1. Justificación técnica del Ecosistema Digital para la Alcaldía de Santiago de Cali.

La implementación de un Ecosistema Digital integral para el Distrito de Santiago de Cali se fundamenta en el Plan de Desarrollo Distrital 2024-2027 "Cali, capital pacífica de Colombia" (Acuerdo No.0578 de 2024), que prioriza la consolidación de un Buen Gobierno a través del fortalecimiento institucional y el despliegue de una infraestructura tecnológica de alta disponibilidad y eficiencia. Esta iniciativa responde directamente a las responsabilidades del Departamento Administrativo de las Tecnologías de la Información y las Comunicaciones (DATIC) de modernizar la gestión estratégica de las TIC, optimizar la eficiencia administrativa, y mejorar sustancialmente la prestación de servicios a los ciudadanos, asegurando la interoperabilidad y la seguridad integral de los sistemas de información municipales.

Actualmente, la Alcaldía de Santiago de Cali enfrenta el desafío operativo derivado de la existencia de procesos críticos soportados en aproximadamente diez (10) soluciones tecnológicas que operan de manera no integrada. Esta situación genera fragmentación de datos, limita la capacidad para la toma de decisiones informadas y oportunas, e incrementa la exposición de la información institucional a riesgos de seguridad. Paralelamente, existe una creciente y legítima demanda ciudadana por acceder a servicios digitales que sean intuitivos, ágiles, seguros y transparentes.

Para superar estos retos estructurales, se requiere la provisión de un Ecosistema Digital robusto, cohesionado e interoperable, que será adquirido y operado bajo una **modalidad de solución tecnológica como servicio gestionado y evolutivo**. La columna vertebral de este ecosistema será el **Sistema Central de Interoperabilidad (SCI)**, un componente de middleware avanzado diseñado para: unificar la gestión de identidades y accesos; orquestar los servicios entre los diferentes módulos; consolidar la auditoría de transacciones y eventos; y garantizar la integración segura y eficiente de las **diez (10) soluciones que lo componen** *(el propio SCI y las nueve aplicaciones sectoriales detalladas en el Anexo Técnico).* Esta solución integral incluirá, como mínimo, autenticación federada (implementando Single Sign-On y RBAC), autenticación multifactor (MFA) para accesos críticos, y un robusto gobierno de APIs. Todo el ecosistema se alineará con la Política de Gobierno Digital (Decreto 767 de 2022), el Modelo de Arquitectura Empresarial (MAE) y las guías de interoperabilidad de MinTIC.

Un requisito fundamental y no negociable de esta contratación es que, **al finalizar el contrato de servicio gestionado, el oferente deberá entregar a la Alcaldía de Santiago de Cali el código fuente completo y toda la documentación técnica asociada de todas las soluciones implementadas y configuradas dentro del ecosistema**. Esta entrega es crucial para asegurar la soberanía tecnológica del Distrito, la continuidad operativa a largo plazo, y la capacidad de evolución independiente de la plataforma.

Este Ecosistema Digital, provisto como servicio gestionado con transferencia final de conocimiento y activos, generará beneficios clave para el Distrito:

1. **Ciudadanía empoderada:** Acceso unificado (SSO), simplificado y ágil a trámites y servicios digitales, mejorando la experiencia del usuario.
2. **Administración eficiente:** Optimización de procesos internos, reducción de redundancias y una toma de decisiones basada en datos integrados y consolidados, provenientes de los diversos sistemas interconectados.
3. **Gobierno abierto y confiable:** Mayor transparencia en la gestión pública y facilitación de la rendición de cuentas mediante la trazabilidad de las operaciones y el acceso controlado a la información.
4. **Plataforma sostenible y adaptable:** Implementación de una arquitectura moderna (ej. microservicios para el SCI) que permita la escalabilidad horizontal y vertical, y la evolución futura de los servicios. La **continuidad operativa y la soberanía tecnológica estarán aseguradas por la propiedad del código fuente** transferido al finalizar el periodo de servicio.

2. Objeto y Alcance

2.1. Objeto del contrato

Implementar una solución Web en la infraestructura nube del Distrito de Santiago de Cali, adaptada a sus necesidades institucionales, mediante prácticas modernas de desarrollo y gestión de aplicaciones.

3. Alcance general

El proyecto tiene como alcance la **provisión, parametrización, puesta en marcha, operación y evolución de un Ecosistema Digital integral como servicio** para el Distrito de Santiago de Cali. Este servicio incluye la habilitación de una plataforma tecnológica robusta y segura que integre las siguientes soluciones informáticas, las cuales serán operadas y optimizadas por el oferente dentro de un entorno unificado y seguro, y cuyo código fuente será transferido a la Alcaldía al finalizar el contrato:

Soluciones a Configurar e Integrar

Las soluciones que serán implementados e interconectados dentro de la nueva plataforma incluyen:

- Sistema de información de Seguridad Alimentaria
- Sistema de información de Bienestar Animal
- Sistema de información de Administración y Gestión de Grupos Poblacionales
- Sistema de información de planificación estratégica y articulación intermunicipal AMSO (Área Metropolitana del Suroccidente)

- Plataforma para la administración de juntas comunales y su relación con la ciudadanía.
- Sistema de información para el análisis de datos y seguimiento de políticas de equidad de género.
- Plataforma para auditoría y seguimiento de procesos administrativos.
- Sistema de información integrado de datos para la planificación y desarrollo integral
- Aplicación para la gestión y administración de Ecoparques del Distrito de Cali

Cada una de estas soluciones será diseñada para operar en sinergia con el resto del ecosistema digital, asegurando un flujo de información eficiente y seguro.

Implementación del Control de Acceso Federado y Autenticación Centralizada

Uno de los aspectos más innovadores del proyecto es la incorporación de un **modelo de autenticación y acceso unificado**, el cual garantizará:

- **Acceso único (Single Sign-On, SSO):** Los usuarios solo necesitarán autenticarse una vez para acceder a todas las soluciones y servicios digitales.
- **Gestión eficiente de permisos:** Se establecerán políticas centralizadas para definir quién puede acceder a qué recursos y bajo qué condiciones.
- **Mayor seguridad:** Se integrarán mecanismos avanzados de protección, como autenticación multifactor (MFA), detección de accesos sospechosos y cifrado de datos sensibles.
- **Reducción de riesgos operativos:** Al eliminar múltiples puntos de autenticación dispersos, se minimizan errores en la gestión de accesos y se fortalece la seguridad de la información.

Este enfoque **mejorará significativamente la experiencia del usuario**, agilizando el acceso a los servicios digitales y eliminando la necesidad de múltiples contraseñas, al mismo tiempo que refuerza la ciberseguridad institucional.

4. Especificaciones técnicas – Ficha Técnica

4.1. Principios Arquitectónicos y Técnicos Generales

La arquitectura del ecosistema se fundamentará en principios clave para asegurar su robustez y alineación con las necesidades del Distrito. Se priorizará la **interoperabilidad**, definida como la capacidad de los distintos sistemas, plataformas o aplicaciones para intercambiar información y operar de manera coordinada. Esta interoperabilidad será gestionada centralmente por el Sistema Central de Interoperabilidad (SCI), que actuará como un middleware, ya sea a través de un Enterprise Service Bus (ESB) o un API Gateway.

Un pilar fundamental será el **Control de Acceso Federado y la Autenticación Centralizada**. Este enfoque permitirá un acceso único (Single Sign-On, SSO), donde los usuarios se autenticarán una vez para acceder a todas las soluciones. La gestión de permisos se realizará de manera eficiente mediante el Control de Acceso Basado en Roles (RBAC) y se integrará con el

Directorio Activo (AD) de la Alcaldía. Se emplearán estándares como OAuth 2.0, OpenID Connect y SAML, y se implementará la autenticación multifactor (MFA) para los accesos considerados críticos.

La plataforma adoptará una **arquitectura basada en microservicios** para el SCI, lo que garantizará la modularidad y escalabilidad del sistema. La comunicación entre los diversos módulos y servicios se realizará predominantemente a través de **APIs**, utilizando formatos estándar como JSON y XML para las respuestas estructuradas.

Se incorporará la **seguridad en el software (DevSecOps implícito)**, aplicando prácticas para minimizar riesgos desde las fases iniciales, lo que incluye autenticación robusta y el cifrado de datos sensibles, como el uso del algoritmo AES-256. La **escalabilidad** será un criterio de diseño esencial, buscando una infraestructura flexible que permita la incorporación de nuevas funcionalidades y un diseño modular que facilite la escalada horizontal, apoyándose en tecnologías de contenedores como Docker/Kubernetes.

La gestión del proyecto se realizará bajo **Metodologías Ágiles**, específicamente Scrum, y se aplicarán prácticas de **DevOps** para la entrega y mantenimiento del software.

4.2. Componentes centrales de la Plataforma Imágenes de referencia

imagen 1: Pantalla de autenticación





Imagen 2: Pantalla de módulos



Imagen 3: Pantalla de indicadores de módulo

La plataforma tecnológica integrada permitirá la gestión eficiente de los procesos administrativos y operativos de la Administración Distrital, asegurando el cumplimiento de los requerimientos específicos de cada iniciativa:

4.3. MÓDULO INTEGRADOR Cloud Sistema Central de Interoperabilidad (SCI)

El SCI es el componente clave diseñado para facilitar la interoperabilidad eficiente entre los módulos de la plataforma, mejorar la seguridad a través de la autenticación centralizada y garantizar la escalabilidad del ecosistema digital. Su integración con el Directorio Activo de la Alcaldía permitirá una gestión unificada de identidades y permisos.

Gestión de Interoperabilidad: El SCI actuará como un middleware, utilizando un Enterprise Service Bus (ESB) o un API Gateway, para permitir una comunicación fluida, segura, rápida y normalizada entre los diferentes módulos del ecosistema.

Flujo de Datos y Procesos: Las entradas consistirán en solicitudes de acceso a datos y servicios provenientes de los módulos, mientras que las salidas serán respuestas estructuradas conforme a estándares definidos como JSON o XML. El flujo de procesos se iniciará cuando un módulo realice una solicitud; el SCI verificará la autenticación y los permisos en el Directorio Activo de la Alcaldía, normalizará la solicitud según los estándares, la enrutará al módulo correspondiente, donde será procesada para generar una respuesta que el SCI formateará y entregará al módulo solicitante.

Reglas de Negocio y Excepciones: Será mandatorio que todos los módulos estén registrados en el catálogo de servicios del SCI. Se implementarán políticas para el control de tráfico y la limitación de consultas. El manejo de errores incluirá respuestas específicas como HTTP 401 para fallos de autenticación, HTTP 503 con reintento programado para servicios no disponibles, y HTTP 400 con detalle del problema para formatos incorrectos de solicitud.

Autenticación Federada y Gestión de Identidad: Descripción: El SCI empleará autenticación centralizada y federada mediante los protocolos estándar OAuth 2.0, OpenID Connect y SAML. Esta funcionalidad se integrará con el Directorio Activo de la Alcaldía para consolidar una gestión de identidades y accesos única y segura.

Flujo de Datos y Procesos: Como entrada, el sistema recibirá las credenciales del usuario o un token de sesión. La salida será un token de acceso con permisos definidos según el rol del usuario. El proceso de autenticación comenzará cuando un usuario o módulo solicite acceso a un servicio; se verificará la identidad contra el Directorio Activo, y si la autenticación es exitosa, se generará un token de acceso que habilitará el uso de los servicios permitidos.

Reglas de Negocio y Excepciones: Toda autenticación de usuario deberá pasar por el Directorio Activo. Los permisos se gestionarán mediante un Control de Acceso Basado en Roles (RBAC), y se requerirá autenticación multifactor (MFA) para accesos considerados críticos. Los errores comunes gestionados incluirán HTTP 401 para credenciales incorrectas, la necesidad de renovación de token o reautenticación para tokens expirados, y respuestas HTTP 403 para accesos no autorizados.

Registro, Monitoreo y Auditoría de Eventos: El sistema incorporará un módulo de auditoría robusto encargado de registrar todas las acciones realizadas por usuarios y módulos dentro de la plataforma, con el fin de garantizar la trazabilidad completa y la seguridad del ecosistema.

Flujo de Datos y Procesos: Las entradas para este módulo serán los registros de accesos,

modificaciones de datos y errores que ocurran en los sistemas integrados. Como salida, el módulo generará reportes detallados y alertas sobre actividades que se consideren sospechosas. El flujo operativo consistirá en la captura de eventos de acceso y transacciones en tiempo real, su almacenamiento seguro en una base de datos dedicada y la activación de alertas automáticas ante la detección de actividades anómalas o sospechosas.

Reglas de Negocio y Excepciones: Se establecerá como regla de negocio el registro de todos los accesos, modificaciones y errores críticos que se presenten. El acceso para consultar estos registros de auditoría estará restringido únicamente a personal debidamente autorizado. En caso de excepciones, como la pérdida de conexión con el sistema de auditoría, se almacenará un log temporal y se intentará el envío posteriormente; si se detecta un intento de acceso no autorizado a los registros, se generará una alerta inmediata y se procederá al bloqueo de la sesión correspondiente.

Integrador de Indicadores: Conforme al Anexo Técnico, este módulo se encargará de consolidar y visualizar los Indicadores Clave de Desempeño (KPIs) provenientes de los diversos sistemas fuente que conforman la plataforma.

Arquitectura del SCI: La arquitectura propuesta para el Sistema Central de Interoperabilidad se basará en un modelo de microservicios, lo cual promueve la modularidad y facilita la escalabilidad. Un componente central de esta arquitectura será el API Gateway, encargado de centralizar y gestionar las solicitudes.

5. Soluciones Específicas del Ecosistema

5.1. Solución Web Sistema Integral de Gestión de la Seguridad Alimentaria

Esta plataforma tecnológica está diseñada para optimizar la administración, el monitoreo y el control de los procesos relacionados con la distribución de alimentos a poblaciones vulnerables. Su finalidad principal es garantizar la trazabilidad, la eficiencia y la transparencia en todas las etapas del proceso.

Componentes Técnicos y Funcionalidades Clave:

5.1.1. Se realizará el registro y caracterización de la población beneficiaria, asignando un código único y permitiendo la integración de datos con el SISBEN.

5.1.2. El monitoreo y control de inventarios en centros de acopio y distribución se efectuará en tiempo real, incluyendo alertas de vencimiento de productos y condiciones críticas de almacenamiento. Se implementarán mecanismos para la redistribución eficiente de alimentos con el fin de evitar desperdicios.

5.1.3. Se establecerá un riguroso control de calidad e inocuidad de los alimentos, que incluirá el registro de inspecciones por lote y la generación de alertas para productos no aptos.

5.1.4. La interoperabilidad con sistemas externos, tanto gubernamentales como de proveedores, se facilitará mediante el uso de APIs o servicios web, asegurando la encriptación de datos y la validación de la información intercambiada.

5.1.5. El sistema emitirá alertas y notificaciones automáticas ante situaciones críticas como escasez de inventario, fechas de vencimiento próximas o problemas de calidad, utilizando umbrales configurables por los administradores.

5.1.6. Se dispondrá de un panel de control y dashboard de análisis que permitirá visualizar indicadores de desempeño en tiempo real, con capacidad de exportar reportes en formatos estándar como PDF, Excel y CSV.

5.1.7. La seguridad del sistema se gestionará a través de un módulo específico que controlará la autenticación (incluyendo MFA para roles críticos), la autorización basada en roles, y mantendrá un log de auditoría inmutable para todas las actividades, en cumplimiento con normativas como ISO 27001 y GDPR si aplica.

5.1.8. Un módulo de gestión de seguridad alimentaria permitirá administrar programas de Alimentación Escolar,centralizar y contrastar la información de beneficiarios frente a requisitos normativos predefinidos. El sistema facilitará la validación de condiciones de elegibilidad y la trazabilidad del impacto, optimizando la transparencia en la ejecución presupuestal.

5.2. Solución Web Sistema Aplicativo Bienestar Animal

Este sistema tiene como finalidad fortalecer la gestión y protección de los animales mediante la implementación de herramientas tecnológicas que faciliten la identificación, el registro, la trazabilidad, el acceso a servicios veterinarios, la promoción de adopciones y la gestión de reportes de maltrato o abandono.

Componentes Técnicos y Funcionalidades Clave:

5.2.1. El registro y gestión de animales se realizará asignando un código de identificación único, ya sea mediante microchip o código QR, generando una ficha digital para cada animal que incluirá su historial clínico vinculado.

5.2.2. La gestión de la atención veterinaria permitirá el registro de consultas, diagnósticos, procedimientos realizados y medicamentos administrados, actualizando el historial clínico y programando recordatorios para vacunas y esterilizaciones.

5.2.3. El módulo de adopciones facilitará el proceso mediante la evaluación de adoptantes, la generación de certificados de adopción (potencialmente digitales) y la programación de visitas de seguimiento post-adopción.

5.2.4. Se gestionarán las denuncias por maltrato o abandono, permitiendo la georreferenciación del caso, la asignación a la Unidad de Rescate Animal correspondiente y la documentación detallada de las intervenciones realizadas.

5.2.5. La administración del sistema incluirá la gestión de usuarios y sus permisos, el control de inventario de insumos veterinarios con alertas automáticas para stock mínimo, y la generación de reportes automáticos

sobre las operaciones del sistema.

5.3. Solución Web Sistema de Administración y Gestión de Grupos Poblacionales

Este sistema está diseñado para permitir el registro, seguimiento, análisis y gestión de datos de los distintos grupos poblacionales, con el fin de garantizar una administración eficiente y facilitar la toma de decisiones basada en información socioeconómica y de acceso a servicios actualizada.

Componentes Técnicos y Funcionalidades Clave:

5.3.1. Se implementará un módulo para el registro y gestión de la población, permitiendo la actualización de información de individuos y comunidades con asignación de un número de identificación único. Este registro validará datos y permitirá el cruce con fuentes oficiales como SISBEN y RUAF.

5.3.2. La gestión de programas sociales y beneficios incluirá la identificación, asignación y seguimiento de ayudas, con validación automatizada de criterios de elegibilidad y un historial de los apoyos recibidos por individuo o comunidad.

5.3.3. El monitoreo de condiciones de vida se realizará a través del análisis de datos demográficos y socioeconómicos, así como del acceso a derechos básicos. Se generarán reportes estadísticos, mapas de Vulnerabilidad Social georreferenciados y alertas tempranas sobre problemáticas emergentes o riesgos sociales.

5.3.4. La seguridad del sistema se garantizará mediante una robusta administración de accesos, roles y permisos, el cifrado de datos sensibles y un detallado registro de auditoría de todas las acciones realizadas en el sistema.

5.3.5. Se proveerá una funcionalidad para la generación de reportes y análisis de datos en tiempo real, con opciones de personalización, filtros y visualización en gráficos y dashboards, además de la exportación de informes.

5.4. Solución Web Sistema de Información de Planificación Estratégica y Articulación Intermunicipal AMSO

Esta plataforma centralizada busca fortalecer la cooperación y el desarrollo regional en el Área Metropolitana del Suroccidente (AMSO), facilitando la planificación estratégica, la gestión de proyectos intermunicipales y el monitoreo del impacto de políticas metropolitanas.

Componentes Técnicos y Funcionalidades Clave:

5.4.1. Se dispondrá de una base de datos para proyectos intermunicipales que permitirá su registro, actualización y consulta, asignando un ID único y gestionando información como municipios involucrados, presupuesto, cronograma de ejecución (con visualización tipo Gantt), estado del proyecto y documentos asociados, además de generar alertas sobre plazos y presupuesto.

5.4.2. Un módulo para la coordinación de estrategias de desarrollo regional facilitará la planificación conjunta, permitiendo definir estrategias, objetivos comunes, líneas de acción e indicadores de éxito, y generando reportes comparativos entre municipios.

5.4.3. El monitoreo del impacto de políticas metropolitanas se realizará mediante la recopilación de datos, el análisis de indicadores clave (económicos, de movilidad, ambientales) habilitando una capacidad robusta para el cargue de archivos con datos masivos, permitiendo la recopilación y consolidación de los insumos necesarios y la integración potencial con fuentes externas, tales como sensores urbanos

o datos de gestión provenientes de Secretarías y Dependencias de los diferentes municipios que integran el área metropolitana. El sistema generará reportes de impacto y alertas por resultados negativos o desviaciones críticas.

5.4.4. El módulo procesará datos de sistemas de transporte público para mejorar la planificación y movilidad urbana, recopilando datos consolidados y de frecuencia actualizada sobre rutas, tráfico y uso, con el fin de analizar patrones, optimizar rutas y generar recomendaciones. Se desarrollarán indicadores de gestión territorial para el monitoreo del desarrollo urbano, económico, social o ambiental, presentados en tableros de control interactivos.

5.5. Solución Web Sistema Aplicativo Control y Gestión JAL/JAC

Este sistema tiene como objetivo central facilitar la administración integral de las Juntas de Acción Comunal (JAC) y Juntas Administradoras Locales (JAL) mediante herramientas digitales que optimicen sus procesos.

Componentes Técnicos y Funcionalidades Clave:

5.5.1. Se implementará un módulo para el registro e inscripción de miembros de las JAC y JAL, que incluirá la validación de identidad del ciudadano mediante integración con bases de datos gubernamentales como RENEC, y la generación de una credencial digital con código QR.

5.5.2. La gestión de juntas y dignatarios permitirá administrar la estructura organizativa, los dignatarios electos, sus períodos de vigencia y la gestión documental, destacando el almacenamiento de documentos administrativos, como actas, en tecnología Blockchain para garantizar su inmutabilidad y respaldo seguro.

5.5.3. Se facilitará la consulta y el seguimiento de proyectos comunitarios, permitiendo a ciudadanos y miembros de las juntas acceder a detalles de estado, avance y documentación, y habilitando la posibilidad de comentar y calificar dichos proyectos.

5.5.4. Los ciudadanos podrán presentar solicitudes comunitarias y reportar necesidades a través de un módulo dedicado, que asignará un número de solicitud y permitirá el seguimiento en tiempo real de su estado.

5.5.5. Se implementará una plataforma de participación ciudadana que incluirá un módulo de votaciones electrónicas y deliberación comunitaria, utilizando tecnologías de contratos inteligentes (Blockchain) para asegurar la transparencia e inmutabilidad de los resultados.

5.5.6. Se incorporará una plataforma de indicadores de bienestar para medir la calidad de vida de los ciudadanos, mediante el análisis de datos de salud, vivienda, educación, alimentación y empleo, utilizando modelos de análisis predictivo.

5.5.7. Finalmente, un sistema de evaluación de proyectos comunitarios empleará herramientas de inteligencia artificial para analizar la viabilidad, el impacto social y financiero de las propuestas, y para ayudar en la priorización de proyectos.

5.6. Solución Web Sistema Aplicativo Observatorio de Género (OGEN)

Este sistema especializado está orientado al fortalecimiento de la gestión pública en materia de prevención, atención y seguimiento de la violencia de género, consolidando información clave para la toma de decisiones estratégicas e interinstitucionales.

Componentes Técnicos y Funcionalidades Clave:

5.6.1. Se implementará un módulo para el registro y gestión de casos de violencia de género, garantizando la trazabilidad de la información. Este permitirá registrar datos del caso (tipo de violencia), de la víctima, del agresor (si se conoce), fecha, lugar, evidencias y entidad reportante, asignando un número único de identificación a cada caso y manteniendo un historial de seguimiento y acciones tomadas, con posible vinculación a entidades judiciales.

5.6.2. Un módulo de clasificación y validación de datos permitirá la categorización automática de los casos y la verificación de duplicidad, comparando la información con la base de datos existente y solicitando verificación manual si se detecta una alta probabilidad de duplicidad o inconsistencias en formatos.

5.6.3. La generación de reportes y análisis de datos facilitará la creación de informes estadísticos, gráficos, tablas y tableros de control sobre la violencia de género. Esto permitirá identificar tendencias y patrones, realizar comparaciones anuales y geográficas, y exportar la información en formatos como PDF y Excel.

5.6.4. Se habilitará un sistema de alertas y notificaciones automáticas para informar a las entidades responsables sobre casos críticos o situaciones que requieran intervención inmediata. Estas alertas se configurarán según parámetros como tipo de violencia, nivel de riesgo y entidad responsable, y se enviarán por correo electrónico, SMS o notificaciones en el sistema.

5.7. Solución Web Sistema de información Control Interno

Esta plataforma de auditoría y cumplimiento normativo está destinada a fortalecer la gestión administrativa y financiera del Distrito Especial.

Componentes Técnicos y Funcionalidades Clave:

5.7.1. Se definirá una funcionalidad para los Indicadores de Alerta Temprana y Desviación de Procesos que defina y monitoree indicadores clave de riesgo operacional (KRI) (ej. tiempo promedio de un proceso de contratación, número de documentos pendientes en un flujo de aprobación). Debe contar un sistema de "semáforo" de alertas que identifique automáticamente y notifique a la dependencia cuando un proceso se desvía de su línea base de eficiencia o está próximo a un incumplimiento, permitiendo la corrección *antes* de que se convierta en un hallazgo de auditoría.

5.7.2. Se implementará un Modelo de Alerta Temprana de Desembolsos (ATD) el cual analiza patrones históricos de ejecución presupuestal (tiempo de aprobación de pagos, retrasos en hitos de contrato, cambios de interventores) para generar un índice de riesgo de retraso o incumplimiento para cada contrato activo.

5.7.3. Contará con un Monitoreo de Patrones de Gasto Atípicos (MPGA) para

rastrea transacciones (gastos de caja menor, órdenes de servicio, viáticos) y compara el comportamiento de cada funcionario/dependencia con su patrón de gasto histórico normal.

5.7.4. Un módulo de Índice de Riesgo de Recidiva (IRR) el cual asigna una puntuación a cada dependencia o proceso que mide la probabilidad de que un hallazgo clasificado sea recurrente en el próximo ciclo de auditoría. Se basa en el tiempo que tardó el plan de mejora en cerrarse, la naturaleza del hallazgo y si la causa raíz fue atacada.

5.7.5. Se desplegará un Mapa de Riesgo de Cobertura (MRC) el cual combina el historial de auditorías realizadas con el nivel de riesgo inherente de la dependencia (definido por el presupuesto, número de funcionarios, criticidad misional). Genera una visualización de las

áreas que están sub-auditadas en relación con su nivel de riesgo. Este módulo usa el historial para identificar dónde no ha habido hallazgos durante mucho tiempo, lo que puede significar que el control está funcionando bien, o más probablemente, que la auditoría no está mirando en el lugar correcto (un punto ciego).

5.7.6. Un panel para Análisis Geográfico de Datos (Mapping) y Puntuación Ponderada el cual visualiza gráficamente las áreas de alto riesgo que han tenido cero o pocos hallazgos, priorizándolas automáticamente para futuras auditorías.

5.8. Solución Web Sistema Integrado de Datos para la Planificación y Desarrollo Integral

Este sistema proporcionará una infraestructura tecnológica, desplegable localmente o en la nube, diseñada para soportar la ingesta segura de información desde diversas fuentes, su almacenamiento estructurado y la ejecución automatizada de procesos ETL (Extracción, Transformación y Carga). Operará sobre el Data Lake con el que actualmente cuenta la Alcaldía, garantizando el acceso controlado por roles y una interfaz geográfica para visualizar la eficacia del gasto social, además de permitir el consumo de datos vía API.

Funcionalidades Técnicas Clave: Almacenamiento de Datos: Los datos se almacenarán en una base de datos relacional que permitirá accesos diferidos y seguros a la información contenida.

Gestión de Calidad de Datos: El sistema implementará puntos de control durante la carga de información para asegurar la calidad de los datos, estableciendo alertas y gestionando solicitudes referentes a datos inconsistentes, incoherentes o desactualizados.

Interoperabilidad y Actualización de Datos Maestros: Se habilitará la conexión continua y segura con otros sistemas de información o lagos de datos en la nube, sincronizada con los procesos de actualización de datos maestros. El sistema cruzará datos de diferentes fuentes de forma secuencial, asegurando su actualización en temporalidades flexibles (por demanda o por activación de proceso).

Información Georreferenciada y Visualización: Contendrá la información geográfica espacial de la ciudad de Santiago de Cali, permitiendo la visualización territorial de información social y la generación de resultados georreferenciados sobre la localización de personas registradas en SISBEN IV y/o beneficiarias de programas sociales. Se podrán filtrar resultados por población objetivo (beneficiada, propensa a serlo según SISBEN IV).

Control de Acceso e Interfaz: El acceso será diferido según roles de usuario: operarios de campo, coordinadores de área o administradores de sistemas (interesados en reportes agregados), y directivos o líderes de planeación. Se dispondrá de una interfaz web amigable e intuitiva para el consumo de los datos.

Gestión de Beneficiarios y Reportes: Permitirá la carga de información de caracterización de personas beneficiarias mediante formularios específicos y la actualización de sus datos básicos. Se podrán generar reportes estructurados con información histórica por organismo, programa, proyecto o año, con acceso segmentado por entidad usuaria.

Seguridad, Auditoría y Respaldo: Contará con mecanismos de seguridad para evitar el acceso no autorizado a información sensible. Se implementarán procesos de respaldo para casos de pérdida catastrófica de información y se mantendrán logs para auditar la actividad de carga, actualización y acceso por parte de los usuarios.

Administración y Mantenimiento: Incluirá una instancia para la gestión de usuarios nuevos y

la actualización de permisos de acceso. Permitirá la integración constante mediante APIs o VPN para el intercambio de información entre repositorios locales o en nube. Validará automáticamente la calidad, integridad y consistencia de los datos durante la carga e intercambio. Su arquitectura será escalable y manejable en términos del ciclo de vida de la información, permitiendo la depuración de datos cuando sea necesario. Los procesos ETL serán monitoreados con logs y alertas de fallos.

5.9. Solución Web Sistema Administración Ecoparques del Distrito de Cali

Esta solución web está diseñada para optimizar, centralizar y hacer más eficiente la administración operativa, administrativa, financiera y logística de los ecoparques del Distrito, buscando mejorar la experiencia ciudadana y promover la sostenibilidad ambiental.

Componentes Técnicos y Funcionalidades Clave:

5.9.1. La gestión de ingresos permitirá el registro, validación y control de accesos a los ecoparques utilizando tecnologías como códigos QR o PIN. El sistema proporcionará una confirmación inmediata de acceso (válido/inválido) y mantendrá un registro detallado de los accesos, incluyendo horarios, además de generar alertas automáticas ante accesos no autorizados o fuera de horario.

5.9.2. Un módulo para la gestión de reservas y actividades facilitará la reserva autónoma por parte de los ciudadanos, gestionando eficientemente el aforo disponible y la asignación de horarios. Se generará un comprobante digital de la reserva y se proveerá una potencial integración con pasarelas de pago.

5.9.3. Se podrán generar reportes operativos, administrativos y financieros detallados, exportables en formatos Excel y PDF, con una completa auditoría de acciones y registros. Cada solicitud de reporte quedará registrada para fines de auditoría.

5.9.4. Un dashboard global y específico por ecoparque ofrecerá la visualización dinámica de estadísticas e indicadores clave de gestión, como número de visitas, reservas activas, ingresos por pagos, cancelaciones, uso por horario e información de aforo en tiempo real.

5.9.5. Se aclara que la interoperabilidad inicial, una auditoría OWASP formal y un plan de mantenimiento o soporte extendido no están incluidos en la versión inicial del sistema, aunque la interoperabilidad está diseñada para una activación futura sencilla.

6. Requerimientos técnicos no funcionales comunes

- **Seguridad:** Se implementará autenticación multifactor (MFA) para los accesos considerados críticos. Los datos sensibles serán cifrados utilizando el estándar AES-256. Se registrarán logs de auditoría para todos los accesos y modificaciones realizadas en los sistemas.
- **Rendimiento:** Se garantizarán tiempos de respuesta inferiores a 2 segundos para las consultas más frecuentes. Los sistemas críticos deberán soportar hasta 1,000 usuarios concurrentes. Los procesos de Extracción, Transformación y Carga (ETL) de grandes volúmenes de datos se ejecutarán en ventanas nocturnas, con una duración máxima de 4

horas.

- **Disponibilidad:** Se asegurará un tiempo de actividad (uptime) del 99.9% para los sistemas críticos. Se implementarán mecanismos de redundancia para servidores y bases de datos. Se realizarán copias de seguridad (backups) diarias, con una política de retención de 30

días.

- **Interoperabilidad:** La integración entre los diferentes sistemas se realizará mediante APIs estándar, preferentemente REST con formato JSON. Se soportará la autenticación federada con el Directorio Activo de la Alcaldía. Los sistemas deberán cumplir con los estándares de interoperabilidad gubernamental aplicables, como la integración con RUAF.
- **Escalabilidad:** La arquitectura de los sistemas será modular, lo que permitirá escalar horizontalmente según las necesidades. Se promoverá el uso de tecnologías de contenedores, como Docker y Kubernetes, para ofrecer servicios flexibles y escalables.
- **Usabilidad:** Las interfaces de usuario serán diseñadas de forma intuitiva y deberán cumplir con los estándares de accesibilidad WCAG 2.1. Se ofrecerá capacitación a los usuarios finales para el manejo de las nuevas plataformas.
- **Cumplimiento Normativo:** Todos los sistemas deberán cumplir con la Ley de Protección de Datos Personales vigente en Colombia. En los casos que aplique, como la gestión de documentos legales en el sistema JAL/JAC, se utilizará tecnología blockchain para garantizar la integridad de dichos documentos.

7. Metodología y Buenas Prácticas:

- El ecosistema de sistemas de información se gestionará utilizando **Metodologías Ágiles**, con un enfoque particular en el marco de trabajo **Scrum**. Esto implica un **Desarrollo Incremental**, donde el software se construirá en pequeñas partes funcionales (incrementos) que se entregarán periódicamente. El trabajo se organizará en **Sprints**, periodos con una duración fija (generalmente de 2 a 4 semanas).
- Se adoptarán prácticas de **DevOps**, combinando el desarrollo de software (Dev) con las operaciones de TI (Ops) para promover la automatización, la colaboración, y mejorar la entrega y el mantenimiento continuo del software.
- La **Seguridad en el Software** será una prioridad, integrando prácticas para minimizar riesgos de ciberseguridad desde las fases iniciales. Esto incluye la implementación de autenticación robusta (como OAuth2) y el cifrado de las comunicaciones (HTTPS).
- El proceso de **pruebas** será exhaustivo, abarcando pruebas unitarias con el objetivo de alcanzar al menos un 80% de cobertura de código y generando reportes de las mismas. Se realizarán también pruebas funcionales, de integración, de regresión, pruebas de rendimiento y carga, así como evaluaciones de seguridad y pruebas de penetración antes del despliegue definitivo.
- Se generará **documentación técnica completa**, que incluirá el código fuente debidamente documentado y versionado, la documentación de las APIs configuradas, manuales de usuario y guías de administración detalladas. La arquitectura de software será documentada utilizando el modelo C4.

8. Consideraciones de Infraestructura:

- El **modelo de despliegue** de las soluciones se definirá en la fase de diseño arquitectónico y podrá ser en la nube, on-premise, o un esquema híbrido que asigne el Distrito de Santiago de Cali.
- Para los **servidores de aplicaciones y API Gateways**, se contempla el uso de sistemas operativos Linux, como RHEL o Ubuntu. Los **servidores destinados a la autenticación** podrían operar bajo Windows Server.

- En cuanto a nodos Blockchain, específicamente para el sistema de Control y Gestión JAL/JAC, **la plataforma seleccionada es Ethereum**, para la cual se considera un despliegue en la nube.
- La gestión de **bases de datos** incluirá tecnologías relacionales como PostgreSQL, SQL Server y Oracle (con Oracle Linux para el servidor de BD física del SIDEPDI).
- Se utilizará **tecnologías de contenedores** como Docker y Kubernetes, empleando sistemas operativos ligeros como Alpine Linux para algunos servicios web o procesos ETL, con el fin de optimizar los recursos y facilitar la escalabilidad.

9. Fases de implementación y forma de pago

Porcentaje de Pago	**Entregables claves**	**Fases correspondientes**
Primer pago 20%	● Presentación del Plan General del proyecto, que debe incluir: Plan de gestión de alcance, Plan de gestión de riesgos, Plan de gestión de calidad del proyecto, Cronograma - GANTT, Matriz de asignación de responsabilidades, Requerimientos de recursos del proyecto, y Plan de gestión de comunicaciones. ● Presentación del Informe de Instalación de la solución inicial	Esta etapa corresponde principalmente a la culminación de: **Fase 1: Análisis y Refinamiento de Requerimientos** (ERS validado, historias de usuario, diagramas BPMN, análisis de riesgos). Inicio y avances significativos en la **Fase 2: Diseño y Arquitectura del Ecosistema** (trabajo inicial en el Documento de Arquitectura, especificación de APIs, y prototipos).
Segundo pago 55%	● Presentación y demostración de los siguientes Módulos Funcionales en el Ambiente de Pruebas: Módulo Integrador Cloud Sistema Central de Interoperabilidad (SCI), Solución Web Sistema Integral de Gestión de la Seguridad Alimentaria, Solución Web Sistema Aplicativo Bienestar Animal, Solución Web Sistema de Administración y	Esta etapa se alinea con la finalización de: **Fase 3: Configuración, Parametrización e Integración** (código fuente, APIs, aplicaciones en ambiente de prueba, reportes de pruebas unitarias). El inicio y progreso sustancial de la **Fase 4: Pruebas e Implementación Piloto** (pruebas

	Gestión de Grupos Poblacionales, Solución Web Sistema de Información de Planificación Estratégica y Articulación Intermunicipal AMSO, Solución Web Sistema Aplicativo Control y Gestión JAL/JAC, Solución Web Sistema Aplicativo Observatorio de Género, Solución Web Sistema de información Control Interno, Solución Web Sistema Integrado de Datos para la Planificación y Desarrollo Integral, y Solución Web Sistema Administración Ecoparques. ● Constatación de un Ambiente de pruebas activo y funcional para dichos módulos	funcionales, de integración, rendimiento y seguridad en el ambiente de pruebas).
Tercer pago 25%	● Presentación del Ecosistema Operativo en Producción acompañado de la Documentación Final del proyecto. ● Informe de cumplimiento de todos los entregables establecidos en la propuesta. ● Informe de puesta en marcha en producción de todos los módulos listados en el segundo pago (SCI, Seguridad Alimentaria, Bienestar Animal, Grupos Poblacionales, AMSO, JAL/JAC, Observatorio de Género, Control Interno, Sistema Integrado de Datos, Administración Ecoparques). ● Acta de Entrega de la solución al equipo de soporte y de producción de la Alcaldía. ● Acta de cierre del proyecto	Esta etapa final corresponde a la culminación exitosa de: **Fase 4: Pruebas e Implementación Piloto** (informe de pruebas completo, registro de incidencias resueltas, manuales finales, feedback de piloto implementado). **Fase 5: Implementación Total y Monitoreo** (ecosistema completamente funcional en producción, capacitación completada, reportes iniciales de desempeño).

10. Equipo Requerido (Modalidad híbrida)

Para asegurar el éxito en la provisión, configuración, integración, optimización y evolución del Ecosistema Digital Integral para el Distrito de Santiago de Cali, se ha identificado un equipo multidisciplinario con perfiles y experiencia específicos. Este equipo será responsable de cubrir todas las áreas críticas del proyecto, desde la gestión estratégica y la arquitectura de la solución, hasta la configuración y parametrización del software, la seguridad, la infraestructura y la facilitación de la adopción por parte de los usuarios finales. A continuación, se detalla la composición mínima del equipo técnico y de gestión requerido:

No.	Rol	Formación Profesional Pregrado	Cantidad	Experiencia General
LIDERES DE IMPLEMENTACIÓN				
1	Director de proyecto	Título Profesional en Ingeniería de Sistemas o Ingeniería Telemática o Computación o Ingeniería de Software o Ingeniería Electrónica o Ingeniería Telecomunicaciones, con matrícula profesional vigente. Debe contar con: • Especialización o Maestría en BigData. • Certificación PMP vigente • Certificación ITIL Foundation v4 vigente.	1	Experiencia general mínima de diez (10) años contados a partir de la fecha de expedición de la tarjeta profesional en empresas del sector TIC realizando el gerenciamiento o dirección de proyectos.
2	Líder Desarrollador	Título Profesional en Ingeniería de Sistemas o Ingeniería Telemática o Computación o Ingeniería de Software o Ingeniería Electrónica o Ingeniería Telecomunicaciones, con matrícula profesional vigente. Debe contar con Especialización oMaestría en Informática o Ingeniería de Software o Procesos de Desarrollo de Software.	1	Experiencia general mínima de ocho (8) años contados a partir de la fecha de expedición de la tarjeta profesional.

3	Desarrollado r Senior	Título Profesional en Ingeniería de Sistemas o Ingeniería Telemática o Computación o Ingeniería de Software o Ingeniería Electrónica o Ingeniería Telecomunicaciones, con matrícula profesional vigente. Debe contar con: • Certificado Scrum Master Professional (SMPC) Y • Certificado Scrum Developer (CSD)	1	Experiencia general mínima de ocho (8) años contados a partir de la fecha de expedición de la tarjeta profesional.
4	Ingeniero de Seguridad e Infraestructur a	Título Profesional en Ingeniería de Sistemas o Ingeniería Telemática o Computación o Ingeniería de Software o Ingeniería Electrónica o Ingeniería Telecomunicaciones, con matrícula profesional vigente. Debe contar con Especialización o Maestría en seguridad informática o Ciberseguridad Debe contar con: • Certificación Ethical Hacker (CEH) Y • Certificación de gerente certificado en seguridad de la información o por sus siglas en inglés (Certified Information Security manager - CISM) Y • ISO 27001:2022 Auditor Lider	1	Experiencia general mínima de dos (2) años contados a partir de la fecha de expedición de la tarjeta profesional.

5	Arquitecto	Título Profesional en Ingeniería de Sistemas o Ingeniería Telemática o Computación o Ingeniería de Software o Ingeniería Electrónica o Ingeniería Telecomunicaciones. • Debe contar con Especialización o Maestría en Arquitectura o Desarrollo de software o Tecnologías de Información para Negocios o ingeniería de software	1	Experiencia general mínima de diez (10) años contados a partir de la fecha de expedición de la tarjeta profesional.
6	Líder de uso y apropiación	Título Profesional en Administración de Empresas, Administración Pública Territorial, Administración Pública. Debe contar con Especialización o Maestría en Gestión y Planificación del Desarrollo Urbano y Regional o Gerencia de Proyectos	1	Experiencia general mínima de cuatro (04) años contados a partir de la fecha de grado de pregrado. Experiencia específica mínima de dos (2) años en empresas del sector TIC como líder o coordinador en cargos de uso y apropiación.