

TEMA

Desarrollo de un sistema de facturación electrónica como servicio (SaaS) con arquitectura multitenant

Autores:

Lara Nicolas

Director:

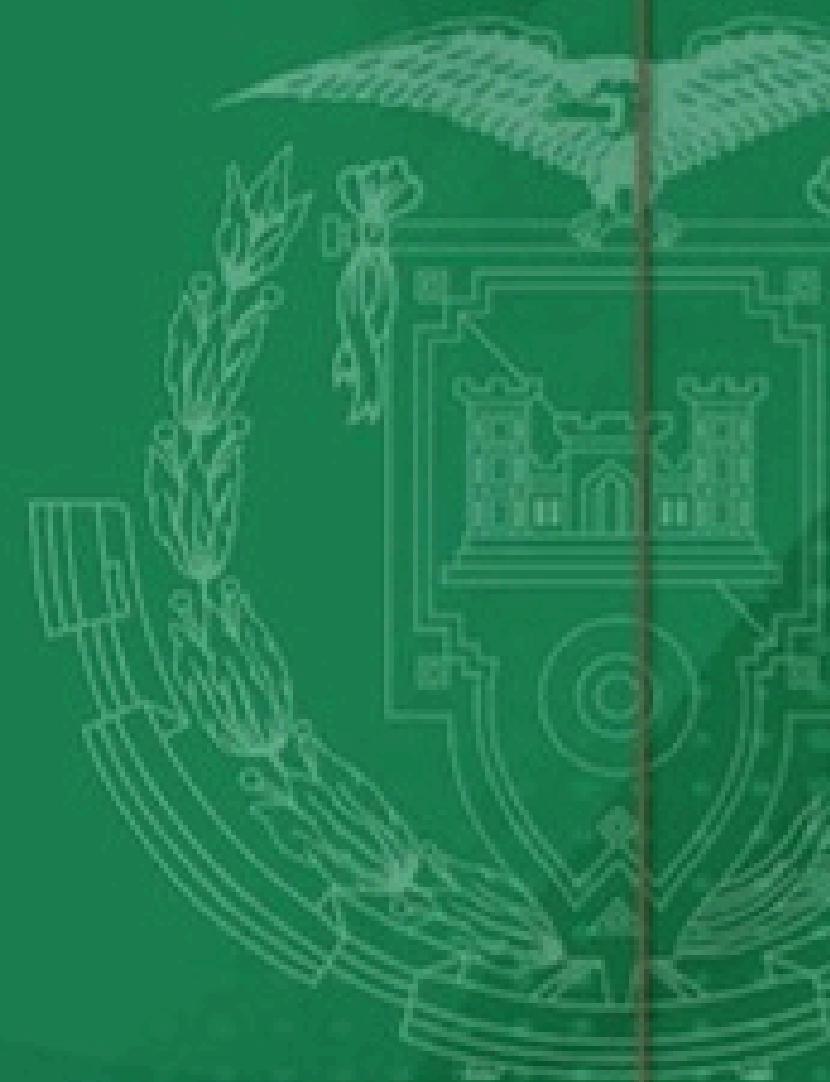
Ing. Núñez Agurto Alberto Daniel, PhD.



ÍNDICE DE CONTENIDO



- Introducción
- Objetivos
- Marco Teórico
- Metodología
- Resultados
- Conclusiones
- Recomendaciones



Introducción



En Ecuador, la facturación electrónica es obligatoria y requiere comprobantes que deben generarse en XML, firmarse con XAdES-BES y enviados via SOAP al SRI.

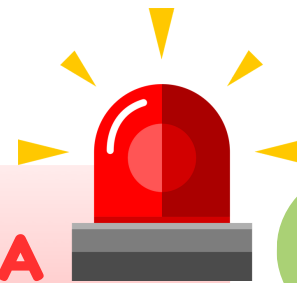


Normativa Ecuador

Cumplimiento obligatorio para todas las empresas y contribuyentes.

1

PROBLEMA



Las PYMEs enfrentan obstáculos con los sistemas tradicionales.



- ✗ Altos costos de licencias e infraestructura.
- ✗ Sistemas locales, difíciles de mantener y actualizar.
- ✗ Sin aislamiento adecuado de datos entre empresas.
- ✗ Mayor riesgo de seguridad e incumplimiento.



Impacto en las PYMEs

Menor competitividad y pérdida de tiempo y recursos.

2

JUSTIFICACIÓN



Se requiere una plataforma moderna que resuelva estas necesidades.



- ✓ Plataforma centralizada.
- ✓ Escalable y disponible.
- ✓ Bajo costo de operación.
- ✓ Actualización normativa inmediata para todos los usuarios.
- ✓ Acceso seguro desde cualquier lugar.



Beneficio

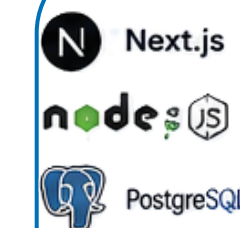
Todas las PYMEs cumplen la normativa de forma simple, segura y eficiente.

3

SOLUCIÓN



Sistema SaaS multitenant seguro, escalable y de bajo costo.



Frontend moderno y rápido.
Backend escalable.
Base de datos robusta.
Seguridad validada bajo OWASP Top 10.
Aislamiento por empresa_id (Multitenant)

Objetivo General

Desarrollar un sistema de facturación electrónica basado en el modelo SaaS, utilizando una arquitectura multitenant, que permita a múltiples empresas gestionar sus procesos de facturación de forma segura, escalable y centralizada, cumpliendo con los requisitos funcionales y normativos vigentes.

Objetivos Específicos

1

Analizar y definir los requisitos funcionales, técnicos y normativos necesarios para el desarrollo de un sistema de facturación electrónica bajo un modelo SaaS multitenant.

2

Diseñar la arquitectura del sistema de facturación electrónica bajo el modelo SaaS con enfoque multitenant, garantizando el aislamiento lógico de datos y la gestión eficiente de múltiples empresas.

3

Implementar los módulos principales del sistema de facturación electrónica, incorporando mecanismos de seguridad y control por tenant.

4

Validar el funcionamiento, desempeño y seguridad del sistema mediante pruebas funcionales, de rendimiento y de mitigación de vulnerabilidades.

Marco Teórico

TECNOLOGÍAS UTILIZADAS

NEXT.js



Desarrollo de la interfaz web.



Ejecución del servidor backend.



Caché para mejorar el rendimiento.

Express JS



Implementación de la API REST.



ORM para la comunicación con la base de datos.



Sistema gestor de base de datos relacional.

SRI



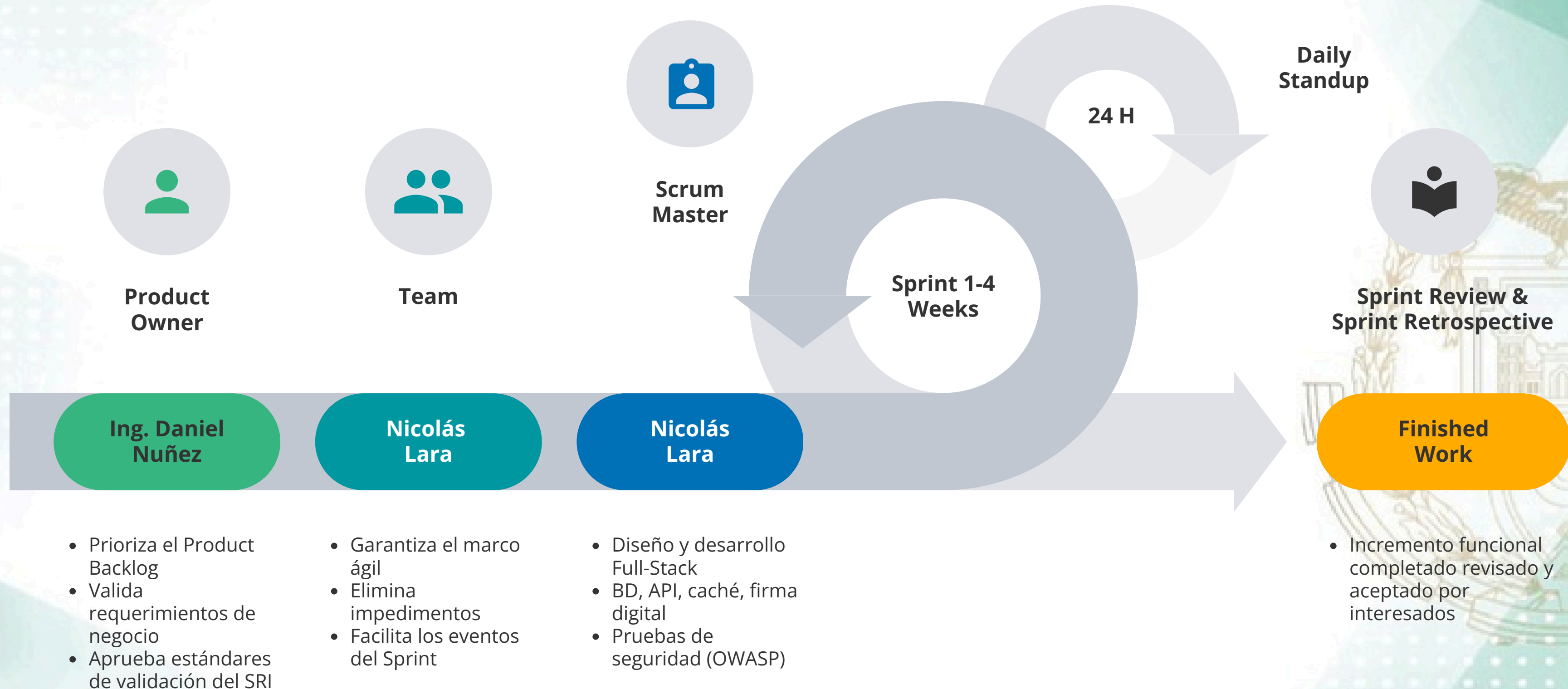
Validación y autorización de comprobantes electrónicos.



Firma electrónica para garantizar la autenticidad y validez.

Metodología

ROLES DE SCRUM



Metodología

SPRINTS COMPLETADOS



Sprint 1

Configuración inicial del sistema y autenticación

- ✓ BD
- ✓ JWT
- ✓ Login

95h



Sprint 2

Gestión empresarial e integración de firma electrónica

- ✓ Firma
- ✓ XAdES
- ✓ XML

105h



Sprint 3

Optimización del backend y módulos administrativos

- ✓ Gestión
- ✓ Empresas
- ✓ Productos

110h



Sprint 4

Implementación de la facturación electrónica

- ✓ XML
- ✓ SOAP
- ✓ PDF

111h



Sprint 5

Seguridad y emisión de comprobantes

- ✓ OWASP
- ✓ Interfaces
- ✓ Comprobantes

137h



Sprint 6

Dashboard, pruebas y documentación

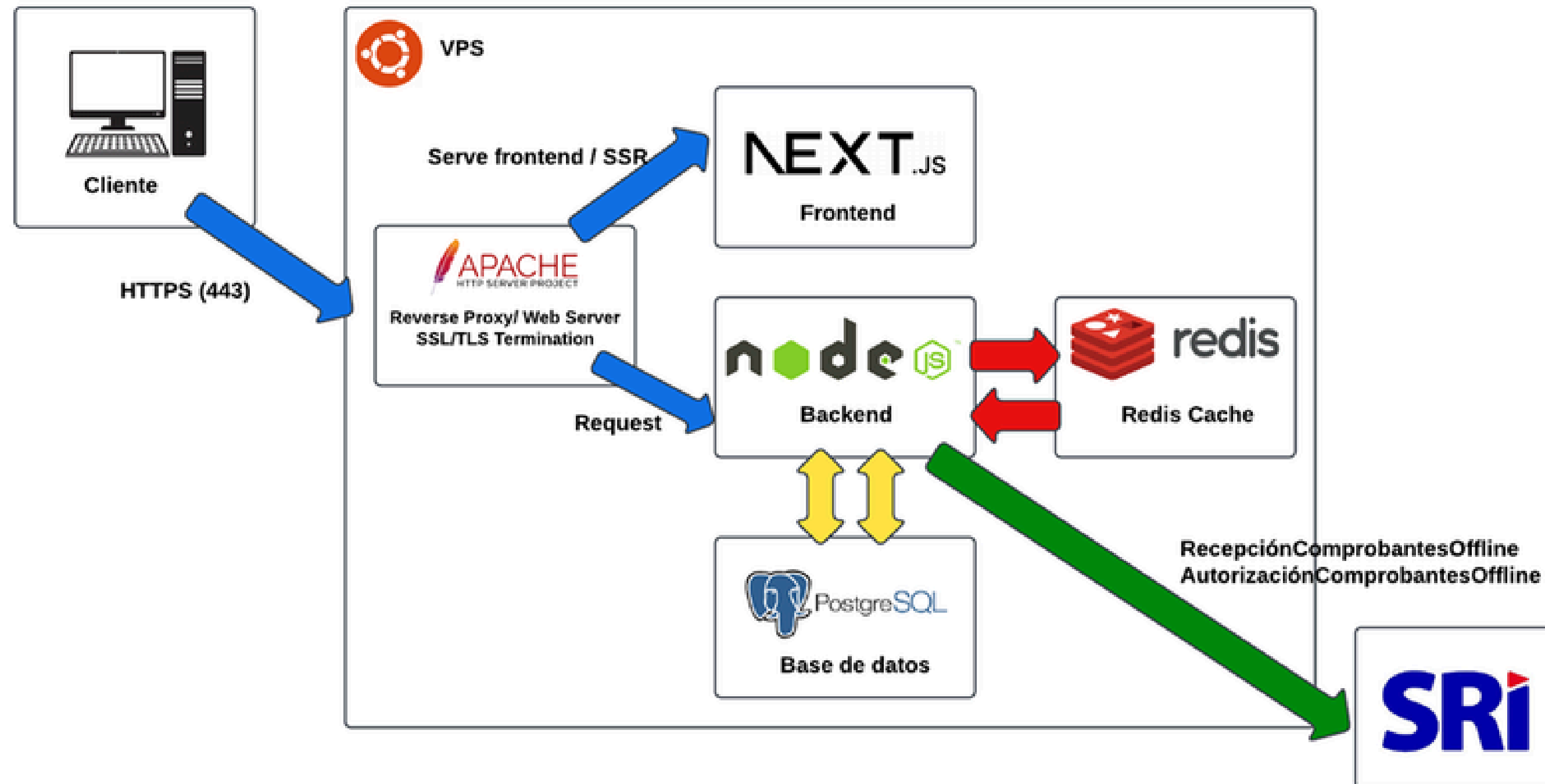
- ✓ KPIs
- ✓ E2E
- ✓ Docs

103h

T.Sprint: 661h

Diseño del Sistema

ARQUITECTURA GENERAL DEL SISTEMA



Resultados



Bienvenido de nuevo

Ingresa tus credenciales para acceder al sistema.

Iniciar sesión

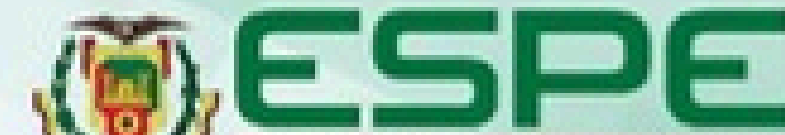
[¿Olvidaste tu contraseña?](#)

[Crear una cuenta](#)

[¿Necesitas ayuda? Contáctanos](#)



© 2026 Factory. Todos los derechos reservados.



DE LAS FUERZAS ARMADAS
PARA LA EXCELENCIA

Gestión de facturación lista para escalar.



Centraliza la operación y mantén todo bajo control en un solo entorno.



Emite facturas electrónicas, notas de crédito y débito en minutos.



Controla productos, clientes, proveedores y puntos de emisión desde un solo lugar.



Administra equipos, permisos y usuarios con trazabilidad completa.



Consulta reportes e impuestos con paneles listos para auditoría.

Resultados

Modo Pruebas

Irreng
ADMINISTRADOR

PRINCIPAL

 Resumen

VENTAS

-  Facturas
-  Notas de Venta
-  Notas de Crédito
-  Notas de Débito
-  Proformas
-  Facturación Recurrente
-  Retenciones
-  Liquidaciones de Compra

INVENTARIO

-  Productos
-  Grupos de Productos

CONTACTOS

-  Clientes
-  Proveedores

LOGÍSTICA

-  Guías de Remisión



Empresa

Configura razón social, RUC, dirección, logo y datos tributarios de tu empresa

Datos de la Empresa

Configuración actual, identidad y detalles fiscales.

 Editar datos



Información General

RAZÓN SOCIAL

Pilla Pago S.A

NOMBRE COMERCIAL

Pilla Pago

RUC

1713113270001

CORREO

jaingamehd7@gmail.com

TELÉFONO

0967214415

DIRECCIÓN MATRIZ

Los Pambiles, cerca del Chifa Huan Fan y clínica Emedycs

Estado de cuenta

Estado

ACTIVO

Registrado en

24/4/2026

Última actualización

1/6/2026

Configuración Fiscal

AMBIENTE SRI

Pruebas

RÉGIMEN

General

RIMPE

No

OBLIGADO CONTABILIDAD

No

AGENTE RETENCIÓN

No

CONTRIBUYENTE ESPECIAL

No

SERVICIO DE CORREO

Configurado

Resultados

 **Crear nuevo producto** ✕

Registra un nuevo producto o servicio con sus datos de clasificación y precios.

 **Datos Básicos**  Precios e Impuestos

☒ **Identificación**

Código

Ej. PROO-001

Tipo

Selecciona un tipo...

Descripción

Nombre o descripción del producto/servicio 0/100

☒ **Clasificación**

Grupo

Medicamentos

IVA

IVA 0% (0%)

Cancelar

Crear producto

Resultados

Pilla Pago

PRINCIPAL

Resumen

VENTAS

Facturas

Notas de Venta

Notas de Crédito

Notas de Débito

Proformas

Facturación Recurrente

Retenciones

Liquidaciones de Compra

INVENTARIO

Productos

Grupos de Productos

CONTACTOS

Cientes

Proveedores

LOGÍSTICA

Guías de Remisión

Facturas

Crea borradores, emite facturas electrónicas al SRI, descarga PDF's e imprime recibos

Buscar factura...

Filtros

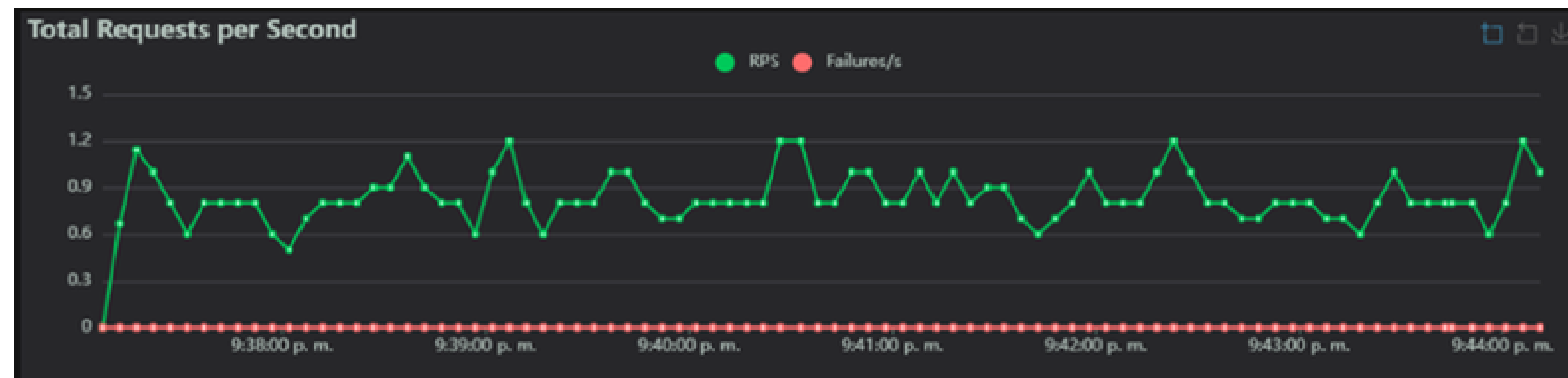
+ Nueva factura

Factura	Cliente	Fecha	Estado	
001-001-000000113 001 - Caja principal	CONSUMIDOR FINAL XXXXXXXXXX	2026-06-03	BORRADOR	
001-001-000000112 001 - Caja principal	Juan Cortez Mendez Mendez 2300132634	2026-06-03	BORRADOR	
001-001-000000111 001 - Caja principal	Juan Cortez Mendez Mendez 2300132634	2026-06-03	AUTORIZADO	
001-001-000000110 001 - Caja principal	Juan Cortez Mendez Mendez 2300132634	2026-06-03	BORRADOR	
001-001-000000109 001 - Caja principal	Nicole Arleth Guadamud Zambrano 1752079298	2026-06-03	AUTORIZADO	
001-001-000000108 001 - Caja principal	Manuel Antonio Valenzuela Quimbulo 1710204155001	2026-06-03	AUTORIZADO	
001-001-000000107 001 - Caja principal	Manuel Antonio Valenzuela Quimbulo 1710204155001	2026-06-03	AUTORIZADO	
001-001-000000106 001 - Caja principal	Manuel Antonio Valenzuela Quimbulo 1710204155001	2026-06-03	AUTORIZADO	
001-001-000000105 001 - Caja principal	Nicolas Andres Lara Calcedo 2350710287	2026-06-03	AUTORIZADO	
001-001-000000104 001 - Caja principal	Nicolas Andres Lara Calcedo 2350710287	2026-06-03	AUTORIZADO	

Filas: 10 - Total: 118 registros

< 1 / 12 >

Resultados



Evolución de las solicitudes por segundo (RPS) y tasa de fallos durante la ejecución de las pruebas automatizadas con Locust.

Resultados

Pruebas de Seguridad — OWASP Top 10 (2021)

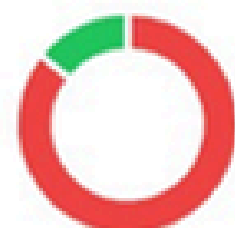
Backend Node.js · Express · Sequelize | 29 pruebas ejecutadas | 29 controles activos

A01:2021

✓ PASS

Control de Acceso Roto

Recursos protegidos no accesibles sin token JWT válido. Se prueba con tokens ausentes, malformados y con firma incorrecta.



■ Bloqueadas sin token ■ Acceso permitido (con token)

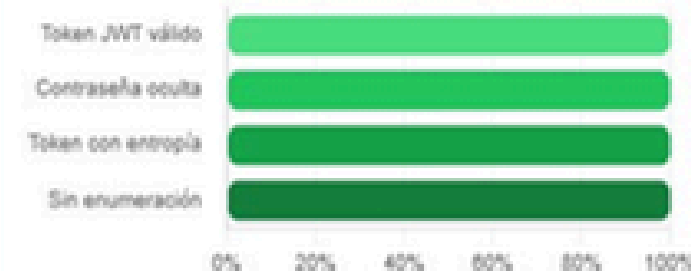
6/6 pruebas superadas · Middleware JWT + roles

A02:2021

✓ PASS

Fallos Criptográficos

Las contraseñas no se exponen en respuestas. El token JWT tiene formato correcto y errores de login no revelan usuarios.



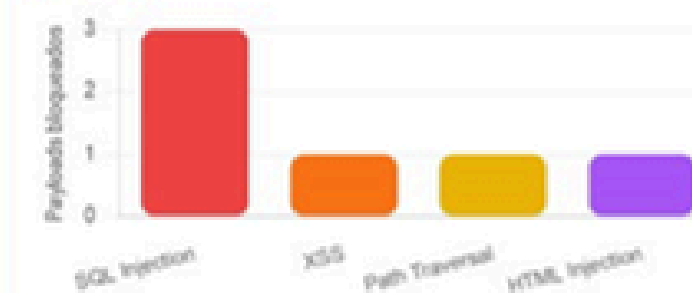
4/4 pruebas superadas · Bcrypt + JWT HS256

A03:2021

✓ PASS

Inyección (SQL · XSS · Path)

Payloads de SQL Injection, XSS y Path Traversal son bloqueados sin devolver errores 500 ni reflejar código malicioso.



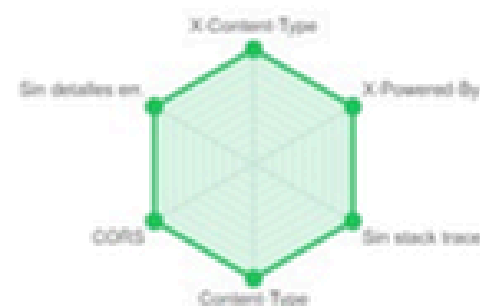
4/4 pruebas superadas · ORM + xssSanitizer

A05:2021

✓ PASS

Configuración de Seguridad Incorrecta

Helmet añade cabeceras de seguridad, X-Powered-By está oculto, CORS es restrictivo y no se exponen stack traces.



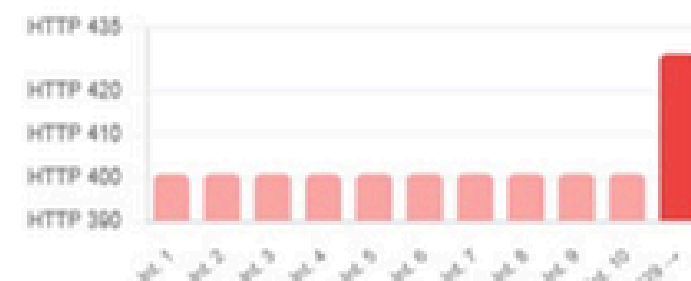
6/6 pruebas superadas · Helmet.js + CORS

A07:2021

✓ PASS

Fallos de Autenticación

Credenciales incorrectas retoman 401, tokens falsos son rechazados y el rate limit bloquea fuerza bruta con HTTP 429.



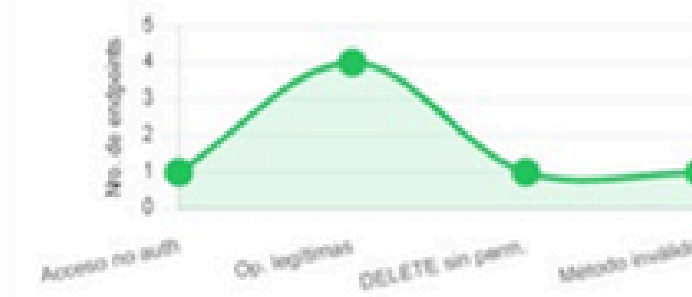
5/5 pruebas superadas · Rate limit + JWT

A09:2021

✓ PASS

Fallos en Registro y Monitoreo

Accesos no autorizados generan eventos 401 auditables. Operaciones normales no producen errores 500.



4/4 pruebas superadas · securityLogger

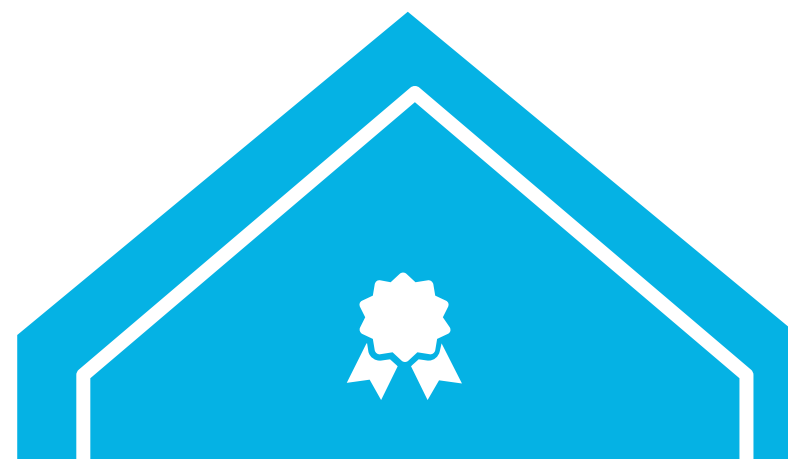
Conclusiones



01

Análisis y justificación

El análisis de la normativa del SRI permitió identificar 25 requerimientos funcionales y 15 no funcionales. La solución local resulta inviable para las PYMES por su carga de mantenimiento y la subutilización de infraestructura, justificando técnicamente el modelo SaaS multitenant.



02

Arquitectura y aislamiento

La arquitectura multitenant con PostgreSQL, Sequelize ORM y el identificador empresa_id garantizó el aislamiento lógico de datos sin aumentar costos. Con Apache (proxy inverso) y Redis (caché), soporta múltiples empresas en una sola infraestructura.



03

Implementación

Se implementaron los 25 RF cubriendo los 7 comprobantes del SRI, con firma XAdES-BES y clave de acceso de 49 dígitos (Algoritmo Módulo 11). Los 6 sprints totalizaron 661 horas sin desviaciones, validando la efectividad de Scrum.



04

Validación y seguridad

Las pruebas de caja negra verificaron los 25 RF con 100% de efectividad, y la auditoría OWASP Top 10 confirmó 6 controles críticos (control de acceso JWT, cifrado de credenciales, prevención de inyección SQL y trazabilidad de auditoría), garantizando un entorno seguro para datos financieros.

Recomendaciones



Row-Level Security (RLS) en PostgreSQL

Implementar RLS como capa de protección independiente de la aplicación, eliminando el riesgo de fuga de datos ante un error de programación que omita el filtro por empresa_id. Al ser nativo de PostgreSQL, no requiere cambios en el stack.

01



Cola de mensajes con BullMQ

Migrar el procesamiento asíncrono actual a una cola persistente con BullMQ sobre Redis (ya incluido en el stack). Aporta persistencia de tareas ante reinicios, control de reintentos por tipo de error y visibilidad del estado desde el dashboard.

02



Comercialización como producto SaaS

Los resultados demuestran que la plataforma es viable para comercializarse por suscripción mensual, con precios escalonados según el volumen de comprobantes e incluyendo un nivel gratuito o de bajo costo para microempresas y personas naturales con RISE.

03

Trabajo futuro

- ✓ Asistente conversacional con IA: ChatBot NPL para guiar emisión y resolver dudas.
- ✓ Automatización inteligente: Data Mining sobre histórico para auto-validar.
- ✓ Mejora continua /DevOps: Establecer ciclo CI/CD, Refactoring para updates y compliance con SRI.

