BOGOTÁ

SUBSECRETARÍA DE SERVICIO A LA CIUDADANÍA - DIRECCIÓN DEL SISTEMA DISTRITAL DE SERVICIO A LA CIUDADANÍA

ANEXO TÉCNICO - MÓDULO ADMINISTRACION Y PLANEACION DEL SERVICIO DE LA RED CADE DEL DISTRITO

Tabla de contenido

1. Identificación de la necesidad 2
2. Objeto 5
3. Alcance 6
4. Contexto Tecnológico de la Plataforma y Software de Base. 7
   a. Contexto de la Plataforma de la Red CADE 7
   b. Descripción del esquema de integración. 12
   c. Integración de la capa de presentación. 12
   f. Integración de servicios backend 13
   g. Manejo de identidad y seguridad. 14
   h. Manejo de navegación dentro de la plataforma unificada. 15
   i. Independencia funcional del módulo. 15
   j. Componentes tecnológicos de la Plataforma Unificada de Servicios de la Red CADE. 15
   i. Características y componentes tecnológicos de la Plataforma Unificada de servicios de la Red CADE 19
5. Especificaciones Técnicas. 21
6. Requerimientos No Funcionales. 32
7. Transferencia de Conocimiento. 34
8. Acuerdos de Niveles de Servicio (ANS). 35
9. Equipo de trabajo mínimo requerido. 37
10. Obligaciones 43
    10.1 Obligaciones generales del Contratista. 43
    10.2 Obligaciones Específicas del Contratista. 44
11. Plazo de Ejecución. 47
12. Garantía y soporte de la solución. 47
    12.1 Garantía. 47

12.2. Soporte de la solución. 47
13. Localización. 48
14. Glosario. 49
15. Anexos. 51

1. Identificación de la necesidad

La Secretaría General de la Alcaldía Mayor de Bogotá D.C., a través de la Subsecretaría de Servicio a la Ciudadanía, realiza la formulación, adopción, dirección de la implementación, seguimiento y evaluación de las políticas, planes y programas de atención y prestación de los servicios distritales a la ciudadanía y de acercamiento de la Administración Distrital, así como la articulación de la gestión intersectorial de Servicio a la Ciudadanía y el liderazgo en el desarrollo y consolidación del Sistema Distrital de Servicio a la Ciudadanía, con el fin de fortalecer la articulación interinstitucional y satisfacer las necesidades y expectativas de la ciudadanía y partes interesadas.1

En desarrollo de estas competencias, se adoptó la "Política Pública Distrital de Servicio a la Ciudadanía 2026-2035", mediante el Documento CONPES 42, cuyo objetivo general es "Garantizar una oferta distrital de servicios digna, accesible y de calidad, a través de un modelo integrado que reconozca la diversidad de la ciudadanía, se anticipe y responda a sus necesidades y fortalezca una relación proactiva, empática y confiable entre la Administración y las personas".

En este contexto, la Red CADE, entendida como el ecosistema integral, sostenible y de iteración ciudadana, mediante el cual el Distrito garantiza a la ciudadanía un acceso ágil, cercano y oportuno a la oferta institucional, así como la agregación y articulación de la oferta institucional en canales de atención compartidos, dispuestos por la Secretaría General de la Alcaldía Mayor de Bogotá, D.C, se convierte en un actor relevante para el cumplimiento de los objetivos de la Política Pública.

Los canales de atención que componen la Red CADE son los siguientes: Canal Presencial: SuperCADE, CADE, SuperCADE Móvil y CADE Exprés; Canal de voz y video: Línea 195 Bogotá y Canal Virtual: Portal transaccional de servicio a la ciudadanía, Asistentes conversacionales y Sistema distrital para la gestión de peticiones ciudadanas - Bogotá Te Escucha. 2

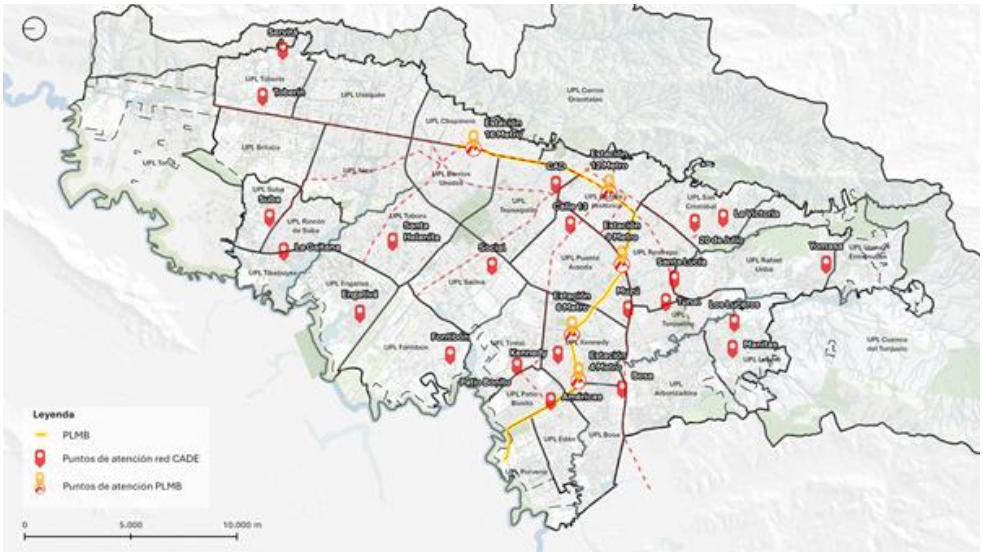
En la actualidad, el canal presencial de la Red CADE cuenta con 22 puntos de atención CADE y Super CADE distribuidos en todo Bogotá y dentro de la Línea 1 del Metro se prevé la presencia de otros 5 puntos. Esto facilita el acceso a la información y servicios y la realización de trámites, en los cuales convergen aproximadamente 50 entidades, entre

[1] Artículo 32, Numerales 1, 2, 3 y 7 del Decreto Distrital 640 de 2025 "Por medio del cual se expide el Decreto Único del Sector Gestión Pública."

[2] Artículo 266 del Decreto 207 del 03 de junio de 2026 "Por medio del cual se modifica la parte 1 del libro 2 y se sustituye el título 10 de la parte 2 del libro 3 del Decreto Distrital 640 de 2025 único del Sector Gestión Pública, respecto a los lineamientos en materia de Servicio a la Ciudadanía y se dictan otras disposiciones".

distritales, nacionales y privados y se prestan cerca de 588 trámites y servicios, con una alta demanda de atención ciudadana. Durante la vigencia 2025 y los cinco primeros meses de la vigencia 2026, el canal presencial de la Red CADE realizó un total de 3.903.841 interacciones, lo cual equivale a un promedio de 229.638 interacciones mensuales, es decir, cerca de 9.300 interacciones diarias en promedio. A lo anterior se suman las cifras de pagos y transacciones que se hacen en los puntos presenciales de la Red CADE que en 2025 llegaron a 2.5 millones y desde enero hasta abril de 2026 se han realizado cerca de 723.000.

Imagen 1. Distribución de los Puntos de Atención Presencial de la Red CADE



Fuente: Dirección del Sistema Distrital de Servicio a la Ciudadanía – DSDSC

En términos de infraestructura, la Red CADE cuenta con 30.637 metros cuadrados y cerca de 1.000 espacios para la prestación de los servicios y la operación. Dichos espacios están compuestos por módulos, locales, oficinas, auditorios, áreas de pago y recaudo, entre otros.

De otra parte, el personal vinculado a la operación de la Red CADE asciende aproximadamente a 1.020 personas, de las cuales cerca de 194 pertenecen a la Secretaría General y las restantes a las entidades públicas y actores privados que hacen presencia en los puntos de atención.

Atendiendo a las cifras expuestas se puede indicar que el canal presencial de la Red CADE ha tenido una evolución favorable; sin embargo, en la actualidad enfrenta importantes retos frente a las dinámicas de ciudad, la velocidad de cambios tecnológicos, las nuevas formas de relacionamiento con los ciudadanos y mayores exigencias en respuestas a demandas y expectativas ciudadanas.

Particularmente se han detectado los siguientes desafíos:

1. La infraestructura actual presenta limitaciones en la funcionalidad de los espacios, deficiencias en accesibilidad y mobiliario inadecuado, lo que impacta la calidad de la atención, la eficiencia operativa y la experiencia de los usuarios.
2. En cuanto al modelo de atención, aún existen tiempos elevados de espera y atención o límites en el número de atenciones diarias por parte de las entidades debido a modelos basados en capacidad de atención.
3. Frente al componente tecnológico, existe una baja incorporación de servicios digitales para el servicio a la ciudadanía, al igual que ausencia de herramientas que soporten la operación, seguimiento y toma de decisiones.

En respuesta a estas problemáticas, en el año 2025 la Secretaría General de la Alcaldía Mayor de Bogotá contrató el diseño de un modelo de operación integral y sostenible de la Red CADE con la finalidad de garantizar el acceso a la ciudadanía a la oferta institucional del Distrito de manera oportuna, ágil y cercana. Dicho modelo integral y sostenible incluye tres componentes, uno de los cuales es el de Inteligencia.

Dentro de este componente, uno de los aspectos relevantes del nuevo modelo contempla la existencia de una plataforma tecnológica de administración de la Red CADE, es decir, un sistema integrado de gestión, análisis y apoyo a la toma de decisiones, orientado a garantizar la operación sostenible, pertinente y centrada en la experiencia ciudadana de la Red. Su objetivo principal es consolidar información estratégica, operativa y perceptual en un único entorno, permitiendo a los equipos directivos y técnicos:

- Mantener visibilidad continua del estado general de la Red.
- Identificar de manera anticipada riesgos y oportunidades.
- Priorizar acciones de intervención con base en evidencia.
- Alinear decisiones territoriales, operativas y de servicio con la demanda real de los ciudadanos.

Así las cosas, la plataforma tecnológica de administración de la Red CADE debe tener capacidades analíticas y de planeación ya que su propósito es transformar los datos operativos y territoriales de la Red en insumos para la toma de decisiones estratégicas.

En este sentido, la operación de la Red CADE implica la gestión articulada de infraestructura, servicios y, de manera especial, del personal que interviene en la prestación de los servicios a la **ciudadanía**, lo cual conlleva la planificación, asignación y seguimiento diario del personal en los diferentes puntos de atención, la coordinación de turnos, la administración de novedades administrativas y el control de la disponibilidad del personal.

En este aspecto de gestión del personal de la Red CADE, en la actualidad se evidencian limitaciones en su administración y operación, entre las cuales se destacan:

- La existencia de varias fuentes de información, generalmente en excel, que consolidan datos sobre las personas que laboran en los puntos de atención de la Red CADE y

cuyo, actualización, gestión y acceso, resultan difíciles para la planeación y el seguimiento del componente humano de la Red.

- Dificultad para realizar procesos de planeación del servicio como la asignación de personal a los puntos de atención, la programación de turnos y roles en cada punto de atención y la gestión de novedades administrativas.
- No se cuenta con mecanismos automatizados que permitan consolidar y analizar información en tiempo real sobre la operación y el servicio, lo que limita la generación de reportes, el seguimiento a indicadores y la toma de decisiones.

Esta situación impacta directamente la eficiencia operativa, los tiempos de respuesta, incrementa la carga laboral, genera dependencia de tareas manuales, eleva el riesgo de errores en el registro, actualización y consulta de la información, entre otros, lo que limita la capacidad de la Dirección del Sistema Distrital de Servicio a la Ciudadanía para contar con una visión integral de su operación, fortalecer los procesos de control administrativo, planear y gestionar la atención y servicio y disponer de insumos confiables para la toma de decisiones. En este sentido, se hace necesario analizar, diseñar, desarrollar, integrar e implementar un módulo de administración y gestión del servicio para la plataforma unificada de servicios de la Red CADE3, con el fin de fortalecer la gestión administrativa y el servicio, mediante la recolección, registro, administración, acceso y análisis de la información asociada al personal de la Red CADE y la automatización de procesos relacionados con la planeación del servicio.

Dicho módulo deberá permitir, entre otros aspectos, la asignación y programación del personal en sus diferentes roles de servicio diarios, la gestión de novedades administrativas, la trazabilidad y seguimiento de las actividades operativas y la generación de reportes e indicadores para la toma de decisiones.

Adicionalmente, el módulo deberá facilitar una gestión más ágil y eficiente de las situaciones administrativas del personal y permitir el diseño e implementación de tableros de control para la visualización de reportes e indicadores asociados a la administración del personal, contribuyendo al mejoramiento continuo en la prestación del servicio a la ciudadanía en los puntos de atención de la Red CADE.

En atención a lo anteriormente expuesto y en el marco del fortalecimiento de la gestión operativa de la Red CADE, la Secretaría General de la Alcaldía Mayor de Bogotá D.C. requiere la contratación del análisis, diseño, desarrollo, integración e implementación de un módulo para la administración y planeación del servicio de la Red CADE.

2. Objeto

Realizar el análisis, diseño, desarrollo, integración e implementación de un módulo para la Plataforma Unificada de Servicios de la Red CADE que permita centralizar la información

[3] La plataforma unificada de servicios de la Red CADE es una solución tecnológica de la Secretaría General que integrará en un único espacio el sistema actual de Asignación de Turnos - SAT y los futuros módulos relacionados con la Red CADE, tales como el módulo de administración de espacios, el módulo de registro de puntos de atención, entre otros. Esta plataforma permitirá centralizar la información y mejorar la eficiencia en la operación de la Red CADE.

del personal vinculado a la Red, mejorar su planificación y asignación, el control administrativo y soportar la toma de decisiones basada en datos.

3. Alcance

El contratista deberá realizar el análisis, diseño, desarrollo, pruebas, implementación y transferencia de conocimiento del módulo de gestión de personal, el cual debe integrarse como componente funcional a la Plataforma Unificada de Servicios de la Red CADE, qué permita centralizar, automatizar e integrar la gestión del personal, garantizando seguridad, trazabilidad e interoperabilidad, a través de la ejecución como mínimo de las siguientes fases:

- **Fase 1 - Análisis y Planeación:** Para esta fase se deberá realizar el levantamiento, validación y priorización de requerimientos funcionales y no funcionales, garantizando las necesidades de los equipos de trabajo y los procesos y procedimientos del Sistema Integrado de Gestión de la Secretaría General, a fin de asegurar una ejecución consistente y trazable.

- **Fase 2 - Diseño:** Se deberá realizar el diseño técnico y funcional detallado del módulo de administración y planeación del servicio de la Red Cade, de acuerdo con el alcance señalado en el numeral 5 de este documento. Dicho diseño debe incluir la definición de la arquitectura lógica y técnica del sistema, bajo el modelo de microservicios y microfrontend conforme a los lineamientos de la plataforma unificada de servicios de la Red CADE.

  Además, el contratista deberá examinar los criterios y controles de seguridad con la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC para el cumplimiento normativo (protección de datos, gobierno digital) y es transversal para la fase de desarrollo.

- **Fase 3 - Desarrollo:** En esta fase se deberá desarrollar el módulo administración y planeación del servicio de la Red CADE, en los tiempos acordados, conforme a lineamientos validados en la Fase 2 y cumpliendo los criterios de calidad y seguridad exigidos.

- **Fase 4 - Pruebas (QA/UAT):** La ejecución integral de pruebas QA/UAT del módulo de administración y planeación del servicio de la Red Cade, deberá incluir pruebas funcionales, no funcionales carga y estrés sobre el módulo de administración y planeación del servicio de la Red Cade. Así mismo, se deberá realizar la validación de reglas de negocio, controles de seguridad aplicados (RBAC, cifrado, DLP y auditoría uniforme), la verificación de trazabilidad de las operaciones end-to-end y la validación de la calidad y consistencia de los datos frente a las fuentes internas del sistema.

- **Fase 5 - Instalación y puesta en operación:** En esta fase se realizará la instalación y despliegue del sistema de módulo de administración y planeación del servicio de la Red Cade, desarrollado en ambientes de certificación y producción, que incluya la

implementación de los componentes del módulo y base de datos en la infraestructura aprovisionada por la entidad, la configuración de integraciones con sistemas internos, la aplicación de los controles de seguridad definidos, la habilitación de mecanismos de monitoreo y auditoría y la validación de la operación end to end del módulo conforme a los criterios técnicos y funcionales aprobados.

- **Fase 6 - Apropiación y transferencia de conocimiento (Componente Transversal):** Se deberá realizar la ejecución de sesiones de transferencia de conocimiento a usuarios funcionales y técnicos, que incluyan la socialización del diseño aprobado, la arquitectura del sistema, la operación del módulo implementado, los flujos funcionales, el uso de tableros de control y las buenas prácticas para la administración y soporte del sistema, dirigidas al equipo de la Dirección del Sistema Distrital de Servicio a la Ciudadanía -DSDSC y la Oficina de Tecnologías de la Información y las Comunicaciones -OTIC.

4. Contexto Tecnológico de la Plataforma y Software de Base.

Actualmente la Red CADE cuenta con el sistema SAT WEB (Sistema de asignación de turnos), el cual soporta los procesos de asignación y gestión de turnos para el acceso a la red de puntos de atención presenciales de la Red CADE. Adicionalmente, se encuentran en proceso de implementación otros módulos funcionales relacionados con la gestión de espacios y operación de los puntos de atención.

Con el fin de consolidar estos sistemas y facilitar su evolución, se está trabajando en la construcción de una Plataforma Unificada de Servicios para la Red CADE, en la cual distintos módulos funcionales se integran dentro de un mismo entorno tecnológico.

Esta plataforma permitirá ofrecer una experiencia de acceso unificada para los usuarios, al tiempo que posibilita que cada módulo evolucione de manera independiente, manteniendo su propia lógica de negocio y sus servicios backend.

a. Contexto de la Plataforma de la Red CADE

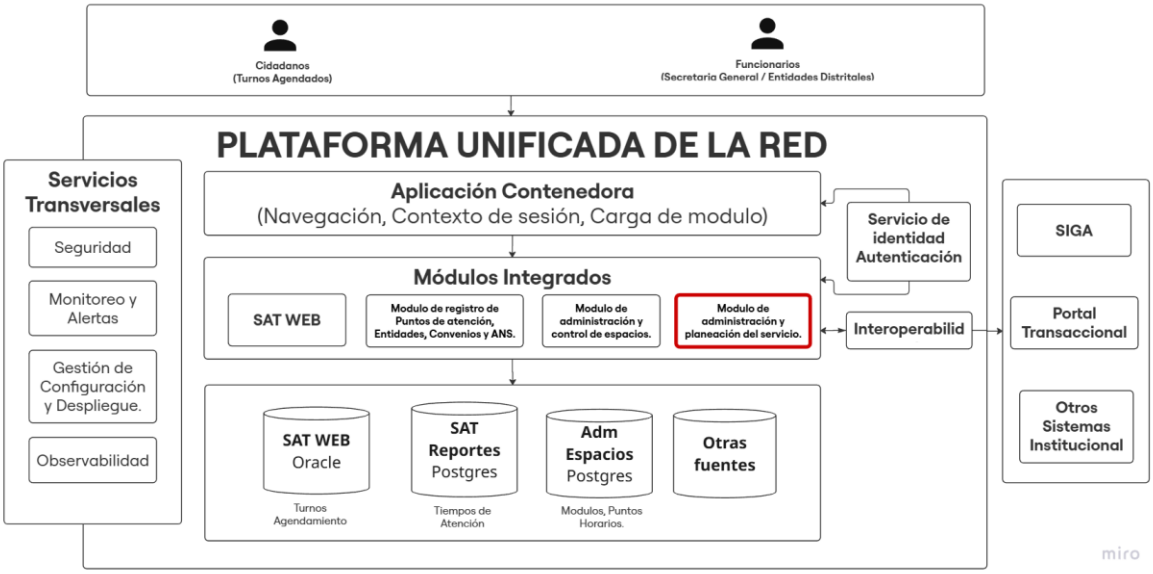
La Plataforma Unificada de Servicios de la Red CADE constituye el punto de acceso centralizado para los usuarios que hacen parte del ecosistema tecnológico de la entidad, incluyendo ciudadanos que agendan turnos, funcionarios de la Secretaría General y de las entidades distritales, así como otros sistemas institucionales que requieren interoperar con los servicios de la plataforma.

A través de una aplicación contenedora, la plataforma gestiona la autenticación, la navegación unificada, el contexto de sesión y la integración de los distintos módulos funcionales que la componen. Este enfoque permite ofrecer una experiencia de usuario consistente y facilita la incorporación progresiva de nuevos módulos dentro de un entorno tecnológico común.

La Plataforma Unificada de Servicios de la Red CADE se construye tomando como referencia la experiencia tecnológica existente en sistemas institucionales actualmente en operación, particularmente el sistema de asignación de turnos SAT WEB. Este sistema constituye uno de los componentes funcionales del ecosistema actual y se espera que evolucione progresivamente para integrarse al modelo de plataforma unificada, manteniendo su independencia funcional y tecnológica.

La Figura 2 presenta una vista conceptual de la arquitectura de la Plataforma Unificada de Servicios de la Red CADE, en la cual se observa la interacción entre los usuarios, la aplicación contenedora, los módulos funcionales integrados, los servicios de interoperabilidad y los repositorios de datos asociados a cada módulo, así como los servicios transversales que soportan la operación de la solución.

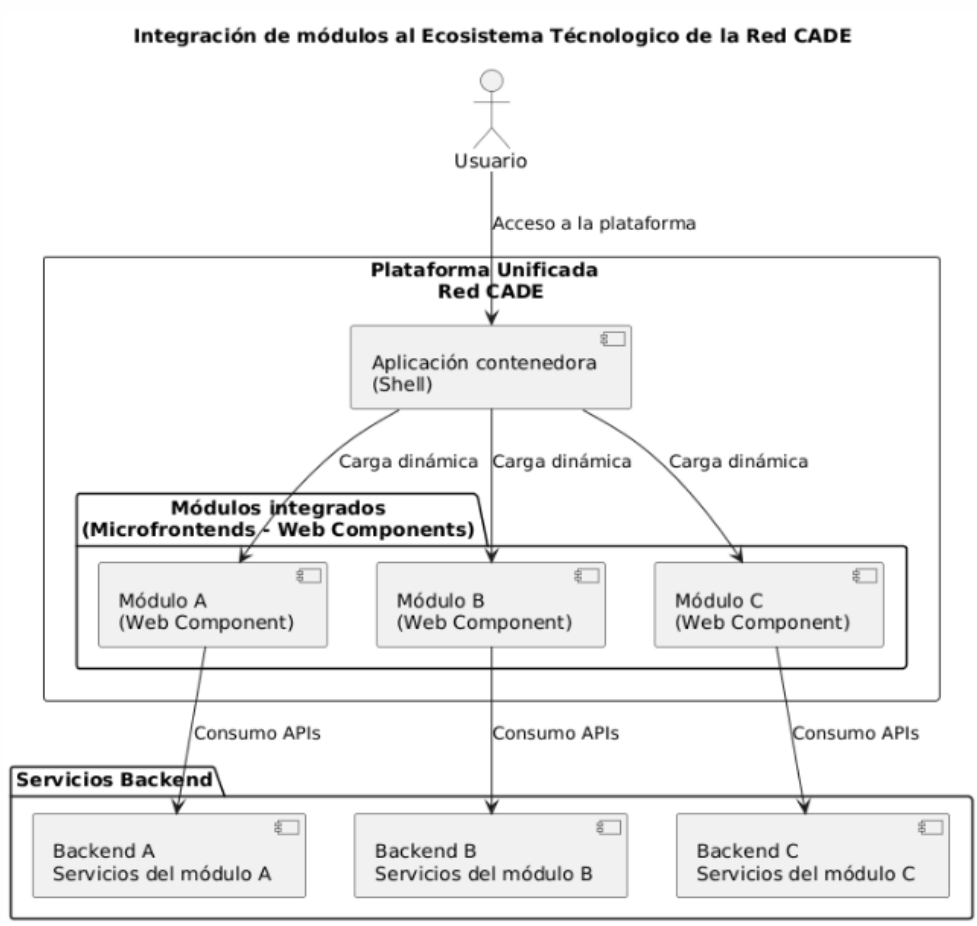
Imagen 2. Arquitectura conceptual de la Plataforma Unificada de servicios de la Red CADE



Fuente: Elaboración propia

Dentro de la plataforma, cada módulo se integra mediante un microfrontend en formato Web Component, el cual es cargado dinámicamente por la aplicación contenedora cuando el usuario accede a las opciones de navegación correspondientes. Este enfoque permite incorporar nuevos módulos de forma desacoplada, sin afectar el funcionamiento de los demás componentes de la plataforma.

Imagen 3. Modelo de integración de módulos mediante microfrontends



Fuente: Elaboración propia

Los microfrontends que se integren a la Plataforma Unificada de Servicios de la Red CADE deberán cumplir los lineamientos de arquitectura, diseño, interoperabilidad, versionamiento y gobierno tecnológico definidos por la OTIC, con el fin de garantizar la consistencia en la experiencia de usuario y la sostenibilidad técnica de la solución.

En este sentido, cada microfrontend deberá:

- Ajustarse a los lineamientos institucionales de experiencia de usuario, diseño visual, accesibilidad, usabilidad y navegación.
- Cumplir los mecanismos de integración definidos por la plataforma base para autenticación, autorización, contexto de sesión, intercambio de información y consumo de servicios.

- Adoptar esquemas de versionamiento, empaquetado, despliegue y compatibilidad que permitan su evolución controlada e independiente, sin afectar la operación de los demás módulos.
- Atender las directrices de gobierno tecnológico, seguridad, trazabilidad, monitoreo, documentación técnica y administración del ciclo de vida establecidas por la OTIC.
- Garantizar compatibilidad con los catálogos, menús, privilegios y mecanismos de carga dinámica definidos por la aplicación contenedora.

El cumplimiento de estos lineamientos será obligatorio para todos los módulos que hagan parte de la Plataforma Unificada de Servicios de la Red CADE, con independencia de su autonomía funcional o tecnológica.

Los módulos integrados mantienen su propia lógica de negocio y operan de forma independiente mediante sus respectivos servicios backend. De esta manera, cada módulo puede evolucionar, desplegarse y escalarse de manera autónoma, mientras que la plataforma unificada se encarga de proporcionar los mecanismos transversales de autenticación, navegación y contexto de operación.

Adicionalmente, la plataforma cuenta con servicios transversales que soportan la operación de la solución, tales como seguridad, monitoreo y alertas, gestión de configuración y despliegue, y observabilidad, los cuales permiten asegurar la disponibilidad, trazabilidad y control operativo de los distintos componentes que conforman el ecosistema tecnológico de la Red CADE.

Este modelo de integración permite consolidar múltiples módulos dentro de una misma plataforma institucional, garantizando una experiencia de usuario unificada y al mismo tiempo, preservando la independencia funcional y tecnológica de los módulos que lo componentes

En relación con la interfaz de usuario, los microfrontends deberán adoptar los lineamientos de diseño, componentes visuales y patrones de experiencia definidos por la Entidad. Para tal fin, la Entidad suministrará al inicio del proyecto los lineamientos de UI, librerías institucionales y/o design system que deban ser utilizados, así como los criterios de integración con la aplicación contenedora (Shell). El uso de estos lineamientos será obligatorio, con el fin de garantizar la coherencia visual, la consistencia en la experiencia de usuario y la integración homogénea de los módulos dentro de la Plataforma Unificada.

En relación con el consumo de servicios backend, la Plataforma contempla el uso de un API Gateway como componente de integración, el cual centraliza la exposición, gestión y control de las APIs de los distintos módulos. En este sentido, los microfrontends no deberán consumir directamente los servicios backend de manera independiente, sino a través de los mecanismos definidos por la arquitectura de la plataforma.

Los lineamientos específicos de enrutamiento, seguridad, autenticación y consumo de APIs serán definidos y entregados por la Entidad al inicio del proyecto, garantizando la correcta integración con el proveedor de identidad (Keycloak) y el cumplimiento de los estándares de interoperabilidad, seguridad y gobierno de APIs establecidos por la OTIC.

b. Descripción del esquema de integración.

Los módulos que se integren a la Plataforma Unificada de Servicios de la Red CADE deberán ajustarse al modelo arquitectónico definido por la Entidad, el cual se basa en una aplicación contenedora, un proveedor central de identidad y la incorporación de funcionalidades mediante microfrontends desacoplados, tal como se ilustra en la arquitectura conceptual de la Plataforma Unificada.

En este contexto, los módulos funcionales que formen parte del ecosistema de la Plataforma Unificada deberán diseñarse de forma compatible con los mecanismos de autenticación, navegación y contexto definidos por la plataforma base, garantizando su interoperabilidad con el resto de sus componentes.

c. Integración de la capa de presentación.

Los módulos funcionales deberán integrarse a la Plataforma Unificada mediante el modelo de microfrontend en formato Web Component, conforme a los lineamientos definidos por la Entidad. Este enfoque permite que cada módulo sea desarrollado, evolucionado y desplegado de forma desacoplada, sin afectar la estabilidad de los demás componentes de la solución.

Los microfrontends deberán ser compatibles con los mecanismos de integración definidos por la plataforma (por ejemplo, carga dinámica en la Shell, manejo de contexto, eventos y comunicación con el contenedor), asegurando su correcta interacción dentro del ecosistema de la Plataforma Unificada

Con el fin de facilitar la integración temprana, se proporcionará acceso a un entorno de integración de la Plataforma Unificada. Este acceso permitirá validar la correcta incorporación, visualización y funcionamiento de los módulos dentro del contenedor de la plataforma.

El contratista deberá suministrar los artefactos necesarios para la integración (por ejemplo, URL, recursos estáticos o builds del microfrontend), garantizando su compatibilidad con los lineamientos definidos

Es importante precisar que no se entregará el código fuente de la Shell ni del proveedor de identidad, sino únicamente los accesos y configuraciones requeridas para la integración, pruebas y validación dentro de los entornos habilitados.

d. Distribución de Responsabilidades.

La arquitectura se basa en una separación clara de funciones:

- Aplicación Contenedora (Shell): Es la responsable de la autenticación, la navegación global, la gestión del contexto de sesión y la carga dinámica de los microfrontends cuando el usuario accede a las opciones correspondientes, está desarrollada en Angular v21 y expondrá los lineamientos, contratos de integración y mecanismos de comunicación necesarios para la incorporación de los microfrontends (basados en Web Components), incluyendo el manejo de contexto, eventos y la interacción con el contenedor.

Así mismo, la Entidad proporcionará la documentación técnica del Shell y un entorno de integración (sandbox) que permitirá validar la correcta carga, visualización y funcionamiento de los microfrontends desde etapas tempranas del proyecto.

- Módulos Funcionales: Cada módulo mantiene la responsabilidad exclusiva sobre su lógica de negocio, servicios backend, reglas funcionales y su interfaz de usuario.

e. Requisitos de Integración para el Contratista.

Para garantizar la interoperabilidad, el módulo desarrollado deberá cumplir con los siguientes estándares:

- Formato de Entrega: Exponer su interfaz como un Web Component compatible con la aplicación contenedora.
- Gestión de Contexto: Permitir la inicialización dinámica a partir del contexto suministrado por el contenedor, el cual incluye:
  - Token de autenticación.
  - Información básica del usuario y rol activo.
  - Contexto operativo (ej. sede o punto de atención seleccionado).
- Autonomía: Gestionar internamente su estado inicial y lógica a partir de la información del contexto recibido.
- Interoperabilidad: Garantizar la compatibilidad con los mecanismos de gestión de eventos y comunicación entre componentes definidos por la Entidad.

f. Integración de servicios backend.

Cada módulo integrado deberá contar con sus propios servicios backend responsables de la lógica funcional del sistema.

Estos servicios deberán:

- Exponer APIs REST seguras para el consumo del microfrontend correspondiente.
- Utilizar el token de autenticación emitido por el proveedor de identidad institucional para validar las solicitudes.
- Gestionar internamente la lógica de negocio, las reglas funcionales y la autorización específica del dominio.

La aplicación contenedora de la Plataforma Unificada no administra la lógica funcional de los módulos integrados; su función principal es gestionar la autenticación, la navegación, el contexto de sesión y la carga dinámica de los microfrontends.

Las tecnologías, versiones y frameworks utilizados en los servicios backend (como Java, Spring Boot u otros) deberán definirse durante la fase de análisis y diseño, empleando siempre versiones estables, soportadas y alineadas con los lineamientos técnicos de la OTIC. Los servicios deberán garantizar compatibilidad con la arquitectura de la Plataforma Unificada, incluyendo estándares de seguridad, interoperabilidad, versionamiento de APIs y buenas prácticas de desarrollo. Asimismo, cualquier decisión tecnológica deberá ser

validada con la Entidad, asegurando su sostenibilidad, mantenibilidad y adecuada integración con los componentes existentes.

En relación con el uso de frameworks, componentes de terceros y librerías open source, el contratista podrá proponer las tecnologías que considere adecuadas durante la fase de análisis y diseño. Estas deberán ser evaluadas y validadas por la OTIC, con el fin de garantizar su alineación con los lineamientos de arquitectura, seguridad y sostenibilidad de la Entidad. En todo caso, las tecnologías seleccionadas deberán corresponder a versiones estables y con soporte activo, y no deberán presentar restricciones de licenciamiento que afecten la operación, mantenimiento o evolución de la solución dentro del entorno institucional

En relación con la tecnología de base de datos, el contratista podrá proponer el motor o motores que considere más adecuados durante la fase de análisis y diseño de la solución, en función de los requerimientos funcionales, de desempeño y de escalabilidad del módulo. La propuesta podrá contemplar el uso de uno o más motores de base de datos, siempre que dicha decisión se encuentre debidamente justificada desde el punto de vista técnico y arquitectónico. En todos los casos, la tecnología seleccionada deberá ser evaluada y validada por la OTIC, garantizando su alineación con los lineamientos institucionales de arquitectura, seguridad, interoperabilidad y sostenibilidad.

Para el módulo objeto del presente proceso, se contempla que este contará con un esquema de base de datos propio, garantizando el aislamiento lógico de la información frente a otros módulos. La implementación de dicho esquema (como base de datos independiente o como esquema dentro de una instancia compartida) dependerá de los requerimientos técnicos, de desempeño y de escalabilidad definidos durante la fase de análisis y diseño, así como de los lineamientos y validación de la OTIC

g. Manejo de identidad y seguridad.

La autenticación de usuarios será gestionada por el proveedor central de identidad de la Plataforma (Keycloak), el cual será responsable de:

- Validar las credenciales de los usuarios
- Emitir los tokens de autenticación
- Administrar la sesión del usuario
- Gestionar los roles o grupos de acceso de alto nivel.
- Los módulos integrados deberán consumir estos tokens para validar el acceso a sus servicios backend.

Los roles emitidos por el proveedor de identidad (Keycloak) deberán utilizarse como roles de acceso general, mientras que los permisos funcionales específicos del módulo deberán ser administrados por el propio módulo.

La definición de los roles de alto nivel del módulo deberá realizarse durante la fase de análisis y diseño, en conjunto con los equipos funcionales de la Entidad, de acuerdo con los perfiles y necesidades operativas del sistema. Una vez definidos, dichos roles deberán ser formalmente solicitados a la OTIC para su configuración e implementación en el proveedor de identidad (Keycloak), garantizando su correcta integración con el modelo de autenticación y autorización de la Plataforma

En caso de requerirse la integración con servicios institucionales de directorio (como LDAP), esta se realizará a través del proveedor de identidad de la Plataforma (Keycloak). En consecuencia, los módulos no deberán integrarse directamente con el directorio institucional, sino consumir la información de usuario disponible en los tokens de autenticación y/o en los servicios definidos por la plataforma, garantizando la coherencia con el modelo de identidad centralizado

h. Manejo de navegación dentro de la plataforma unificada.

Las opciones de navegación del módulo deberán ser registradas en la aplicación contenedora mediante el catálogo de menús definido para el portal.

Esto permitirá que:

- La estructura del menú de la Plataforma se construya dinámicamente según los privilegios del usuario.
- El microfrontend del módulo sea cargado automáticamente al seleccionar la opción correspondiente.
- La visibilidad de las opciones dependa de los privilegios de navegación definidos en la Plataforma.

La inclusión de una opción dentro del menú del portal no implica autorización funcional dentro del módulo integrado, la cual deberá ser validada por el propio módulo.

i. Independencia funcional del módulo.

Cada módulo integrado deberá conservar la autonomía sobre:

- Su modelo de datos.
- Su lógica de negocio.
- Sus reglas funcionales.
- La administración de permisos operativos específicos.

La Plataforma Unificada provee los mecanismos transversales de identidad, navegación, interoperabilidad y contexto de sesión, mientras que la lógica funcional y las reglas de negocio permanecen bajo responsabilidad del módulo integrado.

j. Componentes tecnológicos de la Plataforma Unificada de Servicios de la Red CADE.

La Plataforma Unificada de Servicios de la Red CADE se soporta sobre un conjunto de componentes tecnológicos que permiten gestionar la autenticación, la capa de presentación, los servicios transversales de la plataforma y el almacenamiento de información de configuración.

La selección de estos componentes se realiza tomando como referencia la arquitectura tecnológica definida por la Entidad, en la cual se establecen los lineamientos para la integración de servicios, gestión de identidad, interoperabilidad, procesamiento de datos, monitoreo y operación de la solución. Estos componentes han sido seleccionados bajo criterios de escalabilidad, modularidad, interoperabilidad y uso de tecnologías ampliamente adoptadas, empleando versiones estables y soportadas que permitan garantizar la sostenibilidad técnica de la plataforma.

Los componentes tecnológicos descritos a continuación corresponden a los elementos utilizados para soportar la operación de la Plataforma:

- ***Gestión de identidad***

La Plataforma Unificada utiliza Keycloak como proveedor central de identidad, encargado de la autenticación de usuarios, la gestión de sesiones y la emisión de tokens de seguridad.

En este modelo, la autenticación es gestionada de forma centralizada por la plataforma, por lo que los módulos integrados mediante microfrontends no deberán implementar mecanismos propios de autenticación en el flujo productivo.

Los módulos deberán consumir los tokens emitidos por el proveedor de identidad para validar el acceso a sus servicios backend, mientras que la definición de roles específicos del módulo se realizará durante la fase de análisis y diseño.

Para los ambientes de desarrollo propios del contratista, se podrán utilizar mecanismos de simulación o generación de tokens con fines de desarrollo y pruebas locales, sin requerir la integración directa con el proveedor de identidad institucional.

No obstante, para los procesos de integración, validación y operación en los ambientes institucionales (certificación y producción), será obligatorio el uso del proveedor de identidad definido por la Entidad (Keycloak). La autenticación será gestionada por la aplicación contenedora (Shell), la cual suministrará los tokens de seguridad a los microfrontends como parte del contexto de sesión, siendo responsabilidad de los servicios backend de cada módulo validar dichos tokens conforme a los lineamientos de seguridad de la Plataforma.

- ***Capa de presentación.***

La aplicación contenedora de la plataforma se encuentra desarrollada utilizando Angular 21, bajo un modelo de aplicaciones web orientadas a componentes, permitiendo la integración dinámica de microfrontends y la interacción con los servicios backend.

- ***Capa de servicios.***

Los servicios asociados a la aplicación contenedora de la Plataforma se encuentran desarrollados utilizando Spring Boot, exponiendo APIs REST para el consumo del frontend y gestionando la lógica funcional transversal de la Plataforma.

Para los módulos funcionales que se integren a la Plataforma Unificada de Servicios de la Red CADE, se recomienda mantener alineación con las tecnologías base adoptadas por la plataforma, con el fin de facilitar la interoperabilidad, el soporte, el mantenimiento y la operación de la solución. No obstante, podrán utilizarse otras tecnologías, siempre que su implementación se ajuste a los lineamientos de arquitectura de referencia definidos por la entidad y garantice compatibilidad con los mecanismos de autenticación, integración, monitoreo, seguridad y despliegue establecidos para la plataforma.

Independientemente de la tecnología utilizada, los servicios backend deberán diseñarse bajo un enfoque de arquitectura orientada a microservicios, donde cada servicio opere de

manera independiente, escalable y desacoplada, siguiendo principios de modularidad, interoperabilidad y autonomía funcional

- ***Persistencia de datos.***

La información de configuración de la Plataforma se gestiona mediante PostgreSQL, utilizada para almacenar los catálogos y parámetros necesarios para la operación de la aplicación contenedora y la administración de la Plataforma Unificada.

Adicionalmente, cada módulo funcional integrado podrá gestionar su propio repositorio de datos, de acuerdo con las necesidades tecnológicas y funcionales de cada sistema.

La selección de tecnologías de persistencia de datos deberá alinearse con la arquitectura de referencia tecnológica definida por la Entidad, permitiendo el uso de diferentes motores de bases de datos cuando la naturaleza de los sistemas lo requiera, siempre que se garantice la interoperabilidad, seguridad, trazabilidad y administración adecuada de la información.

- ***Interoperabilidad e integración de servicios.***

La Plataforma Unificada de Servicios de la Red CADE incorpora mecanismos de interoperabilidad que permiten la integración de los diferentes módulos funcionales entre sí y con otros sistemas institucionales o externos.

Estos mecanismos facilitan el intercambio seguro de información entre los componentes de la Plataforma y los sistemas distritales asociados. La integración entre sistemas se realizará principalmente mediante APIs REST seguras, utilizando estándares de la industria para autenticación, autorización y protección de la información, garantizando la interoperabilidad entre los diferentes sistemas que hacen parte del ecosistema tecnológico de la entidad.

Cuando la naturaleza de la integración lo requiera, podrán emplearse mecanismos adicionales de integración definidos dentro de la arquitectura de referencia de la entidad, tales como bus de servicios, herramientas de integración o mecanismos de mensajería, que permitan desacoplar los sistemas y facilitar la interoperabilidad entre plataformas heterogéneas.

- ***Caché de información.***

Se utiliza Redis como mecanismo de almacenamiento en caché con el objetivo de:

- Reducir la carga sobre los servicios backend.
- Mejorar los tiempos de respuesta del sistema.
- Optimizar consultas de información de alta frecuencia.

- ***Monitoreo y observabilidad.***

La Plataforma cuenta con herramientas de monitoreo y observabilidad que permiten supervisar el estado operativo de sus servicios.

Entre las herramientas utilizadas se encuentran:

- Prometheus: Utilizado para la recolección de métricas de los diferentes servicios y componentes del sistema.
- Grafana: Utilizado para la visualización de métricas y la construcción de tableros de monitoreo.
- Zipkin: Utilizado para el seguimiento de trazas distribuidas entre los distintos servicios, permitiendo analizar el comportamiento de las solicitudes a través de la arquitectura.

El stack de observabilidad (Prometheus, Grafana y Zipkin) ya se encuentra desplegado y operativo dentro de la infraestructura. En este sentido, el contratista no deberá aprovisionar componentes adicionales de observabilidad, sino garantizar la correcta integración del módulo desarrollado con las herramientas existentes.

Para ello, el módulo deberá exponer los endpoints y configuraciones necesarias, tales como métricas y mecanismos de trazabilidad (tracing), permitiendo su adecuada recolección, visualización y seguimiento dentro de la plataforma.

- ***Infraestructura y despliegue.***

La Plataforma Unificada de Servicios de la Red CADE se encuentra desplegada sobre un clúster de Docker Swarm en la infraestructura on-premise de la Entidad. El uso de contenedores permite estandarizar los procesos de despliegue, facilitar la portabilidad de los servicios y optimizar la operación en los diferentes ambientes de la solución.

El clúster admite el despliegue de nuevos stacks, siempre que estos cumplan con los lineamientos técnicos, de seguridad y de operación definidos por la Entidad. En este sentido, no se establecen restricciones estrictas sobre el sistema operativo base o versiones específicas de tecnologías (como JDK o Node); sin embargo, se deberán utilizar versiones estables, soportadas y alineadas con buenas prácticas de seguridad y construcción de contenedores.

Para la incorporación de nuevos módulos, el contratista deberá estimar los requerimientos de CPU, memoria, almacenamiento y carga transaccional durante la fase de análisis y diseño. Con base en este dimensionamiento técnico, la OTIC evaluará la viabilidad de utilizar la infraestructura existente o determinará la necesidad de realizar ajustes y ampliaciones de capacidad.

Actualmente, no se encuentran definidas cuotas específicas de recursos para el nuevo módulo; por lo tanto, la asignación de capacidad se realizará con base en el análisis técnico presentado por el contratista y la disponibilidad del clúster.

Si bien los componentes descritos en esta sección constituyen la base de la Plataforma, la integración de nuevas funcionalidades podría requerir elementos adicionales de la arquitectura de referencia de la Entidad (herramientas de integración, procesamiento de datos, analítica o mensajería). En estos casos, la selección tecnológica deberá alinearse estrictamente con los lineamientos de arquitectura de la Entidad, garantizando la interoperabilidad con los componentes actuales y la sostenibilidad de la solución a largo plazo.

- ***Accesos a herramientas institucionales.***

El acceso a los repositorios institucionales en GitLab o Azure DevOps será habilitado conforme a las necesidades del proyecto, principalmente en las etapas de integración, despliegue en certificación y producción.

La gestión de dichos accesos estará a cargo de la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) y se realizará de acuerdo con los procedimientos y controles de seguridad definidos por la Entidad.

El contratista deberá iniciar las actividades de desarrollo y pruebas en sus propios repositorios y ambientes, y posteriormente integrarse con las herramientas institucionales para los procesos de versionamiento, integración continua y despliegue en los ambientes de la Entidad.

i. Características y componentes tecnológicos de la Plataforma Unificada de servicios de la Red CADE

Actualmente, los servicios existentes se encuentran desplegados sobre infraestructura on-premise en el centro de datos de la Entidad, utilizando servidores virtualizados que soportan los diferentes componentes del sistema. Esta infraestructura, utilizada actualmente por el Sistema de Asignación de Turnos – SAT WEB, constituye la base tecnológica sobre la cual se implementarán los nuevos módulos y capacidades de la Plataforma Unificada.

La infraestructura permite gestionar los procesos de desarrollo, pruebas y operación mediante ambientes diferenciados, garantizando la estabilidad del sistema y el control de cambios antes de su despliegue en producción.

Actualmente la plataforma cuenta con los siguientes ambientes:

- ***Ambiente de desarrollo y certificación.***

La Entidad dispone de ambientes institucionales de desarrollo interno, certificación y producción, los cuales se utilizan para actividades de integración, despliegue y certificación funcional de las entregas, y no como ambientes de desarrollo del proveedor. En particular, el ambiente de certificación se emplea para procesos de validación y certificación funcional, previo al paso a producción.

Las principales características de estos ambientes son:

- Sistemas operativos: Oracle Linux Server 9.6.
- Arquitectura de servicios: Arquitectura de microservicios desplegados sobre contenedores Docker (versión 28.3.3).
- Base de datos: Oracle Database 19c (SAT WEB) / PostgreSQL 17 (SHELL)
- Control de versiones: Repositorios de código gestionados mediante sistemas de control de versiones GitLab.
- Despliegue de servicios: Automatizado mediante pipelines de integración continua (CI) implementados en Jenkins.

Estos ambientes permiten validar técnicamente los cambios realizados antes de su promoción al ambiente de producción.

Actualmente, la Entidad cuenta con pipelines CI/CD en Jenkins utilizados para los procesos de construcción y despliegue de los sistemas. No obstante, dichos pipelines no constituyen plantillas obligatorias o inmutables. En este sentido, el contratista deberá definir, ajustar o implementar sus propios pipelines, tomando como base las buenas prácticas existentes y los lineamientos técnicos de la Entidad, garantizando la correcta integración, construcción y despliegue de los nuevos módulos.

El contratista deberá implementar y gestionar su propio ambiente de desarrollo sobre su infraestructura, incluyendo todos los componentes necesarios para el ciclo de desarrollo, integración y pruebas técnicas de la solución.

Una vez se cuente con versiones estables o avances funcionales, la Entidad proveerá el ambiente de certificación para la validación y certificación funcional de la solución, previo a su paso a producción. El despliegue se realizará a través de pipelines CI/CD, mediante la entrega de imágenes a los repositorios definidos por la Entidad. No se proporcionará acceso SSH directo a los nodos del clúster, ya que este es administrado por la OTIC.

La Entidad dispone de un registry de contenedores institucional para los ambientes de certificación y producción, el cual será utilizado para el almacenamiento y gestión de las imágenes de los servicios. En este sentido, el contratista deberá publicar las imágenes en los repositorios definidos por la Entidad como parte del proceso de despliegue.

Para los ambientes de desarrollo propios, el contratista podrá utilizar sus propios mecanismos de almacenamiento de imágenes. No obstante, previo a los despliegues en los ambientes institucionales, las imágenes deberán ser migradas y gestionadas en el registry definido por la Entidad, cumpliendo con los lineamientos de seguridad, versionamiento y los controles establecidos por la OTIC.

En relación con los repositorios de código, se dispondrá de acceso a GitLab o Azure DevOps desde las fases iniciales del proyecto, permitiendo al equipo del contratista gestionar el código fuente, colaborar con el equipo de la Entidad y habilitar los procesos de integración y despliegue correspondientes.

- ***Ambiente de producción.***

El ambiente de producción corresponde al entorno donde se ejecuta la Plataforma en operación para los usuarios finales, garantizando la disponibilidad, estabilidad y seguridad de los servicios ofrecidos.

Las principales características de este ambiente incluyen:

- Sistema operativo: Oracle Linux Server 9.6.

- Arquitectura de servicios: Arquitectura de microservicios desplegados sobre contenedores Docker.
- Orquestación de contenedores: Clúster Docker Swarm para la gestión y escalamiento de los servicios.
- Base de datos: Oracle Database 19c / PostgreSQL 17.
- Control de versiones: Repositorios de código gestionados mediante el sistema de control de versiones GitLab.
- Despliegue de servicios: Automatizado mediante pipelines de integración continua y despliegue controlado a través de Jenkins.

Este ambiente se encuentra desplegado en infraestructura on-premise, y está orientado a garantizar la operación continua de la plataforma, así como la atención de las solicitudes de los usuarios y la integración con los diferentes sistemas institucionales.

Cada uno de los ambientes (desarrollo, certificación y producción) es independiente a nivel de infraestructura, configuración y bases de datos, garantizando el aislamiento de la información, la estabilidad operativa y la integridad de los procesos. En este sentido, no se comparten datos ni configuraciones entre ambientes, y cualquier promoción de cambios deberá realizarse mediante los procesos de despliegue y control definidos.

Las actividades de despliegue sobre los ambientes de certificación y producción deberán ser coordinadas con el equipo técnico de la Entidad, conforme a los lineamientos operativos definidos. Estas actividades podrán estar sujetas a ventanas de mantenimiento establecidas, para garantizar la continuidad del servicio. En caso de requerirse intervenciones en horarios extendidos o fines de semana (por ejemplo, durante salidas a producción o actividades críticas), estas serán previamente concertadas entre las partes.

El acceso a la infraestructura institucional (como VPN, repositorios GitLab, herramientas de integración y despliegue como Jenkins, permisos en el clúster Docker Swarm o acceso a bases de datos, entre otros) será gestionado por la OTIC conforme a los procedimientos de seguridad y operación definidos. La asignación de estos accesos se realizará de manera progresiva, según las necesidades de cada fase del proyecto (integración, despliegue o certificación), previa solicitud y aprobación por parte de la Entidad. Los tiempos de provisión estarán sujetos a los procesos internos de gestión de accesos, los cuales serán coordinados durante la ejecución del contrato.

En los ambientes institucionales de preproducción y producción, la provisión de la infraestructura y de los recursos de base de datos será responsabilidad de la Entidad, conforme a su arquitectura tecnológica y capacidad instalada. No obstante, el contratista deberá participar activamente en la definición de requerimientos técnicos, diseño del modelo de datos, creación de esquemas, parametrización y despliegue de los componentes necesarios para el correcto funcionamiento del módulo en dichos ambientes.

5. Especificaciones Técnicas.

Las fases que se describen a continuación, así como cada uno de los componentes que integran el presente anexo técnico, deberán ser ejecutados en su totalidad por el

proveedor. Para ello, el proveedor deberá presentar el cronograma y plan de trabajo por cada una de las fases, que deberá ser aprobado por el Supervisor del contrato, así como, la metodología utilizada para el análisis, diseño, desarrollo e implementación del alcance requerido.

Para el desarrollo e implementación del módulo, el contratista deberá proponer y ejecutar una metodología de desarrollo de software ágil (ej. SCRUM, Kanban o programación extrema - XP) que asegure entregas tempranas, continuas y de alta calidad mediante un proceso iterativo e incremental. Así mismo, el desarrollo deberá alinearse estrictamente con el Marco de Referencia de Arquitectura Empresarial (MRAE) y dar cumplimiento obligatorio a las guías institucionales vigentes de la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC): 'Guía metodológica para el desarrollo y mantenimiento de soluciones de software' (COD. 4204000-GS-108), 'Guía de Arquitectura de Software' (COD. 4204000-GS-006) y los 'Estándares de nomenclatura de bases de datos' (COD. 4204000-OT-047).

De acuerdo con lo anterior, se definen las siguientes fases para el desarrollo del módulo de administración y planeación del servicio de la Red Cade que debe integrarse a la plataforma unificada de servicios de la Red CADE.

Fase / Componente	Descripción	Entregables
1. Análisis y Planeación	• El contratista deberá realizar el levantamiento, validación y priorización de requerimientos funcionales y no funcionales garantizando las necesidades de los equipos de trabajo y los procesos y procedimientos del Sistema Integrado de Gestión de la Secretaría General, a fin de asegurar una ejecución consistente y trazable como: asignación a puntos de atención, asignación de turnos y roles, gestión de novedades administrativas, reportes e indicadores operativos, entre otros. • El contratista deberá identificar la arquitectura e infraestructura actual, integraciones, datos,	• Documento de requerimientos (funcionales y no funcionales), con reglas de negocio, flujos y criterios de aceptación validados. • Documento de arquitectura actual y diagnóstico técnico (infraestructura, Integraciones, seguridad y operación). • Inventario de activos tecnológicos y matriz de riesgos técnicos. • Mapa de interoperabilidad. • Plan de proyecto (cronograma, riesgos, recursos) y actas de

	seguridad y operación; verificación de paridad Dev/QA/Prod. • El contratista deberá definir y confirmar con los actores responsables de las reglas de negocio, los flujos operativos y criterios de aceptación para el registro, novedades, registro y almacenamiento de documentos en el servidor del sistema, consultas y notificaciones. • El contratista deberá evaluar la calidad de los datos, la interoperabilidad y los controles de seguridad (Ejemplo: RBAC, cifrado en tránsito y en reposo, DLP y auditoría uniforme), garantizando que dichos controles se definan, implementen y operen conforme a las políticas y lineamientos de seguridad de la información establecidos por la OTIC de la Entidad. Estos controles deberán ser incorporados de manera transversal en el diseño de la solución, como parte de buenas prácticas estándar, sin que esto represente desarrollos adicionales significativos. • El contratista deberá detallar y documentar los requerimientos funcionales y no funcionales, dentro de los límites del alcance establecido en el presente anexo técnico, definiendo las exclusiones, los desarrollos, los riesgos, el cronograma y los	levantamiento/validación funcional firmadas. • Plan de calidad y pruebas.

	lineamientos de calidad (SLA/SLO). • El contratista deberá usar el diseño integral de la Plataforma Unificada de Servicios de la Red CADE, como insumo para diseño y desarrollo del módulo. No se contempla la migración ni carga masiva de datos históricos provenientes de los archivos de Excel actuales. El módulo iniciará su operación con la parametrización inicial y la recolección de nueva información.	
2. Diseño	• El contratista deberá diseñar la arquitectura lógica y técnica de la solución, basada en un modelo de microservicios (backend) y microfrontend (capa de presentación), y el detalle de sus componentes. • El contratista deberá definir de manera detallada los flujos (UI/UX) y funcionalidades del módulo de administración y planeación del servicio de la Red Cade. • El contratista deberá diseñar el modelo de datos, diccionario y reglas de calidad; también definir los datos documentales (trazabilidad e integridad). • El contratista deberá definir los mecanismos de integración mediante APIs del módulo de administración y planeación del servicio de la Red Cade, que permitan su interoperabilidad futura con otros sistemas, garantizando trazabilidad y segregación por ambientes	• Documento de Diseño Funcional Detallado, que incluya el detalle de flujos de usuario, mapeo de reglas de negocio, perfiles, y prototipos/mockups de la interfaz de usuario. • Documento de arquitectura de la solución siguiendo un enfoque estructurado, preferiblemente basado en el modelo C4 (Contexto, Contenedores, Componentes y Despliegue), o en un modelo equivalente que permita representar de manera clara y consistente la arquitectura de la solución. Este documento deberá incluir, como mínimo, la

	conforme a los lineamientos definidos por la entidad. • El contratista deberá establecer el diseño de seguridad y observabilidad (métricas, logs, trazas) según los lineamientos que OTIC le provea. • El contratista deberá adelantar las reuniones y sesiones requeridas, con el equipo de la Dirección del Sistema Distrital de Servicio a la Ciudadanía y con la OTIC. Estas sesiones podrán desarrollarse de manera virtual o presencial en la sede de la Secretaría General, según se acuerde previamente con la supervisión del contrato.	definición de la arquitectura lógica, componentes, despliegue, integraciones, seguridad y observabilidad, así como diagramas de secuencia y, cuando aplique, diagramas de actividades necesarios para describir el comportamiento del sistema. • Modelo de datos y diccionario; reglas de calidad y gobierno de datos. • Documentación técnica en formato OpenAPI/Swagger orientada a la interoperabilidad, junto con los lineamientos de seguridad aplicados (RBAC, cifrado, auditoría y DLP, entre otros). • Plan de pruebas detallado (QA/UAT), incluyendo criterios de aceptación. **Nota**: Los diseños deberán ser aprobados por la supervisión del contrato. Así mismo, los diagramas deberán ser cargados en la herramienta de

		arquitectura empresarial de la entidad.
3. Desarrollo	• El contratista deberá desarrollar el módulo de administración y planeación del personal de la Secretaría General que labora en la Red CADE, conforme al diseño aprobado en la Fase 2. Las funcionalidades mínimas del módulo son las siguientes: – Gestión de Usuarios: La solución debe permitir el registro, actualización, activación y desactivación de funcionarios incluyendo contratistas y/o practicantes. El número de personas vinculadas a la Red CADE actualmente es de 194, de los cuales 146 están en los puntos de atención presencial. Esta cifra puede cambiar conforme procesos de selección que se adelanten, aunque no de forma significativa. – Procesos de Ingreso: La solución debe permitir la activación y el registro de los procesos derivados del ingreso de personal a la Red CADE (capacitación, asignación de usuarios, generación de credenciales, entre otros definidos en el diseño), incluyendo la generación de formatos y las notificaciones respectivas.	• Módulo de administración y planeación del servicio de la Red Cade (planta, contratistas y practicantes) desarrollado de acuerdo con el alcance definido, con documentación de flujos funcionales implementados. • Informe de pruebas de desarrollo (pruebas unitarias, análisis de código estático y validación preliminar de seguridad). • Código Fuente Versionado y Documentación Técnica, el código debe ser alojado en los repositorios dispuestos por la Entidad, debidamente comentado y acompañado de la documentación técnica de despliegue. • Artefactos de Despliegue, Scripts de base de datos, imágenes de contenedores y configuración de ambientes requeridos para iniciar el despliegue en certificación

	– Asignación a Puntos: La solución debe permitir asignar cada persona a un punto de atención presencial de la Red CADE, así como la reasignación temporal o definitiva de una o varios puntos de atención, incluyendo trazabilidad de fechas. Actualmente existen 22 puntos de atención. – Programación Operativa (Turnos y Roles): La solución debe permitir la programación de turnos de personal asignado a cada punto de atención y los roles por cada persona que atiende en los puntos presenciales de la Red CADE. Para ello debe identificar la disponibilidad de cada persona, generar alertas automáticas por conflictos de horario y demás aspectos para hacer programación por roles. Tener en cuenta las reglas de negocio aprobadas. - Gestión de Novedades: La solución debe permitir la solicitud, revisión, aprobación y cancelación de novedades administrativas (permisos, incapacidades, vacaciones, compensaciones, etc.). incluyendo la generación de formatos y las notificaciones respectivas.	

	– Gestión Documental Transaccional: La solución debe permitir la generación, almacenamiento, flujo y custodia de soportes documentales, en el servidor del sistema. Se aclara que la solución no debe tener un componente de sistema de Gestión de Documentos Electrónicos de Archivo - SGDEA. – Notificaciones: La solución debe permitir la notificación automática por correo electrónico en hitos (radicación, validación, aprobación/rechazo/cambios y archivo, etc). – Firma de Documentos: La solución debe permitir la firma de documentos asociados a los flujos mediante mecanismos de firma electrónica simple o validación electrónica con trazabilidad (logs de auditoría ligados a la sesión de Keycloak y estampas de tiempo), asegurando la integridad del documento generado. No se requiere la adquisición de firmas digitales certificadas por terceros. – Reportes y Tableros de Control (Power BI): La solución debe permitir la generación y visualización de reportes asociados a la administración y planeación	

	del servicio de la Red CADE, de manera general, por punto de atención y por rol. Los reportes mínimos sugeridos son: ✓ Número personas por punto de atención comparado con los mínimos que se requieren para la operación (Por Rol). ✓ Ausentismo (General, por punto de atención, por rol y por persona). ✓ Reporte de novedades administrativas, por tipo, general, por punto, por rol y por persona). ✓ Asignación diaria de turno de acuerdo con los roles (Anfitrión, turnos, salas, etc). ✓ Historico completo de cambios de personal por cargo asignado. Los reportes deben ser exportables, mínimo formato Excel y PDF. • Estándares y Ambientes: La solución deberá cumplir con estándares definidos (frontend, backend, BD), con código fuente versionado y documentación técnica. El contratista deberá proveer los ambientes de desarrollo y pruebas y la aplicación de seguridad (RBAC, cifrado, auditoría, DLP); control de conectores/endpoints autorizados.	

4. Pruebas (QA/UAT)	• El contratista deberá hace la ejecución de pruebas funcionales, no funcionales, integración, carga y estrés sobre el módulo desarrollado, tanto en el ambiente de pruebas como en el ambiente de certificación. • El contratista deberá hacer la validación de reglas de negocio, seguridad (RBAC, cifrado, DLP) y trazabilidad; auditoría uniforme de operaciones. • El contratista deberá hacer la validación de calidad y consistencia de datos e indicadores frente a las fuentes internas ofrecidas por la entidad. • El contratista deberá hacer la ejecución de QA/UAT con paridad de configuración respecto a producción, gestión de incidentes y correcciones. • El contratista deberá ejecutar pruebas de desempeño que evalúen latencia, concurrencia, tiempos de respuesta verificando que las operaciones críticas de la solución presenten tiempos de respuesta menores a tres (3) segundos, bajo condiciones normales de operación. • Las pruebas se ejecutarán de manera centralizada con un grupo de colaboradores de la Dirección del Sistema Distrital de Servicio a la Ciudadanía.	• Plan y evidencias de pruebas (QA/UAT), incluyendo pruebas de integración, carga y estrés. • Informe de resultados (funcional, técnico, seguridad) con hallazgos, correcciones aplicadas y recomendaciones. • Registro de incidentes y correcciones, con trazabilidad de cambios. No se aprueba la fase si existen vulnerabilidades de severidad Crítica o Alta sin resolver. • Concepto técnico de viabilidad y solicitud formal de paso a producción.
5. Instalación y Puesta en Operación.	• El contratista debe hacer el despliegue en conjunto con la Oficina de Tecnologías de la Información y las Comunicaciones	• Manuales de instalación, operación, administración y usuario, junto con la

	- OTIC de la Secretaría General del ambiente de certificación y producción. • El contratista debe hacer la validación de operación end-to-end. • El contratista deberá entregar los artefactos instalables y la documentación. • La solución debe pasar por un escaneo de seguridad realizado por la entidad, así mismo la solución debe pasar a la aceptación por parte de la entidad.	documentación técnica actualizada de la arquitectura desplegada. • Componentes instalados (app y BD) y operativos. • Acta de recibo a satisfacción. • Evidencias de despliegue exitoso. **Nota:** No se aprueba la fase si existen vulnerabilidades de severidad Crítica o Alta sin resolver.
6. Apropiación y Transferencia de Conocimiento uso y apropiación.	• El contratista debe capacitar a usuarios funcionales (Se estiman 10 sesiones de 2 horas c/u) y técnicos (4 sesiones de 2 horas c/u), de forma presencial y cuando sea necesario de forma virtual. • El contratista debe transferir el conocimiento sobre operación, administración y soporte. • El contratista debe hacer la socialización de funcionalidades y buenas prácticas. • El contratista debe hacer la entrega de material de apoyo utilizado para la transferencia del conocimiento. (Lista de asistencia, diapositivas, manuales entre otros). • El contratista deberá hacer la cesión de derechos de autor a favor de la Secretaría General, entregando el código fuente completo, scripts, configuraciones y documentación asociada.	• Plan de transferencia de conocimiento y uso y apropiación. • Registro y memorias de las transferencias de conocimiento. • Documento de Cesión de Derechos. • Informe final del desarrollo de todas las fases. **Nota:** el Contratista deberá efectuar la entrega de los insumos y soportes requeridos para el ingreso al almacén de los desarrollos realizados, para lo cual deberá presentar la documentación exigida por la Entidad, con el fin de adelantar la gestión y

		formalización del trámite correspondiente.

Nota: Toda la documentación técnica, manuales y modelos de arquitectura deberán entregarse tanto en formato PDF como en sus formatos nativos editables y de diagramación originales (ej. Word, Excel, .vsdx, .drawio o equivalentes), evitando representaciones estáticas. Adicionalmente, el código fuente entregado deberá estar debidamente comentado, aplicar reglas de Clean Code, e incluir un archivo 'README' estructurado dentro de cada microservicio, detallando explícitamente su propósito, dependencias y las instrucciones precisas para su ejecución, configuración y despliegue local y en servidor.

6. Requerimientos No Funcionales.

La solución deberá cumplir con los siguientes requerimientos no funcionales, los cuales se consolidan como base inicial y deberán ser considerados de manera transversal en el diseño, desarrollo, pruebas e implementación. Estos requerimientos, junto con los requerimientos funcionales deben ser validados, ajustados y detallados durante las fases iniciales del proyecto, conforme a los hallazgos del análisis y diseño:

- Desempeño: Las operaciones críticas deberán presentar tiempos de respuesta inferiores a tres (3) segundos bajo condiciones normales de operación. La identificación de dichas operaciones, así como la definición de las condiciones de operación (usuarios concurrentes, volumetría de datos y criterios de medición), serán precisadas durante las fases de análisis y diseño y formalizadas en el plan de pruebas, el cual establecerá la línea base de desempeño para la validación de este requisito.
- Escalabilidad: La solución deberá soportar incrementos en la carga de usuarios y transacciones, conforme al crecimiento de la operación.
- Disponibilidad: La solución deberá alinearse con los niveles de disponibilidad definidos por la Entidad y los acuerdos de nivel de servicio (ANS).
- Seguridad: Se deberán implementar controles de seguridad conforme a los lineamientos de la OTIC, incluyendo mecanismos de cifrado en tránsito mediante protocolos seguros (TLS), gestión de certificados digitales y protección de la información. La definición específica de versiones de protocolo (por ejemplo, TLS 1.2 o superior), algoritmos y configuraciones será validada durante la fase de análisis y diseño. La provisión y gestión de certificados digitales en los ambientes institucionales será responsabilidad de la Entidad, a través de sus equipos de infraestructura

- Seguridad (pruebas de vulnerabilidades): Previo al paso a producción, la solución deberá someterse a procesos de evaluación de seguridad, tales como análisis de vulnerabilidades, ejecutados por la Entidad o por los equipos designados por la OTIC. Como criterio de aprobación, la solución deberá presentar resultados satisfactorios en dichas evaluaciones. En caso de identificarse vulnerabilidades, estas deberán ser atendidas y corregidas por el contratista antes de autorizar el despliegue en el ambiente productivo, conforme a los lineamientos de seguridad definidos por la Entidad
- Auditoría y trazabilidad: La solución deberá implementar mecanismos de auditoría que permitan registrar y consultar las operaciones realizadas sobre el sistema, garantizando la trazabilidad de las acciones de los usuarios. El nivel de detalle de la auditoría (a nivel de aplicación o base de datos) y los tiempos de retención de los logs serán definidos durante la fase de análisis y diseño, conforme a los lineamientos de seguridad, auditoría y gestión de la información establecidos por la OTIC.
- Interoperabilidad: La solución deberá integrarse mediante APIs, cumpliendo estándares definidos por la Entidad.
- Observabilidad: Se deberán implementar mecanismos de monitoreo, logging y trazas para seguimiento operativo.
- Calidad de datos: Se deberán definir reglas de validación, consistencia e integridad de la información.
- Portabilidad y despliegue: La solución deberá ser desplegable en contenedores Docker y compatible con la infraestructura definida por la Entidad.
- Mantenibilidad: El código deberá estar documentado, versionado y alineado con buenas prácticas de desarrollo.
- Gestión de Obsolescencia (End of Life - EoL): Las versiones del sistema de información y de cada uno de sus componentes tecnológicos (frameworks, bases de datos, sistemas operativos, librerías) deberán mantenerse alineadas con los ciclos de vida y las políticas de fin de soporte oficial (EoL) de los fabricantes. El contratista deberá garantizar que ningún componente utilizado entre en estado de obsolescencia durante la vigencia del contrato ni en su respectivo periodo de garantía. En caso de requerirse, el contratista asumirá la responsabilidad técnica de su actualización oportuna para evitar riesgos de seguridad, incompatibilidad o pérdida de soporte.
- Calidad del software (pruebas): La solución deberá contar con pruebas unitarias que garanticen la calidad del código desarrollado. El porcentaje mínimo de cobertura y el tipo de métricas para utilizar serán definidos durante la fase de análisis y diseño, conforme a los lineamientos de calidad establecidos por la Entidad.
- Diseño responsive: La solución debe diseñarse y desarrollarse de tal manera que funcione correctamente en cualquier dispositivo.

- Accesibilidad y usabilidad: La solución debe cumplir con estándares de accesibilidad hasta el nivel AA.

Los lineamientos de aseguramiento de calidad, desarrollo y pruebas de la solución deberán ser validados y definidos al inicio del proyecto, conforme a las políticas y prácticas vigentes de la OTIC. Estos incluyen aspectos como revisión de código, análisis de código estático, definición de métricas de calidad, cobertura de pruebas unitarias, criterios de paso a producción y ejecución de pruebas de seguridad, en donde el contratista será responsable de su implementación y la OTIC de su validación. Así mismo, las pruebas funcionales, de carga y de experiencia de usuario (UX), notificaciones, concurrencia y dimensionamiento de la solución, serán definidos y ajustados durante las fases de análisis, planeación y pruebas del proyecto. La solución deberá garantizar su operación bajo condiciones de concurrencia estimadas, soportar acceso desde distintos dispositivos, exponer mecanismos de monitoreo como health checks y cumplir con los lineamientos de infraestructura definidos.

7. Transferencia de Conocimiento.

El contratista deberá garantizar un proceso de transferencia de conocimiento efectivo hacia el equipo técnico de la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) y el equipo técnico funcional de la Dirección del Sistema Distrital de Servicio a la Ciudadanía (DSDSC) de la Secretaría General. El objetivo es asegurar que la entidad comprenda integralmente el sistema de información desarrollado.

El contratista deberá realizar, como mínimo, las siguientes sesiones de transferencia de conocimiento durante la ejecución del contrato:

- Sesión de socialización de diseño y validación de infraestructura (Fase 1).
- Sesiones dirigidas al equipo técnico y funcional para presentar el estado de la arquitectura, la operatividad de los módulos actuales con nuevos desarrollos.
- Sesiones de socialización de avances de desarrollo e implementación de nuevo desarrollo módulo administración y planeación del servicio de la Red Cade (Fase 2): Sesión dirigida a explicar los prototipos (mockups) y la lógica de negocio propuesta para la operación de administración de personal que labora para la Red Cade.
- Sesión de capacitaciones a usuario final (Fase 6): Sesiones para contextualizar la operación del módulo de administración y planeación de personal, 10 sesiones de 2 horas c/u y 4 sesiones técnicas de 2 horas c/u. Las sesiones funcionales deben realizarse en horario laboral y en la ciudad de Bogotá. Las sesiones técnicas se desarrollarán igualmente en horario laboral. No obstante, en casos puntuales como actividades de despliegue o tareas que requieran ventanas de mantenimiento, estas podrán realizarse fuera del horario laboral o en fin de semana, previa coordinación y acuerdo con el equipo de tecnología de la Entidad.

Las sesiones podrán realizarse de manera presencial y cuando sea estrictamente necesario de forma virtual y/o de acuerdo con lo que se defina con la supervisión del contrato, así como el número de participantes, la frecuencia y cantidad de sesiones requeridas. Adicionalmente, el contratista deberá entregar el material de soporte correspondiente, tales como presentaciones utilizadas, grabaciones, listas de asistencia, actas de las sesiones u otros insumos pertinentes, garantizando que la información sea clara, completa y adecuada para los diferentes perfiles de la entidad.

8. Acuerdos de Niveles de Servicio (ANS).

Los ANS se aplicarán de forma independiente para cada uno de los entregables definidos en las fases / componentes del proyecto. El incumplimiento de estos niveles generará descuentos en la factura correspondiente a la fase evaluada.

A continuación, se detallan los ANS:

Indicador	Descripción	Meta / Nivel Mínimo	Impacto en la Facturación de la Fase
Oportunidad en la Entrega	Entrega de los productos de cada fase dentro de los plazos establecidos en el cronograma aprobado.	100% de los productos entregados en la fecha pactada.	Descuento del 0.5% del valor de la fase por cada día hábil de retraso, hasta un máximo del 5%.
Calidad y Efectividad	Nivel de precisión de los informes y en los desarrollos entregados y anexos frente a los requerimientos del supervisor.	Máximo dos (2) rondas de observaciones en informes y máximo (3) rondas en correcciones de errores por producto de desarrollo.	A partir de la tercera ronda de correcciones, descuento del 2% del valor de la fase por cada nueva revisión hasta un máximo del 20%.
Respuesta a Observaciones	Tiempo que tarda el contratista en subsanar y devolver los productos tras recibir comentarios del supervisor.	Máximo tres (3) días hábiles tras la notificación.	Descuento del 1% del valor de la fase por cada día de demora adicional en la entrega de los ajustes hasta un máximo del 10%.
Disponibilidad del Equipo Base Clave.	Asistencia obligatoria del Gerente de Proyecto o Arquitecto de Software a las mesas técnicas de validación.	100% de asistencia del personal requerido.	Descuento del 1% del valor de la fase por cada inasistencia no justificada de un perfil clave. hasta un máximo del 10%.
Estabilidad del Personal Clave	Mide el porcentaje de permanencia de los perfiles	0% de rotación	Descuento de hasta el2% del valor de la fase por cada cambio

	principales (Gerente, Arquitecto, desarrollador, analista de pruebas) durante la fase.		de personal clave no atribuible a fuerza mayor.
Oportunidad en el Reemplazo	Tiempo transcurrido desde la salida de un profesional hasta la presentación por parte del contratista de la hoja de vida y los soportes del perfil de reemplazo para su verificación y aprobación por parte de la entidad	Máximo 3 días hábiles para la presentación de la hoja de vida y soportes del perfil de reemplazo	Descuento del 1% del valor de la fase por cada día de retraso en la entrega de los documentos del reemplazo

Nota 1: La aplicación de los descuentos asociados a los ANS estará precedida de la verificación por parte de la supervisión del contrato. Para tal efecto, la supervisión deberá dejar constancia del incumplimiento evidenciado, identificar el indicador afectado, recopilar los soportes respectivos y permitir al contratista presentar las aclaraciones o justificaciones correspondientes. Si el incumplimiento resulta atribuible al contratista, el descuento será aplicado en la facturación de la fase siguiente. En los eventos en que el incumplimiento sea grave, reiterado o pueda generar consecuencias contractuales adicionales, la supervisión dará traslado al área contractual competente para el trámite a que haya lugar.

Nota 2: No habrá lugar a descuentos derivados de ANS cuando el incumplimiento obedezca a fuerza mayor, caso fortuito debidamente acreditado y aceptado por la supervisión, o a causas atribuibles exclusivamente a la Entidad.

Nota 3: La aplicación de descuentos o el inicio del trámite contractual correspondiente no implica la aceptación automática de productos, entregables, informes o desarrollos, ni exonera al contratista de realizar los ajustes necesarios hasta obtener el recibo a satisfacción.

Clasificación de Errores para ANS y Pruebas UAT: Para garantizar una medición objetiva del desempeño funcional y la calidad del software, los incidentes detectados se clasificarán en dos tipos:

a) Error Bloqueante (Criticidad Alta): Falla que impide por completo el uso de una funcionalidad principal, genera resultados incorrectos que afectan la operación o imposibilita continuar las pruebas.

b) Error de Presentación (Criticidad Baja): Incidencia de carácter estético o menor (ej. ortografía, alineación) que no afecta la integridad de los datos ni el

funcionamiento lógico del sistema. Para efectos de penalización en los ANS por 'Calidad y Efectividad' y para la autorización del paso a producción, únicamente se tendrán en cuenta como no conformidades los Errores Bloqueantes.

9. Equipo de trabajo mínimo requerido.

El proveedor deberá disponer del personal idóneo, competente, calificado y suficiente para garantizar la correcta ejecución del contrato, de conformidad con el alcance, las fases definidas y los tiempos establecidos por la Entidad. El equipo de trabajo deberá acreditar experiencia específica en proyectos de diseño, desarrollo, implementación y puesta en operación de sistemas de información, asegurando la calidad técnica de la solución, la seguridad de la información, la adecuada gestión del proyecto y el cumplimiento de los objetivos institucionales.

Como mínimo, el proveedor deberá disponer del siguiente equipo de trabajo:

Rol	Cantidad	Formación Académica	Experiencia Profesional General	Experiencia Específica Mínima	Dedicación
Gerente de Proyecto	1	Título profesional perteneciente al NBC de Ingeniería de Sistemas, Telemática y Afines, o al NBC de Ingeniería Electrónica, Telecomunicaciones y Afines, o al NBC de Ingeniería Industrial y afines. Título de posgrado pertenecientes al NBC de Administración; Ingeniería de Sistemas, Telemática y Afines; Ingeniería Electrónica, Telecomunicaciones y Afines; o Matemáticas, Estadística y Afines, con énfasis en Gerencia de Proyectos, Gestión de Proyectos, Dirección	Mínimo cinco (5) años de experiencia profesional.	Acreditar mínimo tres (3) años de experiencia como Gerente, Director, Coordinador o Líder de proyectos TIC relacionados con el desarrollo, implementación, mantenimiento o evolución de sistemas de información o soluciones de software, realizando actividades de planeación, seguimiento, control y coordinación técnica y administrativa del proyecto.	100%

		de Proyectos, Gestión de Tecnologías de la Información (TI), Ingeniería de Software, Arquitectura de Software, Gestión de Servicios de TI, Transformación Digital, Gobierno de TI o áreas afines relacionadas con el objeto contractual. Deberá acreditar certificación vigente en un marco de gestión de servicios de TI (ITIL Foundation v3, ITIL 4 Foundation o superior) y/o certificación vigente en dirección de proyectos o metodologías ágiles, tales como PMP®, PRINCE2®, PMI-ACP®, Scrum Máster o certificaciones equivalentes emitidas por organismos reconocidos internacionalmente.			
Líder Técnico	1	Título profesional en programas académicos perteneciente al NBC de Ingeniería de Sistemas, Telemática y Afines, o en otros NBC relacionados con tecnologías de la información, ingeniería de software, desarrollo de sistemas de información o áreas	Mínimo cuatro (4) años de experiencia profesional.	Mínimo tres (3) años de experiencia profesional relacionada con el liderazgo técnico de equipos de desarrollo de software o equipos multidisciplinarios de tecnología, participando en proyectos de construcción,	100%

		afines. Deberá contar con título de posgrado a nivel de especialización en Arquitectura de Software, Ingeniería de Software, Desarrollo de Software, Arquitectura Empresarial, Gerencia de Sistemas de Información, Gerencia de Proyectos de Sistemas de Información, o disciplinas relacionadas con la arquitectura, diseño, construcción, implementación y gestión de soluciones de software.		implementación, evolución, integración, modernización o mantenimiento de sistemas de información. La experiencia deberá incluir actividades asociadas con la definición y validación de arquitecturas de solución, diseño técnico de componentes de software, establecimiento de lineamientos y estándares de desarrollo, aseguramiento de buenas prácticas de ingeniería de software, revisión técnica de código, integración de componentes, gestión de aspectos técnicos, acompañamiento a equipos de desarrollo y apoyo en la toma de decisiones tecnológicas durante el ciclo de vida de los proyectos.	

Documentador Técnico	1	Título profesional en programas académicos pertenecientes al NBC de Ingeniería de Sistemas, Telemática y Afines, Ingeniería Industrial y Afines, o en áreas del conocimiento relacionadas con la gestión, análisis, implementación, operación y/o mejoramiento de procesos asociados al objeto contractual.	Mínimo tres (3) años de experiencia profesional.	Mínimo tres (3) años de experiencia en la elaboración, actualización y gestión de documentación técnica y funcional asociada a proyectos de desarrollo, implementación, evolución o mantenimiento de sistemas de información, incluyendo documentación de código fuente, documentos de arquitectura y diseño técnico, manuales de instalación y configuración, documentación de servicios y APIs, especificaciones funcionales, casos de uso, historias de usuario y manuales dirigidos a usuarios finales, bajo metodologías de desarrollo de software.	100%

Desarrollador de Software	2	Título profesional en programas académicos perteneciente al NBC en Ingeniería de Sistemas, Telemática y Afines; Ingeniería Electrónica, Telecomunicaciones y Afines; Ingeniería Industrial y Afines, o demás NBC afines cuya formación guarde relación con el objeto del contrato.	Mínimo dos (2) años de experiencia profesional.	Acreditar mínimo dos (2) años de experiencia como desarrollador de software, participando en al menos un (1) proyecto ejecutado durante los últimos cinco (5) años, relacionado con el análisis, diseño, construcción, desarrollo, implementación, integración, mantenimiento o evolución de sistemas de información o soluciones de software. La experiencia deberá acreditar actividades de desarrollo backend con Java y Spring Boot o tecnologías equivalentes, construcción de APIs REST, arquitecturas de microservicios, desarrollo frontend con Angular o tecnologías equivalentes, manejo de bases de datos relacionales, herramientas de control de versiones (Git o equivalente) y contenedores (Docker o equivalente).	100%

Analista de Calidad (QA)	1	Título de Tecnólogo en Sistemas, Informática, Desarrollo de Software, Telemática o áreas afines, o Título Profesional perteneciente al NBC en Ingeniería de Sistemas, Telemática y Afines; Ingeniería Electrónica, Telecomunicaciones y Afines; Ingeniería Industrial y Afines, o demás NBC afines cuya formación guarde relación con el objeto del contrato.	Mínimo dos (2) años de experiencia profesional o tecnológica, según corresponda.	Acreditar mínimo cinco (5) años de experiencia desempeñándose como Analista de Calidad (QA) o en roles equivalentes, en proyectos de desarrollo, implementación, mantenimiento o evolución de sistemas de información o soluciones de software, realizando actividades de planeación, diseño, ejecución y documentación de pruebas funcionales, de integración, regresión y aceptación, gestión y seguimiento de incidencias, validación de requisitos funcionales y no funcionales, y apoyo a los procesos de aseguramiento de la calidad del software bajo metodologías ágiles o tradicionales.	50%

Nota: El porcentaje de dedicación del equipo de trabajo es referencial y podrá ser ajustado, previa aprobación del supervisor del contrato, por el proveedor conforme a su propuesta técnica y las necesidades de cada fase del proyecto. Lo anterior, siempre que se garantice en todo momento la disponibilidad del equipo mínimo requerido, la continuidad en la ejecución contractual y el cumplimiento del objeto, alcance, fases, cronograma, entregables y ANS establecidos en los documentos del proceso. En todo caso, la variación en la dedicación no modifica ni elimina la obligación del contratista de disponer y mantener

el equipo mínimo requerido, ni lo exime del cumplimiento de los indicadores asociados a la disponibilidad y estabilidad del personal clave.

10. Obligaciones.

10.1 Obligaciones generales del Contratista.

1. Cumplir con el objeto, alcance, propuesta, actividades y entregables del contrato, en el plazo establecido y según los parámetros fijados en el contrato
2. Ejecutar el objeto del contrato con total autonomía técnica y sin subordinación con respecto a la Secretaría General de la Secretaría General. Queda entendido que no habrá vínculo laboral alguno entre el personal utilizado por el contratista y la Secretaría General de la Alcaldía de Bogotá. D.C., por lo tanto, serán de su cargo el reclutamiento, calificación, vinculación, entrenamiento del personal que utilice, lo mismo que el pago de salarios, prestaciones e indemnizaciones, de conformidad con lo señalado en la Ley.
3. Mantener actualizado el domicilio durante la vigencia del contrato y seis (6) meses más y presentarse a la Secretaría General en el momento en que sea requerido por la misma para la suscripción de la respectiva acta de liquidación, si a ello hubiere lugar.
4. Tener una cuenta corriente o de ahorros en una entidad bancaria afiliada al S.A.P. (Sistema Automático de Pagos).
5. Presentar oportunamente las facturas, los soportes correspondientes y demás documentos necesarios para su pago. así como aportar el certificado de cumplimiento en el pago de seguridad social y aportes parafiscales, expedida por el representante legal y/o revisor fiscal y/o quien haga sus veces
6. Obrar con lealtad y buena fe en todo momento y en las distintas etapas contractuales, evitando dilaciones y en trabamientos.
7. Asumir todos los costos que genere la legalización del contrato.
8. No acceder a peticiones o amenazas de quienes actúen por fuera de la ley con el fin de hacer u omitir algún hecho.
9. Asumir los efectos derivados de todos y cada uno de los riesgos asociados a este contrato, al igual que respecto a los que logre determinar, salvo los casos en que expresamente se determine lo contrario.
10. Asumir los efectos económicos de todos aquellos sucesos previsibles y de normal ocurrencia para las actividades que son objeto de la presente contratación. Por lo tanto, deberá asumir los riesgos asociados a su tipo de actividad ordinaria que sean previsibles, así mismo, asumirá aquellos riesgos propios de su actividad empresarial y de persona natural o jurídica que tiene que cumplir con determinadas cargas y deberes frente al Estado y la sociedad. En consecuencia, solo procederán reclamaciones por hechos o circunstancias imprevisibles.
11. Constituir y mantener vigentes las garantías exigidas en el proceso de selección y en el contrato, en las condiciones, amparos, valores asegurados y plazos establecidos, cubriendo los riesgos definidos, y garantizando su vigencia durante la ejecución del contrato y el término previsto para su liquidación y garantías posteriores, cuando a ello haya lugar.
12. Asumir el pago de salarios, honorarios, prestaciones e indemnizaciones de carácter laboral del personal que contrate para la ejecución del contrato, lo mismo que el pago

de honorarios, los impuestos, gravámenes, aportes y servicios de cualquier género que establezcan las leyes colombianas y demás erogaciones necesarias para la ejecución del contrato

13. Velar por el respeto de los Derechos Constitucionales y Laborales de los trabajadores que utilice para la ejecución del contrato, para lo cual, eliminará formas de contratación lesiva para los Derechos Laborales.
14. El personal del contratista debe participar activamente en las actividades de prevención y promoción en Seguridad y Salud en el Trabajo, si aplica
15. Responder ante las autoridades competentes por los actos u omisiones que ejecute en desarrollo del contrato cuando en ellos se cause perjuicio a la administración o a terceros en los términos del artículo 52 de la ley 80 de 1993.
16. Reparar los daños e indemnizar los perjuicios que cause a la Secretaría General, por el incumplimiento del contrato.
17. Responder por los actos que le sean imputables al Contratista, es decir todas las acciones y omisiones de su personal, subcontratistas y proveedores, así como del personal al servicio de estos últimos.
18. Responder por los costos, daños y perjuicios que se generen como consecuencia del incumplimiento de la normatividad ambiental o de seguridad y salud en el trabajo, incluidos los derivados de accidentes, incidentes o siniestros ocurridos durante la ejecución del contrato.
19. Garantizar un canal de comunicación permanente y directo con la supervisión, con el fin de asegurar la atención oportuna de las solicitudes, observaciones y recomendaciones que se generen o que puedan tener algún efecto sobre el objeto del Contrato o sobre sus obligaciones.
20. Estar bajo la supervisión directa de la Secretaría General.
21. Difundir la Cartilla PIGA de la Secretaría General de la Alcaldía Mayor de Bogotá vigente o el documento que haga sus veces, al personal que asigne para la ejecución del contrato
22. Dar cumplimiento a la política cero papeles de la Secretaría General, la cual se adopta mediante Resolución 718 del 06 de diciembre de 2023
23. Mantener estricta reserva y confidencialidad sobre la información que conozca por causa o con ocasión del contrato.
24. El contratista se obliga a no vincular, contratar, subcontratar o establecer cualquier tipo de relación laboral o comercial, durante la ejecución del contrato, con miembros del equipo estructurador del proyecto ni con terceros que, por su participación o conocimiento en la etapa precontractual, puedan generar un conflicto de interés o afectar la transparencia e imparcialidad del proceso.
25. Las demás inherentes al objeto y a la naturaleza del contrato que llegare a celebrarse

10.2 Obligaciones Específicas del Contratista.

1. Cumplir con el objeto del presente contrato dentro de los plazos establecidos, atendiendo las especificaciones técnicas mínimas descritas en el estudio previo, el anexo técnico y la propuesta, la cual para todos los efectos forma parte integral del contrato, en lo que no contravengan con el mismo.

2. El contratista deberá garantizar que el personal asignado para la ejecución del contrato corresponda al equipo mínimo propuesto en la oferta. Para ello, deberá entregar al supervisor del contrato dentro de los tres (3) días hábiles siguientes de la firma del contrato y como requisito previo para la firma del acta de inicio, las hojas de vida de los profesionales, certificaciones de experiencia, certificaciones de estudio y demás documentos exigidos para cada rol, a fin de que éstas sean avaladas y aprobadas por el supervisor del contrato con un tiempo no superior a tres (3) días hábiles.
3. Presentar, disponer y garantizar el equipo mínimo requerido, durante la ejecución del contrato, necesario e idóneo para la prestación de los servicios requeridos, según los requisitos exigidos en el Anexo técnico, los cuales estarán bajo cuenta y riesgo del contratista. En caso de requerirse el cambio de alguno de los profesionales, este deberá ser informado previamente al supervisor del contrato y solo podrá efectuarse previa aprobación expresa de este, y siempre que el perfil propuesto cuente con igual o mejores calidades de formación académica y experiencia laboral respecto del profesional a reemplazar. El CONTRATISTA deberá presentar la hoja de vida del perfil de reemplazo a más tardar dentro de los tres (3) días hábiles siguientes a la ocurrencia de la vacante, conforme a los niveles de servicio establecidos. El contratista debe garantizar en todo momento la continuidad en la prestación del servicio
4. Presentar, dentro de los diez (10) días hábiles siguientes a la suscripción del contrato, el plan de trabajo y cronograma de ejecución, el cual deberá ser aprobado por el supervisor.
5. De conformidad con lo establecido en el artículo 29 del Decreto 643 de 2025, el contratista deberá vincular y mantener durante la ejecución del contrato al menos un 49,5% de mujeres, porcentaje que se aplicará sobre el equipo mínimo requerido en el presente anexo técnico. Dicha vinculación deberá atender los requisitos de perfiles, formación y experiencia exigidos en este Anexo Técnico y realizarse con plena observancia de las normas laborales o contractuales aplicables.
6. En cumplimiento de lo dispuesto en el artículo 2.2.1.2.4.2.7.5 del Decreto 287 de 2026, el contratista deberá priorizar la vinculación de personas naturales con discapacidad cuando para la ejecución del contrato se requiera la conformación de equipos de trabajo. Cuando el contratista vincule personas con discapacidad para la ejecución del contrato, estas deberán cumplir los perfiles, competencias y requisitos exigidos para el respectivo rol.

   El contratista deberá acreditar ante el supervisor del contrato el cumplimiento de esta condición especial de ejecución mediante los soportes correspondientes, incluyendo la certificación de discapacidad expedida conforme a la normatividad vigente y la documentación que evidencie la vinculación de la persona al equipo de trabajo del contrato, cuando ello aplique. El cumplimiento de esta obligación será verificado por la Entidad en el marco del seguimiento a la ejecución contractual.
7. Ejecutar las actividades necesarias para la puesta en operación de la solución y cumplir las fases/componentes establecidas en el anexo técnico, garantizando calidad, oportunidad, trazabilidad y cumplimiento de los criterios definidos por la entidad.
8. Cumplir con la totalidad de los ofrecimientos adicionales presentados en la propuesta que hayan sido objeto de puntaje dentro del proceso de selección.
9. El contratista deberá contar con sus propios ambientes de desarrollo para la construcción y pruebas iniciales de la solución.

10. Desarrollar la solución tecnológica conforme a las fases/componentes definidos en el anexo técnico asegurando su correcta ejecución y trazabilidad.
11. Garantizar la calidad técnica de la solución, así como la consistencia, integridad y disponibilidad de la información generada o administrada en el marco del contrato
12. Implementar la solución tecnológica asegurando su integración con los sistemas definidos por la entidad y su adecuada operación en los ambientes establecidos.
13. Realizar las pruebas necesarias para garantizar el correcto funcionamiento de la solución y efectuar los ajustes requeridos hasta su aprobación por parte del supervisor.
14. Realizar el despliegue y puesta en operación de la solución en los ambientes definidos por la entidad.
15. Garantizar la documentación técnica y funcional necesaria para la operación, administración y mantenimiento de la solución.
16. Realizar la transferencia de conocimiento técnico y funcional a los equipos definidos por la entidad.
17. Entregar los informes correspondientes al finalizar cada una de las fases/componentes, que incluya el detalle del cumplimiento de las obligaciones contractuales, registro fotográfico, cantidades ejecutadas, entre otros incluyendo lecciones aprendidas, para ser analizado y aprobado por el supervisor del contrato. Igualmente, deberá presentar los demás informes que sean requeridos por el supervisor o por el equipo de trabajo indicado por la Secretaría General durante la ejecución del contrato.
18. El Contratista en ejercicio de su obligación legal responderá por el soporte, calidad, idoneidad, seguridad, buen estado y correcto funcionamiento de la solución desarrollada, por un (1) año contado a partir de la terminación del contrato, en los términos de los artículos 8 y 11 de la Ley 1480 de 2011. Esta obligación constituye el término mínimo de garantía exigido en el presente proceso. En caso de que el contratista, en su oferta, haya establecido un mayor tiempo de garantía, estará obligado a mantener las condiciones de soporte, calidad y funcionamiento de la solución durante el término ofrecido, el cual se incorporará automáticamente como parte de sus obligaciones contractuales. En todo caso, el cumplimiento de esta obligación se mantendrá como una responsabilidad legal y contractual derivada del desarrollo de la solución tecnológica, exigible directamente al contratista durante todo el período de garantía.
19. Atender y corregir, sin costo adicional para la entidad, los errores o fallas que se presenten durante la ejecución y el periodo de garantía.
20. Entregar al supervisor el código fuente, repositorios, configuraciones y demás artefactos necesarios para la administración de la solución por parte de la entidad, con su respectiva documentación.
21. Garantizar que la solución propuesta y sus componentes (frameworks, librerías, motores de bases de datos) sean de código abierto (Open Source) libre de regalías, o que sus costos de licenciamiento a perpetuidad estén cubiertos al 100% dentro del valor de la oferta. Queda expresamente prohibido implementar componentes que generen costos de licenciamiento, suscripción o renovación ocultos para la Entidad posteriores a la liquidación del contrato, salvo aprobación previa y escrita de la supervisión.

22. Atender a las instrucciones y demás requerimientos que realice el supervisor del contrato relacionados con el objeto del contrato.
23. Garantizar la articulación técnica y operativa con las dependencias de la entidad que participen en el proyecto, así como con los sistemas de información que deban integrarse.
24. Realizar la cesión de derechos a la Secretaría General de los desarrollos a la medida generados durante la ejecución del contrato, así como, entregar los insumos requeridos para el ingreso al almacén de estos.
25. Cumplir con los lineamientos de seguridad de la información, protección de datos personales y gobierno digital definidos por la entidad y la normativa vigente.
26. Presentar informe consolidado final, conforme a los estándares y lineamientos establecidos por la supervisión y la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC de la Secretaría General.
27. Asistir a las reuniones a los cuales sea convocado por el supervisor del contrato.
28. Apoyar **el proceso de cierre contractual, incluyendo la suscripción del acta de recibo a satisfacción y la entrega de la documentación requerida para la liquidación del contrato.**
29. Mantener durante la vigencia del contrato los valores ofertados, sin lugar a reajustes.
30. Cumplir con las demás obligaciones que se deriven de la naturaleza del contrato y de su correcta ejecución.

11. Plazo de Ejecución.

El plazo total previsto para la ejecución del contrato es de cuatro (4) meses distribuidos conforme a las fases, actividades y entregables establecidos en el presente anexo técnico.

12. Garantía y soporte de la solución.

12.1 Garantía.

El proveedor en ejercicio de su obligación legal responderá por la calidad, idoneidad, seguridad, buen estado y correcto funcionamiento de la solución desarrollada, por un (1) año contado a partir de la terminación del contrato, en los términos de los artículos 8º y 11º de la Ley 1480 de 2011. Se entenderán incluidos dentro de la garantía todos los aspectos de los que habla el artículo 11º de la Ley 1480 de 2011, entre los que se encuentran los defectos en el software, así como las correcciones producto de defectos, en manuales u otros artefactos del proyecto, sin que ello genere costos adicionales para la Entidad.

12.2. Soporte de la solución.

El proveedor brindará administración, soporte funcional y técnico de las soluciones implementadas, desde la puesta en producción de cada iteración o paquete de trabajo y hasta la finalización del contrato, dicho soporte técnico deberá contemplar:

- Soporte 24/7 para problemas críticos que afecten la operación completa, como caídas del sistema o fallos masivos en transacciones, clasificando las incidencias por niveles de severidad: críticas, altas, medias y bajas.

- Soporte para las consultas generales o ajustes menores podrá brindarse en horarios laborales a través de correo electrónico, teléfono, chat en línea o sistemas de tickets.

- Mantenimiento preventivo, correctivo y evolutivo para garantizar estabilidad, nuevas funcionalidades y cumplimiento de regulaciones.

- Escalabilidad de la infraestructura para soportar aumentos en la cantidad de usuarios o transacciones.

- Monitoreo continuo 24/7, con generación de reportes regulares sobre rendimiento, tiempo de inactividad y resolución de incidencias.

- Alertas o alarmas que permitan anticipar y mitigar problemas que afecten a los usuarios finales y a los servicios.

- Registro de las solicitudes de servicio a través de los medios establecidos, como mesa de ayuda (nivel 1), llamadas telefónicas y correos electrónicos.

- Análisis de los casos recibidos en nivel 1 y escalarlos a nivel 2 o 3 cuando sea necesario.

- Resolución de las solicitudes según los tiempos establecidos en los Acuerdos de Nivel de Servicio (ANS).

- Análisis de vulnerabilidades semestrales sobre la solución tecnológica y generar informes detallados. Todas las vulnerabilidades detectadas deberán ser remediadas y/o mitigadas, priorizando aquellas de severidad alta o media. En caso de que alguna vulnerabilidad no pueda ser completamente eliminada, se deberá sustentar el riesgo asociado. Estas acciones deberán llevarse a cabo durante la ejecución y hasta el período de garantía.

13. Localización.

El lugar de ejecución será la ciudad de Bogotá. Parte de la ejecución del proyecto se llevará a cabo, si así se requiere, de manera presencial en las instalaciones de la Secretaría General de la Alcaldía Mayor de Bogotá y Puntos de atención de la red Cade los cuales se encuentran en diferentes localidades de la ciudad de Bogotá.

No obstante, con el fin de garantizar flexibilidad, eficiencia y continuidad en las actividades, también se contempla la posibilidad de desarrollar algunas fases mediante herramientas virtuales, aprovechando plataformas digitales para facilitar la interacción, el seguimiento y la gestión remota. Esta modalidad mixta permitirá adaptarse a las necesidades logísticas y operativas del proceso, optimizando recursos y tiempos.

14. Glosario.

- **Plataforma Unificada de Servicios de la Red CADE:** Ecosistema tecnológico donde se integran varios módulos dentro de un mismo entorno, ofreciendo acceso unificado y permitiendo evolución independiente por módulo.
- **Shell:** Aplicación que centraliza autenticación, navegación, contexto de sesión y carga dinámica de módulos. Está desarrollada en Angular v21 y no se entrega el código fuente al contratista.
- **Microfrontend:** Enfoque para construir la capa de presentación como módulos desacoplados que se integran en la plataforma. Debe cumplir lineamientos de arquitectura, interoperabilidad, versionamiento y gobiernos definidos por OTIC.
- **Web Component:** Formato exigido para entregar el microfrontend; se carga dinámicamente por la Shell cuando el usuario navega al módulo.
- **Backend:** Servicios propios del módulo que contienen la lógica de negocio y exponen APIs para consumo del microfrontend.
- **Microservicios:** Estilo arquitectónico requerido para los servicios del módulo: servicios independientes, escalables y desacoplados, alineados con la arquitectura de la plataforma.
- **API Gateway:** Componente de integración que centraliza exposición/gestión/control de APIs; el microfrontend no debe consumir "directo" backends por fuera de los mecanismos definidos por la arquitectura.
- **Versionamiento (de APIs/módulos):** Esquemas de empaquetado, despliegue y compatibilidad para evolución controlada e independiente sin afectar otros módulos.
- **Design system:** Librerías y criterios institucionales de UI/UX (accesibilidad, usabilidad, navegación) que la Entidad suministra para garantizar coherencia visual.
- **Keycloak:** Proveedor central de identidad de la plataforma; valida credenciales, emite tokens, administra sesiones y gestiona roles/grupos de alto nivel.
- **Token de autenticación:** Token emitido por el proveedor de identidad y suministrado por la Shell como parte del contexto; los servicios backend del módulo deben validarlo.
- **LDAP (directorio institucional):** Si se requiere integración con directorio, se realiza a través de Keycloak; el módulo no se integra directamente al directorio.
- **RBAC (Role-Based Access Control):** Control de acceso basado en roles; se menciona como control a validar en pruebas y aplicar transversalmente.
- **DLP (Data Loss Prevention):** Control para prevenir fuga/pérdida de datos; aparece como parte de controles de seguridad a implementar/validar.
- **Cifrado en tránsito:** Protección de datos durante comunicación; se exige uso de protocolos seguros (TLS) y validación de configuraciones en análisis/diseño.
- **Cifrado en reposo:** Protección de datos almacenados; se menciona como control de seguridad a considerar junto con otros (RBAC, DLP, auditoría).

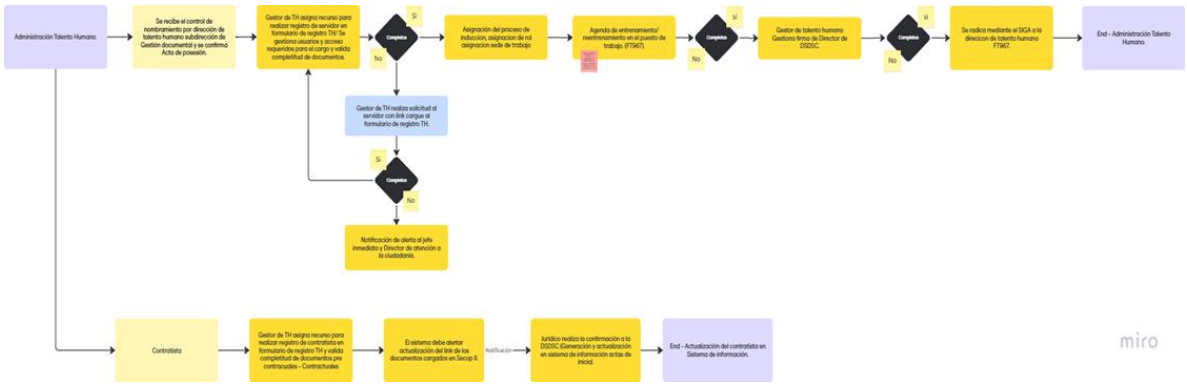
- **TLS:** Protocolo para cifrado en tránsito; versiones/algoritmos se validan en análisis/diseño.
- **Prometheus:** Herramienta para recolección de métricas de servicios/componentes.
- **Grafana:** Herramienta para visualización de métricas y tableros de monitoreo.
- **Zipkin:** Herramienta para trazas distribuidas (tracing) y análisis del recorrido de solicitudes en arquitectura.
- **Endpoints (de métricas/tracing):** Puntos de exposición que permiten recolectar métricas y trazabilidad para integrarse al stack de observabilidad existente.
- **DWH (Data Warehouse):** Almacén para analítica/explotación; se plantea alimentarlo desde la plataforma mediante procesos ETL desde las fuentes de datos de cada módulo.
- **ETL (Extract, Transform, Load):** Procesos de extracción e integración hacia DWH; se describe un esquema desacoplado por módulo y ventanas programadas (ej. nocturnas) para no afectar la operación transaccional.
- **Diccionario de datos:** Documento que define campos/estructura y reglas de calidad/gobierno de datos para el módulo
- **On-premise:** Infraestructura de la Entidad (centro de datos) donde está desplegada la plataforma.
- **Docker:** Contenedores para estandarizar despliegue/portabilidad; el módulo debe ser desplegable en contenedores.
- **Docker Swarm (clúster):** Orquestación/gestión de servicios en la infraestructura institucional; se despliegan stacks cumpliendo lineamientos técnicos/seguridad/operación.
- **Stack (de despliegue):** Conjunto de servicios desplegados en el clúster (se menciona “despliegue de nuevos stacks”).
- **CI/CD (pipelines):** Procesos automatizados de integración y despliegue; en la Entidad se usa Jenkins y el contratista puede ajustar/implementar pipelines alineados a lineamientos.
- **Jenkins:** Herramienta institucional para pipelines CI/CD y despliegues automatizados.
- **Registry (de contenedores):** Repositorio institucional de imágenes para certificación/producción; el contratista debe publicar/migrar imágenes allí siguiendo lineamientos de seguridad y versionamiento.
- **GitLab / Azure DevOps:** Repositorios institucionales para control de versiones; accesos gestionados por OTIC según fases del proyecto.
- **SSH (acceso directo a nodos):** No se proporciona acceso SSH directo a nodos del clúster; la administración es de OTIC.
- **Oracle Linux Server 9.6:** Sistema operativo mencionado para ambientes institucionales.

- **Oracle Database 19c / PostgreSQL 17:** Motores de base de datos mencionados en la plataforma (SAT WEB / Shell).
- **QA (Quality Assurance):** Pruebas de calidad (funcionales y no funcionales) incluidas en fase de pruebas.
- **UAT (User Acceptance Testing):** Pruebas de aceptación con usuarios; se mencionan como parte de las pruebas integrales.
- **SLA/SLO:** Referencia a lineamientos de calidad (se menciona como “SLA/SLO” en planificación de calidad).
- **OpenAPI/Swagger:** Especificación/documentación técnica de APIs orientada a interoperabilidad; se exige junto con lineamientos de seguridad aplicados.
- **Modelo C4:** Modelo recomendado para documentar arquitectura (Contexto, Contenedores, Componentes y Despliegue) o equivalente.
- **README (por microservicio):** Archivo requerido con propósito, dependencias e instrucciones precisas de ejecución/configuración/despliegue local y servidor.
- **Clean Code:** Requisito de calidad del código (código comentado y buenas prácticas).
- **EoL (End of Life):** Exigencia de mantener componentes alineados con ciclos de vida/soporte; evitar tecnologías que entren en fin de soporte durante contrato/garantía.

15. Anexos.

Se relacionan dos flujos del proceso como referencia. Se aclara que estos flujos deben ser confirmados y complementados durante las fases 1 y 2.

1. Flujo de registro Personal en el módulo de administración y planeación del servicio de la Red Cade.



2. Flujo de registro de novedades administrativas del personal que labora para la Red Cade.



Proyectó	Edwar Alexis Silva Angulo	Contratista - Dirección del Sistema Distrital de Servicio a la Ciudadanía
Proyectó	Cristian Camilo Wilches Parada	Practicante - Dirección del Sistema Distrital de Servicio a la Ciudadanía
Proyectó	Claudia Lorena Usuga Gil	Contratista - Dirección del Sistema Distrital de Servicio a la Ciudadanía
Proyectó	Erney Octavio Tulande Dulcey	Contratista - Oficina de Tecnologías de la Información y las Comunicaciones
Proyectó	Carlos Andrés Castro Cuello	Técnico Operativo - Oficina de Tecnologías de la Información y las Comunicaciones
Revisó	Erika Tatiana Quintero Quintero	Contratista - Oficina de Tecnologías de la Información y las Comunicaciones
Revisó	Juan Camilo Parra Rojas	Contratista - Subsecretaría de Servicio a la Ciudadanía
Aprobó:	Arleth Patricia Saurith Contreras	Jefe - Oficina de Tecnologías de la Información y las Comunicaciones
Aprobó:	Enrique Cusba García	Director del Sistema Distrital de Servicio a la Ciudadanía