Imagen 23

Construcción del Back-end en Docker

```yaml
# 4. Backend (sin puerto expuesto directamente)
  backend:
    build: ./backend
    # ports: Solo accesible a través de nginx
    #   - "8000:8000"
    volumes:
      - ./backend:/code
    environment:
      - DJANGO_SETTINGS_MODULE=voxlyne.settings
      - DB_HOST=db
      - REDIS_HOST=redis
    env_file:
      - .env
    command: >
      sh -c "python manage.py makemigrations && python manage.py migrate && python manage.py runserver 0.0.0.0:8000"
    depends_on:
      db:
        condition: service_healthy
      redis:
        condition: service_started
```

Nota: la construcción de esta imagen de Backend depende del archivo Dockerfile ubicado en la carpeta backend, por eso el build busca dicho archivo en el directorio ./backend. Fuente: autoría propia.

Imagen 24

Construcción del Front-end en Docker

```yaml
# 5. Frontend (sin puerto expuesto directamente)
  frontend:
    build: ./frontend
    # ports: Solo accesible a través de nginx
    #   - "3000:3000"
    depends_on:
      - backend
```

Nota: al igual que la imagen de backend está también busca el archivo Dockerfile ubicado en el directorio frontend (./frontend), esta imagen es co-dependiente de la anterior, backend. Al igual ambas, en el servidor de Nginx. Fuente: autoría propia.

Imagen 25

Volúmenes de Datos dentro de Docker

```
volumes:
  postgres_data:
  redis_data:
```

Entorno de Producción

Para el entorno de producción ya utilizamos un entorno más profesional en el cual contamos con un VPS (Virtual Private Server) en el que podemos desplegar el proyecto como tal. Para este deploy se utilizó Azure Cloud, y se configuró un VPS con todas sus interfaces de redes y recursos necesarios lanzar el proyecto.

Diagrama 38

Visualizador de recursos creados conectados a la máquina virtual

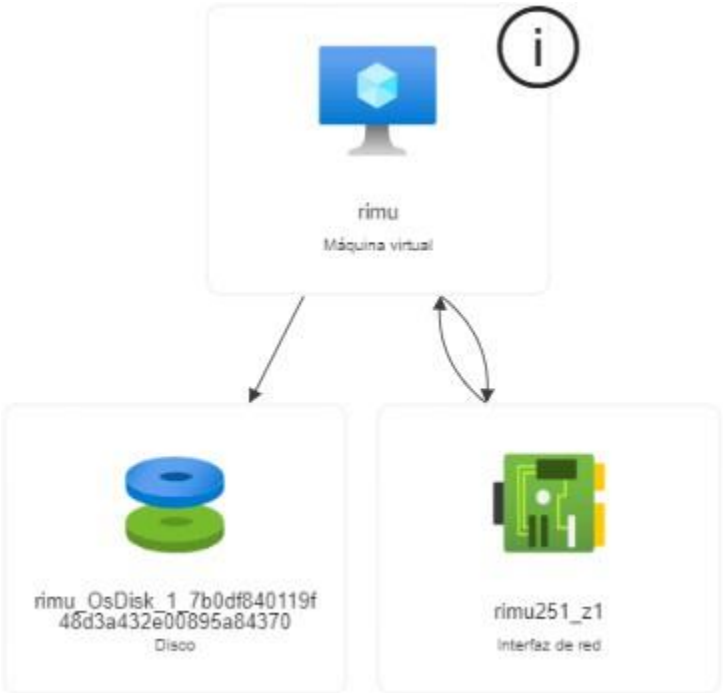
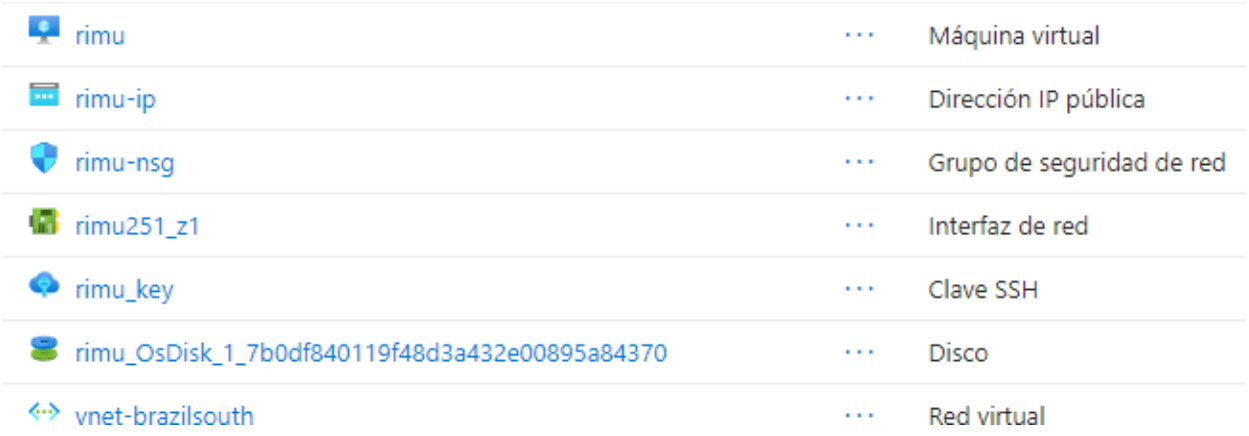


Imagen 26

Total de grupos de recursos creados para la máquina virtual



Nota: la máquina virtual está configurada en un servidor con sistema operativo Linux y con su imagen Ubuntu-24_04.

En el entorno donde la aplicación esta activa y funcional es primordial el uso de flujos de trabajo (Git Flows) que ayuden a registrar eventos relacionados con el sistema, estos pueden ser fallos de este o incluso fallos con algunos de los recursos de servidor, estos se agregaran a un registro en nuestro server en el cual posteriormente podemos consultar evaluar o solucionar fallos.

Plan de Mantenimiento

En el plan de mantenimiento se implementa una estrategia la cual consta de:

Monitoreo

En el monitoreo, se prioriza una observabilidad integral del entorno de producción. Como se mencionó anteriormente, se supervisan los registros generados por el sistema en busca de anomalías que puedan surgir. Este enfoque permite identificar y abordar cualquier problema de manera efectiva, garantizando que la producción del sistema no se vea afectada.

Además, se implementan herramientas de análisis en tiempo real que facilitan la detección proactiva de incidencias, lo que permite a los equipos de desarrollo y operaciones reaccionar rápidamente. Las alertas personalizadas también contribuyen a una respuesta ágil ante situaciones críticas, asegurando que se mantenga la estabilidad y el rendimiento óptimo del sistema en todo momento. La integración de flujos de trabajo de Git en este proceso permite una gestión más eficiente de las actualizaciones y cambios, mejorando aún más la capacidad de respuesta y la calidad del servicio.

Actualizaciones

El plan de actualizaciones o evolución continua se llevará a cabo de manera escalonada, aprovechando todas las ventajas del desarrollo compartido que ofrece Git. Este proceso se realiza de forma controlada mediante un sistema de revisión de ramas (Actions), a partir del cual se implementarán nuevas funcionalidades y soluciones. Estas acciones están programadas para que, con cada merge o creación de un nuevo flujo, se realicen pruebas automatizadas que verifiquen la integridad del código y la funcionalidad de la aplicación.

Además, se establecen protocolos de comunicación entre los equipos para asegurar que todos los miembros estén al tanto de los cambios y puedan colaborar de manera efectiva. Esto incluye la documentación de cada actualización, así como la creación de un registro de cambios que facilite el seguimiento de las modificaciones realizadas. De esta manera, se garantiza una evolución continua y fluida del entorno de desarrollo, minimizando riesgos y maximizando la calidad del producto final.

Conclusiones y Trabajo Futuro

Logros del Proyecto

El desarrollo de la plataforma RIMU, representa un avance significativo en la intersección entre tecnologías criptográficas, gestión documental y transformación digital de procesos laborales. Este proyecto ha logrado consolidar múltiples tecnologías emergentes en una solución coherente y escalable, demostrando la viabilidad técnica y comercial de una solución innovadora que combina tecnologías emergentes para revolucionar la gestión de historiales laborales. Entre los logros destacados se incluyen la integración exitosa de diversas tecnologías de la web tradicional junto con seguridad criptográfica basada en blockchain, permitiendo la creación de registros inmutables y verificables que eliminan la posibilidad de alteraciones no autorizadas y fortalecen la confianza en los procesos de verificación de empleos. La plataforma ha logrado desarrollar una arquitectura escalable y modular, utilizando microservicios implementados en lenguajes modernos como Python, JavaScript, Go y Rust, lo que facilita el mantenimiento, la expansión y la integración con sistemas externos. Además, se ha implementado soporte multilingüe para español, francés y portugués, ampliando el alcance global de la solución y mejorando la accesibilidad para usuarios internacionales. Estas implementaciones generarán un precedente para futuras innovaciones en la intersección de criptografía, gestión documental y automatización inteligente.

Lecciones Aprendidas

Las lecciones que ha proporcionado la realización de este proyecto han sido fundamentales para el avance y desarrollo de soluciones tecnológicas innovadoras, destacando la complejidad inherente a las arquitecturas de microservicios que, aunque ofrecen beneficios significativos en escalabilidad y mantenibilidad, introducen desafíos sustanciales en la

coordinación entre servicios, el debugging distribuido y la gestión de transacciones, enfatizando la necesidad de invertir tiempo considerable en el diseño de APIs consistentes y la implementación de sistemas de observabilidad robustos desde las primeras etapas del proyecto. La integración de tecnologías heterogéneas ha revelado oportunidades y desafíos, demostrando que la combinación de lenguajes de programación maduros con tecnologías emergentes requiere no solo experticia técnica, sino también una comprensión profunda de los trade-offs entre rendimiento, mantenibilidad y velocidad de desarrollo, subrayando la importancia de evaluar cuidadosamente el stack tecnológico en función de los requisitos específicos. El enfoque proactivo en seguridad ha demostrado ser invaluable, revelando que esta no puede ser tratada como un componente adicional, sino que debe ser integrada desde el diseño arquitectónico, incluyendo la implementación de defensa a profundidad, auditorías de seguridad regulares y el fomento de una cultura de seguridad en todo el equipo de desarrollo. Finalmente, la gestión de estado distribuido mediante sistemas de caché y sesiones ha proporcionado perspectivas valiosas sobre los desafíos de la consistencia en entornos distribuidos, donde experiencias con las condiciones del proyecto y problemas de sincronización han enfatizado la necesidad de diseñar protocolos de comunicación robustos y estrategias de manejo de fallos comprehensivas para asegurar la fiabilidad y el rendimiento del sistema.

Líneas de Trabajo Futuras

Las líneas de trabajo futuras del proyecto se centran en la evolución tecnológica y funcional para potenciar la plataforma, destacando áreas clave como, inteligencia artificial, arquitectura de sistemas y seguridad, con el objetivo de expandir capacidades y mejorar la eficiencia en la gestión de historiales laborales.

Algunas de estas implementaciones futuras incluirían:

- **Inteligencia Artificial y Aprendizaje Automático:** Análisis predictivo de documentos mediante machine learning para identificar patrones y riesgos, procesamiento de lenguaje natural para extracción automática de información estructurada, y sistemas de recomendación para mejoras en contratos basadas en análisis comparativo.
- **Arquitectura de microservicios avanzada:** Implementación de service mesh para observabilidad y seguridad, transición a arquitectura basada en eventos, y exploración de funciones serverless para componentes variables.
- **Expansión de la plataforma:** Sistema de evaluación continua con verificación criptográfica de talento para conectar empresas con candidatos verificados, e integraciones con sistemas de RR. HH. para automatizar onboarding y offboarding.
- **Mejoras en seguridad y privacidad:** Encriptación homomórfica para análisis de datos encriptados, integración con identidad descentralizada para mayor privacidad, y detección de amenazas avanzada basada en machine learning.
- **Investigación en escalabilidad:** Sharding inteligente con particionamiento automático, edge computing para reducir latencia, y estrategias multi-cloud para distribución de carga.
- **Mejoras en experiencia de usuario:** Interfaces adaptativas personalizables e interfaces de voz para accesibilidad.

Impacto Esperado

Debido a que la plataforma cuenta con una gran cantidad de servicios necesarios y con el potencial de transformar cómo las organizaciones gestionan la información laboral y cómo los individuos controlan su historial profesional, se proyecta un impacto económico significativo

mediante ahorros para las empresas al reducir costos en verificación, disputas contractuales y procesos administrativos, mientras facilita a los individuos una mayor movilidad laboral con verificaciones instantáneas de credenciales. Socialmente, la democratización del acceso a verificaciones laborales confiables podría reducir la desigualdad en el mercado laboral, especialmente en economías emergentes donde los sistemas tradicionales son costosos o inexistentes, contribuyendo además a la formalización del empleo y la reducción del trabajo informal. Desde una perspectiva tecnológica, como caso de estudio en la integración de tecnologías emergentes, RIMU avanzará el estado del arte en sistemas distribuidos, blockchain aplicado a casos empresariales y arquitecturas de microservicios heterogéneas, sirviendo sus patrones y soluciones como referencia para proyectos similares en diversos dominios. En términos de sostenibilidad a largo plazo, su diseño modular y arquitectura extensible aseguran una evolución continua, respaldada por documentación comprensiva, pruebas automatizadas y procesos de CI/CD que establecen una base sólida para el mantenimiento y la innovación tecnológica. En conclusión, RIMU representa no solo una solución técnica innovadora, sino también un modelo para el desarrollo de sistemas empresariales que integran tecnologías emergentes de manera responsable y sostenible, donde los logros obtenidos y las lecciones aprendidas servirán como fundamento para futuras innovaciones en la transformación digital de procesos laborales.

Bibliografía

Adams, C., Cain, P., Pinkas, D., & Zuccherato, R. (8 de 2001). *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*. Obtenido de Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP): https://www.rfc-editor.org/rfc/rfc3161

Alvarracín Toledo, M. (2025). *Alvarracín Toledo, M. F. (2025). Blockchain aplicado a contratación pública privilegiando la transparencia; un enfoque desde el proceso de selección de menor cuantía*. Obtenido de Alvarracín Toledo, M. F. (2025). Blockchain aplicado a contratación pública privilegiando la transparencia; un enfoque desde el proceso de selección de menor cuantía: https://dspace.ucuenca.edu.ec/items/2c4978d3-84e0-4816-ab70-a3fa693ad204

Argentina, C. d. (27 de 9 de 1974). *Argentina*. Obtenido de https://www.argentina.gob.ar: https://www.argentina.gob.ar/normativa/nacional/ley-20744-25552

Barrenechea L., C. F. (2020). *Barrenechea L., Castellano F. Á., Guevara S. A., Sánchez R. A. (2020). Modelo de negocio para un sistema de seguridad, respaldo y verificación digital basado en el Blockchain para la gestión documental de notarías en Lima Moderna*. Obtenido de Barrenechea L., Castellano F. Á., Guevara S. A., Sánchez R. A. (2020). Modelo de negocio para un sistema de seguridad, respaldo y verificación digital basado en el Blockchain para la gestión documental de notarías en Lima Moderna: https://repositorio.esan.edu.pe/items/60850ce2-eaae-4869-8261-5ab6b35cfe1d

Bartolomeo, A. M. (2020). *Bartolomeo, A., & Machin Urbay, G. (2020). Introducción a la tecnología blockchain: su impacto en las Ciencias Económicas*. Obtenido de Bartolomeo, A., & Machin Urbay, G. (2020). Introducción a la tecnología blockchain: su impacto en las Ciencias Económicas: https://bdigital.uncu.edu.ar/fichas.php?idobjeto=15304

Cambarieri, M. V. (2024). *Cambarieri, M. G., Viadana, C. A., Rached, S., Jauge, M., Vivas, H. L., & Garcia Martinez, N. (2024). Aplicación de tecnología Blockchain para la emisión y verificación de Microcredenciales*. Obtenido de Cambarieri, M. G., Viadana, C. A., Rached, S., Jauge, M., Vivas, H. L., & Garcia Martinez, N. (2024). Aplicación de tecnología Blockchain para la emisión y verificación de Microcredenciales: https://repositoriosdigitales.mincyt.gob.ar/vufind/Record/RIDUNRN_69e4d0159b9e7d7a8b3c312d024e39d2

Cambarieri, M. V. (2024). *Cambarieri, M., Viadana, A., Rached Galera, S., Jauge, M., & García Martínez, N. (2024). Explorando el potencial de las microcredenciales y la tecnología Blockchain para la Transformación Digital en la Educación Superior*. Obtenido de Cambarieri, M., Viadana, A., Rached Galera, S., Jauge, M., & García Martínez, N. (2024). Explorando el potencial de las microcredenciales y la tecnología Blockchain para la Transformación Digital en la Educación Superior: https://rid.unrn.edu.ar/bitstream/20.500.12049/12336/1/Explorando%20el%20potencial%20de%20las%20microcredenciales%20y%20la%20tecnolog%c3%ada%20blockchain_libroActa.pdf

Cambarieri, M. V. (2024). *Cambarieri, M., Viadana, C. A., García Martínez, N., Vivas, L., Rached, S., & Jauge, M. (2024). Transformación digital en entidades públicas: explorando el potencial de la tecnología blockchain en la gestión de identidad y emisión de credenciales*. Obtenido de Cambarieri, M., Viadana, C. A., García Martínez, N., Vivas, L., Rached, S., & Jauge, M. (2024). Transformación digital en entidades públicas: explorando el potencial de la tecnología blockchain en la gestión de identidad y emisión de credenciales: https://rid.unrn.edu.ar/handle/20.500.12049/150

Chile, C. N. (31 de 7 de 2002). *BCN*. Obtenido de https://www.bcn.cl/: https://www.bcn.cl/leychile/navegar?idNorma=207436

Cuello Velásquez, R. (2020). *Cuello Velásquez, R. A. (2020). Blockchain para optimizar la transparencia dentro de la contratación estatal*. Obtenido de Cuello Velásquez, R. A. (2020). Blockchain para optimizar la transparencia dentro de la contratación estatal: https://repositorio.uniandes.edu.co/entities/publication/432b6345-4d07-4ccf-aef2-60cc459a08d7

Cuevas Olarte, P. (2023). *Cuevas Olarte, P. R. (2023). Sistema de verificación de credenciales profesionales basado en Blockchain Privado*. Obtenido de Cuevas Olarte, P. R. (2023). Sistema de verificación de credenciales profesionales basado en Blockchain Privado: https://repositorio.comillas.edu/xmlui/handle/11531/74730

Diputados, C. d. (4 de 4 de 2024). *Gob mx*. Obtenido de https://www.gob.mx/: https://www.gob.mx/cms/uploads/attachment/file/911476/4._LFT.pdf

Estrada Rivera, C. (2024). *Estrada Rivera, C. A. (2024). Prototipo de un sistema de gestión de identidad usando la tecnología blockchain: Implementación de smart contracts usando el protocolo de consenso RAFT*. Obtenido de Estrada Rivera, C. A. (2024). Prototipo de un sistema de gestión de identidad usando la tecnología blockchain: Implementación de smart contracts usando el protocolo de consenso RAFT: https://bibdigital.epn.edu.ec/handle/15000/25858

Fernández Gonzalvo, B. (2019). *Fernández Gonzalvo, B. (2019). Gestión soberana de identidades descentralizadas con Blockchain*. Obtenido de Fernández Gonzalvo, B. (2019). Gestión soberana de identidades descentralizadas con Blockchain: https://openaccess.uoc.edu/bitstream/10609/91208/6/bfgonzalvoTFM0119memoria.pdf

Fernández Infanzón, L. H. (2021). *Fernández Infanzón, L. I., & Huarac Cuizano, Y. M. (2021). Plan de negocio para integrar a las IPRESS con una plataforma de historia clínica electrónica (HCE) utilizando tecnología blockchain*. Obtenido de Fernández Infanzón, L. I., & Huarac Cuizano, Y. M. (2021). Plan de negocio para integrar a las IPRESS con una plataforma de historia clínica electrónica (HCE) utilizando tecnología blockchain: https://repositorio.esan.edu.pe/server/api/core/bitstreams/f639f09f-537c-4889-ab60-3721b9b47d78/content

Fiaño Rodríguez, J. (2022). *Fiaño Rodríguez, J. (2022). Sistema de Identidad Digital Soberana y Descentralizada basada en Blockchain*. Obtenido de Fiaño Rodríguez, J. (2022). Sistema de Identidad Digital Soberana y Descentralizada basada en Blockchain: https://ruc.udc.es/dspace/bitstream/handle/2183/32059/fianorodriguez_jacobo_tfg_2022.pdf?sequence=3

Gómez Almeyda, S. (2023). *Gómez Almeyda, S. (2023). Diseño e implementación de prototipo basado en Blockchain para verificación automática de requisitos de grado en la Universidad Distrital Francisco José de Caldas*. Obtenido de Gómez Almeyda, S. (2023). Diseño e implementación de prototipo basado en Blockchain para verificación automática de requisitos de grado en la Universidad Distrital Francisco José de Caldas: https://repository.udistrital.edu.co/bitstreams/7350b2c7-2fa8-4bd3-ac33-b42d4655e2c3/download

Gonzales Pulido, G. S. (2024). *Gonzales Pulido, G. D., Salazar Flores, K., & Sarmiento Jurado, M. C. (2024). Plan de negocio para implementar una plataforma que integre historias clínicas electrónicas en el sector privado basado en tecnología Blockchain*. Obtenido de Gonzales Pulido, G. D., Salazar Flores, K., & Sarmiento Jurado, M. C. (2024). Plan de

negocio para implementar una plataforma que integre historias clínicas electrónicas en el sector privado basado en tecnología Blockchain: https://repositorio.cuc.edu.co/entities/publication/1c93e032-aa8a-4a37-bd87-0d4d2218e435/full

Gordillo Alguacil, P. A. (2024). *Gordillo Alguacil, P., Albert Albiol, E. M., Correas Fernández, J., Genaim, S., Isabel Márquez, M., Román Díez, G., & Rubio Gimeno, A. (2024). Estudio de la aplicación de herramientas de análisis de contratos inteligentes de Ethereum en las asignaturas de blockchain de las titulaciones de la Facultad de Informática*. Obtenido de Gordillo Alguacil, P., Albert Albiol, E. M., Correas Fernández, J., Genaim, S., Isabel Márquez, M., Román Díez, G., & Rubio Gimeno, A. (2024). Estudio de la aplicación de herramientas de análisis de contratos inteligentes de Ethereum en las asignaturas de blockchain de las titulaciones de la Facultad de Informática: https://scholar.google.com/citations?user=zmfpVj4AAAAJ&hl=es

Gutiérrez Martínez, P. (2024). *Gutiérrez Martínez, P. (2024). ContractMe: aplicación móvil basada en Blockchain que simplifica la contratación y verificación a través de contratos inteligentes*. Obtenido de Gutiérrez Martínez, P. (2024). ContractMe: aplicación móvil basada en Blockchain que simplifica la contratación y verificación a través de contratos inteligentes: https://uvadoc.uva.es/handle/10324/71383

Hernández-Sampieri, R. &. (2018). *unam*. Obtenido de unam.mx: https://virtual.cuautitlan.unam.mx/rudics/?p=2612

Ligarreto Avendaño, N. L. (2024). *Ligarreto Avendaño, N., & López Rivera, L. A. (2024). Proceso de reclutamiento y selección implementando inteligencia artificial Aira en empresa: sector retail colombo-chilena 2023*. Obtenido de Ligarreto Avendaño, N., &

López Rivera, L. A. (2024). Proceso de reclutamiento y selección implementando inteligencia artificial Aira en empresa: sector retail colombo-chilena 2023: https://alejandria.poligran.edu.co/bitstream/handle/10823/7453/64.pdf?sequence=1

Maza, M. (2019). *Maza, M. V. (2019). El auge de blockchain y sus posibilidades reales de aplicación en los registros de las administraciones públicas*. Obtenido de Maza, M. V. (2019). El auge de blockchain y sus posibilidades reales de aplicación en los registros de las administraciones públicas: https://dialnet.unirioja.es/servlet/articulo?codigo=7329069

Montoya Acevedo, A. (2023). *Montoya Acevedo, A. J. (2023). Modelo de gestión tecnológica digital para el proceso de contratación inteligente en las Instituciones de Educación Superior de la ciudad de Medellín*. Obtenido de Montoya Acevedo, A. J. (2023). Modelo de gestión tecnológica digital para el proceso de contratación inteligente en las Instituciones de Educación Superior de la ciudad de Medellín: https://repositorio.itm.edu.co/handle/20.500.12622/6005

Networking and Cryptography Library. (15 de 03 de 2016). *Networking and Cryptography Library*. Obtenido de Networking and Cryptography Library: https://nacl.cr.yp.to/

Nieto Ripoll, M. (2021). *Nieto Ripoll, M. A. (2021). Modelo de mejora de los procesos de selección y contratación de personal con el uso de la tecnología blockchain*. Obtenido de Nieto Ripoll, M. A. (2021). Modelo de mejora de los procesos de selección y contratación de personal con el uso de la tecnología blockchain: https://repository.eafit.edu.co/server/api/core/bitstreams/0385da93-0c33-4c9c-86a6-ac2a5bb6eabe/content

Parada Gonzales, J. M. (2023). *Parada Gonzales, J. A., & Marín León, K. Y. (2023). Optimización de procesos de contratación en Instituciones Públicas mediante el uso de*

Contratos Inteligentes basado en tecnología Blockchain. Obtenido de Parada Gonzales, J. A., & Marín León, K. Y. (2023). Optimización de procesos de contratación en Instituciones Públicas mediante el uso de Contratos Inteligentes basado en tecnología Blockchain: http://repositorio.uts.edu.co:8080/xmlui/handle/123456789/13199

Perú, M. d. (21 de 10 de 2024). *Gob pe*. Obtenido de https://www.gob.pe/: https://www.gob.pe/institucion/mtpe/informes-publicaciones/6359927-compendio-de-normas-laborales-del-regimen-laboral-privado

Senado. (15 de 7 de 2025). *Secretariasenado*. Obtenido de http://www.secretariasenado.gov.co/: http://www.secretariasenado.gov.co/senado/basedoc/codigo_sustantivo_trabajo.html

Suárez, L. (2021). *Suárez, L. A. (2021). La aplicación de la tecnología blockchain en las ciudades inteligentes: hacia una gestión urbana descentralizada e inteligente*. Obtenido de Suárez, L. A. (2021). La aplicación de la tecnología blockchain en las ciudades inteligentes: hacia una gestión urbana descentralizada e inteligente: https://www.erdalreview.eu/free-download/97912599424328.pdf

Tamayo. (2004). *Tamayo*. Obtenido de books google: https://books.google.co.ve/books?id=BhymmEqkkJwC&printsec=frontcover&hl=es#v=onepage&q&f=false

Vicente Valle, S. (2022). *Vicente Valle, S. (2022). Sistema de verificación de certificados académicos basado en blockchain*. Obtenido de Vicente Valle, S. (2022). Sistema de verificación de certificados académicos basado en blockchain: https://brumario.usal.es/permalink/34BUC_USAL/e9i5co/alma991010184552205773

Glosario

AES-256: Algoritmo de cifrado simétrico avanzado utilizado para proteger datos en reposo y en tránsito, garantizando alta seguridad en el sistema.

API RESTful: Interfaz de programación de aplicaciones basada en REST, utilizada para la comunicación entre el front-end y back-end del sistema RIMU.

Axios: Cliente HTTP basado en promesas, empleado en el front-end para solicitudes a la API.

Azure Cloud: Plataforma de nube de Microsoft empleada para el despliegue de la aplicación en un entorno de producción virtual.

Blockchain: Tecnología de registro distribuido e inmutable utilizada para asegurar la integridad de los historiales laborales mediante criptografía.

CCPA: Ley de Privacidad del Consumidor de California, norma estadounidense que regula el manejo de datos personales.

Celery: Herramienta para ejecutar tareas asíncronas en segundo plano, utilizada en el back-end para procesos como notificaciones.

CI/CD: Práctica de integración y despliegue continuos, implementada con GitHub Actions para automatizar el desarrollo.

CNUDMI: Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, organismo que establece normas sobre comercio electrónico y firmas digitales.

Cryptography: Algoritmo de protección de información mediante técnicas de cifrado, fundamental en RIMU para la verificación de documentos.

DevOps: Metodología que integra desarrollo y operaciones, aplicada en la estrategia de despliegue para mejorar la eficiencia.

Django: Framework web de Python utilizado para construir el back-end robusto y escalable del sistema.

Docker: Plataforma que permite ejecutar servicios aislados, como bases de datos y aplicaciones, en entornos consistentes llamados contenedores.

eIDAS: Reglamento de la Unión Europea sobre identificación y firma digital, que valida transacciones electrónicas en el proyecto.

ESIGN Act: Ley estadounidense que otorga validez legal a firmas electrónicas y contratos digitales.

Framework: Estructura de software reutilizable que facilita el desarrollo de aplicaciones, como Django o Next.js utilizadas en el proyecto.

GDPR: Reglamento General de Protección de Datos de la Unión Europea, que establece principios para el manejo ético de datos personales.

Git: Sistema de control de versiones que permite gestionar y rastrear cambios en archivos.

Git Flow: Modelo de ramificación en Git para gestionar el desarrollo colaborativo y versiones del código.

GitHub Actions: Herramienta de automatización para CI/CD, utilizada para pruebas y despliegues en el proyecto.

Gunicorn: Servidor WSGI para aplicaciones Python, que maneja solicitudes HTTP en el back-end.

Jest: Framework de pruebas para JavaScript, empleado en el front-end para validar componentes y funcionalidades.

JWT: JSON Web Tokens, método de autenticación basado en tokens para gestionar sesiones seguras en el sistema.

Kubernetes: Plataforma de orquestación de contenedores, utilizada para gestionar servicios en entornos de producción.

LGPD: Ley General de Protección de Datos de Brasil, normativa que regula el tratamiento de datos personales en América Latina.

Material-UI: Biblioteca de componentes de interfaz para React, utilizada en el front-end para diseños consistentes.

Microservicios: Arquitectura que divide la aplicación en servicios independientes, facilitando escalabilidad y mantenimiento.

Next.js: Framework de React para renderizado del lado del servidor, empleado en el front-end para optimizar el rendimiento.

Nginx: Servidor web y proxy inverso, utilizado para balanceo de carga y comunicación entre servicios.

Node.js: Entorno de ejecución de JavaScript del lado del servidor, base para el desarrollo front-end con Next.js.

OAuth 2: Protocolo de autorización que permite acceso seguro a recursos, implementado para autenticación en RIMU.

PostgreSQL: Sistema de gestión de bases de datos relacional, utilizado para almacenar datos del sistema de manera robusta.

PostCSS: Herramienta para procesar CSS, integrada con Tailwind CSS para estilos en el front-end.

PyNaCl: Biblioteca criptográfica moderna derivada de NaCl, empleada para firmas digitales y cifrado en el back-end.

Python: Lenguaje de programación utilizado en el back-end con Django para lógica de negocio y APIs.

React: Biblioteca de JavaScript para construir interfaces de usuario interactivas en el front-end.

Redis: Sistema de almacenamiento en memoria, utilizado como caché y broker de mensajes para mejorar el rendimiento.

Redux Toolkit: Biblioteca para gestión de estado global en aplicaciones React, facilitando el manejo de datos en el front-end.

Rest-framework: Extensión de Django (Django REST Framework) para construir APIs RESTful de manera eficiente.

RFC 3161: Estándar para timestamps criptográficos, utilizado para sellar fechas y horas de documentos en RIMU.

RIMU: Nombre del proyecto web para verificación digital de historiales laborales. (Susceptible a cambios futuros).

TailwindCss: Framework de CSS utilitario para diseños responsivos y rápidos en el front-end.

Terser: Herramienta para minificar código JavaScript, optimizando el rendimiento en el front-end.

TypeScript: Superset de JavaScript con tipado estático, utilizado en React para mayor robustez del código.

Ubuntu: Sistema operativo Linux utilizado en el VPS de Azure para el despliegue de la aplicación.

VPS: Servidor Privado Virtual, infraestructura en la nube para alojar el sistema en producción.

Webpack: Empaquetador de módulos para JavaScript, utilizado en Next.js para gestionar recursos y optimizar builds.

Anexos

Anexo 1

Título: Instrumento de Recolección de Datos

Encuesta sobre Eficiencia en Procesos de Verificación Laboral

Objetivo: Identificar las principales falencias, costos y riesgos asociados a los métodos tradicionales de verificación de antecedentes laborales en el sector de Recursos Humanos.

Público Objetivo: Gerentes de RR.HH., Reclutadores y Analistas de Selección.

Formato: Cuestionario estructurado de selección múltiple.

Cuestionario:

1. **¿Cuál es el método principal que utiliza su organización actualmente para verificar los antecedentes laborales de un candidato?**
    A. Llamadas telefónicas a referencias.
    B. Solicitud de certificados físicos/escaneados por correo electrónico.
    C. Contratación de empresas externas de seguridad (Outsourcing).
    D. No realizamos verificación formal.
2. **En promedio, ¿cuánto tiempo transcurre desde que solicita una verificación laboral hasta que recibe la confirmación definitiva?**
    A. Menos de 24 horas.
    B. Entre 1 y 2 días hábiles.
    C. Entre 3 y 4 días hábiles.
    D. 5 días hábiles o más.
3. **¿Considera que el tiempo actual invertido en la verificación de documentos es eficiente para el ritmo de contratación que requiere su empresa?**

A. Sí, es adecuado.

B. Es aceptable, pero podría mejorar.

C. No, es ineficiente y lento.

D. No, representa un cuello de botella crítico.

4. **¿Con qué frecuencia ha detectado discrepancias, alteraciones o información falsa en los currículums o certificados presentados por los postulantes?**

A. Nunca.

B. Rara vez (Menos del 5% de los casos).

C. Ocasionalmente (Entre el 10% y 20% de los casos).

D. Frecuentemente (Más del 20% de los casos).

5. **¿Ha perdido algún candidato viable debido a la demora en los procesos administrativos de verificación y contratación?**

A. No, nunca ha sucedido.

B. Sí, ha ocurrido en algunas ocasiones (aprox. 10-20% de los casos).

C. Sí, es un problema recurrente (más del 20% de los casos).

6. **Estimando el tiempo del personal y recursos utilizados, ¿cuál es el costo aproximado por cada verificación individual realizada?**

A. Menos de $1 USD.

B. Entre $1 y $3 USD.

C. Entre $3 y $5 USD.

D. Más de $5 USD.

7. **En una escala del 1 al 10, ¿qué nivel de seguridad y confianza le genera recibir un certificado laboral en formato PDF simple enviado por el candidato?**

A. 1 - 3 (Baja confianza / Fácil de falsificar).

B. 4 - 6 (Confianza media / Requiere validación extra).

C. 7 - 8 (Confianza alta).

D. 9 - 10 (Total seguridad).

8. **¿Cuál es la principal dificultad operativa que enfrenta su departamento al validar la experiencia laboral?**

A. Las empresas anteriores no contestan los teléfonos/correos.

B. La empresa anterior ya no existe.

C. El costo de contratar servicios de terceros.

D. La gestión manual de archivos y papeles.

9. **¿Estaría dispuesto a implementar una plataforma digital que permita verificar historiales laborales en tiempo real mediante criptografía, eliminando las llamadas telefónicas?**

A. Sí, definitivamente.

B. Probablemente, si el costo es accesible.

C. No, prefiero el método tradicional.

10. **¿Qué importancia le daría a la característica de "inmutabilidad" (imposibilidad de alterar un documento una vez emitido) en sus procesos de selección?**

A. Irrelevante.

B. Importante.

C. Crítica / Indispensable para evitar fraudes.

Anexo 2

Título: RIMU

URL: www.rockislife.qzz.io

Descripción: Esta página web aloja la versión beta del proyecto RIMU, una plataforma web para la gestión y verificación de historiales laborales, permitiendo a empresas y empleados compartir registros de empleo seguros e inmutables.