ANEXO NRO 1. ESPECIFICACIONES TÉCNICAS

PROCESO N°16640

MODALIDAD CONTRACTUAL: Selección Abreviada de menor cuantía.
OBJETO: "DISEÑO, IMPLEMENTACIÓN Y PUESTA EN MARCHA DE UN SISTEMA DE GESTIÓN DE PQRSDF CON INTELIGENCIA ARTIFICIAL".
PRESUPUESTO (VALOR): SEISCIENTOS OCHENTA Y TRES MILLONES OCHOCIENTOS OCHENTA Y OCHO MIL NOVECIENTOS VEINTIDÓS M/L ($683.888.922) IVA incluido.
PLAZO: Cuatro (4) sin superar el 12 de diciembre de 2025.

El presente documento tiene como objetivo recopilar y describir en detalle los requerimientos necesarios para el desarrollo de un sistema de información que sea capaz de:

- Capturar del Sistema Mercurio y/o SAC la PQRSDF presentada a la Entidad.
- A través de IA leer el documento de solicitud digitalizado (OCR) desde Mercurio y/o SAC
- Acorde a su lectura que pueda clasificar, realizar el direccionamiento a la dependencia encargada de dar respuesta de la PQRSDF
- Una vez enviada la PQRSDF, realizar el seguimiento y control para que se de respuesta oportuna en los tiempos estipulados de la PQRSDF.
- Validar que la respuesta a brindar este acorde a la PQRSDF recibida
- Entregar la respuesta de la PQRSDF recibida al ciudadano a través de Mercurio y/o SAC

De esta forma el Departamento de Antioquia, se pretende agilizar el proceso de respuesta a las PQRSDF. Este sistema será diseñado con base en el procedimiento establecido por la Dirección de Relación Estado Ciudadano adscrita a la Secretaria de Talento Humano y Servicios Administrativos. La correcta identificación y definición de estos requerimientos es esencial para garantizar que el sistema cumpla con las necesidades y expectativas de los diferentes usuarios. Además, se busca optimizar la eficiencia operativa del proceso, mejorar los tiempos de respuesta de las PQRSDF y precisión de las respuestas entregadas.

1.1. Alcance

El sistema propuesto busca automatizar y mejorar diversas actividades descritas en el procedimiento, entre las que se incluyen:

- Lectura de la PQRSDF y clasificación.
- La asignación y gestión de responsables de contestar la PQRSDF para el seguimiento.
- La generación de semáforos y alertas a los responsables de las respuestas sobre el vencimiento de términos para la respuesta de las PQRSDF.
- Confirmación de envió de la PQRSDF a Mercurio para que traslade la respuesta al solicitante.

Este levantamiento de requerimientos considera tanto los funcionales como los no funcionales del sistema:

- **Requerimientos funcionales**: Describen las funciones específicas que el sistema debe realizar, tales como el registro de la PQRSDF, lectura digital de la misma, asignación y envió al responsable de responder la PQRSDF, reportar PQR próximas a vencer, vencidas y realizar las alertas respectivas a los responsables de generar la respuesta, validar la respuesta valida y oportuna de la PQRSDF, envío de la respuesta a Mercurio y/o SAC para el respectivo tramite de la misma.

- **Requerimientos no funcionales**: Incluirán aspectos como la seguridad del sistema, la capacidad de procesamiento, la usabilidad, la escalabilidad, la interoperabilidad con otras plataformas (como Mercurio y SAC) y el cumplimiento de estándares normativos del sector público.

Además, el sistema debe ser un desarrollo basado en entorno web que cumpla con los lineamientos de seguridad de la Gobernación de Antioquia. El sistema operará con diferentes roles, tales como administrador, enlaces, visualizador, y diferentes módulos como módulo de seguridad, ingreso y gestión de usuarios y roles, seguimientos y módulo de reportes y visualizaciones.

El sistema debe ser capaz de manejar múltiples usuarios simultáneamente, garantizando un rendimiento óptimo y una experiencia de usuario fluida. La interfaz debe ser intuitiva y fácil de usar, permitiendo a los usuarios acceder rápidamente a la información que necesitan y realizar sus tareas de manera eficiente. Además, el sistema debe ser escalable para adaptarse a futuros aumentos en la cantidad de datos y usuarios, y debe ser interoperable con otras plataformas y sistemas utilizados por la Gobernación de Antioquia.

Con este documento, se establece una base clara para el diseño, desarrollo e implementación del sistema, asegurando la alineación con los objetivos estratégicos de la Dirección Relación Estado Ciudadano y del gobierno departamental. La implementación exitosa de este sistema contribuirá a mejorar la gestión y el seguimiento de las PQRSDF, dando valor agregado a la atención de las solicitudes recibidas.

1.2. Definiciones y Acrónimos

UI (User Interface): Interfaz de Usuario. Es el espacio donde las interacciones entre humanos y máquinas ocurren.

UX (User Experience): Experiencia de Usuario. Se refiere a cómo una persona se siente al interactuar con un sistema.

MERCURIO: Sistema de Gestión documental utilizado por el Departamento de Antioquia

SAC: Sistema de Gestión documental utilizado por la Secretaria de Educación del Departamento de Antioquia

KPI (Key Performance Indicator): Indicador Clave de Desempeño. Es una medida utilizada para evaluar el éxito de una organización o de una actividad en particular.

CRM (Customer Relationship Management): Gestión de Relaciones con Clientes. Es una estrategia para gestionar las interacciones de una empresa con sus clientes actuales y potenciales.

API (Application Programming Interface): Interfaz de Programación de Aplicaciones. Es un conjunto de definiciones y protocolos para construir e integrar software de aplicaciones.

HTTPS (Hypertext Transfer Protocol Secure): Protocolo de Transferencia de Hipertexto Seguro. Es una extensión del protocolo HTTP para la comunicación segura a través de una red de computadoras.

SSL (Secure Sockets Layer): Capa de Conexión Segura. Es un protocolo criptográfico diseñado para proporcionar comunicaciones seguras a través de una red informática.

SQL (Structured Query Language): Lenguaje de Consulta Estructurada. Es un lenguaje de programación utilizado para gestionar y manipular bases de datos relacionales.

Middleware de Consolidación de Información: Un sistema integrador que actuará como núcleo de comunicación entre diferentes plataformas documentales que se usan actualmente en la Gobernación de Antioquia.

Asistente Virtual con Inteligencia Artificial: Una herramienta inteligente diseñada para gestionar integralmente las Peticiones, Quejas, Reclamos, Sugerencias, Denuncias y Felicitaciones (PQRSDF).

Integración de Sistemas: Articulación precisa entre el sistema Mercurio (gestor documental de la Gobernación), el sistema SAC del Ministerio de Educación.

DESCRIPCIÓN GENERAL

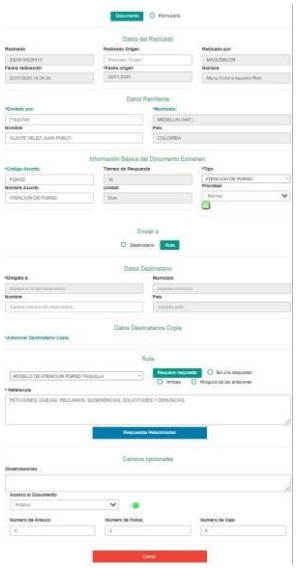
Actualmente, el Departamento de Antioquia cuenta con el sistema SAC para la recepción de PQRSDF, gestión documental de la secretaria de educación y las restantes dependencias de la administración registran sus PQRSDF en el sistema Mercurio.

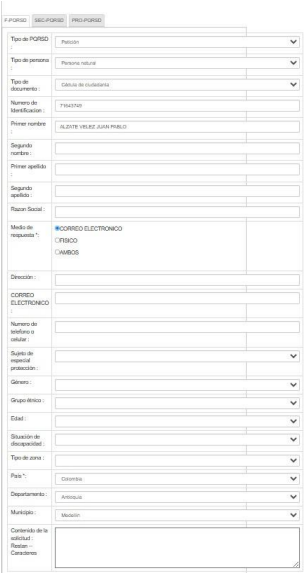
Las PQRSDF ingresan por 3 modelos diferentes, por el portal de la Gobernación con el llenado del formulario, por la taquilla física o por dos correos corporativos. Los radicados se hacen en el sistema Mercurio, el cual si se hace físico o por el portal llegan de una vez al siguiente paso que es el enlace. Si es por el boot de radicación del correo, se hace un ingreso al back office para que sea validada la

información y/o complementada en el formulario antes de ser enviada al enlace del área competente. El área competente elabora la respuesta y/o la delega según el caso y hace firmar la carta para dar respuesta al ciudadano.

La carta respuesta es radicada en mercurio y según el modelo de radicación, desde gestión documental se hace el envió respectivo para que quede notificado. Actualmente todo el procesamiento y revisión es manual por parte de los funcionarios de taquilla excepto el workflow que si controla tiempos y gestores de los documentos.

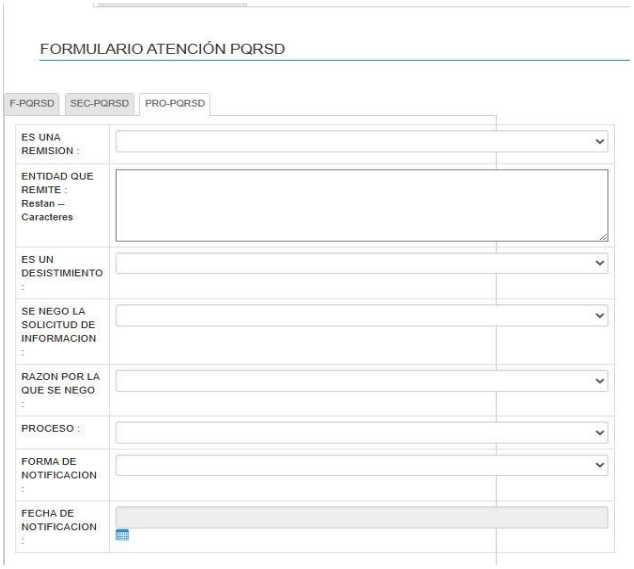
Formularios actuales:











Este método presenta varios desafíos y limitaciones significativas. En primer lugar, la manipulación, revisión, lectura y asignación subjetiva a los responsables de dar respuesta a las PQRSDF. El envío de correos electrónicos incrementa el riesgo de errores humanos, como la entrada incorrecta de datos, la pérdida de archivos o el envío de información incorrecta. Además, el proceso manual de lectura y reparto de datos es lento e involucra una alta probabilidad de enviar la PQRSDF para respuesta a la dependencia equivocada, demanda tiempo, lo que retrasa las repuestas con las consecuentes implicaciones.

La necesidad de un sistema de información competente surge de la necesidad de abordar estos problemas y mejorar la eficiencia y precisión del proceso de respuesta de las PQRSDF. Un sistema automatizado y centralizado permitiría una gestión más eficiente de la información, reduciendo el riesgo de errores y mejorando los tiempos de respuesta a los solicitantes. Además, facilitaría la generación de informes y aseguramiento de las correctas respuestas entregadas a los solicitantes.

Dependencias Involucradas en el Proyecto: El sistema de Inteligencia Artificial para gestión de PQRSDF abarcará las siguientes dependencias de la Gobernación de Antioquia:

1. DAGRAN (Departamento Administrativo de Planeación)
2. Gerencia de Control Interno Disciplinario
3. Oficina Privada
4. Secretaría de Ambiente
5. Secretaría de Desarrollo Económico
6. Secretaría de Educación
7. Secretaría de Gobierno
8. Secretaría de Hacienda
9. Secretaría de Infraestructura Física

10. Secretaría de la Juventud
11. Secretaría de las Mujeres
12. Secretaría de Salud e Inclusión Social
13. Secretaría de Seguridad
14. Secretaría de Justicia y Paz
15. Secretaría General
16. Secretaría de Talento Humano y Servicios Administrativos

1.3. Solución Propuesta: Sistema de Información Competente

Un sistema de información basado en entorno web que cumpla con los lineamientos de seguridad de la Gobernación de Antioquia sería la solución ideal para abordar estos problemas. Este sistema debería incluir las siguientes características:

Automatización de Procesos: El sistema debe automatizar la recepción de la PQRSDF de los sistemas SAC y/o Mercurio, leer la solicitud y la documentación relacionada (OCR), poder interpretar que dependencia debe responder la PQRSDF, enviar la documentación y sus anexos a la dependencia respectiva, validar que la misma sea respondida en los tiempos estipulados y a su vez que la respuesta generada este acorde a lo solicitado. Si cumple con las condiciones remitir dicha respuesta a Mercurio o SAC para la entrega de la respuesta al solicitante.

Gestión de Roles y Permisos: El sistema debe operar con diferentes roles, como administrador, enlaces, responsable de las respuestas y visualizador de retrasos en las respuestas, asegurando que cada usuario tenga acceso solo a la información y funcionalidades que necesita.

Módulos Especializados: El sistema debe contar con módulos específicos para la gestión de la respuesta, seguimiento y generación de reportes y visualizaciones.

Seguridad de la Información: El sistema debe implementar medidas de seguridad robustas, como la autenticación y autorización de usuarios, el cifrado de datos sensibles y la protección contra amenazas cibernéticas.

Interfaz Intuitiva: La interfaz de usuario debe ser intuitiva y fácil de usar, permitiendo a los usuarios acceder rápidamente a la información que necesitan y realizar sus tareas de manera eficiente.

Escalabilidad y Rendimiento: El sistema debe ser escalable para adaptarse a futuros aumentos en la cantidad de datos y usuarios, y debe garantizar un rendimiento óptimo.

Interoperabilidad: El sistema debe ser interoperable con otras plataformas y sistemas utilizados por la Gobernación de Antioquia, como el Módulo Mercurio y SAC.

Generación Automática de Reportes: El sistema debe permitir la generación automática de reportes a necesidad del estado de las PQRSDF (pendientes de respuesta, Con tiempos vencidos, respondidas oportunamente) por dependencia facilitando la toma de decisiones y correcciones.

Validación y Consolidación de Datos: El sistema debe incluir funcionalidades para la lectura del documento, clasificación, validación enrutamiento y seguimiento de la PQRSDF, reduciendo el riesgo de errores y mejorando la consistencia de la información.

Implementar un sistema de información competente no solo mejorará la eficiencia operativa del proceso, sino que también garantizará la precisión en la toma de decisiones y promoverá la rendición de cuentas dentro del Plan de Desarrollo Departamental de Antioquia.

1.4. Ámbito del Sistema

El sistema de información propuesto para la gestión, seguimiento de las PQRSDF de Antioquia debe contemplar los siguientes aspectos:

- **Desarrollo Basado en Entorno Web**

El sistema debe ser desarrollado como una aplicación web, accesible desde cualquier navegador moderno. Esto permitirá a los usuarios acceder al sistema desde cualquier ubicación con conexión a internet, facilitando la colaboración y el acceso a la información en tiempo real. La naturaleza web del sistema también permite actualizaciones y mejoras continuas sin necesidad de instalaciones locales en los dispositivos de los usuarios.

- **Cumplimiento de Lineamientos de la Dirección de Tecnologías de la Información**

El sistema debe cumplir con todos los lineamientos y estándares establecidos por la Dirección de Tecnologías de la Información de la Gobernación de Antioquia. Esto incluye aspectos de seguridad, interoperabilidad, accesibilidad y usabilidad, garantizando que el sistema sea seguro, eficiente y fácil de usar para todos los usuarios. Cumplir con estos lineamientos asegura que el sistema esté alineado con las políticas y prácticas tecnológicas de la gobernación, facilitando su integración y aceptación.

- **Arquitectura del Sistema**

El sistema puede ser desarrollado utilizando una arquitectura monolítica o basada en microservicios, dependiendo de la mejor opción considerando diversos componentes como costos, implementación, seguridad, tiempo, mantenimiento, soporte y la definición técnica del arquitecto. La arquitectura monolítica puede ser más sencilla y rápida de implementar, mientras que la arquitectura de microservicios ofrece mayor flexibilidad y escalabilidad. La decisión sobre la arquitectura debe ser tomada en base a un análisis detallado de estos factores, asegurando que la solución elegida sea la más adecuada para las necesidades del proyecto.

- **Metodologías de Desarrollo**

Si el desarrollo del sistema se realiza desde cero, se recomienda utilizar metodologías ágiles, como Scrum o Kanban, para gestionar el proyecto. Estas metodologías permiten una mayor flexibilidad y adaptabilidad, facilitando la incorporación de cambios y mejoras durante el desarrollo. Además, es importante documentar la estructura integral del software, asegurando que todos los aspectos del sistema estén claramente definidos y comprendidos por el equipo de desarrollo. La documentación adecuada también facilita el mantenimiento y la evolución del sistema a lo largo del tiempo.

- **Incorporación de Nuevos Planteamientos y Mejoras**

El sistema debe ser diseñado de manera que permita la incorporación de nuevos planteamientos y mejoras sugeridas por el dueño del producto, en este caso la Dirección de Relación Estado Ciudadano del Departamento. Esto incluye la capacidad de adaptar el sistema a nuevas necesidades y requerimientos que puedan surgir durante su uso. La flexibilidad para incorporar mejoras asegura que el sistema pueda evolucionar y mantenerse relevante a medida que cambian las necesidades y prioridades.

Inicialmente se contempla un periodo de estabilización de seis meses después de la entrega formal al Departamento (firma del acta de recibo), donde se realizarán las correcciones a fallas reportadas y mejoras, adicionalmente, el contratista deberá garantizar seis (6) meses adicionales de soporte sobre lo construido, por lo que el tiempo total inicial de garantía será de un (1) año.

- **Seguridad y Protección de Datos**

El sistema debe implementar medidas de seguridad robustas para proteger la información sensible. Esto incluye la autenticación y autorización de usuarios, el cifrado de datos sensibles y la protección contra amenazas cibernéticas, implementación de cifrado fuerte (mínimo AES256) para la protección de datos sensibles. Además, el sistema debe cumplir con las normativas y regulaciones de protección de datos aplicables. La seguridad de los datos es fundamental para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada por el sistema.

- **Gestión de Roles y Permisos**

El sistema debe operar con diferentes roles, como administrador, enlaces y visualizador, asegurando que cada usuario tenga acceso solo a la información y funcionalidades que necesita. Esto permitirá una gestión más eficiente y segura de la información. La gestión de roles y permisos asegura que las responsabilidades y accesos estén claramente definidos y controlados, minimizando el riesgo de accesos no autorizados.

- **Administración de Usuarios y Sesiones**

El sistema debe incluir funcionalidades para la administración de usuarios y sesiones. Esto permitirá gestionar el acceso de los usuarios al sistema, asegurando que solo los usuarios autorizados

puedan acceder a la información y funcionalidades del sistema. La administración de usuarios y sesiones también facilita el seguimiento y control de las actividades realizadas en el sistema, mejorando la seguridad y la auditoría.

- **Módulos Especializados**

El sistema debe contar con módulos específicos para la captura de la PQRSDF, la clasificación, enrutamiento, seguimiento, validación de las respuestas contra lo solicitado y posterior envió al sistema Mercurio o SAC para la entrega de la respuesta final al solicitante. Cada módulo debe estar diseñado para facilitar la realización de tareas específicas, mejorando la eficiencia y efectividad del proceso. Los módulos especializados aseguran que las funcionalidades del sistema estén organizadas y optimizadas para las necesidades específicas de cada área de gestión.

- **Interoperabilidad**

El sistema debe ser interoperable con otras plataformas y sistemas utilizados por la Gobernación de Antioquia, como el Sistemas Mercurio y SAC. Esto permitirá una integración fluida de datos y procesos, mejorando la coherencia y consistencia de la información. La interoperabilidad facilita el intercambio de información y la colaboración entre diferentes sistemas y departamentos, mejorando la eficiencia y la efectividad del seguimiento y la respuesta oportuna de las PQRSDF.

- **Escalabilidad y Rendimiento**

El sistema debe ser escalable para adaptarse a futuros aumentos en la cantidad de datos y usuarios, y debe garantizar un rendimiento óptimo. Esto incluye la capacidad de manejar múltiples usuarios simultáneamente sin degradar el rendimiento del sistema. La escalabilidad y el rendimiento aseguran que el sistema pueda crecer y adaptarse a medida que aumentan las demandas y los volúmenes de datos, manteniendo una experiencia de usuario fluida y eficiente.

- **Generación Automática de Reportes**

El sistema debe permitir la generación automática de reportes trimestrales de avance físico y financiero, facilitando la toma de decisiones informadas. Los reportes deben ser claros, precisos y fáciles de interpretar, proporcionando una visión completa del estado del Plan de Desarrollo. La generación automática de reportes reduce el tiempo y el esfuerzo necesarios para preparar informes, mejorando la eficiencia y la precisión del proceso de seguimiento y evaluación.

- **Asistente IA**

El asistente de IA está concebido como una solución integral capaz de:
  - Interconecta diferentes sistemas documentales
  - Leer las PQRSDF (OCR)

- Proponer respuestas automáticas para trámites de todas las dependencias
- Crear un modelo de IA con capacidad de aprendizaje continuo que mejore su rendimiento con cada interacción
- Clasificar y direccionar solicitudes con precisión algorítmica, determinando la ruta que debe tomar, así como la captura de los metadatos esenciales.
- Aplicación de IA para generación automática de respuestas y notificación
- Aplicación de Inteligencia Artificial (IA) para identificar y clasificar los documentos y determinar la ruta que debe tomar, asi como la captura de los metadatos esenciales.
- Aplicación de IA para el auto entrenamiento del sistema ○ Genera informes dinámicos sobre las PQRSDF ○ Realiza seguimiento de solicitudes resueltas y pendientes ○ Facilita la asignación de responsabilidades a funcionarios ○ Trazabilidad completa de cada solicitud ciudadana

- **Motor de Base de Datos Relacional**

El sistema debe utilizar un motor de base de datos relacional para gestionar y almacenar la información. En este caso, se recomienda utilizar Oracle, PostgreSQL o SQL Server como motores de base de datos. Estos motores son conocidos por su robustez, eficiencia y capacidad para manejar grandes volúmenes de datos de manera estructurada. Esto permitirá una gestión eficiente y segura de la información, facilitando las consultas y el análisis de datos.

- **Tecnologías y Frameworks Conocidos**

El desarrollo del sistema debe realizarse utilizando tecnologías y frameworks conocidos y ampliamente utilizados en la comunidad de desarrollo de software. Esto incluye lenguajes de programación como Java, JavaScript, Python, PHP entre otros, así como frameworks como Spring, Angular, React, Djang, Laravel entre otros. Utilizar tecnologías y frameworks reconocidos asegura que el sistema sea robusto, mantenible y escalable, y facilita la incorporación de desarrolladores con experiencia en estas tecnologías.

- **Registro de Logs y Visualización de actividades con las PQRSDF**

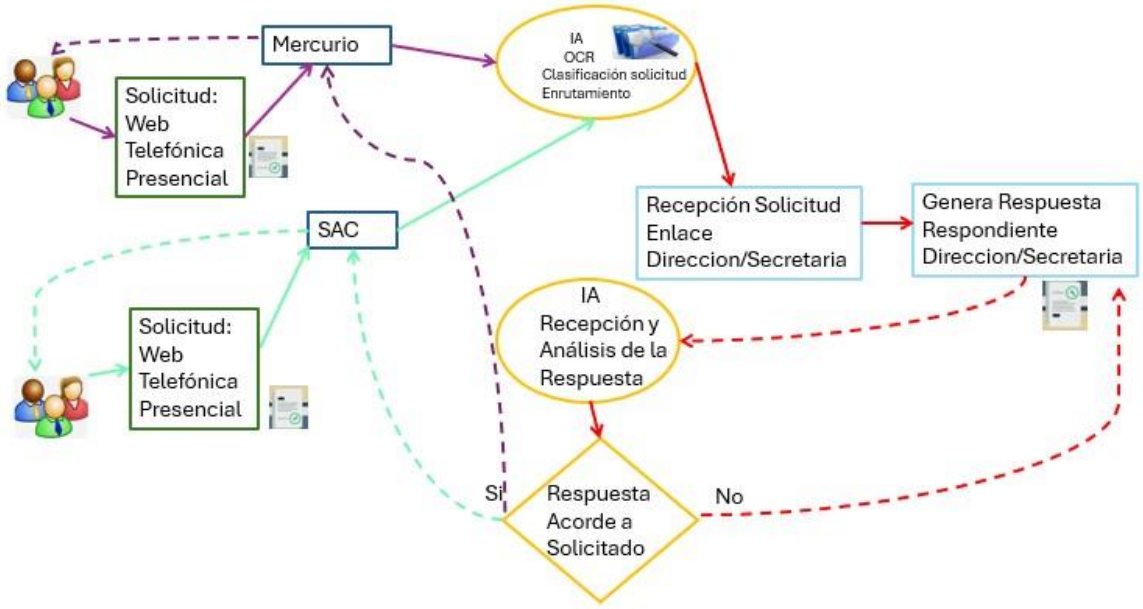
El sistema debe guardar logs detallados de todos los cambios realizados al Adelantar la respuesta de las PQRSDF. Estos logs deben incluir estampa de tiempo y justificaciones para cada cambio. Los administradores del sistema deben tener la capacidad de visualizar estos logs, permitiendo un seguimiento completo de las modificaciones realizadas. Esto asegurará la transparencia y la trazabilidad de los cambios, facilitando la auditoría y el control de la información.

- **Generación de Informes Personalizados**

El sistema debe permitir la generación de informes personalizados según las necesidades específicas de los usuarios. Los administradores y enlaces podrán seleccionar diferentes criterios y

parámetros para crear informes que se ajusten a sus requerimientos. Esto incluye la capacidad de filtrar datos por fechas, dependencias y otros criterios relevantes.

1.5. Descripción General del Producto



El producto es un aplicativo web diseñado para la captura del sistema Mercurio y/o SAC de las PQRSDF, lectura de la PQRSDF (OCR), clasificación, enrutamiento al usuario encargado de la respuesta o enlace designado, monitoreo y seguimiento de los tiempos para la repuesta, validación una vez dada la respuesta que este acorde a lo solicitado, y si es correcta la respuesta, se debe encargar del envío al sistema SA o Mercurio para la respectiva respuesta al solicitante. Este sistema debe ser dinámico, intuitivo y responsive, asegurando una experiencia de usuario óptima en cualquier dispositivo, ya sea un ordenador de escritorio, una tableta o un teléfono móvil. Estrategia conjunta contratistaGobernacion para atender las PQRSDF de las redes sociales de la Gobernacion de Antioquia

El aplicativo debe ser desarrollado utilizando tecnologías de vanguardia que garanticen su robustez, escalabilidad y mantenibilidad. Esto incluye el uso de lenguajes de programación modernos como Java, JavaScript, Python, PHP y/o otros, así como frameworks reconocidos en la comunidad de desarrollo de software, tales como Spring, Angular, React, Django, Laravel y/o otros.

El sistema debe ser capaz de manejar grandes volúmenes de datos de manera eficiente y segura, utilizando motores de base de datos relacionales como Oracle, PostgreSQL o SQL Server. Además, debe cumplir con los lineamientos y estándares establecidos por la Dirección de Tecnologías de la

Información de la Gobernación de Antioquia, asegurando la seguridad, interoperabilidad, accesibilidad y usabilidad del sistema.

El aplicativo web debe permitir el seguimiento del flujo de la solicitud, proporcionando una visión integral del progreso de la respuesta. Esto mejorará la eficiencia operativa, la precisión en la toma de decisiones y la capacidad de adaptación a nuevas necesidades y requerimientos.

El Desarrollo, deberá incluir un tiempo de estabilización de tres meses, en los cuales, se deben atender fallas de funcionalidad inherentes al desarrollo.

1.6. Roles del Sistema:

1.6.1. Administrador General:

- **Descripción:** Este rol tiene acceso completo a todas las funcionalidades del sistema y puede gestionar todos los aspectos de este. Los administradores generales pueden visualizar todas las PQRSDF, ver tiempos de respuesta, visualización de PQRSDF por finalizar los tiempos establecidos para las respuestas, gestionar usuarios y roles.

- **Responsabilidades:**

- Visualizar y filtrar PQRSDF por estados (En verde para respuesta, próximos a vencer y vencidos o demorados en ser respondidos).
- Gestionar usuarios y roles. Generar reportes y visualizar los de cambios.

1.6.2. Enlace:

- **Descripción:** Los usuarios con este rol son los que reciben la PQRSDF que viene del enrutamiento de la aplicación, y este debe enviar al responsable de la dependencia que elaborara el proyecto de respuesta.

- **Responsabilidades:**
- Recepción de las PQRSDF que lleguen a la Dependencia.
- Envió de la PQRSDF al responsable (respondiente) de preparar la respuesta.
- Reasignar internamente las PQRSDF entre los respondientes.
- Ver y Revisar el estado de las PQRSDF de la dependencia, validando los que están en tiempo, por vencer o vencidos.

1.6.3. Respondiente:

- **Descripción:** Este rol tiene acceso a las PQRSDF asignadas a él para su respuesta. Podrá visualizar solo las PQRSDF asignadas y proceder a dar respuesta a las mismas

- **Responsabilidades:**
- Consultar las PQRSDF asignadas a el

- Dar respuesta a la PQRSDF
- Enviar a la IA las respuestas de la PQRSDF para que la IA realice el análisis y validación si la respuesta es acorde a la solicitud. Si esta ok, la descargara del respondiente asignado, de lo contrario volverá al respondiente para su revisión.
- Generar reportes personalizados de las PQRSDF propias para validar el estado de estas (Oportuna, por vencer o vencidas).

Estos roles aseguran que las responsabilidades y accesos estén claramente definidos y controlados, minimizando el riesgo de accesos no autorizados y garantizando una gestión eficiente y segura de la información del sistema.

1.7. Módulos

1.7.1. Módulo de Seguridad

El módulo de seguridad es fundamental para garantizar el acceso controlado y la protección de la información dentro del sistema. Este módulo incluye varias funcionalidades clave que aseguran que solo los usuarios autorizados puedan acceder y realizar acciones específicas dentro del sistema. A continuación, se detallan las funcionalidades y componentes del módulo de seguridad:

Administración de Usuarios

- **CRUD Completo**: Permite la creación, lectura, actualización y eliminación de usuarios. Los administradores pueden gestionar los perfiles de los usuarios, asegurando que la información esté siempre actualizada.
- **Cambios de Contraseñas**: Los usuarios pueden cambiar sus contraseñas de manera segura. Además, los administradores pueden restablecer contraseñas en caso de olvido.
- **Validación de Usuarios por Correos**: El sistema enviará correos electrónicos de validación a los usuarios para confirmar sus cuentas y permitir el acceso seguro al sistema.

Administración de Roles

- **CRUD y Permisos**: Permite la creación, lectura, actualización y eliminación de roles. Los administradores pueden definir y asignar permisos específicos a cada rol, asegurando que los usuarios solo tengan acceso a las funcionalidades necesarias para su trabajo.

Asignación de Enlaces por Dependencia

- **Maestro de Dependencias**: Permite la administración de las dependencias dentro del sistema. Los administradores pueden crear, modificar y eliminar dependencias según sea necesario.
- **Asignación de Dependencias a Enlaces**: Los administradores pueden asignar dependencias específicas a los enlaces, asegurando que cada enlace tenga acceso solo a la información y funcionalidades relacionadas con su dependencia.

- **Asignación de Respondentes por Dependencias:** Los administradores pueden asignar Respondentes asociados a las dependencias que a su vez están asociados a los enlaces, asegurando que cada respondente solo pueda ver las PQRSDF asignada y proceder a la respuesta de estas.

Manejo de Administradores

- **Tipos de Administradores**: El sistema debe soportar tres tipos de administradores:
- **Administrador General**: Tiene acceso completo a todas las funcionalidades del sistema y puede gestionar todos los aspectos de este.
- **Administrador Directivo**: Tiene acceso a funcionalidades específicas relacionadas con la gestión y supervisión de las PQRSDF y dependencias.
- **Administrador de Dependencias**: Tiene acceso a la gestión de usuarios y roles dentro de su dependencia específica.

Seguridad Adicional

- **Estampillas de Tiempo y Justificación**: El sistema debe guardar logs detallados de todas las acciones realizadas por los usuarios, incluyendo estampillas de tiempo y la razón del cambio. Esto permitirá un seguimiento completo de los cambios de estado,de las PQRSDF, resaltando las que se vencieron, o están próximas a vencer.
- **Notificaciones y Alertas**: El sistema debe enviar notificaciones y alertas a los usuarios y administradores sobre PQRSDF pendientes de ser respondidas, próximas a vencer, vencidas y otros eventos relevantes, que el sistema debe permitir parametrizar. Esto asegurará que todos los usuarios estén informados y puedan actuar de manera oportuna.

Este módulo de seguridad garantizará que el sistema sea seguro, eficiente y fácil de usar, permitiendo una gestión adecuada de los usuarios, roles y dependencias, y asegurando que la información esté protegida en todo momento.

Acceso y Roles:

- **Roles de Enlaces:** Los usuarios con el rol de enlace pueden acceder a este módulo y visualizar únicamente las PQRSDF relacionadas con su dependencia o aquellos para los que tienen permisos específicos. Estos usuarios pueden notificar a los respondientes sobre las PQRSDF que tiene el respondiente vencido o por vencer.
- **Roles Administrativos Generales:** Los usuarios con el rol de administrador tendrán la potestad de crear usuarios en la aplicación, agregar dependencias y enlaces, así como la generación de los reportes y creación de los mismos.
- **Roles Administrativos Directivos:** Además de las funciones del rol de administrador general, los administradores directivos pueden abrir la plataforma por rangos de fechas para la verificación del estado de las PQRSDF. Pueden reasignar dentro de su dependencia las PQRSDF para optimizar la evacuación de las mismas.

•

Componentes del Módulo:

Notificaciones y Alertas:

- **Notificaciones:** El sistema deberá alertar referente a agotamiento de tiempos para responder a las PQRSDF, que tenga un respondiente en su bandeja; tanto al respondiente como al enlace de la respectiva secretaria o Dirección
- Cuando un respondiente genera la respuesta de la PQRSDF, el sistema envía una notificación al enlace, para indicar que ya se evacuo la PQRSDF, sin embargo; oe deben poder activar o desactivar las notificaciones acordes a la decisión del usuario con rol de administrador general.

Gestión de Indicadores:

- **Visualización y Filtrado:** Los administradores pueden visualizar todos las PQRSDF, indicando los pendientes de atención, las vencidas.

•

Seguridad y Control de Acceso:

- **Roles y Permisos:** El módulo integra el sistema de roles y permisos, asegurando que solo los usuarios autorizados puedan acceder y modificar la información y parámetros de la aplicación.
- **Logs y Auditoría:** El sistema guarda logs detallados de todas las acciones realizadas en el módulo, permitiendo un seguimiento completo.

1.7.2. Módulo de IA-Seguimiento

El módulo de IA-Seguimiento incluye varias funcionalidades entre las que tenemos:

- Carga de las PQRSDF de los sistemas Mercurio -SAC: El sistema debe permitir que las PQRSDF junto los documentos anexos que se radiquen en la plataforma de Mercurio / SAC (Radicado generado por Mercurio /SAC), las pueda leer en la nueva solución (el oferente determinara el mecanismo),
- Lectura Documento de solicitud y anexos: Se desea que el sistema a implementar lea tanto la PQRSDF como la documentación anexa (a través de OCR) manteniendo el radicado de mercurio.

- Envió Respuesta a sistema Mercurio - SAC: Se desea que el sistema a implementar genere el radicado las respuestas de las PQRSDF, dadas por los respondientes, hacia los sistemas Mercurio o SAC. Se debe solicitar el radicado de mercurio y SAC a la repuesta, igualmente se debe generar la notificación a través de la solución al solicitante.

Lectura y respuesta de la PQRSDF: Con la participación de la Inteligencia Artificial (IA) una vez leída la solicitud y documentación anexa, si la tiene, con la ayuda de un sistema OCR, se pueda interpretar. Validar si es posible dar respuesta a lo peticionado, en caso afirmativo elaborar el documento respuesta y enviar esta respuesta al sistema correspondiente Mercurio o SAC para su entrega al usuario final. Si no le es posible adelantar la respuesta, enrutar la PQRSDF junto con la documentación anexa, al enlace de la secretaria o Dirección competente para adelantar la respuesta.

Clasificación y enrutamiento de la PQRSDF Enrutamiento y Asignación: Una vez enrutada la PQRSDF por parte del sistema, esta llega al enlace de cada secretaria/Dirección, el enlace valida la PQRSDF recibida y la direcciona al funcionario encargado de dar la respuesta acorde a lo solicitado. Por lo anterior la aplicación debe permitir esta revisión y asignación al respondiente para dar curso a lo solicitado. Si la asignación no corresponde a la Secretaria / Dirección como competente de la PQRSDF, el sistema debe permitir su devolución y definirá la forma en que le dará curso o reasignación de esta.

Respuestas PQRSDF: Una vez realizada la respuesta el respondente deberá enviar la mencionada respuesta a la IA para que esta valide si la respuesta dada esta acorde a lo solicitado y en caso afirmativo entregar dicha respuesta al sistema solicitante (Mercurio-SAC), en caso de no estar acorde, se le deberá retroalimentar al usuario la no procedencia y retroalimentar como se debería tratar.

- ✓ **Reporte a Generar**: Se deben tener reportes de las PQRSDF recibidas, clasificadas por Sistema Generador (Mercurio -SAC), Dependencias direccionadas, cuantas respondidas, cuantas respondidas y el estado de las mismas

- ✓ **Asignación de Responsables**: Los administradores deben poder asignar responsables a cada nivel del Plan de Desarrollo. Esto incluye la asignación de enlaces y dependencias responsables de la gestión y seguimiento de los mismos

Seguridad y Control de Acceso

- ✓ **Roles y Permisos**: El módulo debe integrar con el sistema de roles y permisos, asegurando que solo los usuarios autorizados puedan acceder y modificar la información.
- ✓ **Logs y Auditoría**: El sistema debe guardar logs detallados de todas las acciones realizadas en el módulo, incluyendo estampillas de tiempo y justificaciones para cada cambio. Los administradores deben tener la capacidad de visualizar estos logs para realizar un seguimiento completo de las modificaciones.

1.7.3. **Módulo de Respondientes:**

Este módulo permite que el enlace establecido por Secretaria o Dirección, reciba la PQRSDF, valide si es la oficina pertinente para dar respuesta a la solicitud, en caso afirmativo realiza la asignación al respondiente indicado, en caso contrario, debe devolver la PQRSDF para ser Re enrutada a la oficina indicada. Los Respondientes se encargan de elaborar la respuesta y una vez lista se encargarán de enviarla al módulo de clasificación y enrutamiento para la revisión y posterior envió al sistema mercurio o SAC. Este módulo es accesible tanto para los roles de enlaces como para los respondientes.

1.7.4. **Módulo de Reportes**

El módulo de reportes es una parte esencial del sistema de información para la gestión, seguimiento y evaluación del Plan de Desarrollo Departamental de Antioquia. Este módulo permite a los usuarios generar informes detallados y personalizados sobre el estado de las PQRSDF, dependencias, responsables, estados de las PQRSDF (vencidas, por vencer y en atención) promoviendo el cumplimiento legal en las respuestas requeridas por los usuarios.

Componentes del Módulo de Reportes:

- **Reportes Generales de la Plataforma:**
- **Accesos:** Este reporte proporciona información sobre los accesos al sistema, incluyendo detalles sobre los usuarios que han ingresado, las fechas y horas de acceso, y las acciones realizadas. Esto es útil para monitorear el uso del sistema y detectar posibles accesos no autorizados.
- **PQRSDF sin Diligencias:** Este reporte identifica las PQRSDF que no han sido respondidas dentro del período establecido. Permite a los administradores tomar acciones correctivas y asegurar que las respuestas sean dadas oportunamente.
- **Reporte por oficina:** Este reporte muestra las PQRSDF tramitadas por Dependencia, consolidando las atendidas oportunamente, las atendidas extemporáneamente y las que están por atender dentro del plazo, así como las que están vencidas sin responder. Igualmente, se debe identificar el respondiente responsable.

- **Reportes Personalizados:**

  Criterios y Parámetros: Los usuarios pueden generar informes personalizados seleccionando diferentes criterios y parámetros, como fechas, dependencias, estados y otros criterios relevantes. Esto permite obtener información específica y detallada según las necesidades de cada usuario.

  Filtros Avanzados: El sistema debe permitir la aplicación de filtros avanzados para refinar los resultados de los reportes, facilitando la identificación de patrones y tendencias.

1.8. Restricciones del Sistema:

- **Conexión a Internet:** ○ El uso del software requiere una conexión a internet estable para garantizar el acceso y la sincronización de datos en tiempo real.
- **Acceso Único por Usuario:** ○ El sistema solo permitirá el ingreso de un mismo usuario en un solo dispositivo al mismo tiempo para evitar conflictos y asegurar la integridad de los datos.
- **Bloqueo de Registros:** ○ Cuando un usuario esté trabajando sobre un registro, este deberá ser bloqueado para el resto de los usuarios hasta que se complete la edición. Esto previene la sobreescritura y asegura la coherencia de la información.
- **Control de Cambios:** ○ Debe existir un control de cambios estricto que registre todas las modificaciones realizadas, incluyendo quién modificó, cuándo lo modificó, el registro antes de la modificación y después de la modificación. Esto asegura la trazabilidad y transparencia de las acciones.

- **Bloqueo de Usuarios:** ○ Los usuarios serán bloqueados después de un número configurable de intentos fallidos de inicio de sesión. Esta configuración debe ser parametrizable en el sistema para adaptarse a las políticas de seguridad.

- **Compatibilidad con Navegadores:** ○ El sistema debe ser funcional en los navegadores web actuales, garantizando una experiencia de usuario consistente y accesible.

- **Buenas Prácticas de Desarrollo Web:** ○ El desarrollo del sistema debe seguir las buenas prácticas de desarrollo web, asegurando un código limpio, mantenible y eficiente.

- **Estándares de Seguridad:** ○ El sistema debe cumplir con los estándares de seguridad y los lineamientos establecidos por la Dirección de Tecnologías de la Información de la Gobernación de Antioquia, protegiendo la confidencialidad, integridad y disponibilidad de la información.

- **Uso de CAPTCHA:** ○ Se utilizarán CAPTCHAs para el ingreso al aplicativo, previniendo accesos automatizados y mejorando la seguridad del sistema.

- **Protocolo HTTPS:** ○ La comunicación entre el cliente y el servidor deberá establecerse a través del protocolo HTTPS, asegurando la transmisión segura de datos.

- **Validación de Sesión:** ○ El aplicativo debe contar con un sistema de validación de sesión para verificar la autenticidad de los usuarios y prevenir accesos no autorizados.

- **Registro de Logs:** ○ El sistema debe guardar logs detallados de las acciones de los usuarios, incluyendo ingresos, consultas y fechas de las acciones realizadas. Esto facilita la auditoría y el monitoreo del uso del sistema.

- **Asignación de Permisos por Roles:** Los permisos del aplicativo serán asignados por roles, asegurando que los usuarios solo tengan acceso a las funcionalidades y datos necesarios para sus tareas.

- **Respaldo y Recuperación de Datos:** ○ El sistema debe contar con mecanismos de respaldo y recuperación de datos para asegurar la disponibilidad de la información en caso de fallos o incidentes

.

- **Escalabilidad:** El sistema debe ser escalable para manejar futuros aumentos en la cantidad de datos y usuarios, garantizando un rendimiento óptimo.

- **Interoperabilidad:** El sistema debe ser interoperable con otras plataformas y sistemas utilizados por la Gobernación de Antioquia, facilitando la integración y el intercambio de información.

- **Tiempo de Inactividad de Sesión:** ○ Las sesiones de usuario deben expirar automáticamente después de un período de inactividad configurable. Esto ayuda a proteger la información en caso de que un usuario deje su dispositivo desatendido.

- **Actualizaciones y Parches de Seguridad**: El sistema debe ser actualizado regularmente con parches de seguridad y mejoras para proteger contra vulnerabilidades conocidas y emergentes.

- **Capacidad de Exportación de Datos:** Los usuarios deben poder exportar datos en formatos comunes (como CSV, Excel, PDF) para análisis y reportes externos.

- **Documentación y Soporte:** El sistema debe contar con documentación completa y actualizada, así como con un sistema de soporte para ayudar a los usuarios a resolver problemas y entender cómo utilizar las funcionalidades del sistema.

2. Requerimientos Funcionales

2.1. Módulo de seguridad

Sigla	Propósito	Descripción	Entrada	Salida
RF-101	**Administración de Usuarios**	**Permitir la creación, lectura, actualización y eliminación de usuarios.**	**Datos del usuario (nombre, correo, rol, etc.)**	**Confirmación de la acción realizada (usuario creado, actualizado, eliminado)**
RF-102	**Cambio de Contraseñas**	**Permitir a los usuarios cambiar sus contraseñas de manera segura.**	**Contraseña actual, nueva contraseña**	**Confirmación de cambio de contraseña**

RF-103	**Restablecimiento de Contraseñas**	**Permitir a los administradores restablecer contraseñas en caso de olvido.**	**Solicitud de restablecimiento, nueva contraseña**	**Confirmación de restablecimiento de contraseña**
RF-104	**Validación de Usuarios por Correos**	**Enviar correos electrónicos de validación a los usuarios para confirmar sus cuentas.**	**Dirección de correo electrónico del usuario**	**Confirmación de validación de cuenta**
RF-105	**Administración de Roles**	**Permitir la creación, lectura, actualización y eliminación de roles, y la asignación de permisos específicos a cada rol.**	**Datos del rol (nombre, permisos)**	**Confirmación de la acción realizada (rol creado, actualizado, eliminado)**
RF-106	**Asignación de Dependencias a Enlaces**	**Permitir la asignación de dependencias específicas a los enlaces.**	**Datos del enlace y dependencia**	**Confirmación de la asignación realizada**
RF-107	**Manejo de Administradores**	**Soportar tres tipos de administradores: General, Directivo y de Dependencias, con acceso a funcionalidades específicas.**	**Datos del administrador (nombre, tipo, permisos)**	**Confirmación de la acción realizada (administrador creado, actualizado, eliminado)**

RF-108	**Seguridad Adicional**	**Guardar logs detallados de todas las acciones realizadas por los usuarios, incluyendo estampa de tiempo y justificaciones para cada cambio.**	**Acción realizada por el usuario**	**Registro en el log de la acción realizada**
RF-109	**Notificaciones y Alertas**	**Enviar notificaciones y alertas a los usuarios y administradores sobre cambios importantes, aprobaciones, no aprobaciones y**	**Evento que desencadena la notificación**	**Notificación enviada a los usuarios correspondientes**
		otros eventos relevantes.		
RF-110	**Bloqueo de Usuarios**	**Bloquear usuarios después de un número configurable de intentos fallidos de inicio de sesión.**	**Intentos fallidos de inicio de sesión**	**Usuario bloqueado, notificación de bloqueo**
RF-111	**Maestro de Dependencias**	**Permitir la administración de las dependencias dentro del sistema.**	**Datos de la dependencia (nombre, descripción)**	**Confirmación de la acción realizada (dependencia creada, actualizada, eliminada)**

RF-112	Ver Perfil del Usuario	Permitir a los usuarios ver su perfil, incluyendo el último inicio de sesión.	Solicitud de visualización del perfil	Información del perfil del usuario, incluyendo el último inicio de sesión
RF-113	**Actualizar Datos del Usuario**	**Permitir a los usuarios actualizar sus datos personales.**	**Datos actualizados del usuario**	**Confirmación de actualización de datos**
RF-114	Cerrar Sesión	Permitir a los usuarios cerrar sesión de manera segura.	Solicitud de cierre de sesión	Confirmación de cierre de sesión
RF-115	**Logueo con Autenticación**	**Permitir a los usuarios iniciar sesión con autenticación segura.**	**Credenciales de usuario (nombre de usuario, contraseña)**	**Acceso al sistema, inicio de sesión exitoso**

2.2. Módulo de I/A Seguimiento

Sigla	Propósito	Descripción	Entrada	Salida
RF-201	**Carga de la PQRSDF al sistema**	**Permitir la carga de la PQRSDF de Mercurio o SAC para su lectura.**	**Archivo PQRSDF Digital**	**Confirmación de carga exitosa, reporte de errores o inconsistencias**
RF-202	**Lectura PQRSDF**	**Lectura del documento Digital a través de**	**Archivo(s) digitalizado(s)**	**Documento analizado**
		la IA, tanto de la PQRSDF como de documentos anexos.		

RF-203	**Generar respuesta a PQRSDF**	**A partir de la lectura de la PQRSDF y documentos anexos, con el uso de la inteligencia artificial (IA), si es posible Generar respuesta.**	**Archivo(s) digitalizado(s)**	**Archivo respuesta a PQRSDF**
RF-204	**Recibir respuesta PQRSDF del Respondiente**	**IA recepciona la respuesta generada por el respondiente, valida la concordancia de la respuesta y si esta correcta la envía al sistema Mercurio o SAC, para envió al remitente**	**Respuesta en medio digital recibida del respondiente. Si es acorde a la solicitud, envía documento validado y firmado para que Mercurio o SAC lo remita al solicitante**	**Respuesta PQRSDF entregada a mercurio o SAC.**
RF-205	**Respuesta PQRSDF no adecuada**	**Si acorde a la IA la respuesta dada no esta acorde a la PQRSDF solicitada**	**Respuesta en medio digital recibida**	**Respuesta PQRSDF devuelta al respondiente**

2.3. Clasificación y enrutamiento de la PQRSDF

Sigla	Propósito	Descripción	Entrada	Salida

RF-301	**Enrutar PQRSDF**	**A partir de la lectura PQRSDF y no poder dar respuesta, enrutar solicitud al enlace de la secretaria / Dirección competente para generar su respuesta.**	**PQRSDF leída y analizada a través de la IA**	**Envió de PQRSDF a enlace de la secretaria/Dirección responsable de atender la PQRSDF**
RF-302	**Asignación PQRSDF a respondiente**	**El enlace recibe la PQRSDF y la asigna al funcionario (respondiente) encargado de dar oportuna respuesta**	**Datos actualizados del Plan de Desarrollo**	**Confirmación de actualización del plan**

2.4. Módulo de Respondientes

Sigla	Propósito	Descripción	Entrada	Salida
RF-401	**Seguimiento y respuesta a las PQRSDF recibidas**	**Permitir al respondiente consultar las PQRSDF asignadas y dar respuesta a las mismas.**	**PQRSDF digital y documentos anexos**	**Respuesta de las PQRSDF**
RF-402	**Enviar respuestas de PQRSDF**	**Permitir al respondiente enviar la respuesta de la PQRSDF y actualiza el estado de la PQRSDF.**	**PQRSDF y documentos anexos**	**Respuesta PQRSDF para análisis de IA.**

2.5. Módulo de Reportes

Sigla	Propósito	Descripción	Entrada	Salida
RF-501	Reporte de Accesos	Proporcionar información sobre los accesos al sistema, incluyendo detalles sobre los usuarios que han ingresado, las fechas y horas de acceso, y las acciones realizadas.	Solicitud de reporte de accesos	Reporte de accesos generado
RF-502	Reporte de PQRSDF sin Diligencias	Identificar las PQRSDF que no han sido diligenciados dentro del período establecido.	Solicitud de reporte de PQRSDF sin diligencias	Reporte de PQRSDF sin diligencias generado
RF-503	Reporte de Respuestas a	Mostrar las PQRSDF que han sido corregidos por	Solicitud de la IA sobre las	Reporte de PQRSDF
	PQRSDF Corregidos	el respondiente, incluyendo detalles sobre las modificaciones realizadas, las justificaciones y las fechas de corrección.	PQRSDF corregidos	corregidos generado
RF-504	Reporte de Asignación de las PQRSDF	Listar las PQRSDF asignadas y filtradas por dependencia, por usuario indicando la información sobre su estado.	Solicitud de PQRSDF asignadas	Reporte de Asignacion PQRSDF filtrada

RF-505	Reporte Estado PQRSDF	Proporcionar una visión detallada del estado de las PQRSDF respondidas, por responder en el tiempo adecuado, y las PQRSDF con estado en mora.	Solicitud de reporte de estado de las PQRSDF	Reporte de Estado de PQRSDF
RF-506	Generación de Reportes Personalizados	Permitir a los usuarios generar informes personalizados seleccionando diferentes criterios y parámetros, como fechas, dependencias y otros criterios relevantes.	Solicitud de generación de reportes personalizados	Reporte personalizado generado
RF-507	Aplicación de Filtros Avanzados	Permitir la aplicación de filtros avanzados para refinar los resultados de los reportes, facilitando la identificación de patrones y tendencias.	Solicitud de aplicación de filtros avanzados	Reporte filtrado generado
RF-508	Segmentación de Permisos por Roles	Asegurar que los reportes tengan segmentación de permisos por roles, permitiendo que solo los usuarios autorizados puedan acceder a ciertos reportes.	Datos de roles y permisos	Reportes accesibles según los permisos asignados

3. **Requerimientos no funcionales**

Código	Nombre	Descripción
RNF01	**Look and Feel**	**El aspecto del aplicativo debe ser consistente en todas sus páginas, además de amigable e intuitivo de cara al usuario. La aplicación debe ser responsive.**
RNF02	**Seguridad**	**El protocolo o librería usado para manejar la seguridad en la sesión del usuario debe ser lo suficientemente confiable. La información sensible, como contraseñas, debe manipularse bajo algún nivel de encriptación o cifrado. La aplicación debe estar parametrizada para trabajar con protocolo HTTPS.**
RNF03	**Autenticación**	**Todas las páginas y recursos deben requerir autenticación excepto aquellos específicamente destinados a ser públicos. Todos los campos de contraseña no deben repetir la contraseña del usuario cuando esta ha sido ingresada previamente, los campos de contraseña (o las formas que los contienen) tienen autocompletar desactivado. Todos los controles de autenticación deben fallar de forma segura para garantizar que atacantes no puedan entrar. Las credenciales y toda otra información de identidad a cargo de la aplicación no atraviesan enlaces sin cifrar o con cifrado débil. No debe existir contraseñas por defecto.**
RNF04	**Gestión de Sesión**	**La aplicación usa la gestión de la sesión predeterminada del framework (los desarrolladores no deben implementar su propio gestor de sesiones). Las sesiones se deben invalidar cuando el usuario cierra la sesión. Las sesiones se deben vencer (se cerrarán) después de un período de inactividad especificado. Todas las páginas que requieren autenticación para ser accedidas deben tener vínculos de cierre de sesión. El identificador de sesión no se debe dar a conocer en otro lugar que no sea en las cabeceras de cookies; particularmente se debe evitar su aparición en las URL, mensajes de error y logs. Esto incluye que la aplicación no admita la reescritura de URL de cookies de sesión. El identificador de sesión se debe cambiar o se debe borrar al cerrar la sesión.**
RNF05	**Control de Acceso**	**Los usuarios sólo podrán acceder a funciones o servicios seguros para los que poseen una autorización específica. Los usuarios sólo podrán acceder a las URL seguras para los que poseen una autorización específica. Los usuarios sólo podrán acceder a los archivos seguros para los que poseen una autorización específica. Las referencias directas a objetos deberán estar protegidas, de forma que cada usuario sólo pueda acceder a objetos autorizados. La navegación de directorios deberá estar deshabilitada a menos que se desee de forma deliberada. Los usuarios sólo podrán acceder a los datos protegidos para los que poseen una autorización específica (por ejemplo, la protección contra la**

		manipulación de referencias directas a objetos). Los controles de acceso deberán fallar de forma segura.
RNF06	**Validación de Datos**	**El entorno (o sistema) en tiempo de ejecución no deberá ser susceptible a desbordamientos de búfer, o deberán existir controles de seguridad para prevenir desbordamientos de búfer. El entorno (o sistema) en tiempo de ejecución no deberá ser susceptible a la inyección de SQL, o deberán existir controles de seguridad para prevenir la inyección de SQL. El entorno (o sistema) en tiempo de ejecución no deberá ser susceptible a Cross Site Scripting (XSS), o deberán existir controles de seguridad para prevenir XSS. El entorno (o sistema) en tiempo de ejecución no deberá ser susceptible a Inyección de comandos del sistema operativo, o deberán existir controles de seguridad para prevenir la inyección de**
		comandos del sistema operativo. Todos los errores de validación de entrada deberán dar como resultado el rechazo de la entrada o la desinfección de entrada. Todas las rutinas de validación de entrada o de codificación se deberán realizar y se deben hacer cumplir del lado del servidor. Se deberá verificar que todos los datos de salida no confiables que son emitidos a HTML (incluyendo elementos HTML, atributos HTML, los valores de datos de JavaScript, CSS, bloques y atributos URI) son adecuadamente escapados al contexto de aplicación.
RNF07	**Control de Errores y Registro**	**La aplicación no deberá emitir mensajes de error o "stack traces" que contienen datos confidenciales que podrían ayudar a un atacante, incluyendo identificador de sesión e información personal.**
RNF08	**Protección de Datos**	**Todos los formularios que contienen información sensible deberán tener desactivado el almacenamiento en caché del lado del cliente, incluidas las funciones de autocompletado. Todos los datos confidenciales se deberán enviar al servidor en el cuerpo del mensaje HTTP (es decir, los parámetros de URL nunca son utilizados para enviar datos sensibles).**

RNF09	**Seguridad HTTP**	**La aplicación sólo deberá aceptar un conjunto definido de métodos de petición HTTP, como GET y POST y los métodos no utilizados se bloquean de forma explícita. Las respuestas HTTP deberán contener un content-type header que especifica un conjunto seguro de caracteres (por ejemplo, UTF-8).**
RNF10	**Archivos y Recursos**	**Los redireccionamientos de URL no deberán incluir datos no validados. Los nombres de archivos y rutas de datos obtenidos de fuentes no confiables deberán ser procesados para prevenir ataques.**
RNF11	**Confidencialidad**	**Toda la información otorgada por los usuarios se manipulará únicamente con fines corporativos y de manera limpia.**
RNF12	**Integridad de Datos**	**Todos los datos alojados en el sistema y su base de datos deberán gozar de integridad referencial, sin permitir registros huérfanos.**
RNF13	**Rendimiento**	**La aplicación debe ser capaz de manejar múltiples usuarios simultáneamente sin degradar el rendimiento. Las operaciones críticas deben completarse en un tiempo razonable, garantizando una experiencia de usuario fluida.**
RNF14	**Escalabilidad**	**La aplicación debe ser escalable para adaptarse a futuros aumentos en la cantidad de datos y usuarios. Debe soportar tanto el escalado horizontal como vertical.**
RNF17	**Interoperabilidad**	**La aplicación debe ser interoperable con otras plataformas y sistemas utilizados por la Gobernación de Antioquia, facilitando la integración y el intercambio de información.**
RNF18	**Mantenimiento**	**La aplicación debe ser fácil de mantener y actualizar. Debe contar con documentación completa y actualizada, así como con un sistema de soporte para ayudar a los usuarios a resolver problemas y entender cómo utilizar las funcionalidades del sistema.**
RNF22	**Tiempo de Inactividad de Sesión**	**Las sesiones de usuario deben expirar automáticamente después de un período de inactividad configurable. Esto ayuda a proteger la información en caso de que un usuario deje su dispositivo desatendido.**