UNIVERSIDAD SANTO TOMAS
PRIMER CLAUSTRO UNIVERSITARIO DE COLOMBIA
T U N J A

TÍTULO PASANTÍA

Integración de servicios tecnológicos para brindar soluciones a las iniciativas ambientales de la Fundación Cataruben

PROPONENTE(S)
Juan David Buendia Loyo
1049656835
2282206

DIRECTOR
Henry Alfonso Guío Ávila

CODIRECTOR
Martha Susana Contreras Ortiz

Tunja
Fecha de presentación (18, 06, 2025)

CONTENIDO

1. FICHA TÉCNICA DE LA PASANTÍA

Título	Integración de servicios tecnológicos para brindar soluciones a las iniciativas ambientales de la Fundación Cataruben.
Nombre Estudiante	Juan David Buendía Loyo
Documento estudiante	1049656835
Correo electrónico	juan.buendia@usantoto.edu.co
Director	Henry Alfonso Guío Ávila / Martha Susana Contreras Ortiz
Entidad o sector de la empresa	Fundación Cataruben
Lugar de ejecución de la pasantía	Yopal, Casanare
Duración	Seis (6) meses

Los abajo firmantes confirman que todos los datos incluidos en la presente propuesta son correctos y verídicos, que no incumplen ninguna ley o norma vigente. (Incluir nombres y firmas de estudiantes, director y tutor).

Firma del autor
Nombre autor: Juan David Buendía Loyo

Firma del director
Nombre director de la pasantía: Henry Alfonso Guío Ávila / Martha Susana Contreras Ortiz

2. PLANTEAMIENTO DEL PROBLEMA

La Fundación Cataruben se encuentra inmersa en un proceso de transformación digital integral que demanda una cantidad considerable de horas de dedicación y recursos especializados para su correcta implementación. Según McKinsey (2024), la transformación digital va más allá de la simple implementación de tecnología, requiriendo un cambio fundamental en la forma en que las organizaciones operan y entregan valor a sus clientes. Este proceso abarca múltiples frentes tecnológicos simultáneos que incluyen la administración de redes corporativas, el mantenimiento preventivo y correctivo de equipos, el desarrollo y mantenimiento de soluciones web, la gestión de aplicaciones móviles, la administración de software de llamadas, y el manejo completo del sistema CRM CQTX.

La problemática principal radica en que la fundación cuenta con un equipo técnico limitado para atender la amplia diversidad de tareas que requiere esta transformación digital. Esta limitación de personal genera una sobrecarga de trabajo que impacta directamente en la calidad y tiempo de respuesta de los servicios tecnológicos. Las investigaciones de Emerald Insight (2024) sobre transformación digital organizacional identifican que uno de los principales desafíos que enfrentan las organizaciones durante estos procesos es la escasez de talento especializado, lo cual genera cuellos de botella en la implementación de nuevas tecnologías.

Entre las necesidades críticas identificadas se encuentran la gestión eficiente de solicitudes internas y externas, la provisión de soporte técnico oportuno a usuarios, la evaluación e implementación de nuevas tecnologías y soluciones innovadoras, y la administración integral de sistemas existentes. Adicionalmente, se requiere optimizar el manejo del flujo de datos organizacional, implementar sistemas de generación de estadísticas para la toma de decisiones estratégicas, desarrollar procesos de automatización que reduzcan tareas repetitivas, y realizar una optimización integral de flujos y procesos operativos. Wavetec (2024) señala que las tendencias actuales de transformación digital priorizan la automatización de procesos y la integración de sistemas como elementos clave para mejorar la eficiencia operativa.

La acumulación de estas necesidades no resueltas ha comenzado a generar cuellos de botella significativos en los procesos internos de la fundación, afectando la eficiencia operativa, incrementando los tiempos de respuesta, y limitando la capacidad de la organización para responder ágilmente a las crecientes demandas del mercado de carbono y las iniciativas ambientales que gestiona. Quixy (2024) identifica que los procesos manuales y sistemas aislados constituyen uno de los principales obstáculos para el crecimiento organizacional, creando ineficiencias que impactan directamente en la capacidad competitiva de las empresas.

La falta de integración coherente entre los diferentes servicios tecnológicos compromete la efectividad de las operaciones diarias y puede impactar negativamente en el cumplimiento de los compromisos adquiridos con clientes y aliados estratégicos como Ecopetrol, Latam Airlines, USAID, Promigas y Casa Luker así como en los objetivos de expansión internacional de la fundación. Taylor & Francis (2024) destaca que, en economías emergentes, la transformación digital requiere de una coordinación especial entre los diferentes componentes tecnológicos para garantizar el éxito de las iniciativas de crecimiento y expansión organizacional.

3. OBJETIVOS

3.1 Objetivo General

Integrar servicios tecnológicos que brinden soluciones a las iniciativas ambientales de la Fundación Cataruben.

3.2 Objetivos específicos

Tabla 1. Objetivos específicos

Nro.	Objetivo específico
1	Desarrollar módulos que soporten la prestación de servicios tecnológicos para la iniciativa CQTX.
2	Adaptar scripts para la automatización de procesos y orquestación de infraestructura IT.
3	Evaluar la funcionalidad de los servicios tecnológicos a través de pruebas unitarias, de políticas de seguridad y de usabilidad.

Fuente: Autor

4. DESCRIPCIÓN DE LAS ACTIVIDADES REALIZADAS

4.1. Actividades realizadas en el proyecto

Se debe relacionar el conjunto de actividades que realizó en el proyecto estableciendo fechas de los productos entregados.

Tabla 2. Actividades realizadas en la pasantía

Descripción de la actividad	Fecha inicio	Fecha entrega	Producto entregado
Ajustes menores: corrección de bugs, typos, rollbacks, revisión de PRs, subida de datos	24-sep-2024	23-mar-2025	Estabilidad del sistema CQTX mejorada
Operación de servidores: despliegue, monitoreo, mantenimiento	01-nov-2024	23-mar-2025	Infraestructura operativa y actualizada
Mantenimiento de equipos: hardware y software	24-sep-2024	23-mar-2025	Equipos funcionales y documentados
Revisión de retroalimentación y actualización del backlog de desarrollo	28-sep-2024	23-mar-2025	Backlog actualizado y priorizado
Administración de usuarios y accesos	10-oct-2024	23-mar-2025	Gestión de cuentas y permisos en múltiples plataformas
Generación de contratos de iniciativas ambientales	24-sep-2024	26-sep-2024	Contratos generados mediante automatización
Migración SMTP de Google a Amazon SES	01-oct-2024	20-oct-2024	Configuración de correo funcional en AWS SES
Diseño de interfaz para módulo UBE	15-oct-2024	15-nov-2024	Prototipo de interfaz en Figma
Diseño de base de datos para módulo UBE	03-oct-2024	05-oct-2024	Modelo relacional visual
Implementación de CAPTCHA para login en CQTX	10-nov-2024	10-ene-2025	Seguridad reforzada en autenticación
Implementación de Zabbix para monitoreo de servidores	10-nov-2024	10-ene-2025	Sistema de monitoreo activo con alertas y dashboards
Automatización de configuración con Ansible	10-nov-2024	10-ene-2025	Scripts YAML para control automatizado
Redimensionamiento de imágenes en comentarios de CQTX	15-nov-2024	20-nov-2024	Mejora en la experiencia de usuario en el editor de texto
Escritura de pruebas para módulos core, auth y postulaciones	15-nov-2024	15-dic-2024	Cobertura de pruebas aumentada
Creación y modificación de formularios ODK	18-nov-2024	23-mar-2025	Formularios funcionales para recolección de datos en salidas de campo
Cambio a conexión en tiempo real con WebSockets en módulo de postulaciones	10-dic-2024	27-ene-2025	Comunicación asincrónica implementada

Integración de CAPTCHA en endpoints anónimos de todas las plataformas	01-feb-2025	20-feb-2025	Seguridad mejorada en endpoints públicos
Diseño visual de Compensave	15-feb-2025	28-feb-2025	Prototipo visual completo
Separación de aplicaciones en servidores	01-feb-2025	23-mar-2025	Aislamiento de servicios mediante contenedores y droplets
Implementación de norma ISO 27001	01-feb-2025	23-mar-2025	Documentación y controles de seguridad aplicados
Validaciones y configuraciones de red con Aruba	01-mar-2025	23-mar-2025	Red corporativa optimizada
Implementación de stack de monitoreo con Grafana y OTEL-LGTM	01-mar-2025	20-mar-2025	Visualización de métricas y trazabilidad de servicios
Pruebas de seguridad con ZAP	10-mar-2025	15-mar-2025	Vulnerabilidades identificadas y mitigadas
Configuración de logs de servidores	15-mar-2025	23-mar-2025	Centralización de registros para auditoría
Manejo de antivirus Kaspersky	15-oct-2024	23-mar-2025	Protección activa de endpoints
Levantamiento de requisitos y diseño visual de mejoras y módulo PQRS	15-nov-2024	23-mar-2025	Documentación funcional y prototipos en Figma
Diseño funcional y visual del módulo PQRS	01-mar-2025	23-mar-2025	Requisitos, flujos y prototipos entregados
Responsable de seguridad de la información: implementación de SGSI y políticas	01-feb-2025	23-mar-2025	Comité, procedimientos, planes, matrices y cronogramas de seguridad implementados

Fuente: Autor

4.1.0 Stack tecnológico de la Fundación Cataruben

La arquitectura tecnológica de la Fundación Cataruben está diseñada para soportar un ecosistema digital distribuido, escalable y seguro, centrado en su plataforma principal: el sistema CQTX. Esta plataforma permite la gestión de iniciativas ambientales, el seguimiento de beneficiarios y el control operativo de proyectos, integrando diversas herramientas y tecnologías que amplían su funcionalidad y permiten su interoperabilidad con otros sistemas internos y externos.

Backend y procesamiento de datos

El backend de CQTX está construido sobre **Django**, un framework robusto de desarrollo web en Python, complementado por **Django REST Framework** para la exposición de interfaces de programación de aplicaciones (APIs) bajo el estándar REST. La base de datos del sistema es administrada mediante **PostgreSQL**, mientras que **Redis** y **Celery** se

utilizan para la ejecución de tareas asíncronas y la gestión de colas de trabajo. Esta combinación permite la ejecución eficiente de procesos de alto consumo computacional, como la generación de reportes, validaciones masivas y notificaciones automatizadas.

Frontend e interfaces de usuario

El frontend de CQTX está desarrollado con **Vue 3**, integrando **TypeScript** para garantizar tipado estático y robustez en el código, **Pinia** como gestor del estado de la aplicación, y **Radix** como sistema de componentes reutilizables y accesibles. Esta arquitectura garantiza una experiencia de usuario moderna, fluida y coherente. Durante la pasantía, se diseñaron además interfaces adicionales para nuevos módulos (como PQRS y UBE) utilizando herramientas como **Figma** para prototipado visual y **Flutter** para la creación de interfaces móviles.

Infraestructura y despliegue

La infraestructura tecnológica se encuentra desplegada principalmente en **DigitalOcean**, donde se utilizan contenedores Docker gestionados a través de **Dokku**, lo que permite una orquestación simple pero efectiva de las aplicaciones. Los flujos de integración y entrega continua (**CI/CD**) se encuentran automatizados mediante **GitHub Actions**, permitiendo despliegues controlados, reproducibles y consistentes. Como parte de las mejoras realizadas, se implementó la separación lógica de aplicaciones en distintos servidores, lo cual incrementó la seguridad, la disponibilidad de los servicios críticos y la capacidad de mantenimiento. (*TekSystems, 2024*)

Automatización, monitoreo y observabilidad

Como parte del fortalecimiento de la infraestructura tecnológica, se consolidó un stack de automatización y monitoreo que incluye:

- **Ansible**: empleado para la automatización de tareas administrativas (*Hochstein, 2017*), como la configuración remota de estaciones de trabajo y servidores, así como el apagado automatizado al finalizar la jornada laboral.
- **Zabbix**: sistema de monitoreo de código abierto utilizado para la supervisión en tiempo real de estaciones y servidores, con alertas basadas en condiciones críticas y plantillas personalizadas. (*Turnbull, 2021*)
- **Grafana + OTEL-LGTM**: stack de observabilidad que permite la visualización integrada de métricas, logs y trazabilidad de servicios distribuidos, facilitando el análisis de desempeño y la toma de decisiones operativas. (*McCollam, 2022*)

Seguridad informática

En materia de seguridad, se implementaron múltiples controles técnicos y procedimentales:

- **Autenticación basada en JWT**, con segmentación de accesos según roles organizacionales y niveles de privilegio.
- **CAPTCHA** integrado tanto en el inicio de sesión como en todos los endpoints anónimos, como mecanismo de mitigación ante ataques automatizados.
- **Pruebas de seguridad automatizadas** mediante el uso de **OWASP ZAP** (*OWASP, 2024*), lo que permitió detectar vulnerabilidades en los módulos principales antes de su paso a producción.
- **Administración centralizada de antivirus** utilizando **Kaspersky Next**, mediante la definición de políticas de seguridad, grupos de endpoints, monitoreo de amenazas y generación de reportes.
- **Validaciones de red corporativa** utilizando infraestructura **Aruba**, lo que incluyó la revisión de configuraciones de switches, controladores y políticas de control de acceso.

Adicionalmente, se inició el proceso de implementación de un **Sistema de Gestión de Seguridad de la Información (SGSI)** alineado con la norma **ISO/IEC 27001**, el cual incluyó la documentación de políticas internas, procedimientos, cronogramas, matrices de riesgos y planes de acción.

Integraciones externas y herramientas de apoyo

CQTX se comunica activamente con otras plataformas desarrolladas por la fundación o por aliados estratégicos:

- **Compensave**: plataforma basada en **Django** y **Wagtail CMS**, diseñada para la gestión y oferta de Créditos de Conservación Voluntaria (CCV), en proceso de integración con CQTX mediante servicios de consulta de información predial.
- **PL4N3T**: solución especializada en el cálculo de huella de carbono, desarrollada por una empresa del ecosistema de innovación de la fundación.
- **ODK (Open Data Kit)**: plataforma para la recolección de datos en campo, utilizada para el seguimiento de actividades de conservación. Se proyecta su integración directa con CQTX, eliminando la necesidad de herramientas intermedias como Power BI para la visualización macro de datos.

- **Google Workspace**: como suite de productividad organizacional, incluyendo la automatización de procesos con **Google Apps Script**, como la generación masiva de contratos en PDF.
- **Power BI**: herramienta utilizada actualmente para la elaboración de informes estratégicos, con conexión directa a la base de datos de CQTX. Se proyecta su reemplazo gradual mediante el uso de dashboards en **Grafana**. (*The Research Insights, 2025*)

4.1.1. Mantenimiento y operación de infraestructura tecnológica

Durante el desarrollo de la pasantía, se ejecutaron múltiples actividades orientadas a garantizar la continuidad operativa, la seguridad y la escalabilidad de los servicios tecnológicos de la Fundación Cataruben. Estas tareas incluyeron la administración de servidores, la reorganización de la infraestructura digital, la configuración de servicios de red, la migración de sistemas de correo electrónico y la gestión del sistema antivirus empresarial.

Administración de servidores

Al inicio del proceso, la infraestructura de la Fundación estaba compuesta por tres servidores principales, todos alojados en la nube mediante **DigitalOcean** (*DigitalOcean, 2024*): uno para el sistema CQTX y el sitio web institucional, otro para la plataforma Compensave y un tercero para servicios geoespaciales mediante **GeoServer**. Las labores de mantenimiento se centraron en la **gestión reactiva** de estos entornos, incluyendo reinicios planificados ante caídas de servicios (por ejemplo, interrupciones en las conexiones de Power BI con la base de datos), carga manual de archivos CSV, y diagnósticos operativos a través de herramientas como htop, journalctl y ufw.

Aunque no existía un esquema formal de mantenimiento preventivo, se propuso y se comenzó a estructurar un enfoque más sistemático para el monitoreo de recursos y la gestión de eventos críticos.

Reorganización de servicios y separación de entornos

Uno de los avances clave en términos de infraestructura fue la **separación lógica y física de servicios críticos**. El sitio web institucional fue desvinculado del servidor que alojaba CQTX, lo cual mejoró la distribución de recursos, redujo la superficie de ataque y facilitó la administración de accesos.

Asimismo, el droplet que contenía Compensave, originalmente gestionado por un tercero, fue migrado a la infraestructura interna de la Fundación, lo que permitió **recuperar el control total sobre el servicio** y aplicar estándares homogéneos de seguridad y despliegue.

La gestión de entornos de desarrollo y producción se organizó mediante **aplicaciones independientes en Dokku**, una plataforma ligera de orquestación de contenedores **Docker** (*Dokku, 2024*). Aunque ambos entornos aún coexisten en el mismo droplet, esta separación lógica ha facilitado tareas como la detección de errores, la realización de pruebas previas a producción y la reducción de tiempos de inactividad por fallas inesperadas.

Migración y configuración de servicios de correo

Antes de la intervención, el envío de correos desde las plataformas digitales de la Fundación dependía de configuraciones manuales sobre SMTP de Google, sujetas a constantes interrupciones por cambios de credenciales o límites operativos. Con el fin de estabilizar este proceso, se ejecutó la **migración hacia Amazon Simple Email Service (SES)** (*Amazon Web Services, 2024*).

La migración implicó la configuración de la cuenta, la verificación de la dirección remitente y la integración con los sistemas existentes. El dominio de envío ya estaba previamente verificado en **GoDaddy** (*GoDaddy, 2024*), por lo cual se garantizó la autenticidad de los mensajes y se redujo el riesgo de categorización como spam. Como resultado, se logró establecer **un canal de correo robusto, seguro y confiable**, que actualmente opera sin necesidad de intervención manual.

Gestión de red corporativa con Aruba

Se participó activamente en la administración de la red local de la sede operativa mediante la plataforma **Aruba**, utilizada para gestionar **switches y puntos de acceso (APs)** (*Aruba Networks, 2024*). Las tareas incluyeron la **creación y administración de VLANs**, el bloqueo de usuarios según políticas internas y la aplicación de controles de acceso que fortalecen la seguridad del entorno corporativo.

Si bien no se realizaron pruebas de red formales, la topología lógica de la infraestructura fue validada a partir de los diagramas generados automáticamente por la interfaz de administración de Aruba, lo que permitió tener una visión clara de la distribución de dispositivos y rutas de conectividad.

Administración del sistema antivirus corporativo

La Fundación utiliza **Kaspersky Next** como solución de seguridad para endpoints (*Kaspersky, 2024*). Durante la pasantía se brindó soporte en la **gestión centralizada del sistema antivirus**, incluyendo:

- **Creación de políticas de seguridad** y perfiles de comportamiento según el rol de cada dispositivo.
- **Configuración de grupos y segmentación de equipos** según su nivel de criticidad.
- **Definición de exclusiones, programación de escaneos y activación de alertas** para eventos de seguridad.

Aunque el sistema ya estaba desplegado al inicio de la pasantía, se realizó una revisión integral de su configuración, fortaleciendo las capacidades de monitoreo, respuesta ante incidentes y reporte de amenazas.

4.1.2. Seguridad de la información y protección de datos

Como parte de las responsabilidades asumidas durante la pasantía, se abordaron tareas críticas relacionadas con la seguridad de la información, tanto desde la perspectiva operativa como desde una visión estratégica institucional. Estas actividades incluyeron la implementación de controles técnicos en los sistemas desarrollados por la Fundación, la configuración de herramientas de seguridad, la realización de pruebas de vulnerabilidad, así como la estructuración y puesta en marcha del Sistema de Gestión de Seguridad de la Información (SGSI) institucional.

Seguridad en plataformas web

Los sistemas CQTX y Compensave, desarrollados con tecnologías como Django y Vue 3, utilizan **JSON Web Tokens (JWT)** como mecanismo de autenticación principal (*Auth0, 2024*). Si bien al momento de la pasantía no se había implementado autenticación multifactor (MFA), esta se encontraba contemplada como parte de los futuros ajustes de seguridad.

En cuanto al control de accesos, inicialmente no existía un esquema formal de roles y permisos, por lo que se identificó esta ausencia como una debilidad que debía abordarse progresivamente. No obstante, se implementaron controles adicionales en endpoints públicos mediante re**CAPTCHA** (Google Developers, 2024), el cual fue aplicado en los formularios de inicio de sesión del sistema CQTX, tanto en su versión web como en la

aplicación móvil para propietarios de predios. Posteriormente, se extendió esta protección a todos los formularios y endpoints anónimos, como medida de mitigación ante posibles ataques automatizados o intentos de denegación de servicio (DoS).

Durante el ciclo de desarrollo, se aplicaban prácticas de revisión por pares en los pull requests (PRs), y como parte de la pasantía se asumió la responsabilidad de **revisar y aprobar los cambios en el entorno de pruebas**, velando por la incorporación de buenas prácticas en materia de desarrollo seguro.

Endurecimiento de sistemas y red

Se realizaron ajustes de **endurecimiento de servidores (hardening)**, tales como la **desactivación del acceso remoto para el usuario root vía SSH** (*Linux Foundation, 2024*), así como la implementación de túneles seguros para conexiones con herramientas administrativas como **PgAdmin**, evitando exposiciones innecesarias de servicios directamente en la red pública.

En el ámbito de red, se fortalecieron las políticas de seguridad mediante la **administración avanzada de la infraestructura Aruba**, aplicando controles como la **filtración por dirección MAC**, la **segregación de direcciones IP por áreas y funciones**, y el establecimiento de **listas de bloqueo de dispositivos no autorizados**. Estas medidas contribuyeron a mejorar la postura de seguridad de la red corporativa de la Fundación.

Pruebas de seguridad con OWASP ZAP

Se realizaron **pruebas de seguridad iniciales** sobre los sistemas web **cqtx.cataruben.org** y **compensave.co** utilizando la herramienta **OWASP ZAP** (*OWASP Foundation, 2024*), lo cual permitió detectar vulnerabilidades relacionadas con configuraciones inseguras, encabezados HTTP ausentes o mal definidos, y exposición de metadatos innecesarios. Estas pruebas se ejecutaron de forma manual desde la interfaz gráfica de ZAP, dado que se trataba de un análisis exploratorio con fines de diagnóstico. Los hallazgos obtenidos fueron documentados y compartidos con los responsables de cada sistema. En el caso de Compensave, se notificó a la empresa externa a cargo de su desarrollo para su correspondiente corrección.

Implementación del Sistema de Gestión de Seguridad de la Información (SGSI)

Uno de los hitos más relevantes de la pasantía fue la **formulación e implementación inicial del Sistema de Gestión de Seguridad de la Información (SGSI)**, alineado con la norma internacional **ISO/IEC 27001** (*ISO, 2024*). Este proceso incluyó:

- La elaboración y ajuste de **políticas institucionales** de seguridad de la información.
- La redacción de **procedimientos operativos y técnicos**, así como su integración con documentos ya existentes.
- La construcción de **cronogramas de trabajo y planes de acción**.
- La elaboración del **inventario de activos de información** y una **matriz de riesgos**, con planes de tratamiento definidos para riesgos de nivel moderado.

Paralelamente, se formalizó la **creación del Comité de Seguridad de la Información** como ente rector de la política de SI en la organización. Antes de finalizar la pasantía, se asignó formalmente el rol de **Responsable de Seguridad de la Información** al pasante, encargándose de liderar la definición e implementación de medidas técnicas y organizativas orientadas a salvaguardar la confidencialidad, integridad y disponibilidad de la información en toda la Fundación.

Aunque el SGSI se proyectó inicialmente sobre los sistemas CQTX, su alcance es **institucional**, y se espera su progresiva aplicación a todas las plataformas digitales y procesos internos. Según estimaciones del consultor externo que acompaña el proceso, el nivel de avance pasó de un 40 % al inicio de la pasantía a más de un 70 % al cierre del periodo, evidenciando avances sustantivos en documentación, gobernanza, concienciación y controles técnicos.

4.1.3. Desarrollo y mejora de plataformas digitales

Durante la pasantía, se participó activamente en tareas de diseño, desarrollo, pruebas e integración de funcionalidades dentro del ecosistema de plataformas digitales de la Fundación Cataruben. Estas actividades abarcaron desde el diseño de nuevos módulos y mejora de la experiencia de usuario hasta la automatización de procesos y el fortalecimiento de la calidad del código fuente.

Diseño y desarrollo de nuevos módulos

Se colaboró en el diseño e implementación del módulo de **Unidad de Beneficios Económicos (UBE)**, participando tanto en la **construcción de la experiencia de usuario (UX)** como en el **modelo de datos subyacente**, desarrollado sobre PostgreSQL. Aunque la participación en backend y frontend fue tangencial, se contribuyó como **revisor técnico de código**, asegurando la alineación con estándares de calidad y buenas prácticas.

En el caso del módulo de **PQRS (Peticiones, Quejas, Reclamos y Sugerencias)**, se asumió un rol más amplio como **ingeniero de requisitos, diseñador UI/UX y coordinador**

técnico, dado que su desarrollo fue encargado a una empresa externa. Este trabajo implicó la definición de funcionalidades, flujos de interacción y entregables esperados, además del acompañamiento técnico al proveedor para garantizar la coherencia con la arquitectura institucional.

Mejoras funcionales y refactorización de código

Se implementaron diversas **mejoras funcionales** dentro de las plataformas existentes. En el sistema CQTX se desarrolló una **funcionalidad de guardado y lectura de postulaciones en tiempo real** utilizando **WebSockets** implementados mediante **Django Channels y Daphne** (*Django Software Foundation, 2024*), lo cual mejoró significativamente la experiencia de uso y redujo problemas de sincronización.

También se añadió una función de **redimensionamiento automático de imágenes** insertadas en los comentarios del módulo de postulaciones, con el fin de optimizar la carga y visualización de contenido multimedia.

Se atendieron múltiples **ajustes menores y corrección de errores (bugs)**, incluyendo fallas de tipado, errores de despliegue, validaciones ausentes, errores en la carga de datos y ajustes cosméticos. Estos cambios permitieron mantener la estabilidad del sistema y optimizar su rendimiento.

Fortalecimiento de la calidad del software

Como parte del fortalecimiento del ciclo de vida del software, se desarrollaron **pruebas de cobertura automatizadas** para los módulos core, auth y postulaciones del backend, empleando **Coverage.py** como herramienta de medición (*Batchelder, 2024*). Estas pruebas fueron integradas en el flujo de despliegue automatizado mediante **GitHub Actions** (*GitHub, 2024*), asegurando que los entornos de calidad (QA) y producción solo recibieran código que superara umbrales mínimos de cobertura establecidos.

Además, se participó en la **revisión de pull requests (PRs)** como parte del proceso de aseguramiento de calidad, lo cual permitió detectar errores tempranamente y garantizar una evolución controlada del código base.

Diseño de interfaz y experiencia de usuario

Desde el área de diseño se construyeron **pantallas completas y flujos de usuario** para los módulos UBE y PQRS, utilizando Figma (*Figma, 2024*). Asimismo, se realizaron **ajustes de diseño en la plataforma Compensave**, orientados a mejorar la navegación, el acceso a contenidos y la coherencia visual.

Uno de los aportes más relevantes fue la **propuesta y ejecución de un rediseño total de la plataforma CQTX web**, utilizada por el equipo de trabajo de la Fundación. Este rediseño incluyó la **estandarización de elementos de interfaz (UI)**, la mejora en la jerarquía visual y una alineación más estricta con los principios de diseño accesible y responsivo.

Automatización e integración de plataformas

Se desarrollaron integraciones puntuales orientadas a **mejorar el flujo de información entre plataformas**, tales como la **actualización de flujos de datos desde CQTX hacia Power BI** (*Microsoft, 2024*), permitiendo una visualización más precisa y actualizada de indicadores estratégicos.

También se trabajó en la integración con **formularios de recolección de datos en ODK**, usados en campo para actividades asociadas a las iniciativas ambientales.

Adicionalmente, se construyó un sistema de **automatización para la generación de contratos** de propietarios de predios beneficiarios. Este proceso, desarrollado con **Google Apps Script** (Google Developers, 2024), integraba datos extraídos de Monday.com para generar automáticamente los documentos requeridos, reduciendo errores y tiempos operativos.

4.1.4. Monitoreo, trazabilidad y visualización de datos

Durante la pasantía se diseñó, desplegó y configuró un sistema distribuido de monitoreo y visualización, con el objetivo de mejorar la supervisión en tiempo real de la infraestructura tecnológica y reducir los tiempos de respuesta ante incidentes. Esta implementación, aún en fase de consolidación, representa un avance significativo hacia un modelo de operación más proactivo y orientado por datos.

Implementación de monitoreo con Zabbix

Se utilizó **Zabbix** como herramienta principal para el monitoreo de los **equipos de trabajo en la sede de Yopal**, incluyendo dispositivos con sistemas operativos Windows, macOS y Linux (*Zabbix LLC, 2024*). El sistema fue configurado para recolectar métricas críticas como **uso de CPU, consumo de memoria RAM, espacio en disco y conectividad de red**.

Se definieron **alertas por consumo excesivo de recursos sostenido**, con notificaciones enviadas automáticamente por correo electrónico a través del servicio **Amazon Simple Email Service (SES)** (*Amazon Web Services, 2024*). Estas alertas permiten al equipo de TIC anticiparse a posibles fallos operativos, sobrecargas o necesidades de mantenimiento

preventivo. El acceso a los paneles de monitoreo y a las alertas está restringido exclusivamente al **área TIC**, como parte de las políticas internas de seguridad.

Visualización y dashboards con Grafana

Para la visualización centralizada de información técnica se configuró un stack de observabilidad basado en **Grafana, Loki, Promtail y OpenTelemetry**, comúnmente conocido como **OTEL-LGTM** (*Grafana Labs, 2024*). Esta solución permite integrar logs y métricas desde múltiples fuentes en dashboards interactivos, accesibles desde la plataforma https://monitor.app.cataruben.org/.

Grafana está actualmente integrado con los servidores que alojan **CQTX, Compensave** y el propio **servidor de Zabbix**, consolidando tanto logs como métricas de rendimiento. Los dashboards configurados incluyen:

- Monitoreo del uso de recursos de estaciones de trabajo (CPU, RAM, disco, red).
- Visualización y filtrado de logs provenientes de los servicios web y backend desplegados en contenedores Docker.

Estos tableros son consumidos principalmente por el equipo de TIC, aunque se utilizan para **informes semanales y presentaciones internas**, donde se expone el estado operativo de los sistemas al resto de las áreas de la organización.

Centralización de logs y trazabilidad

Previo a esta implementación, los logs de las aplicaciones CQTX y Compensave **no eran persistentes**, ya que residían en memoria y eran accesibles únicamente a través de las herramientas de línea de comandos de Dokku. Esto dificultaba el diagnóstico y limitaba la trazabilidad de errores.

Con la implementación del stack OTEL-LGTM, los logs son recolectados por **Promtail** y enviados a **Loki**, permitiendo su consulta centralizada mediante Grafana. Aunque **la trazabilidad entre servicios (tracing)** no ha sido habilitada aún, se ha preparado la infraestructura base para su integración futura mediante **OpenTelemetry**.

Estado del sistema de monitoreo y pasos siguientes

La implementación del sistema de monitoreo ha generado **mejoras tangibles en el desarrollo, despliegue y mantenimiento** de los sistemas. Ha permitido detectar caídas o anomalías en etapas tempranas, facilitando la atención proactiva de incidentes y mejorando la disponibilidad general del sistema.

Pese a estos avances, el sistema se encuentra **parcialmente implementado**, con varias integraciones aún pendientes. Entre ellas se destacan los registros y métricas provenientes de **Google Workspace, Microsoft 365, Aruba** y otros servidores institucionales. Estas fuentes se consideran prioritarias para la próxima fase del proyecto, una vez se definan los mecanismos de acceso y autenticación con los proveedores respectivos.

4.1.5. Automatización y eficiencia operativa

Durante la pasantía se desarrollaron mecanismos de automatización orientados a reducir tareas manuales, asegurar la consistencia operativa y dar cumplimiento a normativas institucionales, como las políticas de desconexión laboral. Se implementaron soluciones utilizando herramientas como **Ansible** y **Google Apps Script**, enfocadas en tareas críticas de operación técnica y administrativa.

Automatización de tareas operativas con Ansible

Se diseñó e implementó desde cero un sistema de automatización basado en **Ansible**, herramienta de orquestación sin agentes que permite ejecutar comandos remotos sobre múltiples dispositivos mediante scripts YAML (Red Hat, 2024). En este contexto, Ansible se utilizó para:

- Ejecutar el **apagado automatizado de estaciones de trabajo** al finalizar la jornada laboral, en cumplimiento de la política de desconexión laboral.
- Aplicar **actualizaciones automáticas del sistema operativo y navegadores** en las estaciones de trabajo con Windows de la sede Yopal.

El servidor desde el cual se ejecutaban los playbooks coincidía con el **nodo central de monitoreo Zabbix**, lo que facilitaba la sincronización entre el monitoreo y la automatización. Los scripts fueron escritos íntegramente por el pasante, adaptados a la infraestructura existente y sin depender de módulos externos. Esta implementación permitió establecer una **base funcional para futuras automatizaciones más complejas**, como instalaciones masivas, parches de seguridad o administración remota más granular.

Automatización administrativa con Google Apps Script

En paralelo a las automatizaciones técnicas, se desarrolló una solución puntual para la **generación de contratos de propietarios beneficiarios** de iniciativas ambientales. Antes de la automatización, estos documentos eran elaborados de forma manual a partir de plantillas, lo cual resultaba propenso a errores y requería tiempo significativo.

El proceso se optimizó utilizando **Google Apps Script** (Google Developers, 2024), desarrollando un script que:

1. Tomaba como entrada una **hoja de cálculo exportada desde Monday.com** con la información relevante.
2. Procesaba los datos y generaba automáticamente los contratos personalizados.
3. Depositaba los documentos en una carpeta compartida para su posterior validación y envío.

Aunque el script solo se utilizó en una ocasión debido a la falta de estandarización en los campos de entrada provenientes de los proyectos, su efectividad evidenció la **viabilidad de automatizar procesos administrativos repetitivos**, especialmente aquellos basados en datos estructurados. A futuro, se proyecta trasladar este tipo de lógica directamente a CQTX, donde los flujos de datos sí están siendo normalizados.

Impacto y continuidad de las iniciativas de automatización

Las iniciativas de automatización ejecutadas durante la pasantía generaron beneficios concretos en términos de **mayor cumplimiento normativo**, **reducción de errores operativos** y **consistencia en procesos técnicos y administrativos**. En particular:

- El apagado automatizado de equipos aseguró el cumplimiento de políticas internas sin depender del comportamiento individual de los usuarios.
- Las tareas repetitivas como actualizaciones o generación de documentos pasaron a ser tratadas de forma sistemática, con menos intervención manual.
- Se establecieron bases técnicas sólidas para **expandir el uso de Ansible** hacia una administración remota más robusta.

Cabe destacar que, tras la finalización de la pasantía, el autor fue vinculado laboralmente a la Fundación Cataruben, lo cual permite asegurar la **continuidad y evolución de estas soluciones** dentro del ecosistema institucional.

4.1.6. Gestión de desarrollo y requerimientos

A lo largo de la pasantía, se asumieron responsabilidades clave en la organización del flujo de desarrollo, la estandarización de procesos técnicos y la implementación de controles que fortalecen la calidad del software. Estas tareas contribuyeron significativamente a la formalización del ciclo de vida de desarrollo (SDLC) dentro de la Fundación Cataruben, promoviendo buenas prácticas y estructuras sostenibles.

Coordinación técnica y control de calidad *(Atlassian, 2024)***.**

Inicialmente, la participación en el equipo de desarrollo se centró en labores de **control de calidad (QA)**, evaluando funcionalidades y verificando el cumplimiento de criterios antes de los despliegues. Posteriormente, el rol evolucionó hacia **revisor par de pull requests**, asumiendo también la **responsabilidad de los despliegues en el entorno de pruebas**, mediante el uso de flujos automatizados y contenedores aislados.

El flujo de desarrollo estaba estructurado en tres ramas principales (GitHub Docs, 2024):

- **develop**, para integración continua de nuevas funcionalidades,
- **release**, utilizada como staging previo al paso a producción,
- **main**, correspondiente al entorno de producción.

La gestión del backlog de desarrollo fue otra tarea clave asumida por el pasante, incluyendo la revisión de retroalimentación proporcionada por los usuarios y la priorización de tareas en función del impacto y la viabilidad técnica.

Formalización del ciclo de vida del desarrollo (SDLC)

Uno de los aportes más relevantes fue la documentación e implementación del **ciclo de vida del desarrollo de software (SDLC)** de la organización. Esto incluyó la elaboración de procedimientos estructurados para:

- **Levantamiento de requisitos funcionales**
- **Diseño técnico y visual de módulos**
- **Documentación de bases de datos**
- **Implementación de pruebas**
- **Validación y despliegue de mejoras**

Los procedimientos fueron redactados desde cero y están alineados con buenas prácticas de ingeniería de software y control de calidad. Se establecieron lineamientos para el **desarrollo seguro**, incluyendo medidas como control de versiones, protección de ramas críticas y validación de cambios mediante pruebas automatizadas.

Automatización y control en CI/CD

Se modificaron los pipelines de **GitHub Actions** para incluir etapas de validación automatizada antes del despliegue (GitHub Docs, 2024), tales como:

- Ejecución de pruebas unitarias.
- Verificación de cobertura de código con la herramienta **Coverage** en el backend (Coverage.py, 2024).

- Condiciones de paso para permitir el despliegue únicamente si se cumplían los criterios definidos.

Los entornos de prueba y producción están desplegados en **contenedores Docker separados** mediante **aplicaciones independientes en Dokku**, lo que permite simular escenarios reales sin afectar el entorno operativo.

Impacto y sostenibilidad

La contribución más relevante en esta área fue la consolidación del rol de **desarrollador paralelo y QA**, acompañada de la documentación completa del SDLC. Si bien estos procedimientos están actualmente **pendientes de aprobación formal** por parte del Sistema de Gestión Institucional (SGI), su aplicación práctica ha demostrado su utilidad operativa.

Quedan como tareas pendientes la **implementación de roles y segmentación de permisos** más estrictos en los repositorios de código y la **puesta en práctica completa del SDLC** documentado, lo cual servirá como marco base para la madurez técnica futura de la fundación.

4.2. Herramientas utilizadas en el desarrollo del proyecto

Tabla 3. Herramientas tecnológicas

Herramienta utilizada	Para qué la utilizó
Google Workspace Enterprise	Herramientas de productividad y colaboración
Kaspersky Next	Administración de seguridad y protección de endpoints
Aruba	Gestión de red y control de acceso
CQTX	Sistema central de gestión de iniciativas ambientales
Google Apps Script	Automatización de generación de contratos
PgAdmin	Administración de bases de datos PostgreSQL
AWS Console	Configuración de servicios en la nube (Amazon SES)
Figma	Diseño de interfaces de usuario
Excalidraw	Diagramación de bases de datos
Flutter	Desarrollo de interfaces móviles
Zabbix	Monitoreo de servidores, alertas, dashboards, detección de anomalías y rendimiento
Ansible	Automatización de configuración de infraestructura
Coverage	Medición de cobertura de pruebas

ODK	Creación y edición de formularios para recolección de datos
OTEL-LGTM	Visualización de métricas, trazabilidad y monitoreo de servicios
OWASP ZAP	Pruebas de seguridad automatizadas
Django	Desarrollo backend de módulos, autenticación, WebSockets, pruebas y seguridad
PostgreSQL	Gestión de bases de datos para CQTX y módulos nuevos como PQRS
Vue 3	Desarrollo de interfaces de usuario modernas y reactivas
TypeScript	Tipado estático y robustez en el desarrollo frontend con Vue 3

Fuente: Autor

5. CONCLUSIONES

Durante el desarrollo de la pasantía en la Fundación Cataruben, se logró cumplir y superar ampliamente los objetivos propuestos. Las actividades realizadas no solo se alinearon con el cronograma establecido, sino que también incluyeron responsabilidades adicionales de alto impacto, como el liderazgo en seguridad de la información y el diseño de nuevos módulos funcionales.

El objetivo general de integrar servicios tecnológicos se cumplió mediante la implementación de mejoras en el sistema CQTX, automatización de procesos, fortalecimiento de la infraestructura tecnológica y adopción de estándares de seguridad como la norma ISO 27001. Los objetivos específicos también fueron alcanzados: se desarrollaron módulos funcionales, se adaptaron scripts para automatización, y se evaluaron servicios mediante pruebas unitarias y de seguridad.

A partir de noviembre, se asumió el levantamiento de requerimientos para mejoras menores y módulos nuevos, así como la creación de su diseño visual, lo que permitió aplicar metodologías de análisis funcional y diseño centrado en el usuario. Desde febrero, se asumió el rol de responsable de seguridad de la información, liderando la creación del comité de seguridad de la información, la elaboración de procedimientos clave, y la implementación de nuevos sistemas, entre otras acciones estratégicas.

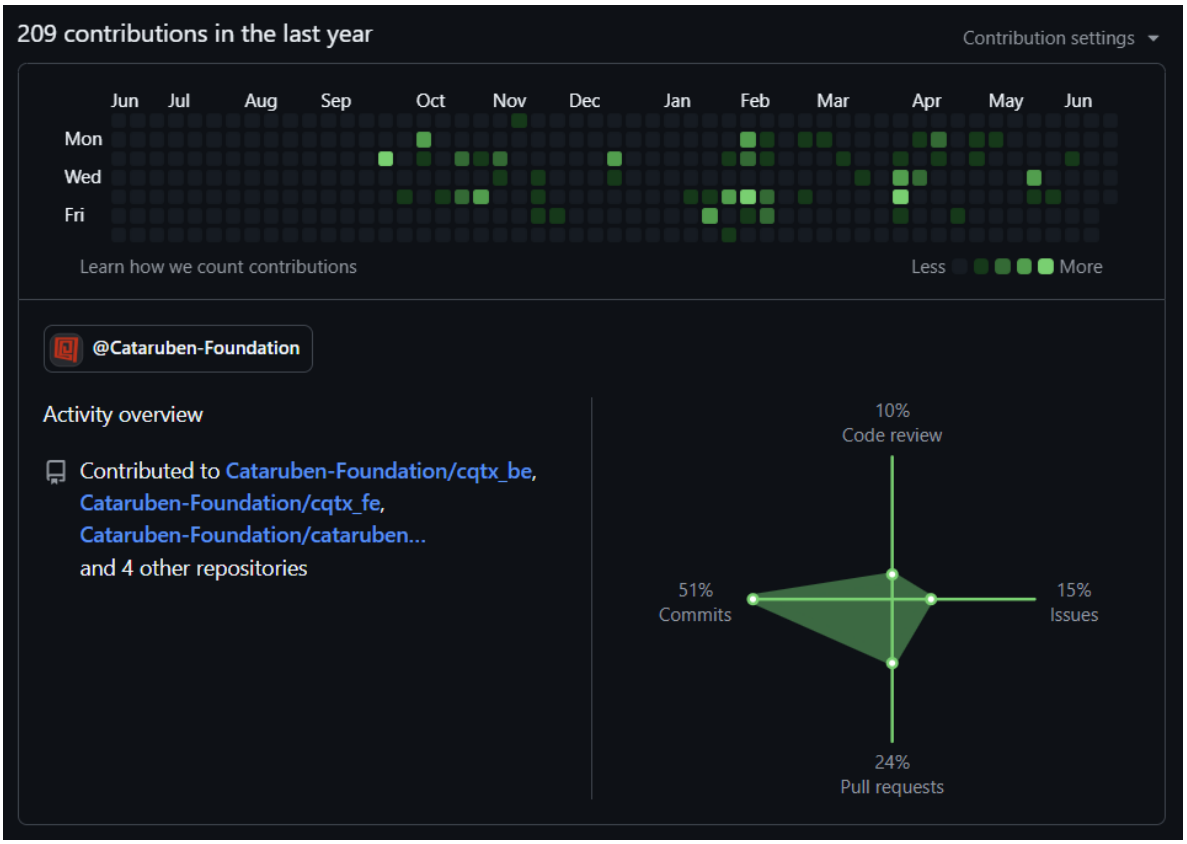
Las principales dificultades incluyeron la gestión del tiempo frente a múltiples responsabilidades simultáneas y la necesidad de dominar herramientas nuevas como Zabbix, Ansible y Grafana. Sin embargo, estas situaciones representaron oportunidades de aprendizaje que fortalecieron las competencias técnicas, organizacionales y de liderazgo del pasante.

En conclusión, la experiencia fue altamente enriquecedora, permitiendo aplicar conocimientos académicos en un entorno real de transformación digital, y contribuyendo significativamente al fortalecimiento institucional de la Fundación Cataruben.

6. ANEXOS

6.1. Anexo 1. Actividad en Github

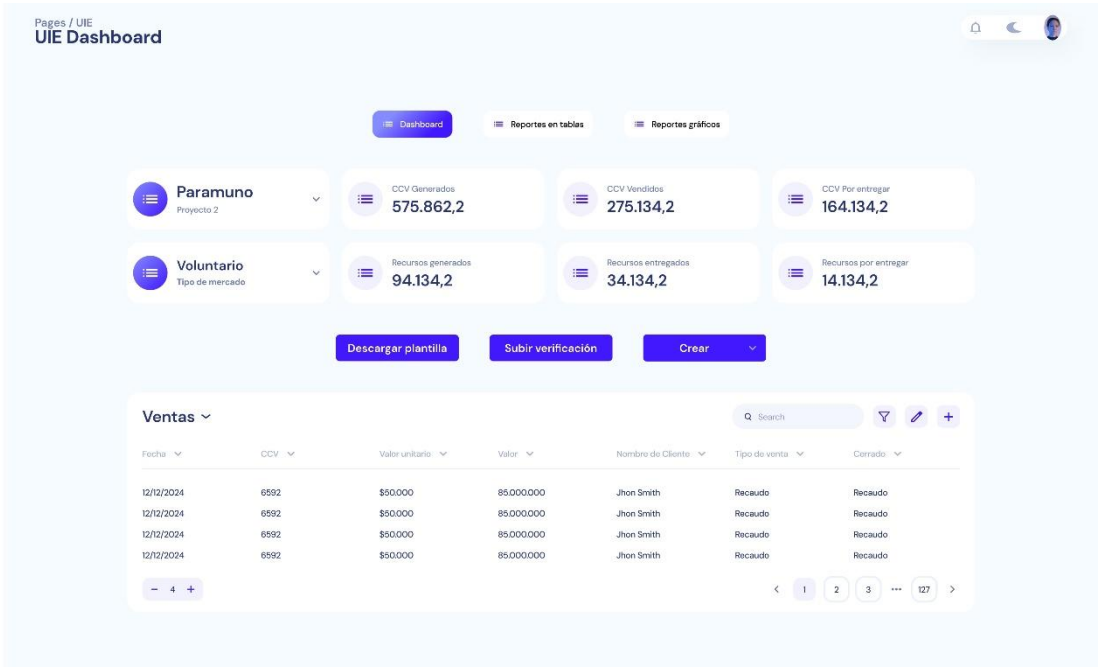
Figura 1. Contribuciones en GitHub desde el inicio de pasantía



Fuente: Autor

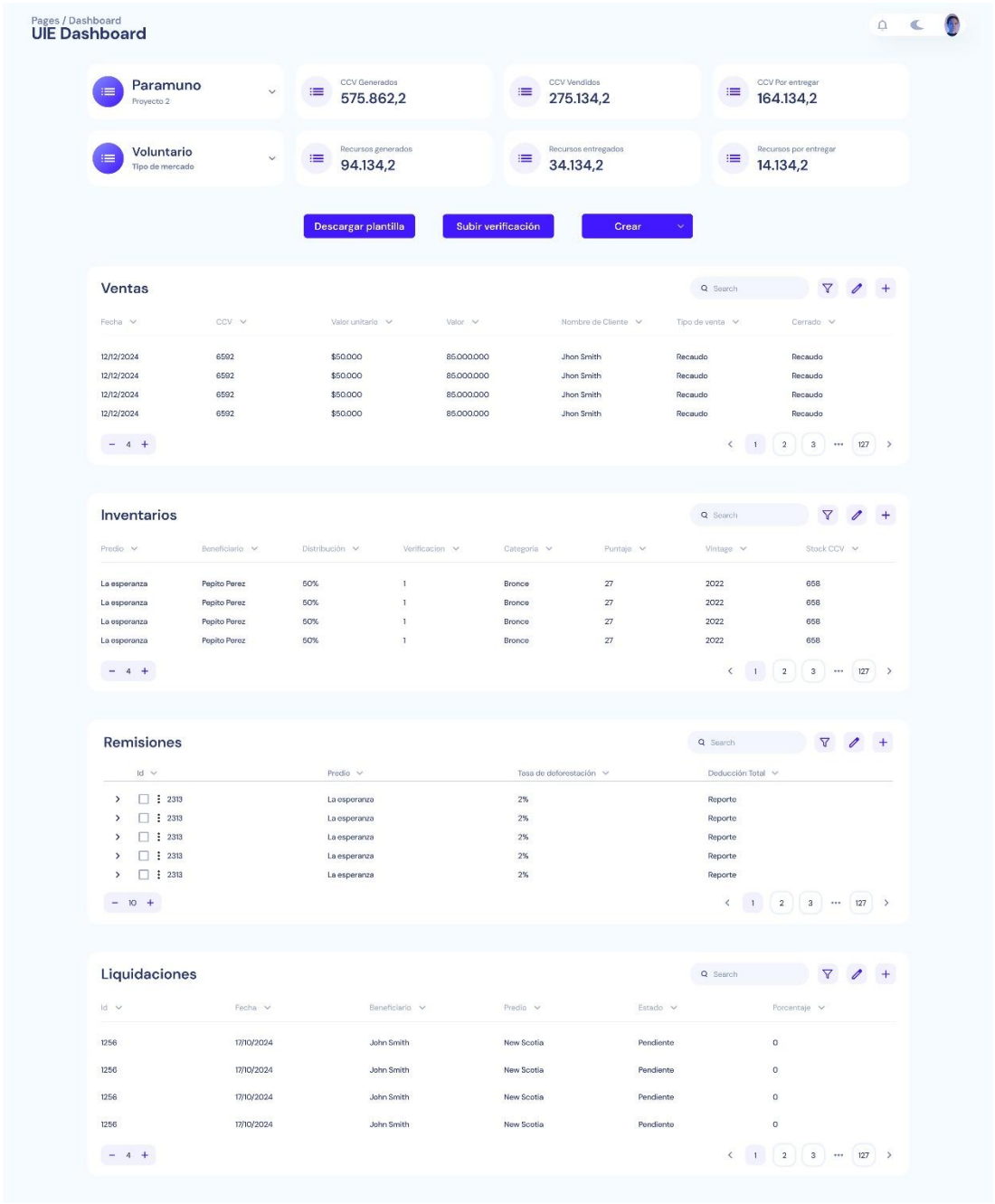
6.2. Anexo 2. Diseño de Modulo Incentivos Económicos

Figura 2 Dashboard de Unidad de Beneficios Económicos - Condensada



Fuente: Autor

Figura 3 Dashboard de Unidad de Beneficios Económicos – Vista Completa

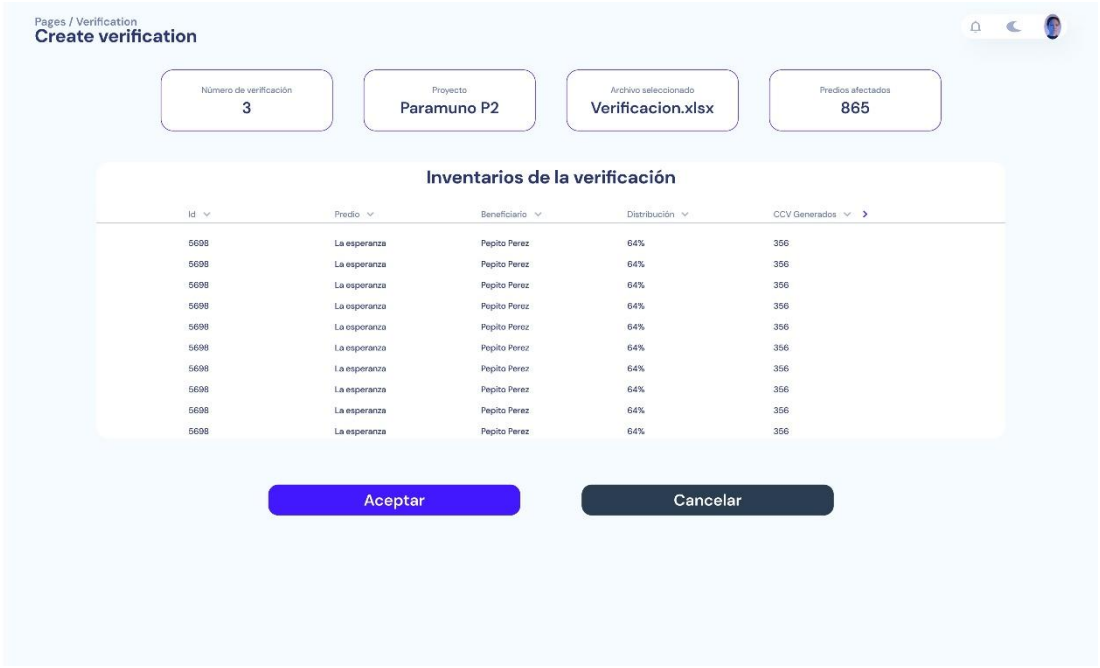


Fuente: Autor

Figura 4 Dialogo de creación de inventarios

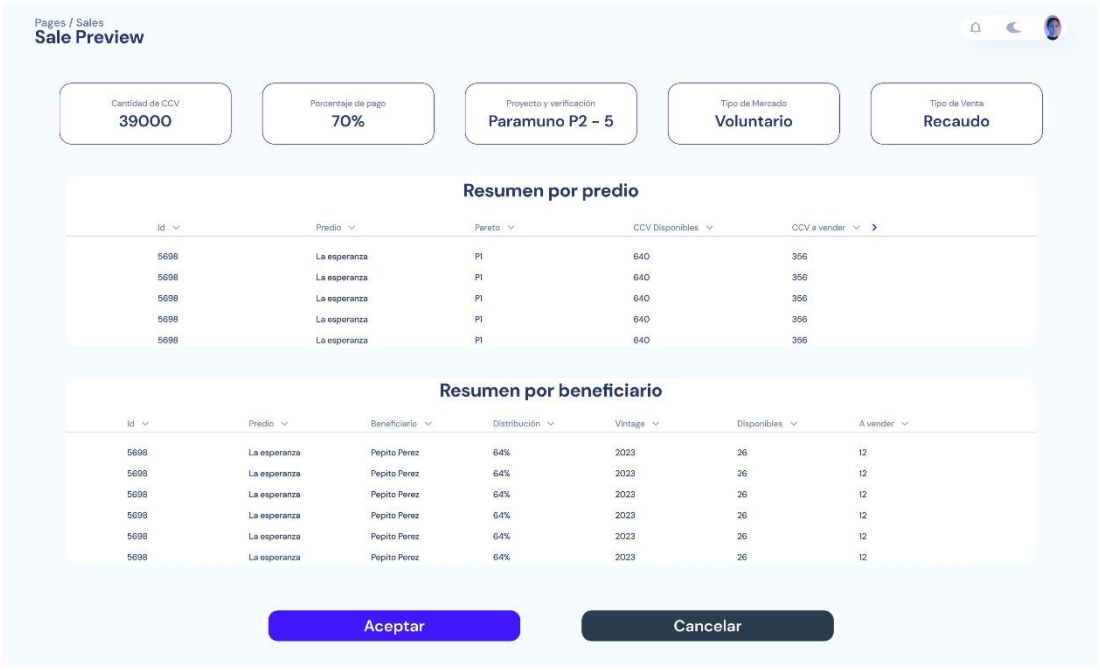
Fuente: Autor

Figura 5 Dialogo de creación de verificación



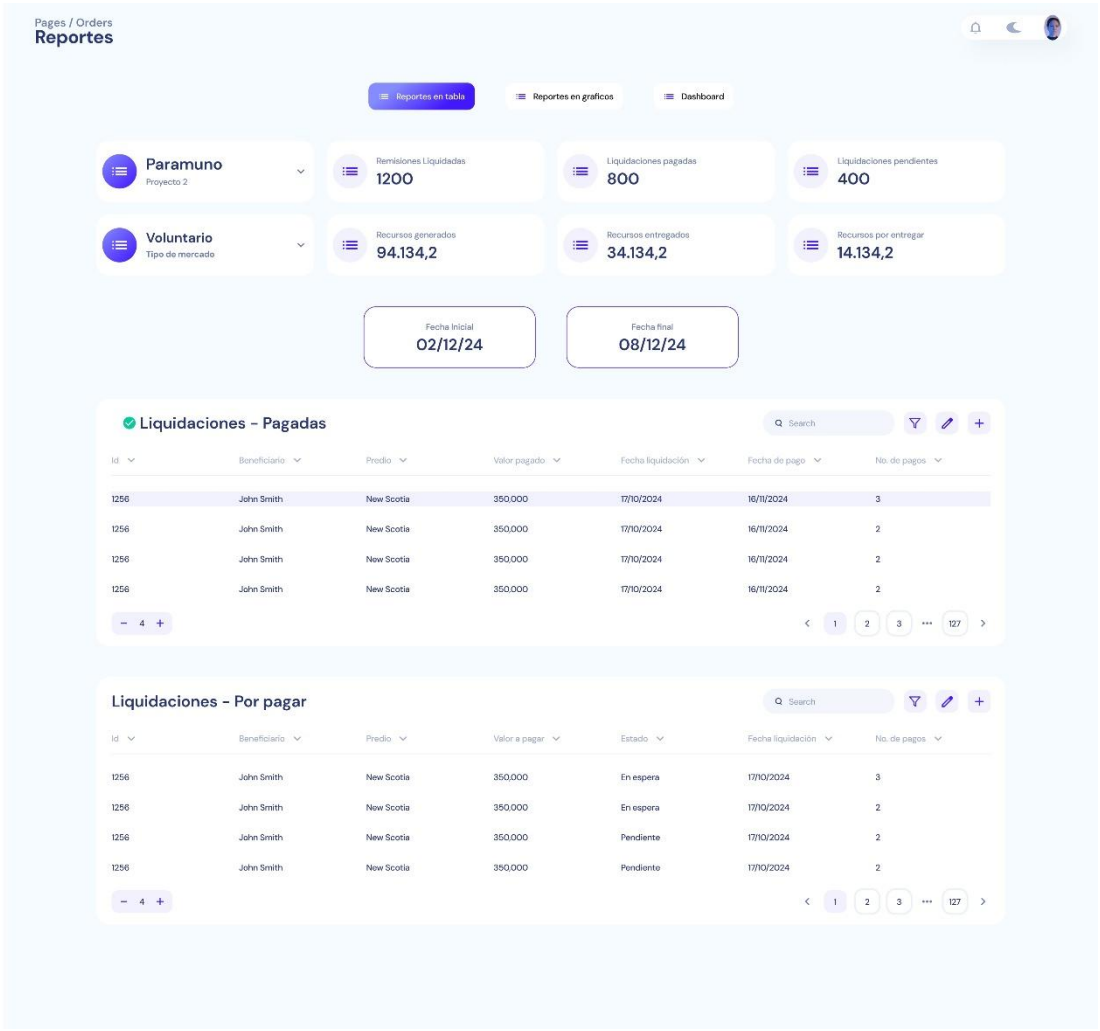
Fuente: Autor

Figura 6 Dialogo de creación de venta



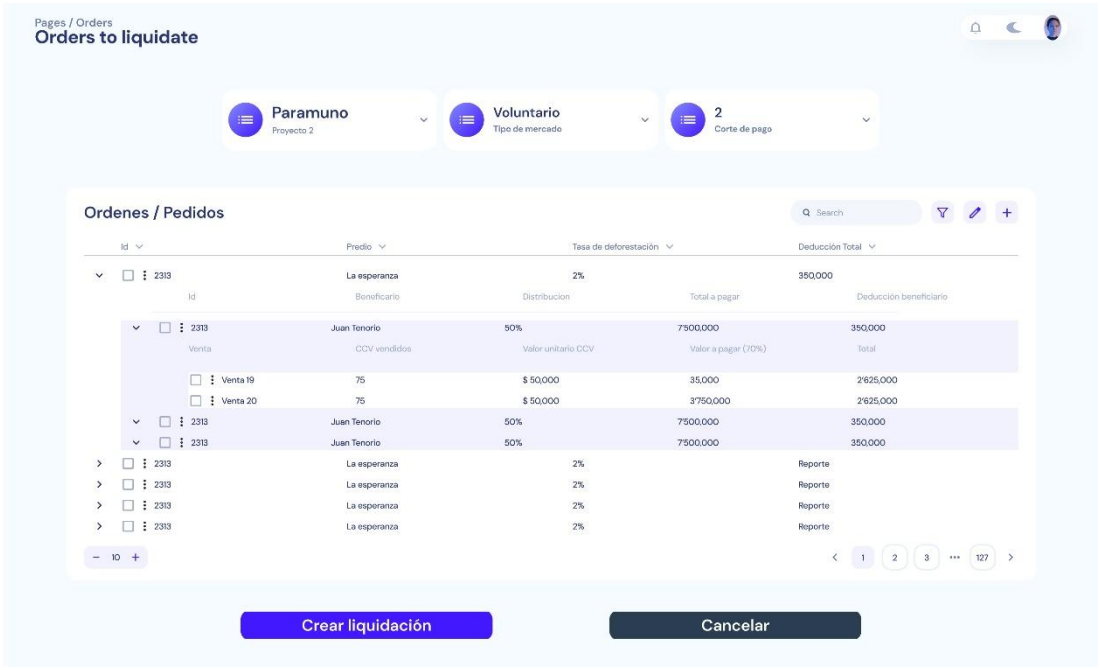
Fuente: Autor

Figura 7 Dashboard de Pagos



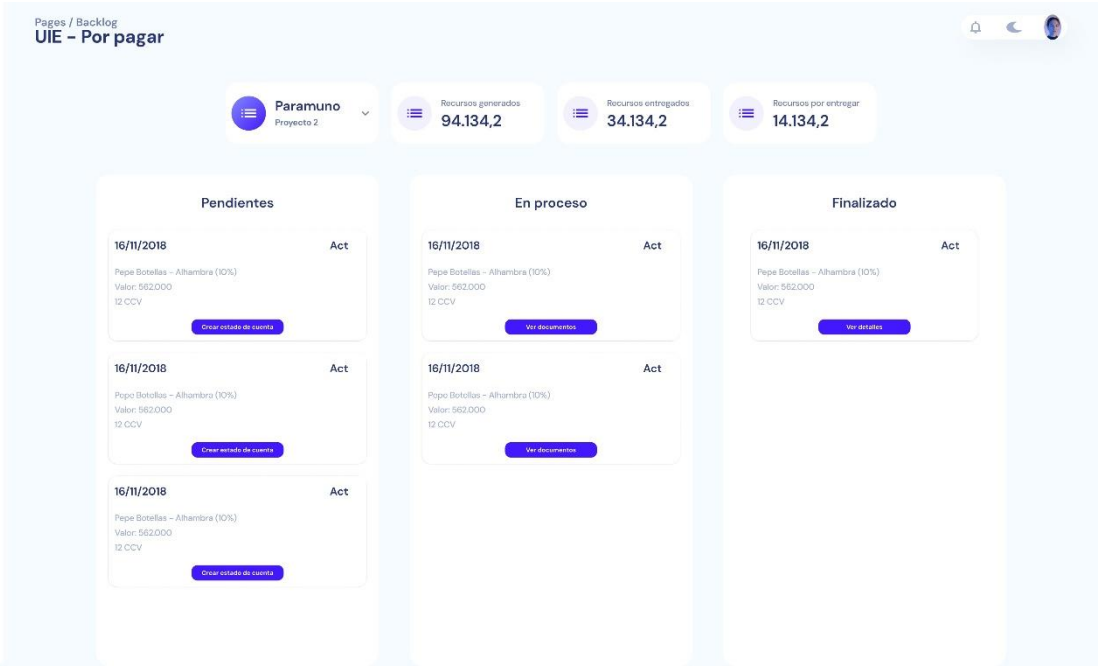
Fuente: Autor

Figura 8 Desglose de Pagos



Fuente: Autor

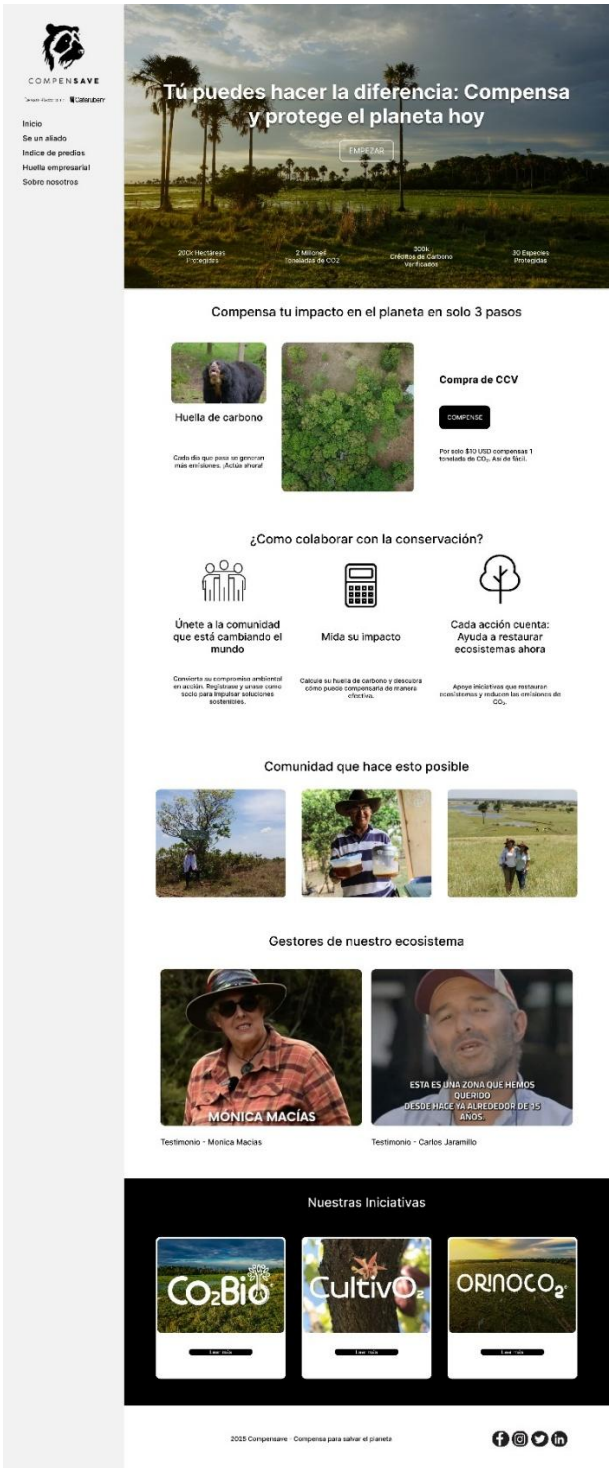
Figura 9 Estado de pagos



Fuente: Autor

6.3. Anexo 3. Cambios de diseño para Compensave.co

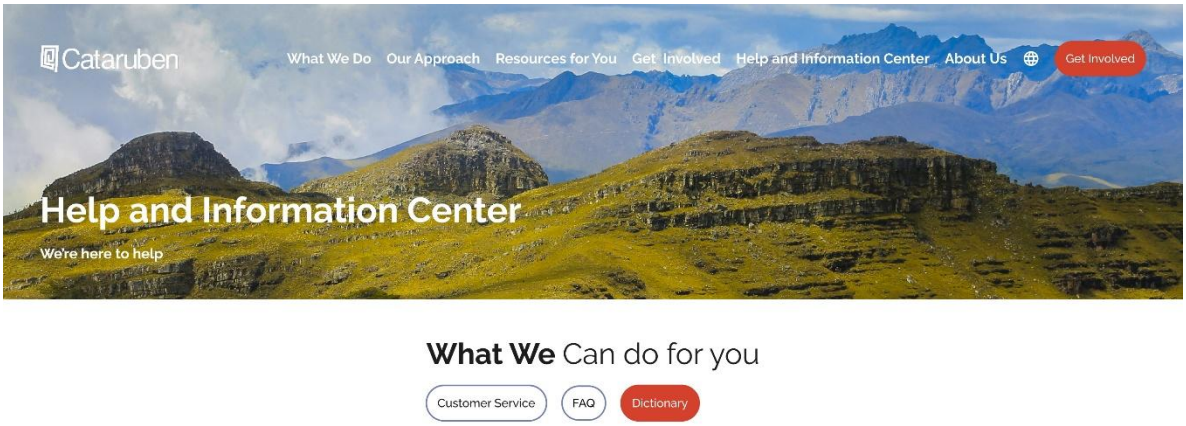
Figura 10 Home de Compensave



Fuente: Autor

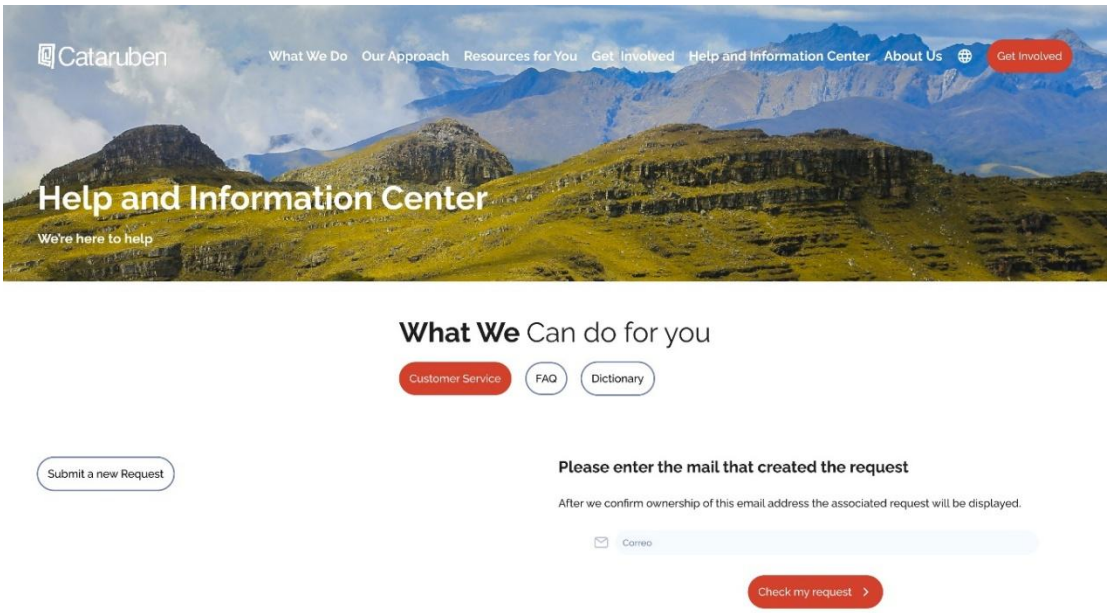
6.4. Anexo 4. Diseño Modulo de PQRS

Figura 11 Modulo de Atención al Ciudadano (Diccionario) en Cataruben.org



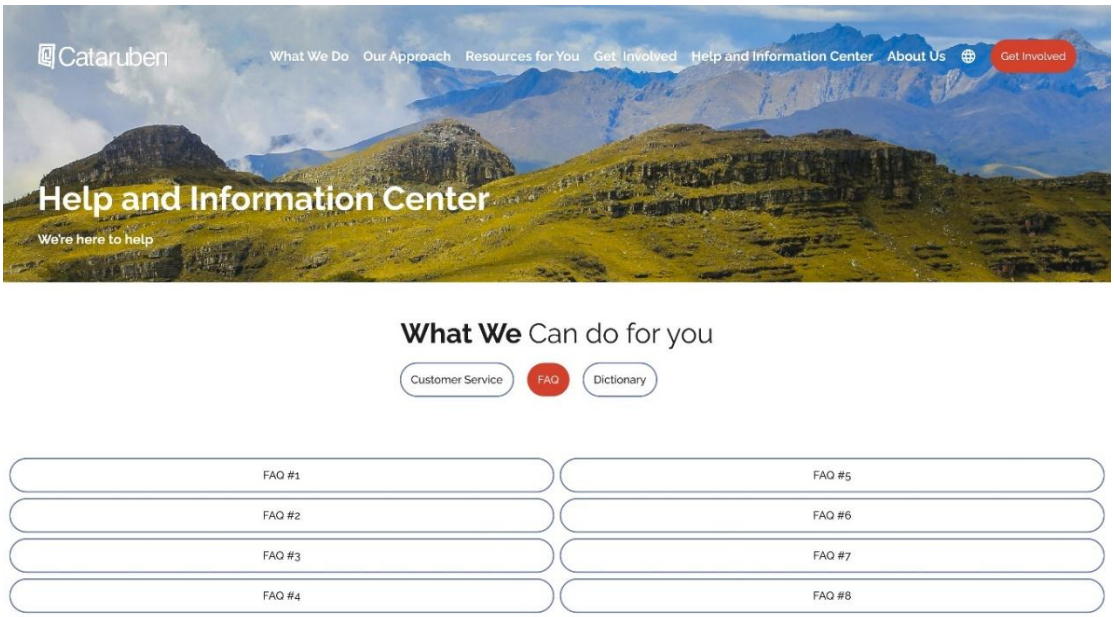
Fuente: Autor

Figura 10 PQRS



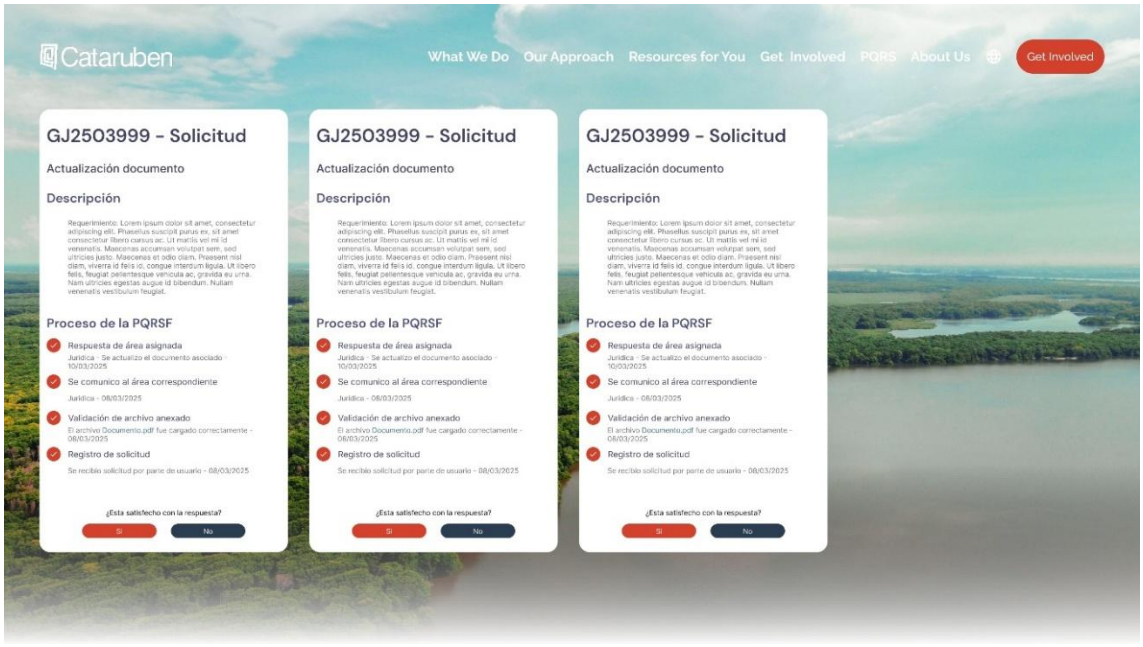
Fuente: Autor

Figura 12 Preguntas Frecuentes



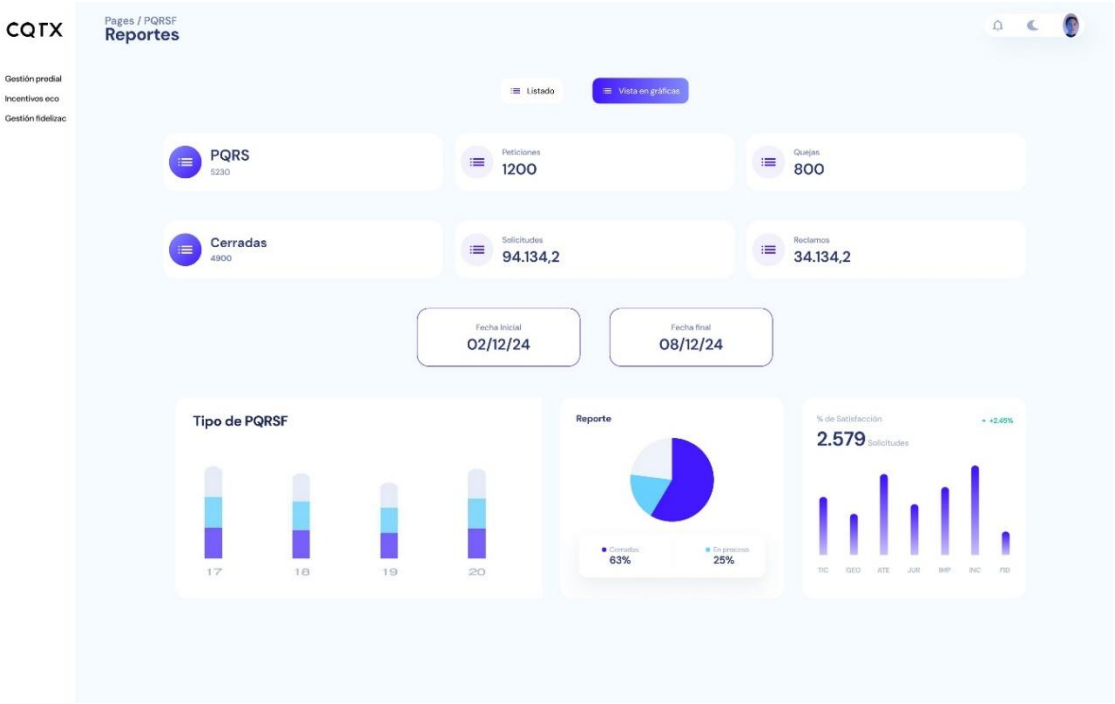
Fuente: Autor

Figura 13 Visualización de historial de PQRS



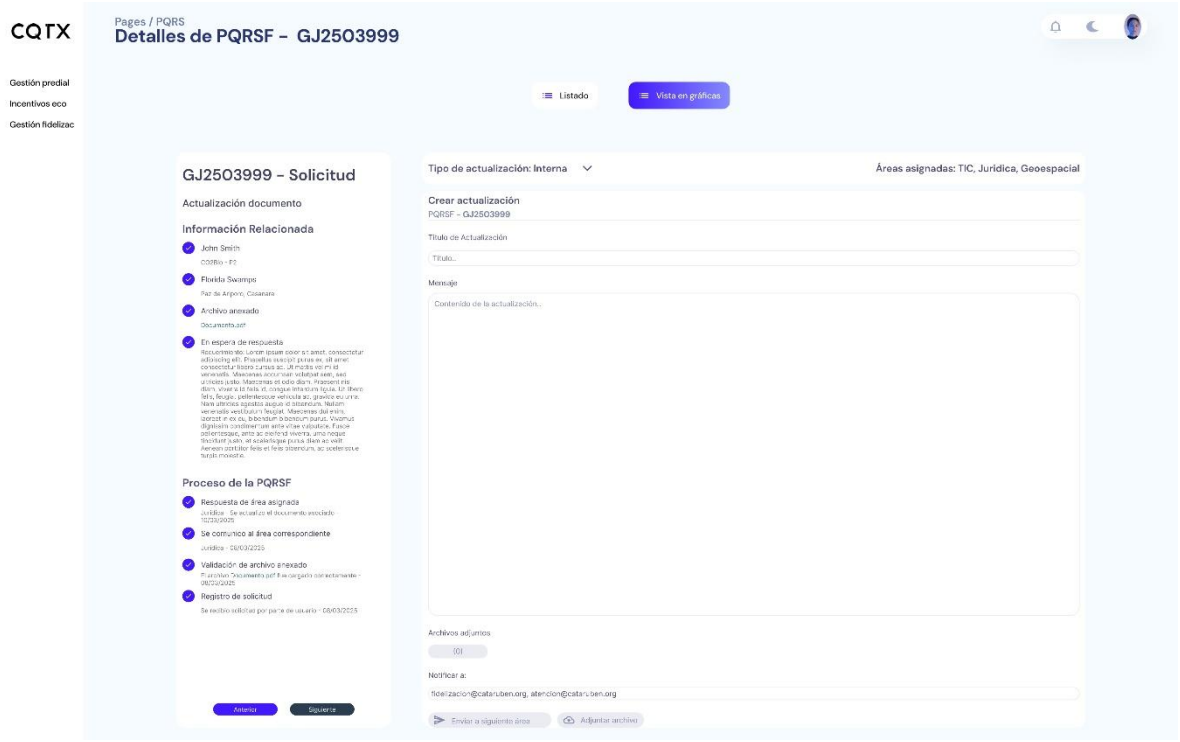
Fuente: Autor

Figura 14 Dasboard de PQRS en CQTX



Fuente: Autor

Figura 15 Detalles y Respuesta a PQRS



Fuente: Autor

6.5. Anexo 5 Levantamiento de requisitos del módulo de PQRS

ERS Módulo de Fidelización

- **1. Introducción**
- **Objetivo**

Describir los requisitos para el módulo de Fidelización, encargado principalmente del manejo de PQRS (Peticiones, Quejas, Reclamos y Sugerencias) y del envío de notificaciones automáticas a los usuarios correspondientes cuando se detectan cambios en la información asociada a las solicitudes.

- **Alcance**

Este módulo formará parte de CQTX y estará disponible para los trabajadores encargados del proceso de fidelización, así como para los usuarios externos que realizan solicitudes a través de la aplicación móvil.

El módulo permitirá la creación, actualización, seguimiento y notificación automática de las PQRS, garantizando la trazabilidad de los eventos y la correcta comunicación con los usuarios involucrados.

- **Actores Involucrados**
- Solicitantes (Usuarios de la aplicación)
- Gestores de Fidelización
- Áreas involucradas en la resolución de PQRS
- **Suposiciones y Dependencias**
- El módulo debe integrarse con el sistema de autenticación existente o debe estar protegido a través de los mecanismos presentes para el manejo de endpoints anónimos.
- Se utilizará el servicio de correo de Amazon SMTP para el envío de las notificaciones.
- Se almacenará un historial de las PQRS y sus paso a paso en la base de datos de CQTX.
- **Descripción de los pasos:**

1. Creación de PQRS: El usuario (solicitante) ingresa su solicitud (Petición, Queja, Reclamo o Sugerencia) a través de la aplicación móvil. Para el caso de pagina web cataruben.org se realiza como anónimo solicitando (Nombre, correo y numero de movil). Para todos los casos debe autorizar política de tratamiento de datos.
2. Registro: El sistema crea un registro en la base de datos con la información básica (fecha, hora, usuario, tipo, etc.).
3. Clasificación: Se determina el tipo de PQRS y su nivel de urgencia, según los criterios (Anexo A).
4. Notificación inicial: El sistema envía un aviso al Gestor o Área de Fidelización asignada.
5. Asignación de responsable: El Gestor revisa la solicitud y asigna la PQRS a la persona o equipo encargado de dar respuesta.
6. Respuesta a la PQRS: El responsable analiza la solicitud, prepara la respuesta o la solución y actualiza la PQRS en el sistema.
7. Notificación al usuario: Una vez registrada la respuesta, el sistema notifica al usuario (por correo y/o push).

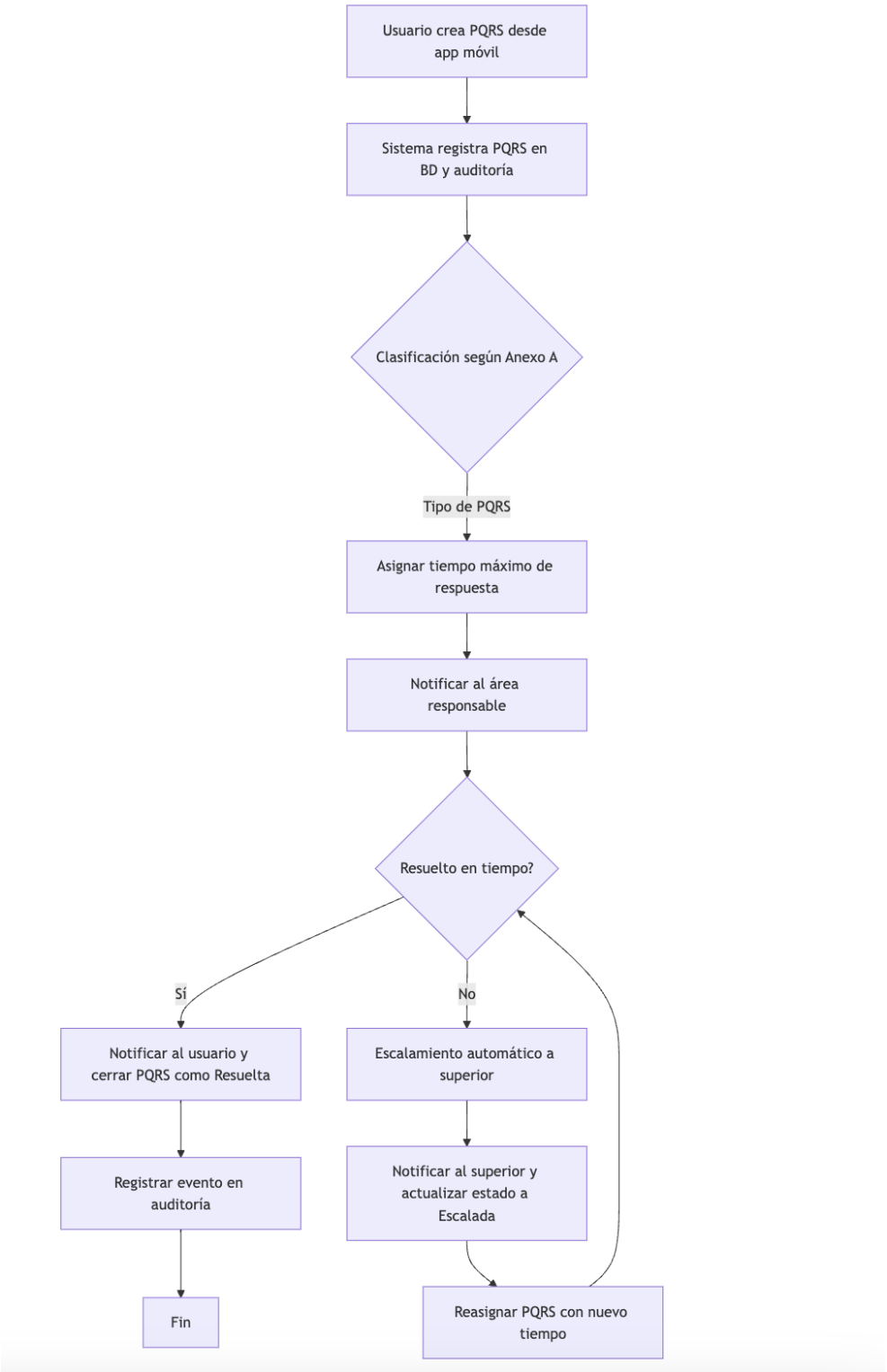
8. Control de tiempos y escalamiento:

a. Si el tiempo de respuesta aún no vence, se continúa el flujo normal.

b. Si vence el tiempo, el sistema escala automáticamente al superior o a la gerencia correspondiente.

9. Cierre o resolución: Cuando la PQRS es resuelta, se marca como “Resuelta” en el sistema.
10. Registro en auditoría: Cada evento (creación, notificación, cambio de estado, cierre) queda guardado en el sistema de auditoría.

Figura 16 Diagrama de Flujo de PQRS



Fuente: Autor

- **2. Requisitos Funcionales**

Tabla 3. Tabla de Requisitos Funcionales Modulo PQRS

ID	Descripción	Prioridad	Dependencias
RF-01	El sistema debe enviar notificaciones por correo con enlace directo a la información relacionada al usuario web, además de notificaciones push.	Alta	Ninguna
RF-02	Permitir la creación de solicitudes PQRS desde la aplicación móvil.	Alta	Ninguna
RF-03	Visualizar las PQRS creadas por el usuario móvil desde la aplicación.	Alta	RF-002
RF-04	Notificar automáticamente al personal asignado cuando se reciba una respuesta a una PQRS.	Alta	RF-002
RF-05	Asignar tiempos de respuesta según la clasificación definida en el Anexo A.	Media	RF-002
RF-06	Notificar a las áreas correspondientes al asignar la PQRS para su resolución.	Alta	RF-005
RF-07	Notificar a los usuarios móviles cuando haya cambios en el estado de su PQRS.	Alta	RF-002
RF-08	Permitir la visualización de la trazabilidad de PQRS para la gerencia, con filtros por estado, tipo de solicitud y fechas.	Media	RF-002
RF-09	Escalamiento automático a superiores si el tiempo de respuesta se encuentra vencido.	Media	RF-005

RF-10	Registrar todos los eventos y cambios en el sistema de auditoría.	Alta	RF-002
RF-11	Permitir la subida de archivos adjuntos en la función de redactar un correo.	Alta	Ninguna

Fuente: Autor

- **3. Requisitos No Funcionales**

Tabla 4. Tabla de Requisitos No Funcionales Modulo PQRS

ID	Descripción	Prioridad
RNF-001	El tiempo de respuesta debe cumplir con los valores definidos en el Anexo de Tiempos de Respuesta.	Alta
RNF-002	La comunicación debe cumplir con los protocolos de seguridad definidos por la política interna.	Alta
RNF-003	Las notificaciones por correo deben enviarse dentro de un tiempo máximo de 2 minutos después de detectado el evento.	Alta

Fuente: Autor

- **4. Requisitos de Integración**

Tabla 5. Tabla de Requisitos de Integración Modulo PQRS

Sistema	Tipo de Integración	Protocolo	Datos Intercambiados
Sistema de Notificaciones	API REST	HTTPS	JSON
Sistema de Auditoría	Base de Datos	ODBC	Información de Eventos
Amazon SMTP	Servicio de Correo	SMTP	Notificaciones por Correo

Fuente: Autor

- **5. Requisitos de Auditoría**

Tabla 6. Tabla de Requisitos Para Lods Modulo PQRS

ID	Evento	Información Registrada	Responsable
RA-001	Creación de solicitud	Fecha, Hora, Usuario, Tipo de solicitud	Sistema
RA-002	Notificación enviada	Destinatario, Fecha, Hora, Tipo de Notificación	Sistema
RA-003	Cambio de estado	Estado anterior, Estado nuevo, Fecha, Responsable	Sistema
RA-004	Escalamiento automático	Responsable Notificado, Fecha, Hora	Sistema

Fuente: Autor

- **6. Criterios de Aceptación**

Tabla 7. Tabla de Criterios de Aceptación Modulo PQRS

ID	Criterio	Método de Validación
CA-001	El sistema envía notificaciones por correo y push a los usuarios correspondientes.	Prueba con datos de prueba
CA-002	El sistema registra los eventos en la auditoría.	Revisión de logs
CA-003	Los tiempos de respuesta se asignan automáticamente según la clasificación definida.	Prueba automatizada

CA-004	Las solicitudes escaladas son notificadas a los responsables superiores.	Prueba con datos de prueba

Fuente: Autor

- **7. Exclusiones**
- No se contemplan notificaciones por SMS.
- No se integrará con redes sociales.
- **8. Glosario**
- Actor: Persona o sistema que interactúa con el módulo.
- Solicitud: Petición que realiza un usuario para iniciar un proceso.
- Notificación: Mensaje enviado por el sistema para informar sobre un evento.
- Escalamiento: Acción automática que notifica a un responsable superior si una solicitud no se resuelve en el tiempo establecido.
- **Anexo A: Tiempos de Respuesta**
- Clasificación por Tipo de Solicitud

Tabla 8. Tabla de Clasificación por Tipo de Solicitud Modulo PQRS

Tipo de Solicitud	**Descripción**	**Tiempo Máximo de Respuesta**	**Etiqueta**
Petición	Información general o trámite sencillo	48 horas	Baja
Queja	Inconformidad con el servicio	24 horas	Media
Reclamo	Error o falla comprobable	12 horas	Alta
Sugerencia	Propuesta de mejora	72 horas	Baja
Urgente	Situaciones críticas (fuga de información, temas legales, etc.)	4 horas	Crítica

Fuente: Autor

- Clasificación por Área Responsable

Tabla 9. Tabla de Clasificación por Área Responsable Modulo PQRS

Área	**Tiempo Máximo de Respuesta**	**Observación**
Atención al Cliente	24 horas	Todas las solicitudes iniciales
Jurídico	48 horas	Quejas legales o datos personales
IT	12 horas	Falla técnica o incidente de seguridad
Comercial	72 horas	Sugerencias o consultas de negocio

Fuente: Autor

- Etiquetas Automáticas

Tabla 10. Tabla de Etiquetas Automaticas Modulo PQRS

Etiqueta	**Definición**
Pendiente	Solicitud recién creada
En proceso	Asignada a un responsable
Vencida	Tiempo de respuesta ha caducado
Escalada	Notificación enviada a superior
Resuelta	Cerrada con respuesta al usuario
Retrasada	Cerrada después del tiempo límite

Este anexo será revisado y actualizado periódicamente para asegurar su alineación con las políticas internas y los compromisos de calidad.

Crear Un buscador de las PQRS
https://susi.fiscalia.gov.co/ui/#/pqr-new-request/1

- **Recomendaciones para Mejorar el Documento**

1. **Roles y Responsabilidades Detallados:**
    - Incluir un apartado o tabla donde se especifiquen claramente los roles (Ej.: Gestor de Fidelización, Área de IT, Área Jurídica, etc.) y sus responsabilidades exactas en el proceso de PQRS.
2. **Estados Intermedios y Flujos de Reapertura:**
    - Podrías detallar si una PQRS puede **reabrirse** en caso de que el usuario no esté conforme con la respuesta, y cómo se gestiona esa reapertura.
3. **Manejo de Errores y Casos Especiales:**
    - Definir qué ocurre si una notificación falla (p. ej., correo no enviado) o si el sistema no puede asignar responsable por falta de disponibilidad.
4. **Seguridad y Accesos:**
    - Describir cómo se controla el acceso al módulo (perfiles de usuario, permisos de lectura/escritura, autenticación).
    - Mencionar si existe cifrado o protección especial para datos sensibles dentro de las PQRS.
5. **Reporte o Estadísticas de PQRS:**
    - Aunque no se contemplen reportes automáticos en esta versión, podrías especificar si se prevé un **panel de indicadores** (número de PQRS por tipo, tiempo promedio de respuesta, etc.) para la gerencia.
6. **Historial de Cambios / Versionado de PQRS:**
    - Señalar si se guarda cada cambio (por ejemplo, cambio de estado o de responsable) en un historial visible, además del registro de auditoría.

6.6. Anexo 6 Reglamento Comité de Seguridad de la Información

Artículo 1. *Objetivo.* El presente reglamento tiene como propósito supervisar y garantizar la implementación, mejora continua y alineación de la estrategia de seguridad de la información con los objetivos de la Fundación Cataruben. El Comité asegurará una gestión efectiva de los riesgos, el cumplimiento normativo y la continuidad operativa ante amenazas tecnológicas.

Artículo 2. *Composición.* El número de integrantes del Comité de Seguridad de la Información (CSI) será proporcional al número de empleados y la complejidad de los riesgos de la Fundación. Para una organización con entre 50 y 100 colaboradores, se recomienda una conformación de entre 5 y 10 miembros clave.

Artículo 3. *Conformación.* El CSI estará compuesto por representantes de diferentes áreas estratégicas, responsables de la gestión y protección de la información.

3.1 Representante de la Alta Dirección

- ***Presidente del Comité y Gerente TIC:*** *Representante de Gerencia, encargado de la ciberseguridad y la infraestructura tecnológica*

3.2 Representantes de Áreas Claves

- **Líder Jurídico (Líder de Cumplimiento Legal)** *Gestión regulatoria y protección de datos*
- ***Gerente Mejora Continua:*** *Supervisión de cumplimiento y auditorías de seguridad.*
- **Profesional Seguridad de la Información** *Responsable de ciberseguridad, confidencialidad, disponibilidad e integridad de la información.*
- **Líder de Abastecimiento (**Seguridad física**)** *Gestión de seguridad en instalaciones y control de acceso físico.*

3.3 Invitados Especiales (cuando sea necesario)

- Expertos externos en seguridad de la información, ciberseguridad o auditoría.
- Representantes de otras áreas según la naturaleza del tema a tratar (ejemplo: Recursos humanos para seguridad del personal).

Parágrafo. El representante de la Alta Dirección es designado por la Gerencia de la Fundación. Los representantes de áreas clave son seleccionados con base en sus competencias.

Artículo 4. *Reuniones.* El CSI se reunirá cada cuatro meses para evaluar el desempeño del **Sistema de Gestión de Seguridad de la Información (SGSI)**. Se convocarán reuniones extraordinarias en caso de incidentes graves, cambios regulatorios o decisiones críticas en seguridad.

Artículo 5. *Actas de Reunión.* Las reuniones del Comité deberán documentarse mediante actas con los siguientes elementos:

a. *Encabezado.* Sección que permite identificar el propósito de la reunión e incluir como mínimo los siguientes elementos:
   - Tipo de reunión (ordinaria o extraordinaria).
   - Número del acta.
   - Fecha y horario de la reunión.
   - Lugar de reunión (si aplica).

b. *Lista de Asistencia.*
   - Nombre y rol de los asistentes.
   - Firma autógrafa de cada asistente.

c. *Verificación de quórum.*
   - El Comité debe contar con la mitad más uno de sus miembros principales.

d. *Desarrollo de la Reunión.*
   - Revisión de compromisos de reuniones anteriores.
   - Seguimiento al cronograma de actividades.
   - Evaluación de incidentes de seguridad y amenazas recientes.
   - Revisión del cumplimiento normativo y auditorías.

e. *Compromisos.*
   - Definir responsables y plazos para la ejecución de actividades pendientes.

Parágrafo. Cada cuatro meses, los resultados de las reuniones serán socializados con el personal mediante los mecanismos definidos por el Comité. Al final de año se entregará un informe gerencial con los resultados del año.

Artículo 6. *Funciones.* El CSI tendrá las siguientes funciones:

a. Definir y supervisar la estrategia de seguridad de la información.
b. Aprobar y actualizar las políticas de seguridad y cumplimiento normativo.
c. Evaluar riesgos estratégicos y definir planes de mitigación.
d. Supervisar la asignación de recursos en seguridad de la información.

e. Revisar auditorías internas y externas, formulando planes de mejora.
f. Garantizar la aplicación del ciclo **PHVA** (Planear, Hacer, Verificar, Actuar).
g. Definir medidas disciplinarias en caso de incumplimiento de políticas de seguridad.
h. Supervisar la correcta gestión de incidentes de seguridad y respuesta ante crisis.
i. Promover programas de capacitación y concienciación en seguridad informática.
j. Evaluar la seguridad en relaciones con terceros y proveedores.
k. Hacer el seguimiento y evaluación de los reportes.
l. Clasificación de la Información: Identificar y clasificar la información por áreas según su uso, considerando perfiles, roles y privilegios de acceso de los usuarios.
m. Definir las competencias y seleccionar las auditorías internas de ISO 27001

Parágrafo. Se establecen funciones específicas para cada rol dentro del Comité.
Funciones del Presidente del Comité y Gerente TIC

1. Convocar y presidir las reuniones del Comité.
2. Revisar estrategias y asignación de recursos.
3. Coordinar la implementación de medidas de ciberseguridad.
4. Supervisar la gestión de copias de seguridad y recuperación ante desastres.
5. Gestionar la actualización y monitoreo de herramientas de seguridad.

Funciones del Líder Jurídico (Cumplimiento Legal)

1. Asegurar el cumplimiento normativo y regulatorio.
2. Gestionar protocolos legales en caso de incidentes de seguridad.
3. Apoyar la negociación de contratos con requisitos de ciberseguridad
4. Socialización de políticas de seguridad de la información
5. Identificación de riesgos

Funciones del Profesional en Seguridad de la Información

1. Monitorear el SGSI y proponer mejoras.
2. Analizar incidentes y amenazas cibernéticas.
3. Supervisar el cumplimiento de estándares como **ISO 27001**.

Funciones del Representante de Abastecimiento y Seguridad Física

1. Gestionar inversiones en seguridad de la información.

2. Coordinar controles de acceso, videovigilancia y seguridad física.
3. Implementar planes de respuesta ante emergencias.

Funciones de Gerente de Mejora Continua.

1. Revisar reportes de auditoría, incidentes de seguridad y gestión de riesgos.
2. Impulsar optimización en controles de seguridad, procesos y procedimientos.
3. Promover cultura de seguridad de la información.

Artículo 7. ***Rendición de Cuentas.*** El Comité elaborará informes cada cuatro meses sobre:

- Evaluación de incidentes de seguridad.
- Cumplimiento de planes de acción.
- Estado del **SGSI** y auditorías realizadas.
- Eficiencia de capacitaciones y campañas de concienciación.

Parágrafo. Informe Anual del Comité de Seguridad de la Información

El Comité de Seguridad de la Información elabora y presenta un informe a la gerencia con el objetivo de proporcionar el estado del Sistema de Gestión de Seguridad de la Información (SGSI) y su evolución en el último período. Este informe incluye:

- Estado de las acciones de revisión previas: Seguimiento y evaluación del cumplimiento de los compromisos adquiridos en reuniones anteriores, detallando los avances, obstáculos y medidas correctivas implementadas.
- Cambios en factores externos e internos: Análisis de cambios internos y externos que puedan impactar la seguridad de la información, incluyendo modificaciones regulatorias, tecnológicas o estructurales dentro de la fundación.
- Evolución de las necesidades y expectativas de las partes interesadas: Evaluación del cambio de requerimientos de clientes, proveedores, empleados y otras partes interesadas en relación con la seguridad de la información.
- Desempeño del SGSI y análisis de tendencias: Presentación de métricas clave sobre la eficacia del SGSI, con análisis estadístico de incidentes, auditorías, cumplimiento de controles y otros indicadores relevantes.

Artículo 8. ***Competencias e Inhabilidades de los Integrantes del Comité.*** Los miembros del Comité deberán:

- Ser colaboradores activos de la Fundación.

- No haber sido sancionados disciplinariamente en el último año.
- Contar con competencias en liderazgo, ética y seguridad de la información.

Parágrafo. El incumplimiento de funciones o ausencias reiteradas serán causales de retiro del Comité.

Artículo 9. ***Recursos para el Funcionamiento.*** La Fundación garantizará:

- Espacios adecuados para reuniones y almacenamiento de documentación.
- Capacitación continua para los integrantes del Comité.
- Herramientas y recursos tecnológicos para el monitoreo de seguridad.

Artículo 10. ***Evaluación y Mejora Continua.*** El Comité será evaluado semestralmente en:

- Cumplimiento de actas y reuniones.
- Participación activa de los integrantes.
- Impacto de las estrategias de seguridad implementadas.

Parágrafo: Los registros de reuniones y evaluaciones deberán archivarse digitalmente para futuras auditorías.

Artículo 11. El presente reglamento entra en vigor a partir del **14 de febrero de 2025** y estará sujeto a revisión y actualización según las necesidades de la organización.

_____

MARÍA FERNANDA WILCHES FONSECA
REPRESENTANTE LEGAL

Control del Documento

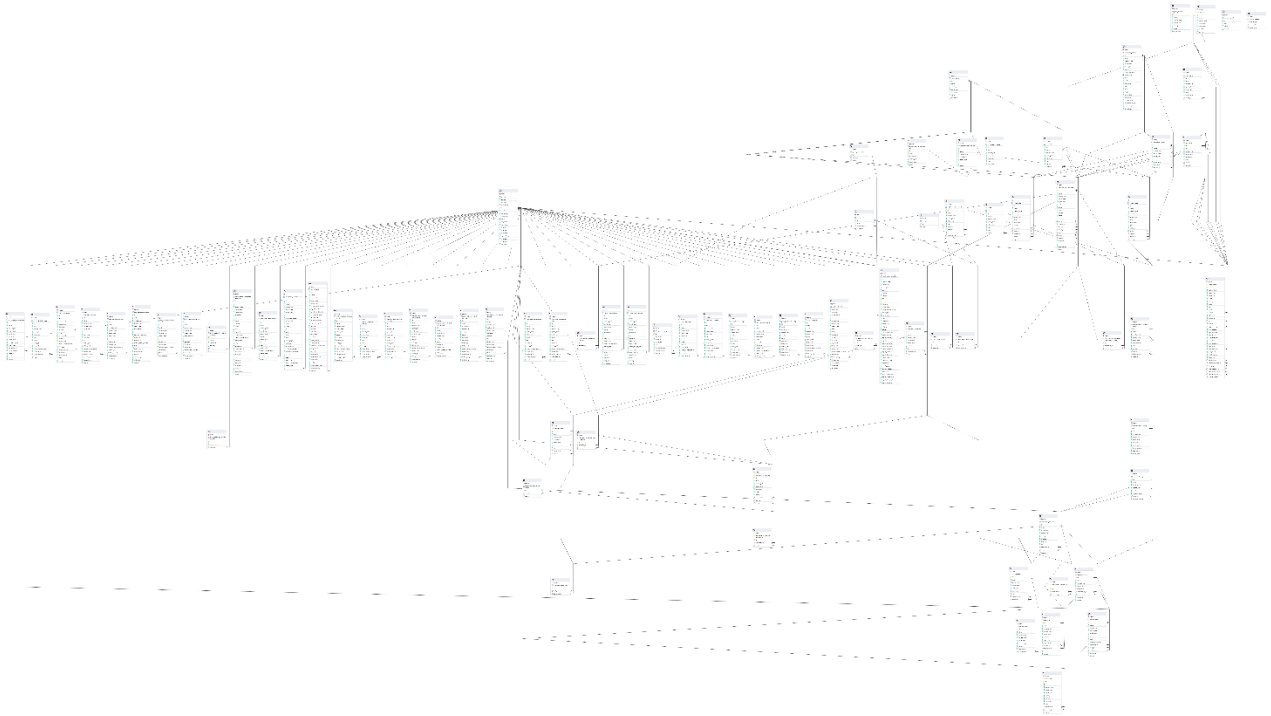
Elaboró	Revisó	Aprobó
Juan Buendía Pasante TIC **Ronny Rojas** Gerente TIC	**Marinela Camargo Torres** Gerente Integral & MC **Ludy Pérez Gutiérrez** Líder Jurídico	**María Fernanda Wilches** Gerente General

Descripción cambio Versión
Versión 01. Elaboración del Documento (06/02/2025)

Documento generado a partir de formatos registrado en el sistema de gestión interno de la Fundación Cataruben

6.7. Anexo 7 Diagrama de Bases de Datos pre-módulo de Beneficios Económicos

Figura 17 Diagrama de Bases de Datos de CQTX pre UBE



Fuente: Autor

6.8. Anexo 8 GTP-01 Procedimiento de Gestión de Roles, Privilegios y Acceso a la Información

1. OBJETIVO

Garantizar que la información, las áreas de procesamiento de información, las redes de datos, los recursos de las plataformas tecnológicas y los sistemas de información de la Fundación Cataruben se encuentren debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico y físico.

Específicos

● Implementar un sistema de seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.

● Implementar un sistema que impida el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.

● Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas de información.

● Garantizar la seguridad, confidencialidad, integridad y disponibilidad de los datos.

● Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de claves, equipos de cómputo e información.

● Cumplir con estándares internacionales de seguridad como ISO 27001.

2. ALCANCE

El presente documento tiene aplicabilidad a todas las formas de acceso, físico y lógico de todos los trabajadores, contratistas o terceros a quienes se les haya otorgado permisos sobre los sistemas de información, bases de datos, documentación, programas o servicios de información, sin importar la función que desempeñe en la Fundación.

3. DOCUMENTOS ASOCIADOS

● Matriz de Usuarios

● Formulario Solicitud de Soporte y Aplicaciones

● Acta de entrega de elementos y equipos

4. ABREVIATURAS

● ISO (Organismo de Estandarización de Internacional)

- PHVA (Planear, Hacer, Verificar, Actuar)
- CSI (Comité Seguridad de la Información)
- TIC (Tecnologías de información y Comunicación)

5. DEFINICIONES

Activo: Cualquier cosa que tenga valor para la organización.

Activos de Información: Es todo aquello que contiene, procesa, trata y/o manipula información valiosa para la fundación y que son necesarios para que la fundación funcione y cumpla con los objetivos establecidos para dicho fin.

Acceso: En relación con la seguridad de la información se refiere a la identificación, autenticación y autorización de un usuario a los sistemas, recursos y áreas de la Fundación Cataruben en un momento dado.

Acceso físico: Significa ingresar a las áreas de misión crítica o instalaciones en general de un sitio de la fundación.

Acceso lógico: En general, el acceso lógico es un acceso electrónico o digital, por ejemplo: acceder a archivos, navegar en el servidor, enviar un correo electrónico o transferir archivos.

Clasificación de la Información: Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la fundación. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuada.

Propietario de la Información: Es una parte designada de la fundación, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información sea clasificada adecuadamente y mantenga una clasificación acorde con su nivel de confidencialidad.

Estimación del riesgo: Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

Identificación del riesgo: Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

Impacto: Cambio adverso en el nivel de los objetivos del negocio logrados.

Incidente: Cualquier evento que no forma parte de una operación normal de un servicio y que causa o puede causar una interrupción o reducción de la calidad del

servicio.

Principio de mínimo privilegio: Solo se asignan los accesos necesarios para cada usuario.

Segregación de funciones: Se evitará que un usuario tenga permisos incompatibles que comprometan la seguridad.

6. RESPONSABILIDADES

6.1. Responsabilidades de la seguridad de la información

A. Área TIC

Supervisar y garantizar la implementación, mejora continua y alineación de la estrategia de seguridad de la información con los objetivos de la Fundación Cataruben. El área TIC garantiza el funcionamiento, cumplimiento normativo y la continuidad operativa ante amenazas tecnológicas. Adicionalmente cumple con las siguientes responsabilidades:

- Asegurar que la seguridad de los datos sea parte integral de la planificación de la información.
- Establecer procesos administrativos para fortalecer la aplicación de políticas de seguridad.
- Identificar y analizar riesgos en los activos de información para implementar controles mitigantes.
- Evaluar solicitudes que puedan afectar la seguridad de la información y pronunciarse sobre modificaciones en procedimientos operativos que impliquen riesgos.
- Evaluar y aprobar los mecanismos de seguridad física en las oficinas y áreas de acceso.
- Administrar y asegurar el acceso a nivel de red, hardware, software y bases de datos.
- Clasificar y asignar adecuadamente el almacenamiento de información, garantizando su confidencialidad, integridad y disponibilidad.
- Supervisar el adecuado manejo de copias de seguridad de acuerdo con las políticas de la fundación.
- Implementar controles y actualizaciones de seguridad en los sistemas de información.

● Desarrollar procedimientos de autorización y autenticación.
● Monitorear el cumplimiento de los procedimientos de resguardo de información en diferentes medios de almacenamiento.
● Liderar para que se garantice la disponibilidad de los servicios claves de la fundación.
● Liderar y gestionar con el fin de garantizar la disponibilidad de la infraestructura tecnológica.
● Liderar aplicar los controles, con el fin que se ejecuten los desarrollos, actualizaciones y los mantenimientos a la plataforma tecnológica.
● Liderar la implementación de políticas que garanticen la ciberseguridad.
● Liderar la transformación digital de la organización
● Realizar un plan de compras adecuado a las políticas y necesidades de la fundación.
● Gestionar el cumplimiento de contratos, seguimiento de los ANS y su compromisos con proveedores.

B. Propietario de la información

Los propietarios de los activos de información deben seguir las normas de control de acceso y la asignación de privilegios sobre está, de acuerdo con las normas establecidas en este procedimiento y el análisis de riesgos. Así mismo, son los responsables de:

● Identificar toda la información que corresponda a su área de responsabilidad cualquiera que sea su forma y medio de conservación.
● Clasificar todos los datos de su propiedad de acuerdo con el grado de criticidad de éstos y mantener un registro actualizado de la información más sensible.
● Autorizar el acceso sobre sus activos de información a colaboradores, contratistas o terceros de la fundación, de acuerdo con sus respectivas funciones.
● Aprobar y solicitar la asignación de privilegios sobre la información a los diferentes usuarios, ya sea en situaciones rutinarias como excepcionales.

C. Usuarios

Los trabajadores, contratistas y terceros que hacen uso de los activos de información de la Fundación Cataruben son responsables de las acciones que, realizadas sobre los mismos, así como de las credenciales de acceso que le son asignadas para su uso.

La cooperación de los usuarios es esencial para la eficacia de la seguridad de la información, por lo tanto, es necesario concientizar a los mismos acerca de sus responsabilidades por el uso y ejecución de controles de acceso eficaces, en particular aquellos relacionados con el uso de credenciales, la seguridad de los equipos de cómputo y la información.

No es permitido compartir sus cuentas de usuario, contraseñas y/o factores de autenticación asignados para el ingreso a los servicios de red y sistemas de información con otros trabajadores o terceros.

Los usuarios que posean acceso a los activos de información de la Fundación Cataruben deben acogerse a las normas y mejores prácticas establecidas para la configuración de contraseñas asignadas por la fundación.

Todos los escritorios físicos y digitales deben permanecer despejados con el fin de reducir los riesgos de acceso no autorizado, pérdida o daño de la información durante la jornada laboral o fuera de ella.

Cuando un trabajador requiera retirar un equipo de cómputo de las instalaciones de la fundación, debe diligenciar el Formulario Solicitud de Soporte y Aplicaciones y esperar que se notifique la aprobación de la solicitud. Adicionalmente, el trabajador se hace responsable de cualquier daño, pérdida o alteración del mismo.

D. Comité de Seguridad de la Información

Su propósito es supervisar y garantizar la implementación, mejora continua y alineación de la estrategia de seguridad de la información con los objetivos de la Fundación Cataruben.

El Comité supervisa una gestión efectiva de los riesgos, el cumplimiento normativo y la continuidad operativa ante amenazas tecnológicas. El CSI tendrá las siguientes funciones:

- Definir y supervisar la estrategia de seguridad de la información.
- Aprobar y actualizar las políticas de seguridad y cumplimiento normativo.
- Evaluar riesgos estratégicos y definir planes de mitigación.
- Supervisar la asignación de recursos en seguridad de la información.
- Revisar auditorías internas y externas, formulando planes de mejora.
- Garantizar la aplicación del ciclo PHVA (Planear, Hacer, Verificar, Actuar).
- Definir medidas disciplinarias en caso de incumplimiento de políticas de seguridad.

● Supervisar la correcta gestión de incidentes de seguridad y respuesta ante crisis.
● Promover programas de capacitación y concienciación en seguridad informática.
● Evaluar la seguridad en relaciones con terceros y proveedores.
● Hacer el seguimiento y evaluación de los reportes.
● Clasificación de la Información: Identificar y clasificar la información por áreas según su uso, considerando perfiles, roles y privilegios de acceso de los usuarios.
● Definir las competencias y seleccionar las auditorías internas de ISO 27001

7. DESCRIPCIÓN DEL PROCEDIMIENTO

Tabla 11. Tabla de Descripción del Procedimiento de Gestión de Roles, Privilegios y Acceso a la Información

No.	Actividad	Responsable	Información documentada	Puntos de Control
1	Ingreso del trabajador, entrega de equipo, acceso a redes y servicios: Una vez ingrese el trabajador se entrega el equipo de cómputo asignado con el acceso a las redes y la información necesaria para el desempeño de su cargo en Fundación Cataruben.	Área TIC	Acta de entrega de elementos y equipos	El acta de entrega de los equipos se almacena en Monday.com / El acceso a redes se registra Plataforma de gestión de red / Las credenciales de usuario se controlan desde Google Workspace
2	Gestión y cancelación de usuarios: Cuando se requiera un cambio de cuenta el área TIC registra o actualiza los usuarios en la Matriz de Usuarios especificando y asociando el rol a desempeñar. La creación de un nuevo usuario solo será realizada después de la solicitud mediante el Formulario de	Área TIC / Líder inmediato del área	Matriz Usuarios Formulario de Soporte y Aplicaciones	El líder inmediato solicita al área TIC la gestión de accesos. Las credenciales de usuario se controlan desde Google Workspace.

No.	Actividad	Responsable	Información documentada	Puntos de Control
	Soporte y Aplicaciones y bajo la aprobación explícita del responsable del área.			
3	Gestión de privilegios y roles: Cuando el usuario requiera accesos privilegiados a un sistema, proceso o servicio, el propietario es el encargado de aprobar la asignación de privilegios a los usuarios en caso de no ser posible la gestión con el propietario debe acudir al área TIC.	Usuario Propietarios de la Información Área TIC	Formulario Soporte y Aplicaciones Matriz Usuarios	El usuario solicita los accesos Google Workspace
4	Gestión de claves de ingreso a las cuentas Mensualmente los sistemas de acceso a la información cierran la sesión para que el usuario cambie su contraseña, esta será conocida únicamente por el usuario; en caso de olvido el área TIC le ayudará con la recuperación de cuenta.	Usuarios / Área TIC	Registro en plataforma de información.	Este registro es archivado por el área TIC.
5	Restricciones de acceso a la información y monitoreo del sistema: El área TIC o un miembro delegado por el Comité de Seguridad de la Información mensualmente verifica los permisos y privilegios de acceso a la información a fin de mantener	Área TIC / Miembro del CSI	Matriz Usuarios, Registro en plataforma de información.	Los logs de modificaciones se encuentran disponibles dentro de cada plataforma de información.

No.	Actividad	Responsable	Información documentada	Puntos de Control
	un control eficaz del acceso a los datos y servicios. En caso de encontrar accesos o privilegios por fuera de las funciones del cargo serán eliminados inmediatamente.			

Fuente: Autor

8. INFORMACIÓN ADICIONAL DEL PROCEDIMIENTO

Elevación de privilegios por líderes de proceso

En los casos donde un líder de proceso autorice la elevación de privilegios para un usuario bajo su responsabilidad, esta decisión deberá ser comunicada formalmente al área de TIC, incluyendo la justificación documentada de la necesidad. La información deberá ser registrada como parte del control de cambios en los accesos y servirá como base para el seguimiento, auditoría y monitoreo por parte del equipo de TIC. Esta práctica asegura la trazabilidad y evita privilegios innecesarios o no controlados.

- Identificador Único por Usuario: Todo usuario creado en los sistemas de información deberá contar con un identificador único, que permita su trazabilidad, autenticación individual y asociación inequívoca con las actividades realizadas dentro del sistema.
- Validación de Existencia de Usuarios: Todo proceso de creación o modificación de cuentas deberá incluir una validación previa de la existencia del usuario, basada en registros internos oficiales (contratos, directorios autorizados o fuentes verificables). No se permitirán cuentas asociadas a identidades no confirmadas. Por tanto, toda solicitud debe ser enviada por el área de antropológica.
- Gestión de Factores de Autenticación: La creación, modificación, adición o eliminación de factores de autenticación deberá ser autorizada previamente por el líder del proceso correspondiente, quien asumirá la responsabilidad de validar la necesidad y el cumplimiento de los controles de seguridad aplicables.
- Límites de Intentos de Autenticación: Los sistemas deberán implementar un control de intentos de autenticación fallidos, permitiendo un número máximo definido (10)

antes de aplicar un bloqueo temporal automático de la cuenta o sesión, conforme a los parámetros de seguridad definidos por el área de TIC.

Gestión de Cuentas y Privilegios

- Cuentas con Privilegios Elevados: Las cuentas con privilegios administrativos o elevados deberán estar protegidas mediante mecanismos reforzados de autenticación, incluyendo obligatoriamente la autenticación multifactor (MFA). Se deberá utilizar herramientas de gestión de privilegios que permitan registrar y auditar el uso de estas cuentas.
- Creación de Cuentas con Privilegios: La creación de cuentas con privilegios deberá estar justificada documentalmente, aprobada por el Comité de Seguridad de la Información y registrada en el sistema de auditoría centralizado. Estas cuentas estarán sujetas a revisión periódica y controles adicionales de seguridad.
- Revisión de Privilegios para Ascensos o Transferencias: Cuando un usuario sea promovido o transferido a otra área, deberán revisarse sus privilegios actuales y, en caso necesario, revocarse los accesos previos y asignar nuevos con base en las funciones del nuevo rol. La reasignación debe quedar documentada y ejecutarse en coordinación con Antropológica.
- Revisión Periódica de Privilegios: El sistema deberá implementar revisiones automáticas y periódicas (al menos cada mes) de los privilegios asignados, con alertas en caso de permisos excesivos o inactivos. Los privilegios que no se justifiquen por uso reciente o función asignada deberán ser removidos automáticamente.
- Baja de Cuentas por Terminación de Relación Laboral: Las cuentas deberán ser desactivadas, eliminadas o transferidas al líder de proceso de forma inmediata una vez se confirme la desvinculación del trabajador. La responsabilidad recae en el área de antropológica en coordinación con TIC, y debe documentarse en el sistema central de registro.

Accesos Externos y Excepcionales

- Cuentas para Terceros o Externos: Las cuentas destinadas a compartir información con terceros o personas externas a la fundación implementarán controles adicionales de seguridad. Estos incluirán mecanismos de monitoreo activo y

restricciones estrictas en los permisos de lectura, edición, creación y eliminación de información, en función del principio de mínimo privilegio.

- Accesos Temporales: Cualquier acceso especial concedido con duración limitada deberá tener definida una fecha de caducidad desde su creación, así como una revocación automática al final del período. Este tipo de accesos será evaluado y aprobado previamente por el área TIC.

Control de Sesiones y Auditoría

- Sesiones Efímeras: Todos los sistemas sobre los cuales la Fundación Cataruben tenga control directo deberán implementar sesiones efímeras (de duración limitada y con cierre automático) para reducir los riesgos de exposición de la información y proteger su confidencialidad e integridad.
- Prohibición de Cuentas Compartidas: El uso de cuentas compartidas entre varios usuarios está terminantemente prohibido. Solo se contemplarán excepciones justificadas en casos específicos de tecnologías que así lo requieran o cuando, tras un análisis, se determine que dicha práctica constituye la solución más eficiente desde el punto de vista económico. Estas excepciones deberán documentarse y contar con aprobación explícita por parte del Comité de Seguridad de la Información.
- Centralización de Registros de Actualización: Toda modificación, alta o baja de cuentas de usuario y privilegios deberá quedar registrada en un sistema de registro centralizado. Esto incluye cambios en factores de autenticación, roles asignados y accesos concedidos o revocados. Los registros deben estar disponibles para revisión por el área TIC.

Control del Documento

Elaboró	Revisó	Aprobó
Juan Buendía Gestor de Ciberseguridad	**Marinela Camargo** G. Mejora Continua	**María Fernanda Wilches** Gerente General

Descripción cambio Versión
Versión 01. Elaboración del Documento (20/02/2025)

Versión 02. Actualización del Documento, Sección de Información Adicional del Procedimiento (21/04/2025)

Documento generado a partir de formatos registrado en el sistema de gestión interno de la Fundación Cataruben

6.9. Anexo 9 FC-GTP-02 Procedimiento de Gestión de Parches y Actualizaciones

1. OBJETIVO

Establecer el procedimiento para la identificación, priorización, planificación, aplicación y validación de parches en los sistemas, aplicaciones y dispositivos tecnológicos de la organización, con el propósito de minimizar los riesgos de seguridad y asegurar la continuidad operativa.

2. ALCANCE

Este procedimiento aplica a todos los activos de información que requieran algún tipo de parche o actualización por parte de la fundación Cataruben.

3. DOCUMENTOS ASOCIADOS

- GTF-06 Parches y Actualizaciones

4. ABREVIATURAS

- CVE: Common Vulnerabilities and Exposures/ Vulnerabilidades y exposiciones comunes
- CVSS: Common Vulnerability Scoring System/ Sistema de puntaje de vulnerabilidades comunes
- TI: Tecnologías de la información
- CSI: Comité de Seguridad de la Información

5. DEFINICIONES

Activo Crítico: Sistema o recurso cuya no disponibilidad o falla puede afectar significativamente la continuidad operativa o la seguridad de la organización.
Activo de Información: Cualquier dato, sistema, aplicación o servicio que tenga valor para la organización y que requiera protección.
Activo Físico: Dispositivos tangibles que permiten el almacenamiento, procesamiento o transmisión de información, como servidores, estaciones de trabajo, routers y dispositivos móviles.
Actualización: Conjunto de cambios o mejoras aplicadas a un sistema o aplicación

para mejorar su seguridad, funcionalidad o rendimiento.

Entorno de Pruebas (Staging): Sistema o plataforma diseñada para probar cambios antes de su implementación en producción, con el fin de minimizar riesgos.

Mitigación Temporal: Medida de seguridad alternativa que se implementa cuando no es posible aplicar un parche de manera inmediata para reducir el riesgo asociado.

Parche: Actualización de software diseñada para corregir vulnerabilidades, errores o mejorar la funcionalidad de un sistema o aplicación.

Riesgo: Posibilidad de que una amenaza explote una vulnerabilidad, causando daños o impactos negativos sobre los activos de información.

Rollback: Proceso para revertir una actualización aplicada y restaurar la versión anterior para garantizar la estabilidad del sistema.

Vulnerabilidad: Debilidad o falla en un sistema de información que puede ser explotada para comprometer la confidencialidad, integridad o disponibilidad de los activos de información.

6. RESPONSABILIDADES

Autoridad de Gestión de Parches (Gerente TIC): Define los lineamientos generales y supervisa el cumplimiento del procedimiento.

Ejecutores de Parches (Área TIC): Ejecuta actualizaciones, realiza pruebas e informa sobre el estado de los parches.

Supervisión (Gerente TIC): Evalúa la efectividad del proceso y verifica el cumplimiento de las directrices establecidas.

7. DESCRIPCIÓN DEL PROCEDIMIENTO

Tabla 12. Tabla de Descripción del Procedimiento de Gestión de Parches y Actualizaciones

No.	Actividad	Responsable	Información documentada	Puntos de Control
1	Identificación de parches y actualizaciones Identificar parches disponibles en bases de datos de vulnerabilidades y notificaciones de proveedores.	Área TIC	GTF-06 Parches y Actualizaciones	Revisión de bases de datos de vulnerabilidades
2	Priorización de vulnerabilidades Evaluar la criticidad de los parches	Autoridad de Gestión de Parches	GTF-06 Parches y Actualizaciones Análisis de criticidad usando CVSS	La evaluación se realiza semanalmente y la aplicación es de acuerdo a la tabla 2.

No.	Actividad	Responsable	Información documentada	Puntos de Control
	para asignar una prioridad con base en el impacto y probabilidad de explotación. Nota: El tiempo de aplicación de acuerdo a la criticidad se define en la tabla 2.			
3	Planificación de la aplicación Definir la estrategia, horarios y recursos necesarios para la implementación del parche de acuerdo al activo afectado.	Área TIC	GTF-06 Parches y Actualizaciones	Programación de ventanas de actualización en registro
4	Preparación para la aplicación Realizar respaldos de los sistemas afectados y pruebas en entornos aislados de ser necesario para verificar la compatibilidad del parche.	Área TIC	GTF-06 Parches y Actualizaciones	Validación en entorno de pruebas y diligenciamiento de registro
5	Aplicación del parche Ejecutar la implementación del parche utilizando herramientas automatizadas o procesos manuales según corresponda.	Área TIC	GTF-06 Parches y Actualizaciones	Monitoreo en registros de plataforma y registro en panel
6	Verificación y Monitoreo Confirmar la correcta aplicación mediante revisión de logs y pruebas funcionales.	Área TIC	GTF-06 Parches y Actualizaciones	Columna de resultados en el panel del Registro de parches y actualizaciones El estado de aplicación de las salientes se actualiza automáticamente, en el

No.	Actividad	Responsable	Información documentada	Puntos de Control
				caso de los entrantes, es actualizado por el personal del área TIC.
7	Gestión de Excepciones Documentar y gestionar las excepciones para parches que no puedan aplicarse, incluyendo medidas de mitigación temporal.	Gerente TIC	GTF-06 Parches y Actualizaciones	Diligenciamiento en la columna de Excepciones y Mitigación del panel de Registro de parches y actualizaciones

Fuente: Autor

8. INFORMACIÓN ADICIONAL DEL PROCEDIMIENTO

Para evaluar la efectividad de la gestión de parches, se establecen los siguientes indicadores de desempeño:

● Porcentaje de parches críticos aplicados dentro del tiempo establecido: Permite medir el cumplimiento de los plazos definidos para la aplicación de parches críticos.

● Tiempo promedio de aplicación para parche: Mide el tiempo transcurrido entre la identificación del parche y su aplicación.

● Número de excepciones documentadas: Indica la cantidad de parches que no pudieron aplicarse dentro del tiempo establecido, con su respectiva justificación y medidas de mitigación.

● Porcentaje de parches validados antes de la aplicación: Permite verificar la aplicación de pruebas previas a la implementación en producción.

● Cantidad de reversión de parches (Rollback): Mide los casos donde fue necesario revertir la actualización debido a fallos o incompatibilidades.

Bimestralmente se hará seguimiento a los indicadores por el Responsable de Gestión de Parches y se implementarán los planes de acción necesarios conforme a los resultados de las auditorías o las necesidades de la organización.

8.1 Parches y actualizaciones automáticas

No todas las actualizaciones y parches estarán sujetos al proceso de registro en la tabla

de Registro de Parches y Actualizaciones. Aquellas actualizaciones que sean aplicadas de manera automática por el proveedor sin intervención del Área TIC por ejemplo, actualizaciones de navegadores o software con mecanismos de autoactualización estarán exentas de este registro.

Tabla 2: Periodos de actualización

Tabla 13. Tabla de Periodos de Actualización Procedimiento de Gestión de Parches y Actualizaciones

Tipo de Parche	**Descripción**	**Tiempo de Aplicación**
Crítico	Vulnerabilidades de alto riesgo con posibilidad de explotación inmediata.	12 a 24 horas después de detección.
Importante	Mejoras significativas en funcionalidad o seguridad.	3 a 5 días
Correctivo	Definir plan de implementación y contingencia	6 a 14 días
Menor	Corrección de errores reportados por usuarios.	20 días

Fuente: Autor

Documento generado a partir de formatos registrado en el sistema de gestión interno de la Fundación Cataruben

6.10. Anexo 10 GTP-03 Procedimiento de monitoreo automatizado de servidores y aplicaciones

1. OBJETIVO

Garantizar la continuidad del negocio, mediante la supervisión continua y eficaz de la infraestructura tecnológica de la Fundación Cataruben mediante la implementación de un sistema de monitoreo automatizado con Grafana.

Específicos:

● Detectar y alertar sobre fallos en los sistemas y servicios críticos.

● Proveer visibilidad en tiempo real sobre el estado de la infraestructura y aplicaciones.

● Facilitar el análisis de rendimiento y la identificación de cuellos de botella.

● Apoyar la toma de decisiones basada en datos para garantizar la continuidad operativa.
● Documentar y mantener un historial de métricas y eventos relevantes.

2. ALCANCE

Aplica a todos los servidores, servicios, bases de datos, redes y aplicaciones gestionadas por el área TIC de la Fundación Cataruben, abarcando tanto los sistemas internos utilizados exclusivamente por el personal, como aquellos servicios expuestos públicamente y accesibles por terceros.
Incluye la infraestructura física y virtual, contemplando entornos locales (on-premise) y servicios en la nube que soporten las operaciones de la Fundación. El sistema de monitoreo cubre recursos críticos como servidores de aplicaciones, bases de datos, balanceadores de carga, firewalls, contenedores y cualquier otro componente que afecte la continuidad del servicio o la experiencia del usuario final.

3. DOCUMENTOS ASOCIADOS

- Instructivo de configuración de Grafana y Stack OTEL - LGTM
- FC- GTF-06 Parches y Actualizaciones

4. ABREVIATURAS

- API: Application Programming Interface — Interfaz que permite la comunicación entre diferentes aplicaciones.
- CPU: Unidad Central de Procesamiento
- HTTP: Hypertext Transfer Protocol — Protocolo para la transferencia de información en la web.
- LGTM: Loki, Grafana, Tempo, Mimir — Stack de observabilidad que combina logs (Loki), visualización (Grafana), trazas (Tempo) y métricas (Prometheus).
- OTEL: OpenTelemetry — Framework para la recolección de datos de telemetría (logs, métricas, trazas).
- RAM: Memoria de Acceso Aleatorio
- TIC: Tecnologías de la Información y Comunicaciones.

5. DEFINICIONES

Alerta: Notificación automática que indica que una métrica ha superado un umbral definido.
Balanceador de carga: Dispositivo o servicio que distribuye el tráfico entrante entre varios servidores para mejorar la disponibilidad y el rendimiento.
Base de datos: Sistema organizado que almacena y gestiona grandes volúmenes de información, permitiendo la consulta y modificación eficiente de los datos.
Contenedor: Unidad de software ligera y portable que incluye todo lo necesario para ejecutar una aplicación (código, bibliotecas, configuraciones), funcionando de forma aislada del sistema anfitrión.
CPU: Es el cerebro de la computadora o servidor. Se encarga de ejecutar las instrucciones de los programas, realizar cálculos y coordinar las operaciones del sistema.
Dashboard: Tablero visual que representa gráficamente las métricas en Grafana.
Experiencia del usuario final: Calidad y eficiencia con la que los usuarios internos o externos interactúan con los sistemas, influenciada por factores como velocidad de respuesta, disponibilidad y estabilidad.
Firewall: Sistema que controla y filtra el tráfico de red según reglas de seguridad, protegiendo la infraestructura contra accesos no autorizados.
Grafana: Plataforma de código abierto para visualizar datos y crear paneles interactivos de monitoreo.
Infraestructura física: Equipos tangibles como servidores, switches, routers y dispositivos de almacenamiento que forman parte de la red y los sistemas de la organización.
Infraestructura virtual: Recursos de cómputo creados mediante software, máquinas virtuales, contenedores, redes virtuales que funcionan sobre hardware físico, optimizando el uso de los servidores.
Latencia: Tiempo que tarda un dato en viajar de un punto a otro en el sistema; por ejemplo, desde que el usuario hace clic hasta que recibe una respuesta. Se mide en milisegundos (ms).
Log: Registro cronológico de eventos que ocurren en un sistema, útil para depuración y auditoría.
Loki: Sistema de almacenamiento de logs optimizado para trabajar con Grafana.

Métrica: Valor numérico que refleja el estado o el rendimiento de una parte del sistema (ejemplo: uso de CPU, memoria, latencia).
Memoria: Espacio temporal donde se almacenan los datos y programas que la CPU está usando activamente. Cuanta más memoria libre haya, más rápido puede trabajar el sistema. El uso de memoria (%) mide qué parte de la memoria total está ocupada.
Observabilidad: Capacidad de medir el estado interno de un sistema complejo a partir de sus salidas (logs, métricas, trazas).
On-premise: Infraestructura de TI alojada físicamente en las instalaciones de la organización, gestionada directamente por el área TIC.
Prometheus: Plataforma de monitoreo que recopila métricas de sistemas y aplicaciones mediante extracción periódica de datos.
Promtail: Agente que recoge logs de servidores y los envía a Loki para su almacenamiento y análisis.
Servicios en la nube: Recursos tecnológicos servidores, almacenamiento, bases de datos, redes, software proporcionados y administrados por terceros a través de Internet.
Servidor de aplicaciones: Sistema que ejecuta software para gestionar las solicitudes de los usuarios y conectar con bases de datos u otros servicios.
Stack: Conjunto de herramientas, tecnologías y servicios que funcionan juntos para lograr una tarea específica; en este caso, la observabilidad y monitoreo.
Traces: Datos que muestran el recorrido de una petición a través de varios servicios dentro de un sistema distribuido.
Umbral: Valor límite que, al ser alcanzado o superado, desencadena una alerta o acción para prevenir o mitigar fallos.

6. RESPONSABILIDADES

6.1 Área TIC

- Implementar y mantener el sistema de monitoreo con Grafana.
- Analizar los datos recolectados
- Garantizar la disponibilidad de los dashboards clave.
- Capacitar a los usuarios clave en la interpretación de los datos.
- Verificar la operación y el correcto funcionamiento dentro de los umbrales establecidos de los servidores y aplicaciones de la Fundación Cataruben.

● Ajustar configuraciones, capacidad, y prioridad de recursos según sea necesario.

6.2 Gerente TIC

● Definir rangos de operación aceptables y umbrales de alerta.

● Supervisar el cumplimiento del procedimiento.

● Garantizar que la información recolectada sea usada únicamente para fines operativos y de mejora continua.

7. DESCRIPCIÓN DEL PROCEDIMIENTO

Tabla 14. Tabla de Descripción del Procedimiento de monitoreo automatizado de servidores y aplicaciones

No.	Actividad	Responsable	Información documentada	Puntos de Control
1	Configuración inicial de Grafana y Promtail Instalación y configuración básica de Grafana como plataforma de visualización y Promtail como agente recolector de logs. Se asegura la conectividad entre los componentes y se verifica el acceso a la interfaz web.	Área TIC	Instructivo de configuración de Grafana y stack OTEL - LGTM	https://monitor.app.cataruben.org/
2	Definición de métricas y umbrales críticos Identificación de las métricas clave a monitorear (CPU, memoria, latencia, disponibilidad, etc.) y establecimiento de los umbrales que disparan alertas en caso de superar los valores normales.	Área TIC	Instructivo de configuración de Grafana y stack OTEL - LGTM	https://monitor.app.cataruben.org/

No.	Actividad	Responsable	Información documentada	Puntos de Control
3	Creación de dashboards personalizados Diseño de tableros visuales adaptados a las necesidades de la Fundación, permitiendo una vista clara y rápida del estado de los sistemas y la infraestructura.	Área TIC		https://monitor.app.cataruben.org/
4	Implementación de alertas automáticas Configuración de reglas de alerta basadas en los umbrales definidos. Se establecen los destinatarios (Gerente TIC y área TIC) para garantizar una reacción oportuna.	Área TIC	monitor.app.cataruben.org/ Correos de área TIC	Reaccionar a las alertas y coordinar acciones inmediatas ante incidentes.
5	Revisión periódica de métricas y alertas Evaluación diaria del rendimiento del sistema y revisión de las alertas registradas. Se busca identificar patrones de fallos y prevenir incidentes recurrentes.	Área TIC	FC-GTF-XX Registro de Parches y Actualizaciones	Diligenciamiento de panel de registro
6	Ajustes según análisis de rendimiento Aplicación de mejoras y ajustes en la configuración de métricas, umbrales y	Responsable de Seguridad de la Información, Área TIC (QA)	FC-GTF-XX Registro de Parches y Actualizaciones	Diligenciamiento de panel de registro

No.	Actividad	Responsable	Información documentada	Puntos de Control
	dashboards según los datos históricos recopilados y el análisis de rendimiento.			

Fuente: Autor

8. INFORMACIÓN ADICIONAL DEL PROCEDIMIENTO

Cuando se sobrepasa el umbral de operación aceptable se generan alertas las cuales deben ser revisadas inmediatamente por el personal del área TIC.

Los sistemas con fallos reiterados deben ser escalados al Gerente TIC para revisión y elaboración de un plan de acción.

Control del Documento

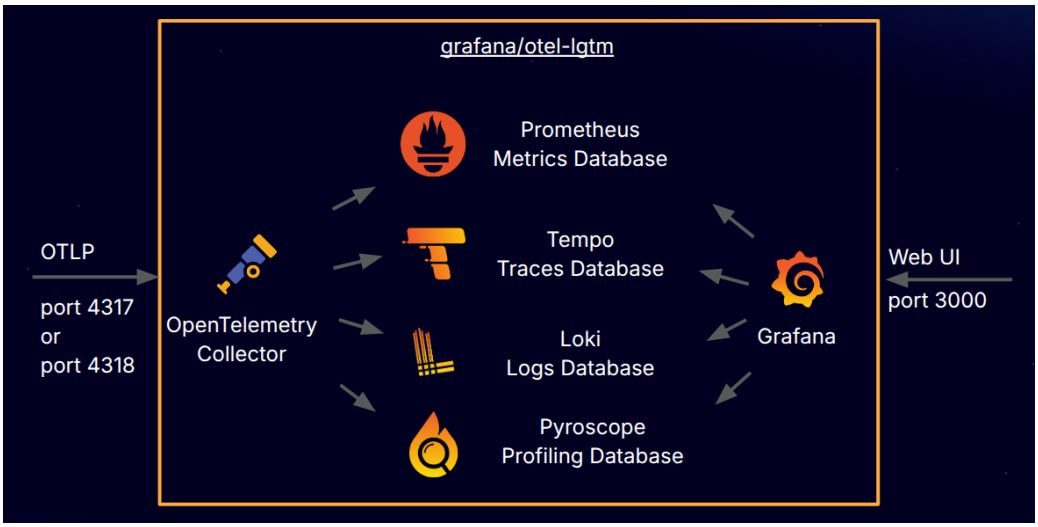
Elaboró	Revisó	Aprobó
Juan Buendía Pasante TIC	**Marinela Camargo** G. Mejora Continua	**María Fernanda Wilches** Gerente General

Descripción cambio Versión
Versión 01. Elaboración del Documento (12/03/2025)

Documento generado a partir de formatos registrado en el sistema de gestión interno de la Fundación Cataruben

6.11. Anexo 11 Stack de Grafana

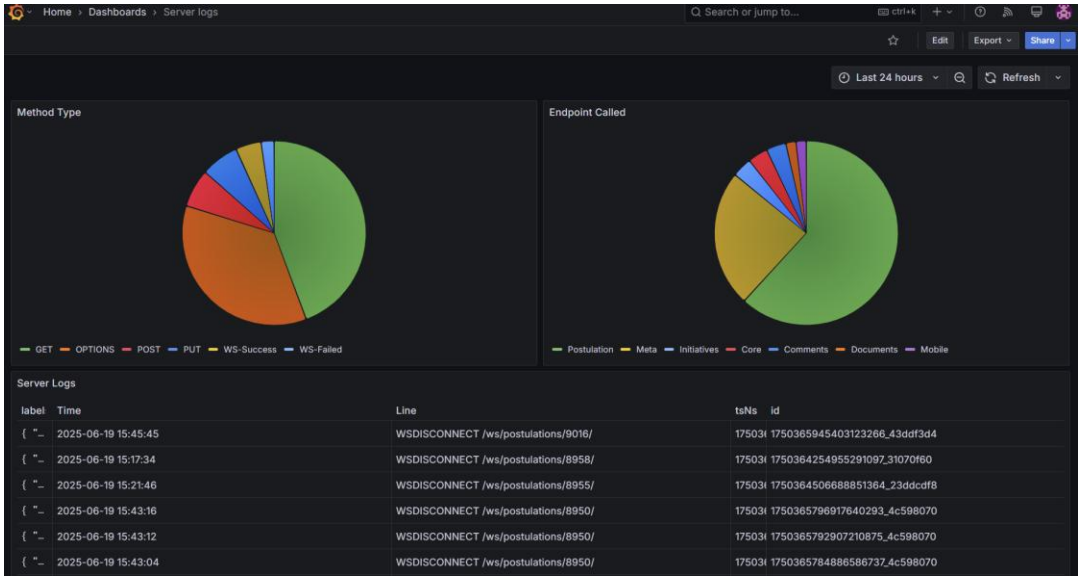
Figura 18 Stack OTEL - LGTM



Fuente: Grafana on Github

6.12. Anexo 12 Ejemplo de logs en Grafana

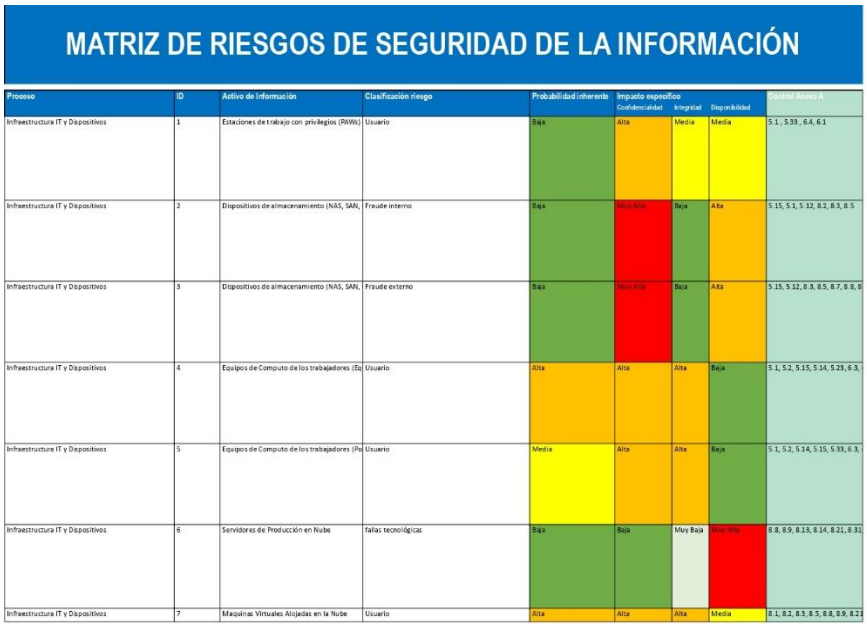
Figura 19 Logs en de CQTX en Grafana



Fuente: Autor

6.13. Anexo 13 Matriz de Riesgos de Seguridad de la Información

Figura 20 Matriz de Seguridad de la Información 1

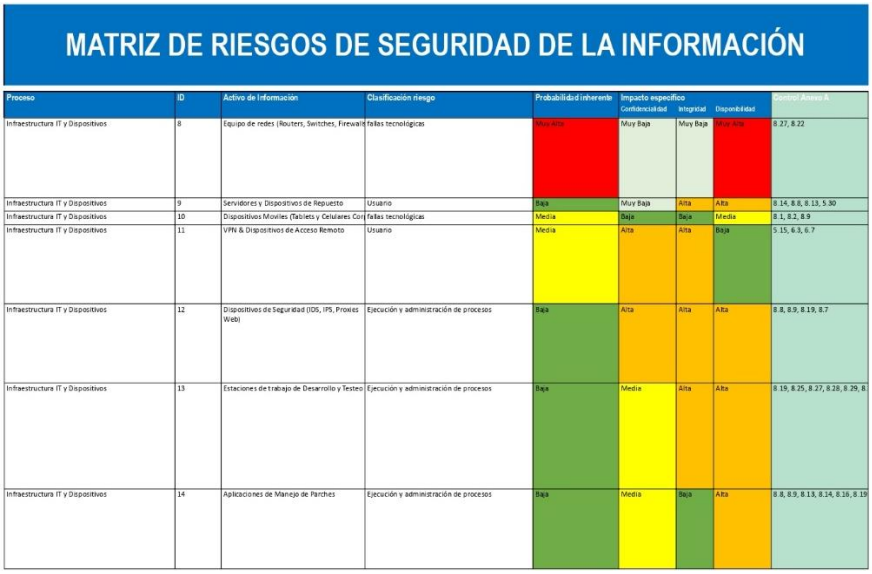


MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Proceso	ID	Activo de Información	Clasificación riesgo	Probabilidad inherente	Impacto específico			Control Anexo A
					Confidencialidad	Integridad	Disponibilidad	
Infraestructura IT y Dispositivos	1	Estaciones de trabajo con privilegios (PAWs)	Usuario	Baja	Alta	Media	Media	5.1 , 5.33 , 6.4, 6.1
Infraestructura IT y Dispositivos	2	Dispositivos de almacenamiento (NAS, SAN,	Fraude interno	Baja	Muy Alta	Baja	Alta	5.15, 5.1, 5.12, 8.2, 8.3, 8.5
Infraestructura IT y Dispositivos	3	Dispositivos de almacenamiento (NAS, SAN,	Fraude externo	Baja	Muy Alta	Baja	Alta	5.15, 5.12, 8.3, 8.5, 8.7, 8.8, 8
Infraestructura IT y Dispositivos	4	Equipos de Computo de los trabajadores (Eq	Usuario	Alta	Alta	Alta	Baja	5.1, 5.2, 5.15, 5.14, 5.23, 6.3,
Infraestructura IT y Dispositivos	5	Equipos de Computo de los trabajadores (Po	Usuario	Media	Alta	Alta	Baja	5.1, 5.2, 5.14, 5.15, 5.33, 6.3,
Infraestructura IT y Dispositivos	6	Servidores de Producción en Nube	fallas tecnológicas	Baja	Baja	Muy Baja	Muy Alta	8.8, 8.9, 8.13, 8.14, 8.21, 8.31
Infraestructura IT y Dispositivos	7	Maquinas Virtuales Alojadas en la Nube	Usuario	Alta	Alta	Alta	Media	8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.2

Fuente: Autor

Figura 21 Matriz de Seguridad de la Información 2



MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Proceso	ID	Activo de Información	Clasificación riesgo	Probabilidad inherente	Impacto específico			Control Anexo A
					Confidencialidad	Integridad	Disponibilidad	
Infraestructura IT y Dispositivos	8	Equipo de redes (Routers, Switches, Firewalls	fallas tecnológicas	Muy Alta	Muy Baja	Muy Baja	Muy Alta	8.27, 8.22
Infraestructura IT y Dispositivos	9	Servidores y Dispositivos de Repuesto	Usuario	Baja	Muy Baja	Alta	Alta	8.14, 8.8, 8.13, 5.30
Infraestructura IT y Dispositivos	10	Dispositivos Moviles (Tablets y Celulares Cor	fallas tecnológicas	Media	Baja	Baja	Media	8.1, 8.2, 8.9
Infraestructura IT y Dispositivos	11	VPN & Dispositivos de Acceso Remoto	Usuario	Media	Alta	Alta	Baja	5.15, 6.3, 6.7
Infraestructura IT y Dispositivos	12	Dispositivos de Seguridad (IDS, IPS, Proxies Web)	Ejecución y administración de procesos	Baja	Alta	Alta	Alta	8.8, 8.9, 8.19, 8.7
Infraestructura IT y Dispositivos	13	Estaciones de trabajo de Desarrollo y Testeo	Ejecución y administración de procesos	Baja	Media	Alta	Alta	8.19, 8.25, 8.27, 8.28, 8.29, 8
Infraestructura IT y Dispositivos	14	Aplicaciones de Manejo de Parches	Ejecución y administración de procesos	Baja	Media	Baja	Alta	8.8, 8.9, 8.13, 8.14, 8.16, 8.19

Fuente: Autor

Figura 22 Matriz de Seguridad de la Información 3

MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Proceso	ID	Activo de Información	Clasificación riesgo	Probabilidad inherente	Impacto específico			Control Anexo A
					Confidencialidad	Integridad	Disponibilidad	
Infraestructura IT y Dispositivos	15	Equipo de Sala de Conferencias (Sistema de	fallas tecnológicas	Muy Baja	Baja	Baja	Media	7.5, 7.8, 7.13
Infraestructura IT y Dispositivos	16	Fuentes de Poder Ininterrumpibles (UPS) y B	fallas tecnológicas	Baja	Muy Baja	Baja	Media	7.12, 7.13, 7.14
Infraestructura IT y Dispositivos	17	Sistemas en desuso y Hardware Antiguo	Ejecución y administración de procesos	Baja	Alta	Baja	Baja	7.10, 7.14
Infraestructura IT y Dispositivos	18	Dispositivos de Almacenamiento Externo (US	Ejecución y administración de procesos	Baja	Alta	Muy Baja	Muy Baja	7.14
Activos de Información	19	Base de datos de propietarios	Fraude externo	Baja	Alta	Alta	Media	8.4, 8.8, 8.9, 8.11, 8.12
Activos de Información	20	Base de datos de propietarios	Fraude externo	Baja	Muy Alta	Media	Baja	8.3, 8.5, 8.12, 8.13, 8.15
Activos de Información	21	Base de datos de propietarios	Ejecución y administración de procesos	Baja	Alta	Alta	Baja	8.9, 8.15, 8.25, 8.26
Activos de Información	22	Base de datos de propietarios	Usuario	Media	Baja	Alta	Muy Baja	5.15, 5.18, 6.4, 8.2, 8.9
Activos de Información	23	Base de datos de clientes	Fraude interno	Baja	Alta	Alta	Muy Baja	5.15, 5.18, 6.4, 8.2, 8.9
Activos de Información	24	Repositorios de código fuente	Ejecución y administración de procesos	Baja	Baja	Alta	Alta	8.2, 8.3, 8.4, 8.9
Activos de Información	25	Registros financieros	Fraude externo	Media	Alta	Alta	Baja	8.4, 8.8, 8.9, 8.11, 8.12
Activos de Información	26	Contratos y acuerdos legales	Ejecución y administración de procesos	Media	Muy Alta	Media	Baja	8.4, 8.8, 8.9, 8.11, 8.12
Activos de Información	27	Habeas Data y Documentación de Cumplimie	Ejecución y administración de procesos	Baja	Alta	Baja	Baja	5.1, 5.2, 5.5, 6.1, 6.2, 6.3
Activos de Información	28	Llaves de encriptación y Certificados	Ejecución y administración de procesos	Media	Alta	Media	Alta	8.24, 8.25, 8.26, 8.27, 8.28
Activos de Información	29	Sistema de Correo Corporativo	Usuario	Media	Alta	Alta	Alta	5.1, 5.10, 5.18, 6.3, 8.12, 8.16
Activos de Información	30	Sistema de Mensajería Instantanea Corporat	Usuario	Alta	Alta	Baja	Baja	5.1, 5.2, 6.3
Activos de Información	31	Documentos de estrategia de negocio	Usuario	Media	Muy Alta	Baja	Baja	5.10, 5.12, 5.13, 5.14, 5.15, 6.
Activos de Información	32	Matriz de Riesgos	Usuario	Baja	Muy Alta	Baja	Baja	5.10, 5.12, 5.13, 5.14, 5.15, 6.
Activos de Información	33	Propiedad Intelectual (Patentes, Marcas Reg	fallas tecnológicas	Media	Media	Media	Alta	5.15, 5.16, 5.17, 8.9, 8.13, 8.1
Activos de Información	34	Configuración de Sistemas IT	Ejecución y administración de procesos	Baja	Alta	Alta	Alta	5.2, 8.8, 8.9, 8.19, 8.32
Activos de Información	35	Incidentes y Registros de Auditoria	Ejecución y administración de procesos	Media	Media	Alta	Media	5.33, 8.13, 8.14, 8.15
Activos de Información	36	Datos del Sistema del CRM	Ejecución y administración de procesos	Muy Alta	Baja	Muy Alta	Baja	5.10, 5.35, 6.3, 8.9, 8.16
Activos de Información	37	Procedimientos de Operación y Políticas	Ejecución y administración de procesos	Baja	Baja	Alta	Media	5.15, 5.18, 8.8, 8.9
Activos de Información	38	Diseños de proyectos y prototipos	Relaciones Laborales	Media	Muy Alta	Media	Media	5.2, 5.10, 5.12, 5.13, 5.14, 5.1
Activos de Información	39	Datos de Marketing y Ventas	Relaciones Laborales	Media	Media	Baja	Baja	5.2, 5.12, 5.13, 5.14, 5.15
Activos de Información	40	Registros de Soporte al Cliente	Ejecución y administración de procesos	Alta	Baja	Alta	Media	5.12, 5.13, 5.15, 8.32
Activos de Información	41	Registros de los trabajadores	Ejecución y administración de procesos	Alta	Baja	Alta	Media	5.12, 5.13, 5.15, 8.32
Activos de Información	42	Minutas y Notas de reuniones Confidenciales	Ejecución y administración de procesos	Media	Baja	Alta	Baja	5.12, 5.13, 5.15, 8.32
Activos de Información	43	Planes de Recuperación de desastres y Copia	Ejecución y administración de procesos	Alta	Baja	Baja	Muy Alta	5.29, 5.30, 5.36, 5.37, 8.13
Trabajadores y Roles	44	CISO / Lider de Seguridad (Personal Ciberseg	Ejecución y administración de procesos	Media	Alta	Alta	Alta	5.2, 5.3, 5.30, 6.2, 8.2, 8.27
Trabajadores y Roles	45	Administradores de Sistema	Ejecución y administración de procesos	Baja	Alta	Alta	Alta	5.2, 5.3, 5.30, 6.2, 8.2, 8.27
Trabajadores y Roles	46	Ingenieros y Desarrolladores	Ejecución y administración de procesos	Baja	Baja	Alta	Baja	5.3, 5.10, 5.15, 6.2, 6.3, 8.2, 8

Fuente: Autor

Figura 23 Matriz de Seguridad de la Información 4

MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Proceso	ID	Activo de Información	Clasificación riesgo	Probabilidad inherente	Impacto específico			Control Anexo A
					Confidencialidad	Integridad	Disponibilidad	
Trabajadores y Roles	47	Usuarios Privilegiados (Root, Superuser, Adm	Ejecución y administración de procesos	Media	Alta	Baja	Baja	5.3, 5.10, 5.15, 6.2, 6.3, 8.2, 8
Trabajadores y Roles	48	Oficiales de Cumplimiento y Riesgos	Ejecución y administración de procesos	Baja	Baja	Alta	Baja	5.15, 5.19, 5.21, 6.2, 6.3, 8.3,
Trabajadores y Roles	49	Equipo de Finanzas y Contabilidad	Ejecución y administración de procesos	Media	Baja	Alta	Media	5.3, 5.8, 5.10, 5.15, 5.18, 6.2,
Trabajadores y Roles	50	Gestores Legales y Contractuales	Ejecución y administración de procesos	Baja	Baja	Alta	Alta	5.12, 8.9, 8.13, 8.19, 8.2, 8.32
Trabajadores y Roles	51	Recursos Humanos y Manejo de Personal	Relaciones Laborales	Media	Alta	Baja	Baja	5.2, 5.10, 5.12, 5.13, 5.14, 6.2
Trabajadores y Roles	52	Oficial de Protección de Datos	Ejecución y administración de procesos	Baja	Alta	Alta	Alta	5.2, 5.3, 5.30, 6.2, 8.2, 8.27
Trabajadores y Roles	53	Administrados y Adquisiciones y Abastecimie	Fraude externo	Media	Alta	Alta	Baja	5.2, 5.15, 6.3, 8.5, 8.8, 8.9
Trabajadores y Roles	54	Personal de Fidelización	Ejecución y administración de procesos	Media	Alta	Baja	Baja	5.1, 5.10, 5.12,5.13, 5.14, 5.15
Trabajadores y Roles	55	Equipo de Ventas y Marketing	Ejecución y administración de procesos	Media	Alta	Baja	Baja	5.12, 5.13, 5.14, 6.3, 6.6, 8.3
Trabajadores y Roles	56	Seguridad de las Instalaciones	Ejecución y administración de procesos	Baja	Baja	Media	Baja	7.5, 7.6, 7.13, 8.1
Trabajadores y Roles	57	Personal OPS y Consultores	Ejecución y administración de procesos	Media	Media	Baja	Baja	5.1, 5.10, 5.12, 5.13, 5.14, 5.1
Trabajadores y Roles	58	Ejecutivos y Miembros de la Junta Directiva	Ejecución y administración de procesos	Media	Alta	Alta	Baja	5.10, 5.12, 5.15, 5.1, 6.3, 6.5
Instalaciones e Infraestructura Física	59	Oficinas y Espacios de Trabajo	Daño de activos	Baja	Baja	Baja	Media	7.4, 7.5
Instalaciones e Infraestructura Física	60	Centros de Datos y Espacio de Servidores	Ejecución y administración de procesos	Baja	Baja	Baja	Alta	8.13
Instalaciones e Infraestructura Física	61	Sistemas de Control de Acceso	fallas tecnológicas	Media	Baja	Baja	Baja	7.1, 7.4, 7.13
Instalaciones e Infraestructura Física	62	Sistemas de Vigilancia (CCTV, motion sensors	Daño de activos	Baja	Baja	Baja	Baja	7.1, 7.3, 7.5, 7.6
Instalaciones e Infraestructura Física	63	Sistema de Alarma de Seguridad	fallas tecnológicas	Muy Baja	Baja	Baja	Alta	7.3, 7.5, 7.6, 7.8, 7.13
Instalaciones e Infraestructura Física	64	Archivo Físico	Daño de activos	Muy Baja	Muy Baja	Muy Baja	Muy Baja	7.3, 7.5, 7.6, 7.8, 7.13
Instalaciones e Infraestructura Física	65	Maquinas de Trabajo y Salas de Juntas	Ejecución y administración de procesos	Baja	Baja	Baja	Media	6.2, 6.3, 7.3, 7.5, 7.6, 7.8, 7.13
Instalaciones e Infraestructura Física	66	Backup Power Systems (UPS, generators)	fallas tecnológicas	Muy Baja	Baja	Baja	Alta	7.3, 7.5, 7.6, 7.8, 7.13
Instalaciones e Infraestructura Física	67	Aireas Acondicionados y Controles Ambienta	fallas tecnológicas	Baja	Muy Baja	Muy Baja	Muy Baja	7.3, 7.5, 7.6, 7.8, 7.13
Instalaciones e Infraestructura Física	68	Cableado de Redes y Conectividad Física	Ejecución y administración de procesos	Baja	Baja	Alta	Media	7.3, 7.5, 7.6, 7.8, 7.13
Instalaciones e Infraestructura Física	69	Cajoneras de los trabajadores	Fraude interno	Muy Baja	Alta	Media	Media	7.3, 7.5, 7.6, 7.8
Instalaciones e Infraestructura Física	70	Equipo de oficinas remotas y trabajo en casa	fallas tecnológicas	Media	Media	Media	Baja	6.7, 7.3, 7.5, 7.6, 7.8, 7.13, 8.1
Instalaciones e Infraestructura Física	71	Branding Físico	Ejecución y administración de procesos	Baja	Baja	Media	Baja	7.3, 7.5, 7.6, 7.8
Instalaciones e Infraestructura Física	72	Garajes y Espacio de Estacionamiento	Daño de activos	Muy Baja	Muy Baja	Muy Baja	Media	7.3, 7.5, 7.6, 7.8
Instalaciones e Infraestructura Física	73	Sistema de Manejo de Visitantes	Ejecución y administración de procesos	Baja	Baja	Baja	Media	7.3, 7.5, 7.6, 7.8
Instalaciones e Infraestructura Física	75	Recepción	Ejecución y administración de procesos	Baja	Baja	Baja	Media	5.9, 5.30, 7.5, 7.13
Terceras Partes y Relaciones de Proveedores	76	Proveedores de Servicios en la Nube (AWS, A	Ejecución y administración de procesos	Baja	Alta	Baja	Alta	5.19, 5.20, 5.22, 5.23, 8.9
Terceras Partes y Relaciones de Proveedores	77	Proveedores de Software como Servicio (Saa	Ejecución y administración de procesos	Baja	Alta	Baja	Alta	5.19, 5.20, 5.22, 5.23, 8.9
Terceras Partes y Relaciones de Proveedores	78	Procesadores de Pago Y Proveedores de Serv	Fraude externo	Media	Baja	Baja	Alta	5.12, 5.19, 5.20, 5.23, 8.12, 8.
Terceras Partes y Relaciones de Proveedores	79	Proveedores de Servicios y Manejo de Identi	Ejecución y administración de procesos	Baja	Baja	Media	Alta	5.19, 5.20, 5.22, 5.23, 8.9
Terceras Partes y Relaciones de Proveedores	80	Firmas de Auditoria y Cumplimiento	Relaciones Laborales	Baja	Alta	Alta	Baja	5.2, 5.3, 5.13, 5.15, 5.16, 8.15
Terceras Partes y Relaciones de Proveedores	81	Proveedores de pruebas de Seguridad	Ejecución y administración de procesos	Baja	Muy Alta	Baja	Baja	5.19, 5.20, 5.22, 6.6, 8.12, 8.2
Terceras Partes y Relaciones de Proveedores	82	Consultores Legales	Fraude interno	Media	Alta	Alta	Baja	5.15, 5.17, 5.18, 8.5, 8.15
Terceras Partes y Relaciones de Proveedores	83	Proveedores de Recursos Humanos y Manejo	Fraude interno	Media	Baja	Alta	Baja	5.15, 5.17, 5.18, 8.5, 8.15

Fuente: Autor

Figura 24 Matriz de Seguridad de la Información 5

MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Proceso	ID	Activo de Información	Clasificación riesgo	Probabilidad inherente	Impacto especifico			Control Anexo A
					Confidencialidad	Integridad	Disponibilidad	
Terceras Partes y Relaciones de Proveedores	84	Proveedores de Software Empresarial (ERP, s	Ejecución y administración de procesos	Baja	Baja	Baja	Muy Alta	5.19, 5.20, 5.22, 5.23, 8.9
Terceras Partes y Relaciones de Proveedores	85	Proveedores de Backup y Recuperación ante	Ejecución y administración de procesos	Muy Baja	Baja	Baja	Muy Alta	5.19, 5.20, 5.22, 5.23, 8.9, 8.1
Terceras Partes y Relaciones de Proveedores	86	Proveedores de Email y Servicios de Comuni	Ejecución y administración de procesos	Baja	Baja	Baja	Muy Alta	5.19, 5.20, 5.22, 8.9, 8.20, 8.2
Terceras Partes y Relaciones de Proveedores	87	Plataformas de Marketing y Analitica	Ejecución y administración de procesos	Media	Media	Baja	Baja	5.13, 5.14, 5.15, 5.19, 5.20, 5
Terceras Partes y Relaciones de Proveedores	88	Proveedores de Viajes y Eventos	Ejecución y administración de procesos	Baja	Media	Alta	Baja	5.14, 5.19, 5.20, 5.22, 8.7
Terceras Partes y Relaciones de Proveedores	89	Proveedores de Logistica y Cadena de sumin	Ejecución y administración de procesos	Baja	Media	Baja	Baja	5.2, 5.19, 5.20, 5.22, 6.3
Terceras Partes y Relaciones de Proveedores	90	Personal de Servicios Generales	Usuario	Baja	Media	Media	Baja	5.15, 6.2, 6.3, 6.4, 8.7
Terceras Partes y Relaciones de Proveedores	91	Freelancers y Consultores Independientes	Relaciones Laborales	Media	Media	Alta	Baja	5.10, 5.12, 5.13, 5.14, 5.15, 5
Terceras Partes y Relaciones de Proveedores	92	Proveedores de Manejo, Generación y Firma	fallas tecnológicas	Media	Baja	Baja	Alta	5.18, 5.19, 5.20, 5.21
Terceras Partes y Relaciones de Proveedores	93	Proveedores de Capacitaciones y Aprendizaj	Fraude interno	Baja	Media	Baja	Muy Baja	5.15, 5.18, 5.19, 5.20, 5.22, 8
Propiedad Intelectual y Activos de Marca	94	Pantentes y Aplicaciones a Patentes	Relaciones Laborales	Baja	Muy Alta	Baja	Muy Baja	5.2, 5.3, 5.10, 5.15, 6.3, 8.2, 8
Propiedad Intelectual y Activos de Marca	95	Marcas Registradas y Nombres de Marca	Relaciones Laborales	Media	Media	Baja	Muy Baja	5.2, 5.3, 5.23, 8.3, 8.15
Propiedad Intelectual y Activos de Marca	96	Materiales con Copyrigth	Relaciones Laborales	Baja	Media	Muy Baja	Muy Baja	5.2, 5.14, 5.31, 5.32, 6.3, 8.2
Propiedad Intelectual y Activos de Marca	97	Software Propio y Código Fuente	Ejecución y administración de procesos	Media	Alta	Media	Media	5.3, 5.15, 5.16, 6.3, 8.2, 8.3, 8
Propiedad Intelectual y Activos de Marca	98	Metodologías Tecnicas	Relaciones Laborales	Media	Alta	Baja	Baja	5.3, 5.15, 5.16, 6.3, 8.9, 8.12
Propiedad Intelectual y Activos de Marca	99	Modelos de Datos y Algoritmos Confidencial	Ejecución y administración de procesos	Baja	Alta	Alta	Media	8.8, 8.9, 8.19, 8.25, 8.28, 8.30
Propiedad Intelectual y Activos de Marca	100	Secretos del Negocio y Conocimiento Interno	Ejecución y administración de procesos	Media	Muy Alta	Baja	Baja	5.2, 5.3, 6.2, 6.3, 6.5, 6.6
Propiedad Intelectual y Activos de Marca	101	Dominios de la Fundación y Activos Web	Ejecución y administración de procesos	Baja	Baja	Alta	Media	8.4, 8.8, 8.9, 8.13, 8.25, 8.26,
Propiedad Intelectual y Activos de Marca	102	Cuentas de Redes Sociales & Handles	Fraude interno	Media	Media	Alta	Media	5.10, 5.15, 5.16, 6.1, 6.2, 6.3,
Propiedad Intelectual y Activos de Marca	103	Lineamientos de Marca e Identidad Visual	Ejecución y administración de procesos	Baja	Baja	Media	Baja	5.2, 5.3, 5.5, 5.9, 5.10, 5.11, 5
Propiedad Intelectual y Activos de Marca	104	Activos de Marketing y Anuncios	Relaciones Laborales	Media	Media	Baja	Baja	5.2, 5.3, 5.5, 5.9, 5.10, 5.11, 5
Propiedad Intelectual y Activos de Marca	105	Nombres de Iniciativas y Oferta de servicios	Ejecución y administración de procesos	Baja	Baja	Media	Baja	5.3, 5.10, 5.12, 5.16, 6.3, 8.15
Propiedad Intelectual y Activos de Marca	106	Acuerdos de Licencia y Contratos de Propied	Ejecución y administración de procesos	Media	Alta	Baja	Alta	5.5, 5.6, 5.10, 5.12, 5.14, 8.10
Propiedad Intelectual y Activos de Marca	107	Alianzas y Acuerdos de Branding conjunto	Ejecución y administración de procesos	Media	Alta	Baja	Media	5.5, 5.6, 5.10, 5.12, 5.14, 8.10
Propiedad Intelectual y Activos de Marca	108	Acuerdos de Uso de Proveedores y Clientes	Ejecución y administración de procesos	Baja	Baja	Alta	Baja	5.12, 8.19, 5.20, 5.22, 8.10, 8
Propiedad Intelectual y Activos de Marca	109	Activos de Marca y Marketing Archivados	Ejecución y administración de procesos	Baja	Media	Baja	Baja	8.9, 8.10, 8.11, 8.13, 8.15
Propiedad Intelectual y Activos de Marca	110	Dotación y Mercancia con branding	Ejecución y administración de procesos	Media	Baja	Baja	Baja	5.2, 5.9, 5.10, 5.12, 6.3, 6.6
Propiedad Intelectual y Activos de Marca	111	Plantillas Web y Elementos de Diseño	Ejecución y administración de procesos	Media	Media	Media	Media	8.4, 8.8, 8.9, 8.13, 8.25, 8.26,
Propiedad Intelectual y Activos de Marca	112	Presentaciones y Contenido creado por traba	Ejecución y administración de procesos	Alta	Alta	Alta	Media	5.10, 5.12, 5.13, 5.15, 5.16, 8
Propiedad Intelectual y Activos de Marca	113	Eventos y Materiales de Patrocinio	Ejecución y administración de procesos	Baja	Media	Baja	Baja	5.5, 5.6, 5.10, 5.12, 5.14, 8.10
Regulaciones y Activos de Cumplimiento	114	Politicas de Seguridad de la Información	Ejecución y administración de procesos	Baja	Baja	Media	Baja	5.1, 5.9, 5.15, 8.15, 8.16, 8.32
Regulaciones y Activos de Cumplimiento	115	Politicas de Protección de Datos y Privacidad	Ejecución y administración de procesos	Baja	Baja	Media	Baja	5.1, 5.9, 5.15, 8.15, 8.16, 8.32
Regulaciones y Activos de Cumplimiento	116	Politicas de Uso Aceptable	Ejecución y administración de procesos	Baja	Baja	Media	Baja	5.1, 5.9, 5.15, 8.15, 8.16, 8.32
Regulaciones y Activos de Cumplimiento	117	Politicas de Control de Acceso	Ejecución y administración de procesos	Baja	Baja	Media	Baja	5.1, 5.9, 5.15, 8.15, 8.16, 8.32
Regulaciones y Activos de Cumplimiento	118	Plan de Respuesta Ante Incidentes	Ejecución y administración de procesos	Baja	Baja	Media	Baja	5.1, 5.9, 5.15, 8.15, 8.16, 8.32
Regulaciones y Activos de Cumplimiento	119	Planes de Continuidad del Negocio y Recupe	Ejecución y administración de procesos	Baja	Baja	Media	Baja	5.1, 5.9, 5.15, 8.15, 8.16, 8.32

Fuente: Autor

Figura 25 Matriz de Seguridad de la Información 6

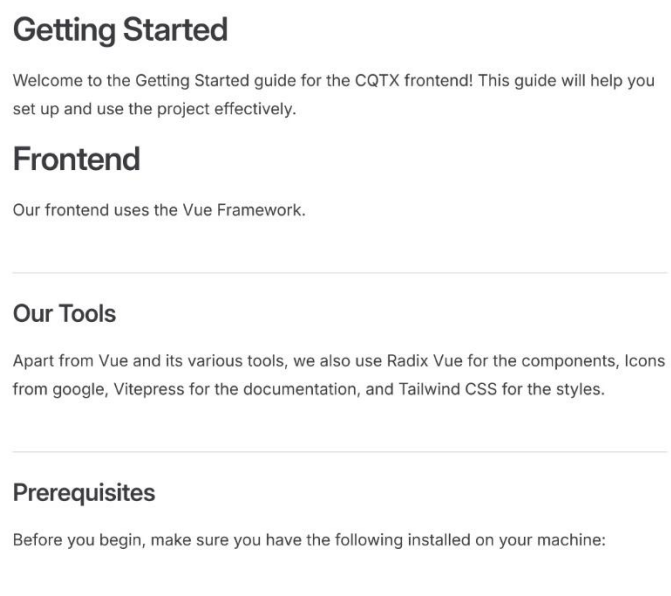
MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Proceso	ID	Activo de Información	Clasificación riesgo	Probabilidad inherente	Impacto especifico			Control Anexo A
					Confidencialidad	Integridad	Disponibilidad	
Regulaciones y Activos de Cumplimiento	120	Estrategia y Analisis de Manejo de Riesgos	Ejecución y administración de procesos	Baja	Baja	Alta	Baja	5.1, 5.9, 5.15, 8.15, 8.16, 8.32
Regulaciones y Activos de Cumplimiento	121	Registros de Auditoria y Reportes de Monito	Ejecución y administración de procesos	Baja	Baja	Alta	Baja	5.1, 5.9, 5.15, 8.15, 8.16, 8.32
Regulaciones y Activos de Cumplimiento	122	Certificaciones de Cumplimiento	Ejecución y administración de procesos	Baja	Baja	Alta	Media	5.1, 5.9, 5.15, 8.15, 8.16, 8.32
Regulaciones y Activos de Cumplimiento	123	Reporte de Riesgos de Proveedores y Debida	Ejecución y administración de procesos	Baja	Baja	Alta	Media	5.1, 5.9, 5.15, 8.15, 8.16, 8.32
Regulaciones y Activos de Cumplimiento	124	Reportes de Pruebas de Penetración y analis	Ejecución y administración de procesos	Baja	Baja	Alta	Baja	5.9, 5.10, 6.2, 6.3, 6.6, 8.15
Regulaciones y Activos de Cumplimiento	125	Declaraciones de Aplicabilidad	Ejecución y administración de procesos	Baja	Baja	Alta	Baja	5.1, 5.9, 5.15, 8.15, 8.16, 8.32
Regulaciones y Activos de Cumplimiento	126	Acuerdos de Procesamiento de Datos	Ejecución y administración de procesos	Baja	Alta	Alta	Media	5.9, 5.14, 5.19, 5.20, 5.22, 5.1
Regulaciones y Activos de Cumplimiento	127	Acuerdos de No Divulgación	Fraude interno	Baja	Baja	Muy Alta	Baja	5.2, 5.15, 6.2, 6.6, 8.15
Regulaciones y Activos de Cumplimiento	128	Security Awareness Training Records Registr	Relaciones Laborales	Baja	Baja	Baja	Baja	5.1, 5.2, 6.3, 8.3, 8.12
Regulaciones y Activos de Cumplimiento	129	Politicas de Encriptación	Relaciones Laborales	Media	Media	Media	Media	5.1, 5.9, 5.15, 8.15, 8.16, 8.32
Regulaciones y Activos de Cumplimiento	130	Pruebas de Cumplimiento de Terceras Partes	Ejecución y administración de procesos	Media	Media	Media	Baja	5.9, 5.10, 6.2, 6.3, 6.6, 8.15
Regulaciones y Activos de Cumplimiento	131	Politicas de Seguridad Fisica y Registro de Ac	Relaciones Laborales	Media	Baja	Baja	Baja	5.2, 7.3, 7.4, 8.16
Regulaciones y Activos de Cumplimiento	132	Registro de Acceso de Usuarios y Revisión de	Ejecución y administración de procesos	Media	Media	Media	Baja	5.1, 5.9, 5.15, 8.15, 8.16, 8.32
Regulaciones y Activos de Cumplimiento	133	Politicas de Retención de Datos	Ejecución y administración de procesos	Baja	Baja	Media	Media	5.1, 5.9, 5.15, 8.15, 8.16, 8.32

Fuente: Autor

6.14. Anexo 14. Documentación Getting started Frontend

Figura 26 Documentación en CQTX Frontend 1



Getting Started

Welcome to the Getting Started guide for the CQTX frontend! This guide will help you set up and use the project effectively.

Frontend

Our frontend uses the Vue Framework.

Our Tools

Apart from Vue and its various tools, we also use Radix Vue for the components, Icons from google, Vitepress for the documentation, and Tailwind CSS for the styles.

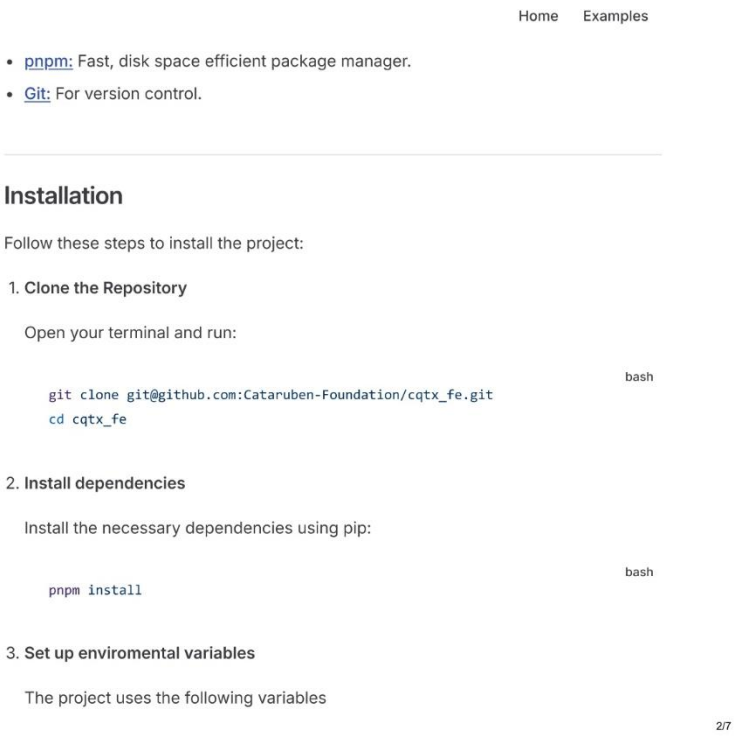
Prerequisites

Before you begin, make sure you have the following installed on your machine:

1/7

Fuente: Autor

Figura 27 Documentación en CQTX Frontend 2



Home Examples

- pnpm: Fast, disk space efficient package manager.
- Git: For version control.

Installation

Follow these steps to install the project:

1. **Clone the Repository**

   Open your terminal and run:

   bash

   ```
   git clone git@github.com:Cataruben-Foundation/cqtx_fe.git
   cd cqtx_fe
   ```

2. **Install dependencies**

   Install the necessary dependencies using pip:

   bash

   ```
   pnpm install
   ```

3. **Set up enviromental variables**

   The project uses the following variables

2/7

Fuente: Autor

Figura 28 Documentación en CQTX Frontend 3

```
VITE_APP_CHATBOT_URL= URL to chatbot api
VITE_APP_CHATBOT_API_KEY= Key to access chatbot service
VITE_DOCS_URL= URL to our internal documentation
```

File Structure

bash

```
.
├ docs
│  ├ .vitepress
│  └ api-examples.md
│  └ getting-started-back.md
│  └ getting-started-front.md
│  └ getting-started.md
│  └ index.md
│  └ logo_dark.webp
│  └ logo.webp
│  └ markdown-examples.md
├ docst
├ public
├ src
│  ├ assets
│  ├ components
│  │    ├ __test__
```

3/7

Fuente: Autor

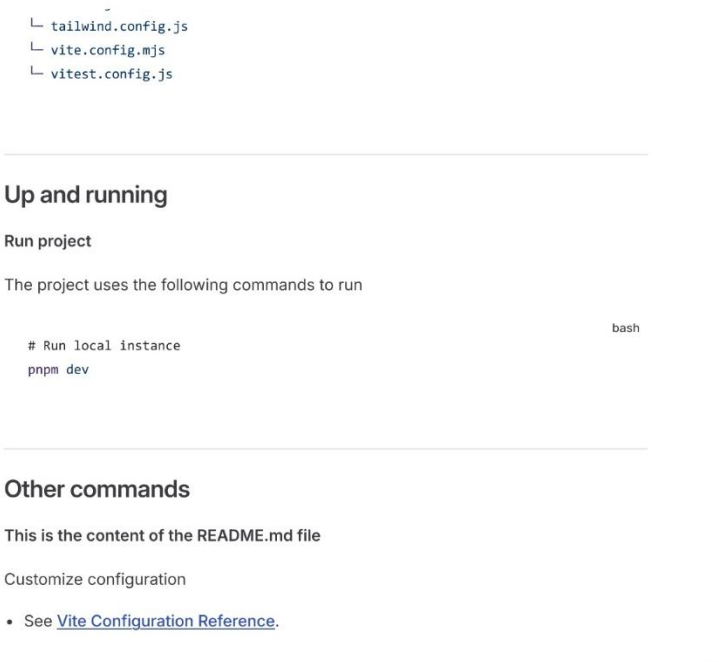
Figura 29 Documentación en CQTX Frontend 4

```
.  .    .
│  │    ├ navigation
│  │    ├ quality
│  │    ├ sections
│  │    ├ widgets
│  ├ plugins
│  │    └ axiosClient.js
│  │    └ createAxiosClient.js
│  │    └ services.js
│  ├ router
│  │    └ index.js
│  ├ stores
│  ├ utils
│  ├ views
│  └ App.vue
│  └ main.js
└ .buildpacks
└ .env
└ .eslint.cjs
└ .gitignore
└ .prettier.json
└ .static
└ .index.html
└ jsonconfig.json
└ LICENSE
└ package.json
└ pnpm-lock.yaml
└ postcss.config.js
```

4/7

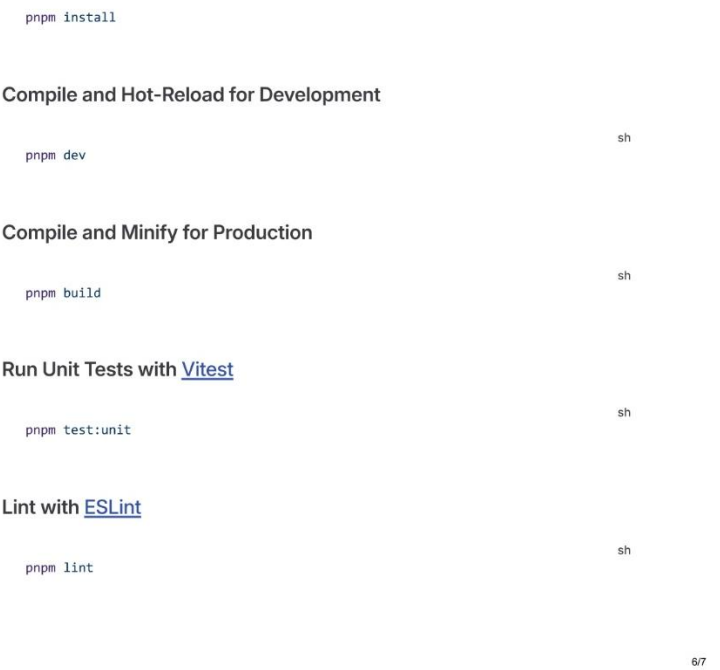
Fuente: Autor

Figura 30 Documentación en CQTX Frontend 5



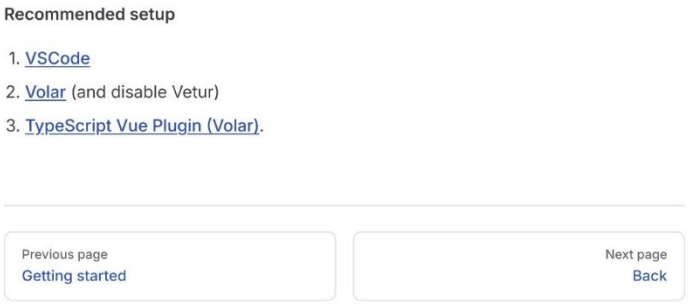
Fuente: Autor

Figura 31 Documentación en CQTX Frontend 6



Fuente: Autor

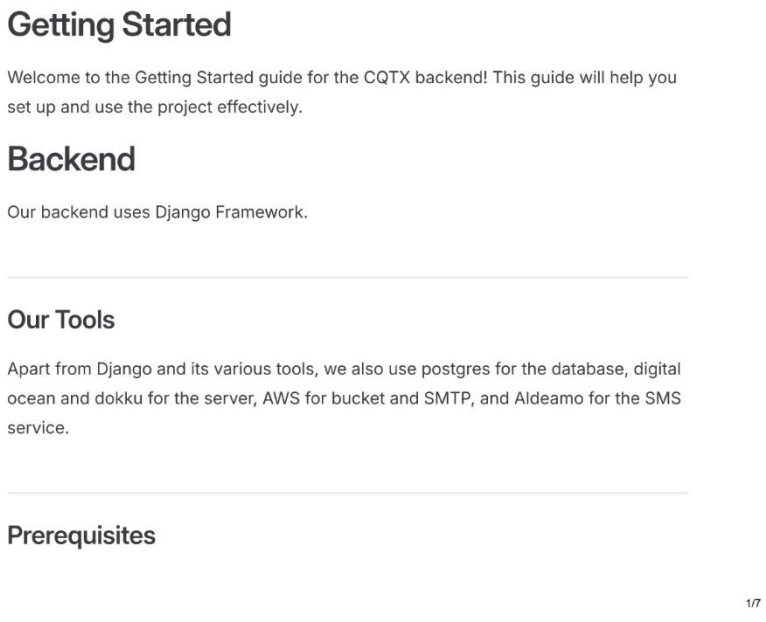
Figura 32 Documentación en CQTX Frontend 7



Fuente: Autor

6.15. Anexo 15. Documentación Getting started Backend

Figura 33 Documentación en CQTX Backend 1



Fuente: Autor

Figura 34 Documentación en CQTX Backend 2

- **pip**: Python package installer, it comes included in the python install.
- Git: For version control.

Installation

Follow these steps to install the project:

1. **Clone the Repository**

   Open your terminal and run:

```bash
git clone git@github.com:Cataruben-Foundation/cqtx_be.git
cd cqtx_be
```

2. **Create a Virtual Environment**

It's a internal practice to use a virtual environment for Python projects. You can create one using the following commands:

```bash
# Install virtualenv if you haven't already
pip install virtualenv
```

2/7

Fuente: Autor

Figura 34 Documentación en CQTX Backend 3

```
# Activate the virtual environment
# On Windows
venv\Scripts\activate
# On macOS/Linux
source venv/bin/activate
```

3. **Install dependencies**

   Install the necessary dependencies using pip:

```bash
pip install -r requirements.txt
```

4. **Set up enviromental variables**

   The project uses the following variables

```bash
ANDROID_VERSION= Version of android SDK
AWS_ACCESS_KEY_ID= Name of acces key
AWS_S3_REGION_NAME= Closest region
AWS_SECRET_ACCESS_KEY= Secret key to acces AWS services
AWS_STORAGE_BUCKET_NAME= Name of AWS bucket
CORS_ALLOWED_ORIGINS= Policy of CORS access
CSRF_TRUSTED_ORIGINS= Policy of trust
POSTGRES_NAME= Database name
POSTGRES_USER= User of database
```

3/7

Fuente: Autor

Figura 35 Documentación en CQTX Backend 4

```
DJANGO_ALLOWED_HOSTS= Acces policy
DJANGO_DEBUG= Debug state
DJANGO_SECRET_KEY= Private key
EMAIL_BACKEND= Provider for email service
EMAIL_HOST= Host of email service
EMAIL_HOST_PASSWORD= Password of email host
EMAIL_HOST_USER= User of email host
EMAIL_PORT= Port that the email uses
EMAIL_USE_TLS= Policy
IOS_VERSION= Version of IOS SDK
NO_VHOST= Number of vhost
ODK_EMAIL= User of another email
ODK_PASSWORD= Password of said another email
ODK_URL= URL of ODK
SETTINGS_MODULE= Dividir between development stages
SMS_API_URL= URL of API for SMS provider
SMS_PASSWORD= Password of said service
SMS_USERNAME= User of SMS service
USE_S3= State of use of Amazon S3
```

File Structure

4/7

Fuente: Autor

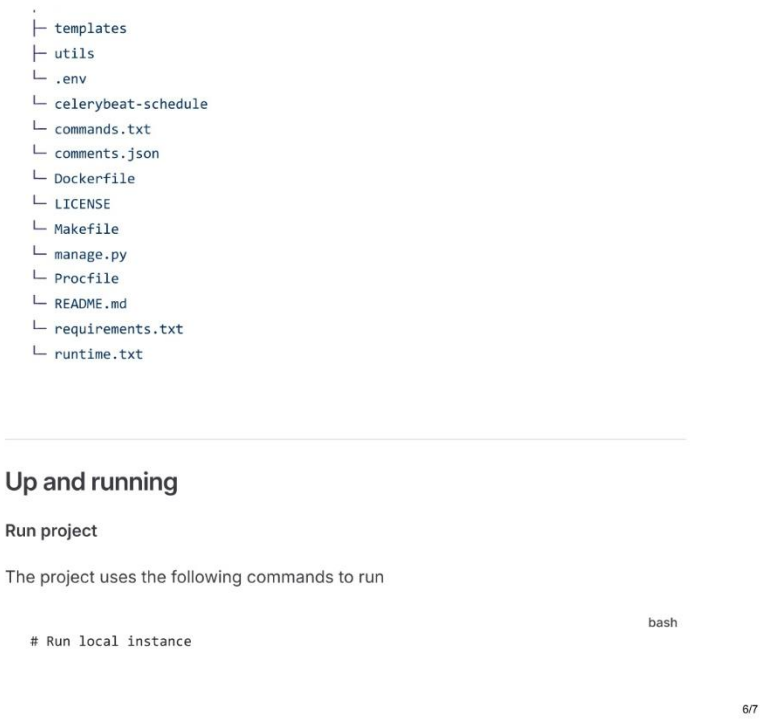
Figura 36 Documentación en CQTX Backend 5

```
| ├─ __pycache__
| ├─ _auth_
| |  ├─ __pycache__
| |  ├─ migrations
| |  ├─ utils
| |  |  └─ __innit.py__
| |  |  └─ admin.py
| |  |  └─ apps.py
| |  |  └─ managers.py
| |  |  └─ models.py
| |  |  └─ serializers.py
| |  |  └─ signals.py
| |  |  └─ test.py
| |  |  └─ urls.py
| |  |  └─ views.py
| ├─ _core
| ├─ _email
| ├─ _fqa
| ├─ _meta
| ├─ _sms
| ├─ comments
| ├─ documents
| ├─ implementation
| ├─ ims
| ├─ innitiatives
| ├─ mobile
| ├─ postulations
```

5/7

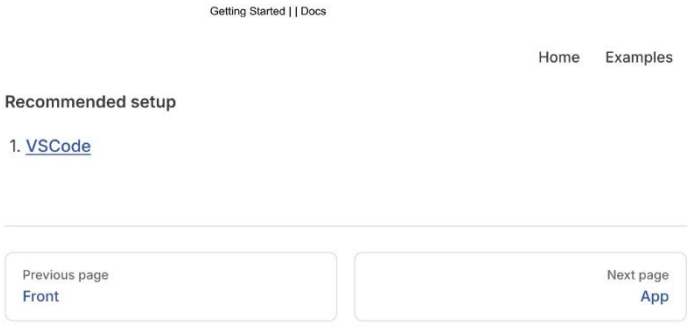
Fuente: Autor

Figura 37 Documentación en CQTX Backend 6



Fuente: Autor

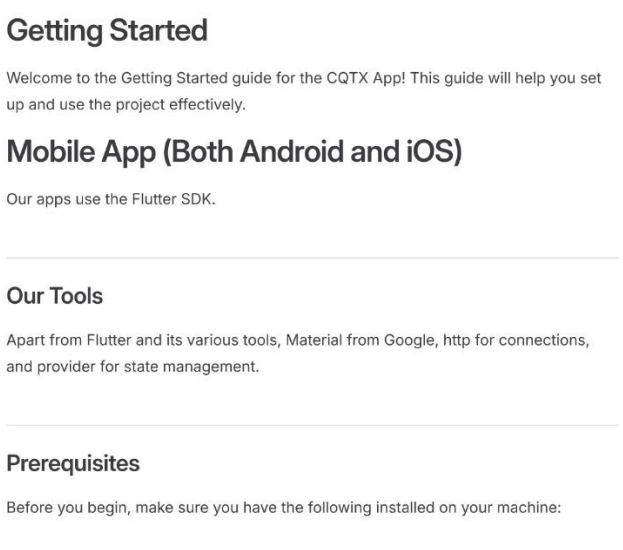
Figura 38 Documentación en CQTX Backend 8



Fuente: Autor

6.16. Anexo 16. Documentación Getting started App

Figura 39 Documentación en CQTX App 1



Getting Started

Welcome to the Getting Started guide for the CQTX App! This guide will help you set up and use the project effectively.

Mobile App (Both Android and iOS)

Our apps use the Flutter SDK.

Our Tools

Apart from Flutter and its various tools, Material from Google, http for connections, and provider for state management.

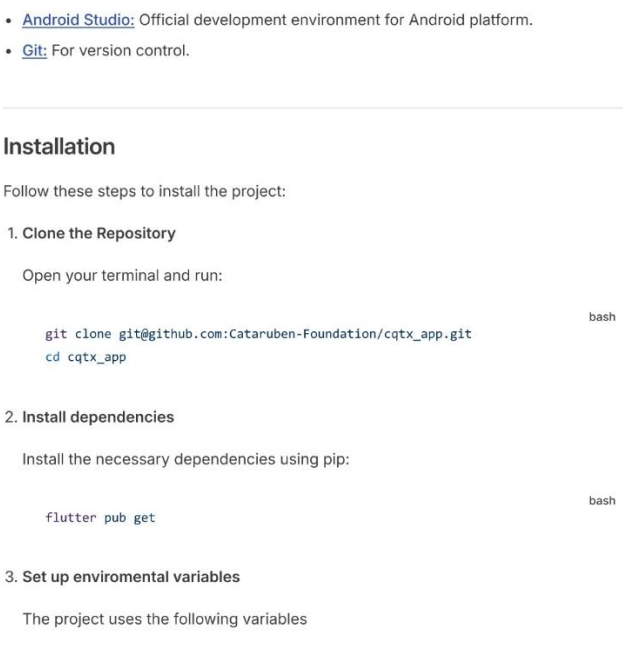
Prerequisites

Before you begin, make sure you have the following installed on your machine:

1/6

Fuente: Autor

Figura 40 Documentación en CQTX App 2



- Android Studio: Official development environment for Android platform.
- Git: For version control.

Installation

Follow these steps to install the project:

1. **Clone the Repository**

   Open your terminal and run:

```bash
git clone git@github.com:Cataruben-Foundation/cqtx_app.git
cd cqtx_app
```

2. **Install dependencies**

   Install the necessary dependencies using pip:

```bash
flutter pub get
```

3. **Set up enviromental variables**

   The project uses the following variables

2/6

Fuente: Autor

Figura 41 Documentación en CQTX App 3

File Structure

bash

```
.
├ .idea
├ android
├ assets
├ fonts
├ ios
├ lib
|  ├ constants
|  ├ pages
|  |    ├ biodiversity
|  |    |    └ biodiversity.dart
|  |    ├ certificates
|  |    ├ implementations
|  |    └ home.dart
|  |    └ login.dart
|  ├ services
|  |    └ api.dart
|  ├ widgets
|  |    ├ charts
|  |    |    ├ utils
```

3/6

Fuente: Autor

Figura 42 Documentación en CQTX App 4

```
|  |    └ loaderr.dart
|  |    └ pageRoute.dart
|  |    └ updatePopUp.dart
|  └ main.dart
├ linux
├ macos
├ test
├ web
├ windows
└ .metadata
└ analysis_options.yaml
└ devtools_options.yaml
└ .pubspeclock
└ README.md
```

Up and running

Run project

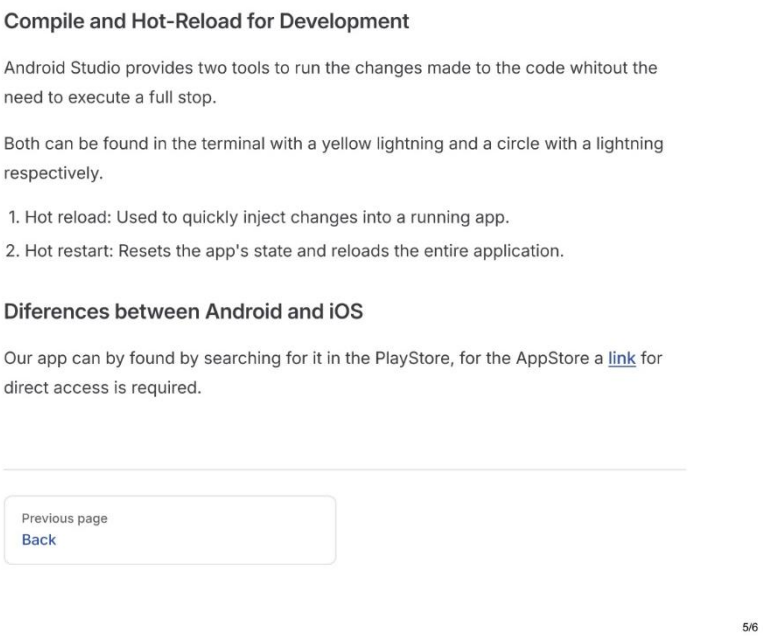
Android Studio provides tools to run the app in an emulated phone.

1. Add a phone to emulate in the Device Manager (We recommend a Pixel 8, and a Pixel 7 for older devices.)
2. Mayus + F10 or clicking the run button at the top right.

4/6

Fuente: Autor

Figura 43 Documentación en CQTX App 5



Compile and Hot-Reload for Development

Android Studio provides two tools to run the changes made to the code whitout the need to execute a full stop.

Both can be found in the terminal with a yellow lightning and a circle with a lightning respectively.

1. Hot reload: Used to quickly inject changes into a running app.
2. Hot restart: Resets the app's state and reloads the entire application.

Diferences between Android and iOS

Our app can by found by searching for it in the PlayStore, for the AppStore a link for direct access is required.

Previous page
Back

5/6

Fuente: Autor

7. REFERENCIAS

Amazon Web Services. (2024). *Amazon Simple Email Service (SES) – Cloud-based email sending service*. https://aws.amazon.com/ses/

Aruba Networks. (2024). *Aruba Central Cloud-Native Network Management*. https://www.arubanetworks.com/products/networking/aruba-central/

Atlassian. (2024). *Software development lifecycle (SDLC)*. https://www.atlassian.com/software-development/software-development-life-cycle

Auth0. (2024). *What is JWT (JSON Web Token)?* https://auth0.com/learn/json-web-tokens/

Cisco. (2024). *IT Automation Best Practices*. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/white-paper-c11-743998.html

DigitalOcean. (2024). *Cloud computing designed for developers*. https://www.digitalocean.com/

Django Software Foundation. (2024). *Django Channels*. https://channels.readthedocs.io/en/stable/

Dokku. (2024). *A Docker-powered mini-Heroku*. https://dokku.com/

Emerald Insight. (2024). *Organizational digital transformation: from evolution to future trends*. https://www.emerald.com/insight/content/doi/10.1108/dts-08-2023-0061/full/html

Figma. (2024). *Collaborative Interface Design Tool*. https://www.figma.com/

GitHub. (2024). *Understanding GitHub Actions*. https://docs.github.com/en/actions/learn-github-actions/understanding-github-actions

GitHub Docs. (2024). *About continuous integration*. https://docs.github.com/en/actions/automating-builds-and-tests/about-continuous-integration

GitHub Docs. (2024). *Understanding the GitHub flow*. https://docs.github.com/en/get-started/quickstart/github-flow

GoDaddy. (2024). *Domain verification and DNS management*. https://www.godaddy.com/help/verify-your-domain-using-dns-records-19236

Google Developers. (2024). *Apps Script Overview*. https://developers.google.com/apps-script/guides

Google Developers. (2024). *reCAPTCHA: Protect your site from spam and abuse*. https://developers.google.com/recaptcha

Grafana Labs. (2024). *Grafana: The open observability platform*. https://grafana.com/

Grafana Labs. (2024). *Observability Stack: LGTM with OpenTelemetry*. https://grafana.com/solutions/lgtm-stack/

Hochstein, L. (2017). *Ansible: Up and Running: Automating Configuration Management and Deployment the Easy Way* (2nd ed.). O'Reilly Media. https://www.oreilly.com/library/view/ansible-up-and/9781491979808/

ISO. (2024). *ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. https://www.iso.org/standard/27001

Kaspersky. (2024). *Kaspersky Next – Endpoint Security and Monitoring Platform*. https://www.kaspersky.com/enterprise-security/next

Linux Foundation. (2024). *Securing SSH: Best Practices for Hardening Linux Servers*. https://training.linuxfoundation.org/blog/securing-ssh-best-practices/

McCollam, T. (2022). *Grafana Observability: Dashboards and Monitoring Made Easy*. O'Reilly Media. https://www.oreilly.com/library/view/grafana-observability/9781098106840/

McKinsey. (2024). *What is digital transformation?* https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-digital-transformation

Microsoft. (2024). *What is Microsoft Power BI?* https://learn.microsoft.com/en-us/power-bi/fundamentals/power-bi-overview

Ned Batchelder. (2024). *Coverage.py: Code coverage measurement for Python*. https://coverage.readthedocs.io/

OpenTelemetry Project. (2024). *OpenTelemetry Documentation*. https://opentelemetry.io/docs/

OWASP Foundation. (2024). *OWASP ZAP - Zed Attack Proxy Project*. https://www.zaproxy.org/

Quixy. (2024). *20+ Most Mind-Blowing Examples of Digital Transformation in 2025*. https://quixy.com/blog/examples-of-digital-transformation/

Red Hat. (2024). *Getting started with Ansible*. https://www.ansible.com/resources/get-started

Taylor & Francis. (2024). *Digital transformation in an emerging economy: exploring organizational drivers*. https://www.tandfonline.com/doi/full/10.1080/23311886.2024.2302217

TekSystems. (2024). *How To Drive Your Digital Business Transformation - State of Digital Transformation 2024*. https://www.teksystems.com/en/insights/state-of-digital-transformation-2024

The Research Insights. (2025). *Beyond IT: Digital Transformation Market Size Set to Hit US$4,617.78 billion by 2030 at 27.6% CAGR*. https://aijourn.com/beyond-it-digital-transformation-market-size-set-to-hit-us4617-78-billion-by-2030-at-27-6-cagr-says-the-research-insights/

Turnbull, J. (2021). *The Book of Zabbix: Monitoring IT Infrastructure*. Turnbull Press. https://www.turnbullpress.org/books/zabbix/

Wavetec. (2024). *Top Digital Transformation Trends for 2024*. https://www.wavetec.com/blog/digital-transformation-trends/

Zabbix LLC. (2024). *Zabbix Documentation 6.0*. https://www.zabbix.com/documentation/6.0/manual