DOCUMENTO DE ESPECIFICACIONES TÉCNICAS

Objeto:

Desarrollar, implementar y estandarizar un sistema de información integral para la gestión, análisis y automatización de procesos relacionados con las dinámicas migratorias en el Distrito Especial de Santiago de Cali.

Alcance:

El Sistema de Información se concibe como una plataforma centralizada y transversal para el Distrito Especial de Santiago de Cali, es decir, el sistema tiene un alcance intersectorial, permitiendo la integración de la oferta de servicios y el intercambio de datos de las distintas secretarías y organismos del Distrito, y no sólo la contabilización de la población, como es el panorama actual de la mayoría de los sistemas de información. Esto permite la integración de la oferta de servicios y el intercambio de datos con otros organismos que priorizan a la población focalizada en el proyecto, tales como: Secretaría de Desarrollo Económico, Secretaría de Salud, Subsecretaría Integral a Víctimas, Paz y Cultura Ciudadana, Subsecretaría de Equidad de Género, y Primera Infancia. Adicionalmente, se incluye en el alcance del propio sistema, la necesidad

particular de establecer, medir y reportar el cálculo de un índice de vulnerabilidad de la población atendida, así como la capacidad de medir y reportar el impacto de las atenciones e intervenciones realizadas por los programas de la Subsecretaría, proveyendo información clave para la evaluación y mejoramiento continuo de la inversión social.

Por otro lado, el sistema de información es concebido a partir de los estándares de habeas data e información verificable, lo cual implica implementación de tecnologías y flujos de datos que no son cubiertos con sistemas de información ya existentes. Capacidad que es cubierta con la necesidad de desarrollo del módulo de verificación de credenciales por tecnología blockchain, como parte del sistema de información.

El sistema será diseñado, desarrollado e implementado bajo una arquitectura tecnológica basada en tecnología web, e incluirá un front office, destinado a usuarios externos (servidores públicos o funcionarios del organismo), y un back office, orientado a usuarios internos responsables de la administración del sistema. Ambos componentes deberán ser independientes y estar debidamente separados, al igual que las capas correspondientes de frontend y backend, garantizando una adecuada escalabilidad, seguridad y mantenimiento de la solución. El Sistema de Información permitirá la gestión, consulta, custodia y análisis de datos e indicadores, organizados a partir de las diferentes bases de datos de los programas sociales que integran la Subsecretaría. De igual forma, funcionará como un repositorio centralizado para el almacenamiento y procesamiento de información proveniente de archivos en formato Excel, archivos planos y formularios web de captura de datos, según las necesidades operativas de cada programa. Adicionalmente, el sistema permitirá la visualización de datos e indicadores mediante gráficos y tablas (dashboard), y permitirá la generación y consulta de documentos asociados, tales como reportes, fichas de indicadores y otros insumos requeridos para la toma de decisiones, el seguimiento, control y la planeación institucional.

DESCRIPCIÓN DETALLADA DEL BIEN Y/O SERVICIO A ADQUIRIR CON LAS ESPECIFICACIONES TÉCNICAS DE ACUERDO A LA NECESIDAD

1. Tres (3) usuarios administradores: Gerente, Coordinador y Asistente, con responsabilidades de gestión, configuración y administración general del sistema.

2. Cuarenta y dos (42) usuarios alimentadores de datos e indicadores, encargados del cargue y actualización de la información. Se estima que, por cada línea misional del Programa de Población Migrante, exista mínimo una persona responsable de esta función; no obstante, en función del volumen y complejidad de los procesos de información de cada grupo, podrá asignarse más de un usuario alimentador por dependencia o línea misional.

3. Número estimado de usuarios concurrentes en el Sistema: 45

4. Número de archivos estimados .pdf, xlm, .docx, .csv .jpg: 350000 por año

5. Tamaño promedio de documentos (KB/MB): 3 MB

6. Crecimiento estimado de la base de datos: La volumetría de datos estructurados para la vigencia contractual es menor a 10GB, mientras que el dimensionamiento a 3 años contempla 5 TB, de los cuales 1.5 TB corresponden a la proyección inicial y el volumen restante se considera para soportar las necesidades de almacenamiento durante el periodo estimado. Se aclara que este estimado corresponde a la proyección teórica de custodia documental global del Distrito, provista por DATIC.

La proyección volumétrica de almacenamiento documental estimada residirá en el repositorio institucional de archivos/objetos provisto por DATIC, mientras que la base de datos relacional transaccional mantendrá únicamente los metadatos y punteros de acceso, asegurando que el motor de base de datos opere con tiempos de respuesta óptimos y una huella de datos estructurados inferior a 10 GB en su fase inicial

7. Estimación del número de transacciones registradas en una hora: En promedio para 300 por hora.

8. Tiempo de disponibilidad: 24 horas/7dias

DESCRIPCIÓN DETALLADA DE LOS REQUERIMIENTOS FUNCIONALES Y NO FUNCIONALES DE LA SOLUCIÓN

El sistema se concibe como una herramienta estratégica para la captura, procesamiento, análisis y visualización de datos en tiempo real, que permita fortalecer la gestión proactiva y eficiente de los recursos institucionales. Su propósito es diseñar, desarrollar e implementar un sistema de información integral que facilite la gestión de los servicios institucionales, optimice la asignación de recursos y garantice el seguimiento y monitoreo de las intervenciones adelantadas por la Subsecretaría Integral de Atención a Víctimas. Asimismo, el sistema permitirá estandarizar y automatizar los procesos asociados a las dinámicas migratorias en el Distrito Especial de Santiago de Cali, contribuyendo a la generación de información confiable para la toma de decisiones estratégicas. La solución operará bajo los lineamientos de Arquitectura Empresarial de DATIC, asegurando la integridad, disponibilidad y calidad de los datos, con el fin de orientar la priorización de servicios dirigidos a la población migrante, refugiada, retornada y a las comunidades de acogida.

Requerimientos funcionales:

RF-01. Módulo de Gestión de Personas, Hogares y Caracterización

1. Permitir crear, consultar, actualizar y desactivar registros de personas atendidas y/o caracterizadas (migrante, refugiada, retornada, víctima y comunidad de acogida).

2. Incluir campos mínimos: tipo y número de documento, nombres y apellidos, fecha de nacimiento, sexo/género, nacionalidad, grupo étnico, escolaridad, ocupación, ingresos económicos, composición del hogar, condición migratoria, condición de víctima (si aplica), estado de salud (a nivel de variables no clínicas sensibles), y ubicación geográfica (comuna/corregimiento/barrio/vereda).

3. El sistema debe proveer la funcionalidad para que cada secretaría o subsecretaría usuaria pueda configurar y gestionar campos de caracterización adicionales a los mínimos, de acuerdo con sus necesidades particulares. La información capturada en estos campos adicionales debe cumplir con las validaciones de integridad y consistencia, y debe mantener un historial de cambios para su trazabilidad y auditoría, según lo estipulado en los siguientes requisitos del módulo.

4. Validar integridad y consistencia: campos obligatorios, formatos, catálogos (listas), reglas para evitar duplicados (por documento, combinación nombre-fecha-nacionalidad, etc.)

5. Mantener historial de cambios (quién, qué, cuándo, antes/después) para trazabilidad y auditoría.

6. Permitir cargues masivos (Excel/CSV) con plantillas estandarizadas, validación previa y reporte y errores.

7. Soportar vinculación de personas a hogares/grupos (jefatura, dependientes, redes de apoyo) y a casos (cuando aplique)

RF-02. Módulo de Registro de Intervenciones y Seguimiento de Casos

1. Registrar intervenciones por persona/hogar/caso: tipo de servicio, fecha, dependencia responsable, profesional/funcionario, canal(presencial/virtual/territorial), lugar, resultado, remisiones y compromisos.

2. Permitir seguimiento por ruta (ej. protección, integración socioeconómica, salud, educación, regularización, atención psicosocial, orientación jurídica, etc.) con estados: abierto/en gestión/cerrado/en espera/escalado.

3. Capturar evidencias (actas, formatos, soportes) con control de versión y metadatos.

4. Generar ficha individual y consolidado por intervención, por periodo, por territorio, por población y por tipo de servicio.

5. Evitar registros en papel mediante formularios digitales y/o captura en campo (móvil/Tablet) cuando aplique.

RF-03. Módulo de oferta institucional, aliados y remisiones

1. Administrar un catálogo de ofertas/servicios: nombre, objetivo, población objetivo, requisitos, cupos/aforo, cobertura territorial, horarios, puntos de atención y responsable.

2. Registrar y gestionar aliados (otras dependencias, ONG, cooperación internacional) y sus ofertas asociadas.

3. Permitir remisiones internas/externas: creación, seguimiento, estado, responsable, fecha de respuesta y cierre.

4. Permitir parametrización de rutas de atención según perfiles (migración/víctimas/acogida) y reglas de priorización.

RF-04. Módulo de georreferenciación territorial

1. Georreferenciar:

- Personas/hogares (a nivel permitido por política: barrio/vereda, o coordenada si está autorizado).
- Puntos de atención.
- Jornadas/intervenciones territoriales.
- Focos/zonas de mayor demanda o riesgo.

2. Visualizar mapas con capas: comunas/corregimientos, zonas priorizadas, puntos de servicio, y densidad de atenciones.

3. Permitir exportación de listados y mapas para planeación (sin exponer datos sensibles en vistas no autorizadas).

4. El Distrito facilitará el acceso a la cartografía oficial y capas espaciales (servicios WMS/WFS de Planeación/DATIC), o podrá autorizar el uso de proveedores de mapas bajo licenciamiento por consumo.

RF-05. Módulo de agenda, cupos y asignación de servicios

1. Permitir preinscripción/agendamiento para servicios con cupo (citas, jornadas, orientación especializada).

2. Soportar preinscripción por:

- Rol institucional (funcionarios), y o ciudadanía (autogestión) con validaciones y aceptación de términos.

3. Administrar cupos, listas de espera, confirmaciones, cancelaciones y reprogramaciones.

4. Registrar asistencia a la atención agendada y resultado (atendido/no asistió/reprogramado).

RF-06. Módulo de reportes, analítica y tableros de Control

1. Generar tablero con indicadores por: periodo, territorio, población, tipo de intervención, dependencia, tiempos de respuesta, remisiones y cierres.

2. Permitir reportes operativos (diarios/semanales) y estratégicos (mensuales/trimestrales), con exportación a Excel/PDF.

3. Incorporar análisis de tendencias y alertas por variaciones (aumento súbito de demanda por zona, servicios saturados, etc.).

4. Habilitar consultas ad-hoc para perfiles autorizados (filtros y segmentación).

RF-07. Integración e interoperabilidad con fuentes externas

1. Permitir cruces y/o enriquecimiento con bases externas pertinentes (p. ej. repositorios de cada secretaría o subsecretaría, SISBÉN, Registraduría, DANE y otras que la Alcaldía autorice), manteniendo trazabilidad de origen.

2. El sistema debe tener la capacidad de consumir y exponer los datos de la caracterización adicional y configurable definida por cada secretaría o subsecretaría usuaria (establecida en el RF-01).

3. Sincronizar datos mediante APIs seguras, con autenticación y cifrado, y registro de logs de consumo.

4. Gestionar reglas de “match” (coincidencia) para actualización automática vs. Actualización asistida (cuando hay ambigüedad).

5. Los servicios expuestos (WebServices) deberán cumplir con los estándares de seguridad y documentación definidos en la sección 4.7.1, incluyendo parámetros de entrada, salida, tipos de datos y validaciones

RF-08. Módulo de Alertas y Notificaciones

1. Alertas por:

- Persona ya registrada (posible duplicidad).
- Persona fallecida (por interoperabilidad con otras fuentes de información)
- No atención, no actualización, o no seguimiento en un periodo definido (ej. 90 días),
- Remisión vencida sin respuesta.
- Cupos críticos/servicios saturados.
- Inconsistencias de datos (campos críticos incompletos).

2. Notificaciones por correo y/o bandeja interna según rol (y opcionalmente SMS/WhatsApp si se habilita institucionalmente).

1. Configuración de umbrales, periodicidad y responsables de atención de alertas

RF-09. Módulo de evaluación de impacto y KPIs (Vista Restringida

1. Definir y administrar KPIs (sociales, técnicos, operativos y financieros) acordados por la dependencia.

2. Visualización solo para roles autorizados (administración/analítica

4. Permitir medir: cobertura, oportunidad, efectividad de remisiones, permanencia en rutas, territorialización, costo/servicio (si aplica) y resultados agregados.

RF-10. Gestión de usuarios, roles y permisos

1. Autenticación por mecanismo institucional (y perfiles por rol).

2. Roles sugeridos: Administrador, Analista, Coordinador, Gestor territorial, profesional de atención, Consulta/lectura, y Usuario ciudadano (si existe portal).
3. Permisos por módulos, campos sensibles y acciones (ver/editar/exportar/eliminar lógico).

4. Registro de auditoría: accesos, exportaciones, modificaciones, integraciones

RF-11. Gestión documental y trazabilidad

1. Adjuntar y clasificar documentos por caso/intervención/persona.

2. Control de acceso a documentos sensibles por rol.

3. Sellos de tiempo, versionamiento, y políticas de retención.

RF-12. Módulo de verificación de credenciales (Blockchain)

1. Debe soportar una funcionalidad de verificación y emisión de credenciales inmutables basada en tecnología blockchain para permitir la revisión y validación de credenciales, certificaciones o documentos emitidos por el sistema o por entidades aliadas, garantizando la inmutabilidad y la trazabilidad de la información verificada.

2. El sistema debe registrar y guardar un historial detallado de todos los elementos (credenciales, certificaciones o documentos) que han sido verificados, incluyendo la fecha, hora, usuario que realizó la verificación y el resultado de la misma, para ello deberá garantizar el acceso, uso e integración a las interfaces de programación de aplicaciones (APIs) necesarias para la interoperabilidad con los sistemas de información

Nota aclaratoria: El módulo consistirá en la verificación mediante API/SDK de credenciales digitales descentralizadas bajo estándares abiertos (W3C Verifiable Credentials / redes compatibles) y los costos de emisión masiva fuera del alcance del software serán gestionados directamente por los programas misionales de la Alcaldía. Garantizando que la lectura sea compatible con las credenciales que la Alcaldía ha emitido previamente.

2) Requerimientos no funcionales:

RNF-01. Seguridad y privacidad

- Transmisión cifrada con TLS y buenas prácticas de configuración.

- Control de acceso por roles y principio de mínimo privilegio.

- Auditoría completa (logs inmutables o con control de integridad): login, consultas sensibles, exportaciones y cambios.

- Manejo de datos sensibles con: enmascaramiento en vistas, segregación por roles, y políticas de retención/eliminación lógica.

- Cumplimiento normativo aplicable (protección de datos personales y lineamientos institucionales del Distrito).

- Toda comunicación entre el cliente y el servidor se realizará exclusivamente bajo el protocolo HTTPS, y se prohíbe el envío de información sensible o parámetros de estado a través de la URL (método GET).

RNF-02. Autenticación e identidad

- Integración con LDAP o Active Directory para usuarios institucionales.

- Soporte de SSO si la arquitectura institucional lo contempla.

- Políticas de contraseñas/rotación/bloqueo y 2FA si se habilita institucionalmente.

RNF-03. Disponibilidad y continuidad

- Alta disponibilidad (redundancia y tolerancia a fallos).

- Backups automáticos y pruebas periódicas de restauración.

- Plan de continuidad/recuperación ante desastres (RPO/RTO definidos por la entidad).

- El sistema debe soportar un estimado de 300 transacciones registradas por hora en promedio, garantizando la estabilidad y el rendimiento.

RNF-04. Rendimiento y concurrencia

- Soporte para múltiples sesiones simultáneas sin degradación significativa.

- Respuesta objetivo para operaciones típicas (búsquedas, carga de ficha, registro de intervención) bajo carga nominal.
- Procesamiento en segundo plano para cargues masivos e integraciones (colas/Jobs) con seguimiento de estado.

RNF-05. Interoperabilidad y arquitectura

- Alineación con lineamientos de Arquitectura Empresarial DATIC (capas, gobierno de datos, integración).
- APIs REST/JSON (u otro estándar institucional) con versionamiento, rate limiting y trazabilidad.

- Capacidad de desplegar en infraestructura institucional (on-premise o nube autorizada).

La obligación del contratista se circunscribe al despliegue, configuración y afinación en dicha infraestructura.

RNF-06. Usabilidad y accesibilidad

- Interfaz amigable, responsive (desktop/Tablet/móvil para campo).
- Flujos simplificados para captura rápida en territorio.
- Cumplimiento de criterios de accesibilidad (buen contraste, navegación por teclado, etc.) según estándar que adopte la Alcaldía.
- La solución debe presentarse al usuario en sus interfaces y/o formulario en idioma español.
- Cumplir con la norma NTC 5854, sobre accesibilidad.
- El sistema debe considerar el acceso a población con discapacidad visual y/o auditiva, teniendo en cuenta los principales estándares de la W3C para facilitar el acceso al mismo, manteniendo la estructura inicial.
- Se deben incluir Widgets que permitan que el contenido sea accesible (alto contraste, aumentar zoom, Acces key, STT - speech to text, browse a loud).

RNF-07. Calidad de datos

- Reglas de validación centralizadas y catálogos parametrizables.
- Detección de duplicados y mecanismos de resolución (fusión controlada / revisión por analista).
- Trazabilidad del dato: fuente, fecha, responsable y confiabilidad.

RNF-08. Mantenibilidad y escalabilidad

- Código modular, documentación técnica y manuales de usuario/administrador.
- Parametrización de catálogos, rutas, alertas e indicadores sin requerir cambios de código.
- Escalabilidad horizontal/vertical según crecimiento de usuarios y datos.

RNF-09. Compatibilidad y exportación

- Exportación a formatos institucionales (Excel/CSV/PDF) con control de permisos.
- Compatibilidad con navegadores modernos y políticas de TI institucionales.

RNF-10. Soporte y operación

- Monitoreo de aplicación (salud, errores, latencia, uso) y alertamiento.
- Registro de incidentes y bitácora de cambios (versionamiento).

- Ambiente de pruebas y jornadas de capacitación para usuarios clave.

RNF-11. Arquitectura y compatibilidad técnica

- La solución implementada o adquirida debe ser 100% WEB.

- El sistema debe ser responsivo (diseño adaptable a diferentes dispositivos y tamaños de pantalla).

- El sistema implementado debe funcionar correctamente en todos los navegadores Firefox, Chrome, Opera, Safari, Microsoft Edge en su última versión estable.

- Los URLS amigables deben ser únicos. (Un enlace sólo podrá accederse por su identificador único y por su único URL amigable).

- Validación del código con W3C. Utilizar como referencia herramientas de validación como TAWDIS y W3C

4.4 USABILIDAD Y ACCESIBILIDAD

El sistema de información como aplicación WEB deberá contener:

a. La solución implementada o adquirida debe ser 100% WEB.

b. La solución debe presentarse al usuario en sus interfaces y/o formulario en idioma español.

c. El contenido del sistema debe cumplir con las pautas de accesibilidad al contenido de la Web para todo tipo de usuarios independientemente de sus capacidades. Las pautas WCAG de la W3C (www.w3c.org) cuentan con priorización en niveles A, AA y AAA; se requiere que cumpla con el nivel AA de las pautas WCAG (Web Content Accessibility Guidelines) en su versión vigente.

d. De igual manera, la solución deberá alinearse con las directrices de accesibilidad, diseño de servicios ciudadanos digitales y estándares establecidos en la Política de Gobierno Digital del MinTIC (Decreto 1078 de 2015, modificado por el Decreto 767 de 2022 y Decreto 1263 de 2022) o las normas que las modifiquen, adicionen o sustituyan.

e. Cumplir con la norma NTC 5854, sobre accesibilidad. e. El sistema debe considerar el acceso a población con discapacidad visual y/o auditiva, teniendo en cuenta los principales estándares de la W3C para facilitar el acceso al mismo, manteniendo la estructura inicial.

f. Widgets que permiten que el contenido sea accesible (alto contraste, aumentar zoom, Acces key, STT (speech to text, browse a loud)).

g. Los URLS amigables deben ser únicos. (Un enlace sólo podrá accederse por su identificador único y por su único URL amigable)

h. Validación del código con W3C. Utilizar como referencia herramientas de validación como TAWDIS y W3C.

i. Cumplimiento de las 10 heurísticas de Nielsen (Visibilidad del estado del sistema, relación entre el sistema y el mundo real, control y libertad del usuario, consistencia y estándares, prevención de

errores, reconocer más que recordar, flexibilidad y eficiencia de uso, estética y diseño minimalista, ayuda a los usuarios a reconocer, diagnosticar y recuperarse de errores, ayuda y documentación).

j. El sistema debe ser responsivo.

k. El sistema implementado debe funcionar correctamente en todos los navegadores Firefox, Chrome, Opera, Safari, Microsoft Edge en su última versión estable.

4.5 AUTENTICACIÓN Y CONTROL DE ACCESO

Los requerimientos y lineamientos que se detallan a continuación constituyen condiciones de obligatorio cumplimiento para el recibo a satisfacción del servicio contratado.

1. Integración con Directorio Activo (DA) y Autenticación Propia ○ La plataforma debe permitir por parametrización la integración con el Directorio Activo de la entidad para los usuarios que se encuentran registrados en este sistema.

◦ Igualmente, la plataforma debe tener su propio sistema de autenticación para aquellos usuarios no registrados en el Directorio Activo. Este sistema debe ser parametrizable.

2. **Políticas de Seguridad y Contraseñas**

◦ En el Directorio Activo, residen las políticas de seguridad y contraseñas de usuario para el inicio de sesión de los usuarios.

◦ Si la aplicación requiere características especiales en la complejidad de contraseña tiene la posibilidad de autenticarse dentro de un grupo del Directorio Activo que tiene esa política específica.

3. Controles Básicos de Autenticación

◦ Bloqueo por Intentos Fallidos: La autenticación debe tener en cuenta dos controles básicos. El primer control debe considerar bloquear a nivel de aplicación el usuario si tiene más de tres (3) intentos fallidos. El Directorio Activo realizará el bloqueo de sesión después de tres (3) autenticaciones fallidas.

◦ Cierre de Sesión por Inactividad: El segundo control es que la aplicación cierre sesión a los cinco (5) minutos de inactividad y deba iniciar sesión nuevamente si esta cierra automáticamente.

4.6 SEGURIDAD

Con el fin de garantizar la seguridad de la información, el proveedor deberá especificar la metodología o norma técnica seleccionada para el desarrollo seguro del software. Asimismo, se establecen los siguientes lineamientos técnicos obligatorios para el correcto funcionamiento de la plataforma:

Autenticación y Control de Acceso: El sistema debe gestionar los accesos de manera controlada y parametrizable. Se debe considerar la definición estricta de roles, permisos y control de acceso a los diferentes módulos, para que la seguridad a nivel de aplicación sea mediante un modelo de Control de Acceso Basado en Roles (RBAC). Este mecanismo permitirá:

- La restricción granular de accesos a nivel de vistas (páginas) y métodos (funcionalidades).

  La inhabilitación de componentes de la interfaz y servicios de *backend* para perfiles no autorizados, asegurando el principio de mínimo privilegio.

- Debe permitir la integración con el Directorio Activo de la entidad para usuarios registrados, donde residen las políticas de contraseñas. Para usuarios externos, la plataforma debe tener su propio sistema de autenticación.

- Se debe bloquear el usuario tras tres (3) intentos fallidos.

- Se debe cerrar la sesión automáticamente tras cinco (5) minutos de inactividad. Auditoría, Trazabilidad y No Repudio Con el fin de garantizar la integridad y el monitoreo de la operación, el software contará con un módulo de logs de auditoría persistente. El sistema registrará de forma automática cada transacción realizada, capturando obligatoriamente los siguientes metadatos:

- Identificador del usuario y descripción/motivo de la transacción.

- Estampa de tiempo precisa (Fecha y hora del servidor).

- Dirección IP de origen del equipo desde el cual se efectuó la petición.

- Las operaciones de los administradores del sistema, los cambios en perfiles de usuario (como cambio de roles o claves) y las operaciones realizadas mediante servicios web externos.

- Registrar cada ingreso exitoso con usuario, IP y tiempo de conexión. Además, antes de pasar a producción, el sistema de información debe someterse a verificaciones rigurosas:

- La plataforma debe ser auditada tanto en capacidad (pruebas de estrés) como en seguridad, siguiendo el estándar OWASP Top 10 en su última versión oficial.

- Durante el periodo de garantía (un año), se deben realizar pruebas de seguridad (Ethical hacking) y corregir las vulnerabilidades encontradas con una periodicidad mínima trimestral. Las pruebas de ethical hacking y mitigación aplican sobre la capa de aplicación/software desarrollado por el contratista y no sobre la infraestructura base de la Alcaldía.

- Se deben entregar los resultados de la auditoría de seguridad una vez finalizada la etapa de pruebas. Seguridad en la Capa de Transporte y Comunicación.

  Para mitigar riesgos de intercepción y asegurar la confidencialidad de los datos en tránsito, se establecen los siguientes lineamientos:

- Protocolo HTTPS: Toda comunicación entre el cliente y el servidor se realizará exclusivamente bajo el protocolo HTTPS, utilizando certificados de seguridad para el cifrado de la información.

- Ocultamiento de Parámetros: Se prohíbe el envío de información sensible o parámetros de estado a través de la URL (método GET). El intercambio de datos se realizará mediante el cuerpo de las peticiones (método POST/PUT/PATCH) para evitar la exposición de datos en el historial del navegador o logs de servidores proxy.

- Las comunicaciones entre formularios públicos y la base de datos deben hacerse a través de servicios, nunca de forma directa. Estos servicios (SOAP/RESTful) deben validar entradas para proteger contra inyecciones SQL y NoSQL.

- Se debe definir el tipo y tamaño de archivos permitidos, obligando el uso de una sintaxis adecuada (sin espacios ni caracteres especiales) y prohibiendo la carga de archivos con etiquetas inseguras. Configuración del Servidor y Sistema Operativo

- No se permitirán permisos de root para usuarios de la aplicación en el sistema operativo. Los permisos sobre archivos y directorios deben ser preferiblemente de solo lectura (read-only).

- La carga de archivos por parte de administradores y la administración del sistema deben realizarse únicamente desde la red interna.

- Se debe reportar hasta qué versión del sistema operativo y componentes se puede actualizar sin afectar la aplicación.

4.7 ARQUITECTURA, METODOLOGÍA, FASES Y PLATAFORMA TECNOLÓGICA

El software adoptará un estilo arquitectónico en capas, promoviendo la separación de responsabilidades, la mantenibilidad y la escalabilidad del sistema. Esta estructura permite desacoplar la lógica de presentación de la lógica de negocio y el acceso a datos. La arquitectura debe estar separada en frontend, backend y base de datos.

La implementación del sistema de información deberá seguir los lineamientos del Marco de Referencia de Arquitectura Empresarial (MRAE) y la Guía del Dominio de Sistemas de Información (G.SIS.01) adoptados por DATIC en el marco de la Política de Gobierno Digital del MinTIC y el Modelo Integrado de Planeación y Gestión (MIPG).

Las tecnologías específicas para el desarrollo del backend y frontend se detallarán más adelante en la sección 4.7.4 Plataforma de desarrollo, asegurando el uso de herramientas permitidas y estandarizadas por la entidad. De preferencia, se espera que la aplicación pueda estar alojada en un servidor con sistema operativo Linux. Respecto al hosting y la administración del sitio, se deberá garantizar el cumplimiento estricto de las políticas de seguridad, lo cual implica que no se permitirán permisos root para usuarios de la aplicación y que la administración del sistema se realizará únicamente desde la red interna, restringiendo el acceso público a dichas funcionalidades.

4.7.1 Arquitectura de software para desarrollo de sistemas de información

El desarrollo del sistema se fundamentará en un estilo arquitectónico robusto, modular y escalable, alineado estrictamente con los lineamientos de la 'G.SIS.01

Guía del dominio de Sistemas de Información'. Características de la arquitectura:

1. Enfoque orientado a servicios (SOA): El sistema deberá construirse bajo una arquitectura SOA y no monolítica. La solución deberá desacoplar la lógica de negocio de la interfaz de usuario, garantizando que el funcionamiento de la aplicación se separe claramente en backend y frontend.

2. Separación por capas: La arquitectura debe implementar una separación física y lógica de capas

para asegurar la mantenibilidad y seguridad:

- Capa de presentación (frontend): Implementará una interfaz de usuario tipo RIA (Rich Internet Applications) o SPA (Single Page Application), consumiendo servicios de manera asíncrona.

- Capa de negocio (Backend): Contendrá la lógica del sistema y expondrá dicha funcionalidad a través de servicios web.

- Capa de persistencia: Gestionará el acceso a datos de manera independiente (usando patrones como DAO u ORM según la tecnología seleccionada en la sección 4.7.4). La persistencia del sistema deberá implementar una separación estricta entre datos transaccionales y archivos binarios/digitales:

  - Base de datos: Repositorio de información separado. El motor de base de datos almacenará exclusivamente estructuras transaccionales, metadatos, índices, tablas maestras y rutas lógicas. Queda prohibido el almacenamiento de documentos, imágenes o PDFs dentro del motor relacional en formato binario.

  - Repositorio de documentos y objetos: Los archivos documentales y soportes adjuntos (PDFs, imágenes .jpg, CSVs) deberán gestionarse a través de un servicio de almacenamiento de objetos desacoplado (servidor dedicado dispuesto por DATIC), garantizando alto rendimiento en consultas relacionales y escalabilidad horizontal del almacenamiento.

3. Exposición a servicios: El backend debe exponer la funcionalidad mediante servicios web bajo especificaciones estándar (REST o SOAP). Para ello, se debe implementar un controlador frontal o API Gateway que administre las peticiones, maneje las sesiones y valide usuarios antes de resolver el servicio. Adicionalmente, se debe contar con una descripción detallada de los servicios (API), indicando parámetros de entrada, salida, tipos de datos y validaciones.

4. Interoperabilidad y escenarios de despliegue: Dependiendo del público objetivo (funcionarios o ciudadanos), la arquitectura deberá soportar los escenarios de integración definidos por la entidad (Portal Web, Sede Electrónica o Aplicaciones Móviles), asegurando que cualquier comunicación entre el frontend y el backend se realice exclusivamente a través de la API expuesta y nunca mediante conexión directa a la base de datos desde el cliente.

5. Patrones de diseño: Se exige el uso de patrones de diseño de software reconocidos (ej. MVC, Inyección de Dependencias, DAO, Singleton, Factory) que aseguren la reutilización de componentes, el modularidad y faciliten el mantenimiento evolutivo del sistema, sin atar la solución a un framework propietario específico que limite la libre concurrencia, siempre y cuando se respete la plataforma tecnológica permitida descrita en la sección 4.7.4.

4.7.2 Metodología y fases para la implementación de la solución Para asegurar la entrega oportuna y la calidad del sistema, el proyecto adoptará un enfoque de desarrollo iterativo e incremental, fundamentado en Metodologías Ágiles. Este enfoque permite mitigar riesgos técnicos y funcionales mediante ciclos cortos de revisión, garantizando que el software evolucione de manera alineada con las necesidades de la Subsecretaría.

Marco de Trabajo: Scrum

Se implementará el marco de trabajo Scrum, el cual facilita la gestión de proyectos complejos a través del

trabajo colaborativo y la inspección constante. Bajo esta metodología, el desarrollo se organiza en ciclos denominados Sprints, permitiendo entregas parciales y funcionales del producto final. Cada iteración o Sprint cumplirá con las siguientes fases del ciclo de vida de desarrollo:

- Planificación (Sprint Planning): Definición de los objetivos y selección de las tareas prioritarias.

Análisis y Diseño: Refinamiento de requerimientos y arquitectura técnica.

- Construcción (Ejecución): Codificación y desarrollo de los componentes definidos.

- Revisión y Retrospectiva: Demostración del incremento funcional y evaluación del proceso para la mejora continua.

Gestión de Requerimientos y Artefactos La captura y formalización de las necesidades del usuario se llevará a cabo mediante la creación de Historias de Usuario (User Stories), las cuales describen las funcionalidades desde la perspectiva del actor final. Para garantizar la trazabilidad y el rigor técnico exigido por la arquitectura empresarial, se generarán los siguientes artefactos:

- Documentación de Requisitos: Levantamiento detallado de necesidades funcionales y técnicas.

- Modelado UML: Elaboración de Diagramas de Casos de Uso para definir el comportamiento del sistema y Diagramas de Clases para representar la estructura lógica de los datos.

- Gestión Documental: Registro de actas de reuniones y talleres de co-creación con los interesados del proyecto.

Planificación de Iteraciones El desarrollo se estructurará en un cronograma de Sprints (por ejemplo, tres ciclos de iteración). En cada uno de ellos, se asignarán historias de usuario específicas a los responsables técnicos, asegurando que al finalizar cada Sprint se cuente con una versión funcional y testeada del software, permitiendo un crecimiento incremental hasta alcanzar la versión final para el recibo a satisfacción.

La metodología de gestión de proyectos que se adopte debe corresponder al planeamiento de un ciclo de vida considerando fases como la ideación, planeamiento, ejecución y post entrega del proyecto, las cuales deben ser documentadas Se deberán realizar mesas de trabajo para el levantamiento de requerimientos y diseño del sistema.

En estas etapas se deben elaborar:

- Actas de las reuniones y talleres

- Historias de usuario y especificaciones funcionales Se deberán elaborar prototipos interactivos de alta fidelidad (tales como mockup) de los componentes del sistema de información antes de proceder a su desarrollo. Estos prototipos permitirán validar y refinar el análisis de requerimientos y el diseño. Los prototipos deberán ser probados y validados de forma interactiva por los usuarios funcionales. Los artefactos que se deben generar en el desarrollo e implementación del sistema son:

a) En esta etapa debe participar como mínimo el equipo o personal de calidad del organismo y el líder del proceso.

b) Documento de arquitectura de la solución y dimensionamiento de los recursos de hardware y software de toda la plataforma.
c) Diseño de la Interfaz del sistema.

d) Diagrama de casos de uso.

e) Diagrama de los organismos Diagrama de clases, contiene las clases más relevantes del sistema.
f) Vista de componentes o módulos del sistema: corresponde a los diagramas con los componentes o módulos del sistema de información y su relación entre
ellos.

g) Diagrama de secuencias: para las funcionalidades más relevantes del sistema, mostrando cómo interactúan los diferentes componentes propuestos por la arquitectura.

h) Modelo de datos, corresponde a los Diagramas con las entidades del sistema de información y su relación entre ellas, se debe elaborar teniendo en cuenta la Guía del metamodelo de datos del Departamento de Planeación Municipal. Una vez se tenga el modelo de datos, este debe ser validado y aprobado por el Departamento Administrativo de Planeación y el DATIC antes de la implementación.

i) Diccionario de datos, descripción de las entidades y atributos que conforman el modelo de datos. (El diccionario debe estar documentado y debe incluir la descripción de la función y/o significado de cada tabla y campo) de acuerdo con los lineamientos del Departamento Administrativo de Planeación de la entidad.

Vista de despliegue físico, vista que muestra cómo va a estar desplegado físicamente el sistema de información.

j) Diagrama de red: El diagrama de red muestra de forma simplificada el recorrido que tomaría una petición para ser procesada. En este diagrama se destacan elementos tales como balanceador de carga, Firewall, Servidores, Database, Firewall, etc.

k) Diagrama de despliegue lógico: Diagrama que muestra cómo va a estar desplegado lógicamente el sistema de información, indicando por ejemplo la relación entre los paquetes y los módulos del sistema.

l) Vista de interoperabilidad, Muestra: a) los Servicios que expone el sistema, y su relación con los sistemas internos y externos que lo usan. b) Servicios expuestos por otros sistemas internos o externos, y su relación con el sistema que se está implementando. c) Para cada servicio expuesto o usado, indicar el tipo de integración: archivos planos, webservices, acceso a base de datos, ETL, EAI, entre otros.

4.7.3 Manuales

Se deben elaborar y entregar los siguientes manuales en idioma español:

1. Manual técnico: el manual técnico debe incluir los siguientes componentes:

a) Versión del documento y fecha de la versión.

b) Versión del sistema de información.

c) Pre-requisitos de instalación del sistema: Sistema operativo de los servidores de aplicaciones y base de datos, marca y versión de la base de datos, marca y versión de los servidores de aplicaciones, navegador, configuraciones de seguridad, etc.

d) Frameworks y estándares: Nombres y versiones de los frameworks y estándares bajo los cuales está construido el sistema.

e) Artefactos y diagramas generados.

f) Modelo entidad relación del sistema.

g)Scripts de instalación del sistema.

h) Diagrama de servicios expuestos por el sistema.

i) Manual o guía de instalación del sistema: Paso a paso con las instrucciones de instalación y configuración del sistema

2. Manual de usuario: el manual de usuario debe estar en línea, incorporado dentro de la aplicación, y debe incluir los siguientes componentes:

a) Versión del documento y fecha de la versión

b) Versión del sistema de información.

c) Manual de uso del sistema: Paso a paso de uso de las principales opciones del sistema. Incluya imágenes para cada paso.

d) Preguntas frecuentes que pueden realizar los usuarios y su respectiva respuesta

4.7.4 Plataforma de desarrollo La plataforma de desarrollo recomendada por el proceso de Administración de TIC es la siguiente:

Componente	Tecnología
Tecnología o lenguaje de programación	Java, PHP
Framework o tecnología de capa de presentación	Bootstrap, Javascript, HTML5, Angular, jQuery, NodeJs.

Framework o tecnología de capa de negocio	Frameworks asociados a PHP, Java, Python o NodeJs.
Framework o tecnología de capa de persistencia	Mybatis o Hibernate
Base de datos	Postgres (con PostGis), Oracle 12c.
Integración	SOAP, REST
Versionamiento	GIT
Sistema operativo	Linux
Virtualización	VMWare

Fuente. Elaboración propia

Es importante hacer notar que el stack tecnológico es una guía sugerida, sin embargo, no es limitante para la implementación del sistema de información.

4.8 SISTEMA CON APERTURA DE DATOS

El Sistema de Información de Población Migrante deberá promover la apertura y reutilización de la información pública, garantizando simultáneamente la protección de los datos personales y sensibles. Para ello, el sistema permitirá generar y publicar conjuntos de datos anonimizados relacionados con procesos, servicios e indicadores asociados a la población migrante, refugiada y retornada, de manera que no exista posibilidad de identificar personas naturales. Los datos abiertos generados deberán estar disponibles en formatos interoperables y reutilizables, tales como CSV, JSON o XLSX, facilitando su uso por parte de entidades públicas, academia, organizaciones sociales y ciudadanía en general.
Adicionalmente, cada conjunto de datos contará con metadatos, diccionario de campos, descripción de la fuente, periodicidad de actualización y responsable institucional, en coherencia con los lineamientos de Gobierno Digital y la Ley 1712 de 2014. El sistema permitirá la parametrización de los reportes para definir rangos de fechas, variables y categorías de consulta, contribuyendo a la transparencia, la rendición de cuentas y la toma de decisiones basada en evidencia. Todo proceso de apertura de datos se realizará bajo criterios de minimización y seguridad de la información, preservando la reserva legal de los datos personales y sensibles de la población migrante.

Para tal fin, el sistema:
Permitirá la generación de conjuntos de datos no sensibles y debidamente anonimizados, evitando cualquier posibilidad de identificación directa o indirecta de personas.
- Generará reportes en formatos abiertos e interoperables (CSV, JSON y XLSX).
- Dispondrá de un módulo de exportación de datos abiertos, configurable por rangos de fechas, variables y categorías.
- Documentará los conjuntos de datos mediante metadatos, diccionario de campos y periodicidad de actualización.
- Publicará la información bajo licencias abiertas y lineamientos de reutilización definidos por la entidad.

4.9 TRAZABILIDAD DE LA INFORMACIÓN Y DE LAS OPERACIONES

El sistema garantizará la trazabilidad integral de la información y de todas las operaciones realizadas por los usuarios autorizados. Para ello registrará de manera automática los eventos relevantes asociados al acceso, consulta, creación, modificación y eliminación de registros, incluyendo fecha, hora, usuario, perfil, dirección IP y descripción de la acción efectuada. Esta bitácora o registro de auditoría permitirá reconstruir

el historial de un dato desde su creación hasta su estado actual, fortaleciendo la integridad, confiabilidad y seguimiento de la información administrada.
Los registros de trazabilidad serán conservados conforme a los tiempos definidos por la normatividad archivística y de seguridad de la información, estarán protegidos contra alteraciones no autorizadas y únicamente podrán ser consultados por perfiles expresamente habilitados por la entidad. La trazabilidad también permitirá identificar errores operativos, comportamientos inusuales o incidentes de seguridad, convirtiéndose en una herramienta de apoyo para los procesos de control interno, auditoría y vigilancia administrativa.
El sistema deberá asegurar la trazabilidad completa de la información y de las operaciones realizadas por los usuarios, garantizando integridad, auditoría y control. Para ello incluirá:

- Registro de auditoría (logs) de acceso, consulta, modificación y eliminación.
- Identificación de usuario, perfil, fecha, hora, dirección IP y acción realizada.
- Histórico de cambios en los registros, con versiones y control de modificaciones.
- Generación de reportes de auditoría para labores de control fiscal y administrativo.
- Mecanismos de cierre y custodia de logs durante el periodo definido por la normativa.
- La información de trazabilidad tendrá tratamiento reservado y sólo podrá ser consultada por perfiles autorizados.

4.10 ADMINISTRACIÓN DEL SISTEMA

El Sistema de Información contará con un módulo especializado para la administración integral de la plataforma, desde el cual será posible gestionar usuarios, roles, perfiles y permisos de acceso a los diferentes módulos y funcionalidades. Dicho módulo permitirá parametrizar tablas maestras, catálogos, listas de valores y configuraciones operativas del sistema, garantizando flexibilidad frente a cambios institucionales o normativos. Asimismo, desde la administración se podrán definir y aplicar políticas de seguridad como caducidad y complejidad de contraseñas, bloqueo de cuentas, autenticación y control de sesiones. El sistema incorporará herramientas para la administración de copias de seguridad y mecanismos de recuperación ante fallas, así como un panel de monitoreo que permita visualizar el estado general de los servicios, el uso de recursos y la disponibilidad de la plataforma. El acceso al módulo de administración estará restringido exclusivamente a funcionarios autorizados y designados formalmente por la entidad responsable del sistema. El Sistema de Información contará con un módulo de administración y gobierno de la plataforma, que incluirá como mínimo:

- Administración de usuarios, roles y perfiles.
- Definición de permisos granulados sobre módulos y funcionalidades.
- Parametrización de catálogos, tablas maestras y listas de valores.
- Configuración de políticas de seguridad (autenticación, contraseñas y bloqueo de cuentas).
- Administración de copias de seguridad y plan de recuperación.
- Monitoreo del estado del sistema, consumo de recursos y disponibilidad de servicios.
- El acceso al módulo de administración será exclusivo para usuarios con perfil de administrador del sistema designado por la entidad.

4.11 COMPONENTE DE INTEGRACIÓN / INTEROPERABILIDAD

El sistema interoperará con:

- Protocolos de comunicación: El sistema debe exponer y consumir servicios mediante arquitecturas RESTful, utilizando JSON como formato principal de intercambio de datos.
- Seguridad en el intercambio: Se debe implementar autenticación y autorización mediante protocolos OAuth 2.0 o OpenID Connect. Todas las transmisiones de datos deben estar cifradas mediante TLS 1.3

o superior.

- Plataforma de integración: El sistema debe estar preparado para integrarse con la Plataforma de Interoperabilidad (X-Road) adoptada por el Estado colombiano para el intercambio de datos entre entidades públicas.
- Catálogos y lenguajes comunes: El sistema debe utilizar los lenguajes de

referencia del Marco de Interoperabilidad de MinTIC para asegurar que el significado de los datos sea consistente.

- Identificación única: Implementar lógica para el reconocimiento de diversos documentos de identidad vigentes en 2026, incluyendo PPT (Permiso por Protección Temporal), Cédula de Extranjería y Pasaporte, vinculando estos campos al Maestro de Identificación de Migración Colombia.
- Consulta externa: El sistema deberá permitir la consulta en tiempo real mediante APIs a:

SISBÉN IV: Para verificar niveles de vulnerabilidad y focalización de subsidios. Migración Colombia: Para validar el estatus migratorio y la vigencia de permisos. Sincronización Territorial: Capacidad de exportar datos en formatos abiertos (CSV, JSON) para alimentar tableros de control de la Alcaldía de Cali y el Observatorio de Migraciones.

La conexión con los sistemas de información propios de cada secretaría y/o subsecretaría relacionada con la población migrante, refugiada y retornada, así como con las comunidades de acogida.

El contratista debe diseñar, construir, exponer y documentar las APIs/WebServices necesarios, pero la integración efectiva en producción con entidades externas (SISBÉN IV, Registraduría, DANE, Migración Colombia, X-Road) queda sujeta a la disponibilidad de convenios, credenciales y accesos suministrados por la Alcaldía.

4.12 MIGRACIÓN DE LOS DATOS

El proceso de migración de datos desde los repositorios actuales hacia la nueva solución tecnológica será responsabilidad del oferente, quien deberá diseñar, documentar y ejecutar un plan de migración estructurado y controlado, mientras que la calidad y completitud de los datos de origen es responsabilidad institucional del Distrito. Este proceso iniciará con el levantamiento de un inventario de fuentes de información existentes, identificación de estructuras de datos, volúmenes de información, formatos y calidad de los registros. Posteriormente, se realizará la limpieza, normalización y depuración de la información, eliminando duplicidades, corrigiendo inconsistencias y estandarizando catálogos y variables.

Una vez preparada la información, se llevará a cabo la carga inicial en el nuevo sistema y se efectuarán validaciones para comprobar la integridad, completitud y correcta correspondencia de los datos migrados. El oferente deberá entregar reportes y actas de verificación que evidencien el proceso de migración, así como garantizar que durante este procedimiento no se pierda información y que la operación institucional no se vea interrumpida.

El proceso contemplará:

- Inventario de fuentes de datos existentes.
- Análisis de estructuras y modelos de información.
- Diseño y documentación del plan de migración.
- Limpieza, normalización y depuración de la información.
- Carga inicial y validación de resultados.
- Generación de actas de cierre del proceso de migración.
- Se deberá garantizar que durante la migración no se pierda información y que los servicios de la entidad no se vean interrumpidos.

Adicionalmente, dentro del proceso de migración, algunos datos corresponderán a la verificación de las credenciales inmutables (RF-12) ya existentes.

- El volumen inicial esperado a migrar es menor a 10GB, sin que esto configure un límite restrictivo a la ejecución.

4.13 REALIZAR EL PROCESO DE PRUEBAS Y ASEGURAMIENTO DE CALIDAD DE LA SOLUCIÓN, GARANTIZANDO UNA IMPLEMENTACIÓN DE ÓPTIMA CALIDAD Y RENDIMIENTO

Antes de la puesta en producción, la solución tecnológica deberá ser sometida a un proceso formal de pruebas y aseguramiento de calidad. Este proceso incluirá pruebas unitarias realizadas por el equipo técnico desarrollador, así como pruebas funcionales por módulos para verificar que cada requerimiento definido se encuentra implementado y opera correctamente. También se ejecutarán pruebas de integración para validar la correcta interacción entre los diferentes componentes del sistema, bases de datos y servicios externos. Igualmente, se desarrollarán pruebas de rendimiento bajo escenarios de carga representativos, con el fin de evaluar tiempos de respuesta, estabilidad y capacidad de procesamiento del sistema.
Adicionalmente se llevarán a cabo pruebas de seguridad orientada a identificar vulnerabilidades y asegurar el cumplimiento de políticas de protección de la información. Los resultados de estas pruebas serán documentados en reportes técnicos y matrices de casos de prueba, y solo después de su aprobación por parte de la supervisión del contrato, la solución podrá avanzar hacia el ambiente de producción.
La implementación del sistema deberá orientarse al cumplimiento de estándares de calidad, disponibilidad y desempeño, garantizando una operación estable, segura y eficiente. La solución deberá estar preparada para soportar el volumen de usuarios y transacciones estimadas, así como para crecer de manera escalable de acuerdo con las necesidades institucionales.
Durante la implementación se realizarán actividades de optimización en la capa de aplicación, base de datos, servidor web y sistema operativo, con el fin de asegurar tiempos de respuesta adecuados y una correcta utilización de los recursos tecnológicos. Se establecerán mecanismos de monitoreo y alerta temprana que permitan detectar oportunamente fallas, degradaciones del servicio o riesgos de seguridad.
La entidad recibirá una solución que cumpla con buenas prácticas de arquitectura tecnológica y que garantice continuidad operativa en los procesos misionales asociados a la atención de población migrante.
El contratista deberá ejecutar un proceso integral de pruebas y aseguramiento de calidad,
que incluirá como mínimo:

- Pruebas unitarias.
- Pruebas funcionales por módulo.
- Pruebas de integración entre componentes.
- Pruebas de rendimiento bajo carga.
- Pruebas de seguridad y vulnerabilidades.
- Pruebas de usabilidad con usuarios finales. Se

deberán entregar:

- Plan de pruebas.
- Matrices de casos de prueba.
- Resultados de pruebas ejecutadas.
- Correcciones implementadas.
- Acta de aprobación funcional emitida por la supervisión.

La solución deberá implementarse garantizando:

- Alta disponibilidad del servicio.

- Tiempos de respuesta adecuados.
- Escalabilidad y estabilidad.
- Buenas prácticas de arquitectura tecnológica.
- Mecanismos de monitoreo y alerta temprana.
- Cumplimiento de estándares de seguridad.

4.13.1 Criterios objetivos y umbrales de aceptación para el recibo a satisfacción

Como condición indispensable y previa para la suscripción del Acta de Recibo a Satisfacción y el paso a producción, el contratista deberá demostrar el cumplimiento estricto de los siguientes umbrales cuantitativos en los informes de pruebas y aseguramiento de la calidad:

Tipo de prueba / estándar	**Criterio de medición**	**Umbral mínimo de aprobación (recibo a satisfacción)**	**Evidencia requerida**
Pruebas de seguridad y vulnerabilidades	Análisis estático y dinámico bajo estándar OWASP TOP 10 y métricas CVSS V3.1 / V4.0 en la capa de aplicación.	• 0 vulnerabilidades críticas (CVSS 9.0 - 10.0). • 0 vulnerabilidades altas (CVSS 7.0 - 8.9). • vulnerabilidades medias o bajas deberán contar con plan de mitigación o remediación acordado con la supervisión.	Informe de escaneo y pruebas de penetración (ethical hacking) firmado por el especialista, con matriz de hallazgos y evidencias de cierre.
Pruebas de rendimiento y carga	Desempeño del sistema bajo escenario de carga nominal de 45 usuarios concurrentes y tasa de hasta 300 transacciones/hora (RNF-03 Y RNF-04).	• tiempo de respuesta ≤ 2.0 segundos en el percentil 95 (p95) para consultas y registros estándar. • tiempo de respuesta ≤ 5.0 segundos para generación de reportes y tableros complejos. • tasa de error ≤ 0.1% durante las pruebas de estrés.	Reporte consolidado de pruebas de carga y estrés con curvas de concurrencia, uso de CPU/memoria y tiempos de respuesta.
Accesibilidad web	Cumplimiento de directrices WCAG 2.0 / 2.1 nivel AA y norma técnica NTC 5854.	• 100% de cumplimiento de los criterios de conformidad nivel a y aa evaluados mediante herramientas automáticas (ej. TAWDIS, AXE, WAVE). • 0 barreras de navegación por teclado en flujos críticos del sistema.	Reporte automatizado de accesibilidad y matriz de verificación manual de accesibilidad debidamente suscrita.
Usabilidad y UX	Evaluación de las 10 heurísticas de nielsen en formularios de captura, módulos de consulta y reportes.	• 0 hallazgos de severidad 3 o 4 (problemas graves o catastróficos de usabilidad). • tasa de éxito en tareas críticas de captura territorial ≥ 95% en pruebas con usuarios funcionales.	Matriz de evaluación heurística y actas de pruebas de usuario (UAT) firmadas por los usuarios delegados.
Pruebas	Matriz de	• 100% de casos de prueba	Matriz de casos de

Tipo de prueba / estándar	Criterio de medición	Umbral mínimo de aprobación (recibo a satisfacción)	Evidencia requerida
funcionales e integración	trazabilidad de requerimientos funcionales (RF-01 a RF-12).	ejecutados y superados sin bloqueos funcionales en ambiente de pruebas previo al despliegue.	prueba con evidencia fotográfica/registro de ejecución y visto bueno de la supervisión.

Es indispensable para el visto bueno para la puesta en producción definitiva y suscripción del acta de recibo a satisfacción que no persistan vulnerabilidades de severidad Alta o Crítica en la capa de aplicación, y se alcancen los tiempos de respuesta mínimos definidos en la presente tabla.

4.14 TRANSFERENCIA DE CONOCIMIENTO

Se realizará una estrategia para para garantizar la transferencia del conocimiento del sistema de información que consiste en los siguientes puntos:

- Capacitación de 3 horas dirigida a tres (3) usuarios administradores del sistema.
- Capacitación de 3 horas dirigida a diez (10) usuarios funcionales.
- Entrega de listados de asistencia y actas de los procesos de capacitación.

4.15 GARANTIZAR EL USO Y APROPIACIÓN DE LOS SISTEMAS

Se realizará una estrategia para para garantizar el uso y la apropiación del sistema información para el Proyecto “Cali Suma: Sin dejar a nadie atrás” que consiste en los siguientes puntos.

- Identificación e Involucramiento de interesados: Este punto consiste en identificar y hacer un listado de cada uno de los actores involucrados y público impactado con la interacción con el sistema.
- Capacitación y entrenamiento: se realizará a través del desarrollo de los planes de capacitación específicos formulados por los líderes funcionales de cada uno de los módulos desarrollados de acuerdo con el manual de uso desarrollado.
- Sostenibilidad del cambio: de manera anual se programan socializaciones sobre las políticas de TI lideradas por el equipo del observatorio de Paz, Derechos Humanos y Cultura Ciudadana, de tal manera que estas actividades reiteradas le permitan a la Entidad generar la cultura de apropiación de herramientas, metodologías y demás documentaciones que permita el cumplimiento de las políticas
- Acciones de mejoras y gestión del cambio: se realizará un acompañamiento a los planes de mantenimiento de los sistemas de información a través de los comités de cambios que se generen de acuerdo con el procedimiento de gestión de cambio.
- Monitoreo: se realizará una revisión y actualización periódicas de la documentación asociada a los sistemas de información. Para la creación de la estrategia deberá, contemplar las acciones recomendadas por la GUÍA PARA LA IMPLEMENTACIÓN DE ESTRATEGIAS DE USO Y APROPIACIÓN y para garantizar la adopción de la estrategia debe considerar los 5 pilares del cambio (Conciencia, Compromiso, Conocimiento, Capacidad y Cultura) que permiten medir el desempeño de los elementos previstos y el impacto en la implementación de una estrategia de Uso y Apropiación.

OBLIGACIONES ESPECÍFICAS DEL CONTRATISTA

1. El contratista deberá realizar la instalación y parametrización completa del sistema de información, así como de los componentes de software y servicios necesarios para su funcionamiento. La implementación se realizará inicialmente en un ambiente de pruebas dispuesto por DATIC o por la

entidad responsable, en el cual se ejecutarán pruebas técnicas y funcionales por parte del contratista, del equipo de calidad y de los usuarios designados para tal fin. Una vez la solución supere satisfactoriamente dichas pruebas, se procederá a su instalación y parametrización definitiva en los servidores de producción. En esta fase, el contratista realizará la afinación del sistema operativo, del servidor web, del motor de base de datos y de los demás servicios asociados, con el objetivo de garantizar un rendimiento óptimo y condiciones adecuadas de seguridad. Como parte del proceso de despliegue, se deberán entregar los manuales técnicos, manuales de usuario y guías de instalación del sistema, en cumplimiento de la Guía de Despliegue de Sistemas de Información adoptada por la entidad. Después de la puesta en marcha, el contratista garantizará un acompañamiento presencial durante un periodo mínimo de diez (10) días hábiles consecutivos sin incidentes, o el plazo que determine la entidad, hasta verificar la estabilidad del sistema y el correcto funcionamiento de los servicios implementados.

2. Instalar y parametrizar la solución, así como los componentes de software y servicios requeridos para su operación.
3. Implementar inicialmente en un ambiente de pruebas provisto por DATIC.
4. Realizar pruebas internas por parte del contratista y pruebas institucionales por parte del equipo de calidad y usuarios designados.
5. Una vez aprobadas las pruebas, realizar la instalación y parametrización en los servidores de producción.
6. Efectuar la afinación del sistema operativo, servidor web, motor de base de datos y servicios asociados, garantizando óptimo rendimiento y seguridad.
7. Entregar:
    a. Manual de usuario.
    b. Manual técnico.
    c. Guías de instalación en cumplimiento de la Guía de Despliegue de Sistema de Información vigente en la entidad.
8. Garantizar acompañamiento presencial posterior a la puesta en marcha por un periodo mínimo de diez (10) días hábiles consecutivos sin incidentes, o el tiempo que defina la entidad contratante.

SOPORTE TECNICO

Objetivo General:

1. El soporte técnico debe ser en Colombia.

2. El soporte de la solución debe tener vigencia de un (1) año contado a partir del recibido a satisfacción por parte del supervisor del contrato, formalizado mediante acta.

3. El oferente deberá establecer los canales oficiales para la recepción y atención de las solicitudes, de acuerdo con los niveles de servicio, entre los cuales se definirán como mínimo:

• Teléfono Fijo

• Teléfono móvil

• Correo electrónico.

A continuación, se definen los niveles de servicio que en términos de cantidad de eventos y tiempo de respuesta deben ser cumplidos por parte del oferente como parte del servicio de soporte y garantía:

4.17.1 Tipo de incidentes:

PRIORIDAD CATEGORÍA 1 – Servicio interrumpido

• Ha ocurrido una falla que inhabilita por completo la ejecución de todas las funcionalidades y los servicios involucrados en este proyecto.

PRIORIDAD CATEGORÍA 2 – Servicio degradado

Ha ocurrido una falla que ocasiona que al menos una de las funcionalidades o servicios involucrados no opere bajo los parámetros normales.

• Ha ocurrido una falla que degrada el desempeño (Tiempo de respuesta) de al menos una funcionalidad o servicio involucrado en el proyecto.

4.17.2 Tiempo de respuesta a incidentes reportados

El oferente deberá cumplir estrictamente con los siguientes tiempos de respuesta contados a partir del reporte de la incidencia por parte del Distrito de Santiago de Cali, de acuerdo a la categorización de la prioridad.

Prioridad	Atención		Solución	
	Remota	En sitio	Temporal	Definitiva
1	< 30 minutos*	< 1 hora*	< 4 horas*	< 24 horas*
2	< 2 horas hábiles	< 4 horas hábiles	< 16 horas hábiles	< 36 horas hábiles

*Sin restricción de horario no hábil

Se excluyen tiempos de indisponibilidad atribuibles a fallas de infraestructura institucional o demoras de acceso físico de DATIC.

4.17.2 Mantenimiento del Sistema:

Se deben realizar 4 mantenimientos del sistema durante un año (uno cada tres meses), contado a partir del recibo a satisfacción. Estos mantenimientos incluyen afinación del sistema y base de datos, actualizaciones de librerías, revisión de logs del sistema y servidores, así como también velar por el cumplimiento y control de los estándares de usabilidad y accesibilidad. El proponente dentro del marco del servicio de garantía por un (1) año debe realizar pruebas de seguridad (Ethical hacking) y corrección de las vulnerabilidades encontradas con una periodicidad mínima de una (1) trimestral para verificar la seguridad del sistema.

Las pruebas de ethical hacking y mitigación aplican sobre la capa de aplicación/software desarrollado por el contratista y no sobre la infraestructura base de la Alcaldía.

4.18 PROPIEDAD INTELECTUAL

Los derechos patrimoniales de autor sobre (obra, modelo de utilidad, invención, producto, aplicación, etc.,) que realice el contratista en virtud del contrato para la ejecución de este proyecto, corresponden en su

totalidad a la Administración Central del Distrito Especial Santiago de Cali. El contratista conservará los derechos morales de autor.

El contratista entregará el código fuente a la Administración Central del Municipio Santiago de Cali. El contratista deberá entregar a la Secretaría de Bienestar Social la totalidad de los accesos, credenciales y cualquier otro elemento necesario para la administración, mantenimiento y futura evolución del Sistema de Información, mientras que los conectores/SDKs/APIs de integración serán entregados y documentados. Para un software comercial requerido dentro de la implementación funcional del sistema de información se debe adquirir licenciamiento a perpetuidad, especificando su tipo.

Se precisa que el licenciamiento perpetuo aplica al núcleo desarrollado y no restringe servicios SaaS/consumo de terceros indispensables (blockchain, mensajería, mapas). Se precisa que la entidad no adquiere una infraestructura propietaria de red Blockchain, sino los componentes de software (APIs, SDKs, conectores y lógica de emisión/verificación) necesarios para interoperar con redes de credenciales verificables bajo estándares abiertos del W3C.

Es fundamental establecer que la adquisición de la solución de software y sus componentes asociados no se realiza bajo un modelo de membresía, suscripción o licencia temporal, sino que debe garantizarse la titularidad y el uso permanente por parte de la Alcaldía de Santiago de Cali, de acuerdo con la normativa vigente en la materia. La prohibición de esquemas de suscripción o licencia temporal aplica exclusivamente al código fuente y lógica de negocio del sistema desarrollado a la medida para el Distrito. Se autoriza la integración de servicios complementarios especializados (SaaS/Cloud APIs para mapas, notificaciones, servicios de validación criptográfica/blockchain) bajo modelos de consumo durante la vigencia del contrato.