Anexo Especificaciones Técnicas Sistemas de Información 2026

Contrato interadministrativo para el soporte, mantenimiento, desarrollo e implementación de sistemas de información SIGESH y BEL del Distrito de Medellín

1. Problema, necesidad u oportunidad a resolver

El Concejo de Medellín como respuesta al complejo sistema social de ciudad metropolitana concibió el Departamento Administrativo de Gestión del Riesgo de Desastres DAGRD, mediante Acuerdo 059 de diciembre de 2011, reglamentado posteriormente por el Decreto 021 del 3 de enero de 2013, el cual busca integrar los recursos logísticos, financieros y el talento humano necesario para direccionar las políticas locales de Gestión del Riesgo para la realización de las labores previas de análisis, estudios y diagnósticos para la prevención de desastres, el diseño, la capacitación y el entrenamiento para la respuesta ante emergencias y la preparación para asumir las actividades consecuentes de las situaciones desastrosas y de calamidad que afectan la jurisdicción urbana y rural del distrito. De igual manera, mediante Decreto 1240 del 23 de julio de 2015 se establece la conformación del Sistema Municipal de Gestión del Riesgo de Desastres y se restructura el DAGRD.

En esta misma línea, el Decreto 0883 de 2015 establece la estructura de la administración distrital de Medellín, las funciones de sus organismos, dependencias y entidades descentralizadas, y determinó en su Artículo 284 que el Departamento Administrativo de Gestión del Riesgo de Desastres –DAGRD, tiene como responsabilidad dirigir la implementación de la gestión del riesgo de desastres, atendiendo las políticas que contribuyan a la seguridad, el bienestar, la calidad de vida de las personas y al desarrollo sostenible y coordinar el funcionamiento y el desarrollo continuo del Sistema Municipal para la Prevención y Atención de Desastres y la adaptación al cambio climático.

El Departamento Administrativo de Gestión del Riesgo de Desastres, en adelante DAGRD, es la dependencia encargada de coordinar y ejecutar acciones de gestión del riesgo en nombre de la administración Distrital en los procesos de conocimiento, reducción del riesgo y manejo de desastres, para lo cual adelanta planes, programas y proyectos para: la identificación, caracterización y análisis de escenarios de riesgos de desastres; seguimiento y monitoreo de los escenarios de riesgo identificados; definición, desarrollo y coordinación de las intervenciones prospectivas y correctivas de las condiciones de riesgo; definición de estrategias de protección financiera para el territorio; preparativos para la respuesta y recuperación frente a la materialización de escenario de riesgo; y ejecución integral de la respuesta y la recuperación de emergencias y desastres generados por fenómenos de origen natural y antrópico no intencional

que se presentan en el distrito de Medellín, de conformidad con el marco normativo internacional, nacional y distrital.

Por su parte, el Decreto 0834 del 7 de octubre de 2021, modificado por el Decreto 100 del 02 de febrero de 2024, en su artículo 4 realizó la delegación en las dependencias ordenadoras del gasto para la celebración de contratos interadministrativos y en el artículo 17, la ordenación del gasto al director del aludido Departamento Administrativo, con cargo a los recursos del Fondo Municipal para la Gestión del Riesgo de Emergencias y Desastres de Medellín, FONGRED.

Cabe resaltar que, el Decreto 0361 del 09 de mayo de 2024 "Por medio del cual se expide el Decreto Único Compilatorio de delegaciones en materia contractual del Distrito de Ciencia, Tecnología e Innovación de Medellín, se derogan los Decretos 834 de 2021 y 100 de 2024 y se dictan otras disposiciones complementarias", en su artículo 18, delegó en el director del Departamento Administrativo de Gestión del Riesgo de Desastres –DAGRD-, los procesos de contratación, en todas sus etapas, sin consideración a la cuantía, para la adquisición de bienes, obras y servicios que se adelanten con recursos del Fondo Municipal para la Gestión del Riesgo de Emergencias y Desastres de Medellín –FONGRED-, de conformidad con lo establecido en el artículo 17 del Acuerdo municipal 59 de 2011.

Igualmente, estableció que, la elaboración de los documentos precontractuales y contractuales, así como la supervisión y liquidación del respectivo contrato estará a cargo de la dependencia que lo genere.

1.1 SIGESH

Actualmente, el Distrito de Medellín cuenta con el Sistema de Información de Gestión de Seguridad Humana (SIGESH), el cual está activo y disponible para los ciudadanos desde octubre de 2023. Este sistema ha sido oficialmente definido para la gestión de inspecciones oculares de seguridad humana y sistemas contra incendios, así como las inspecciones que realiza el equipo de seguridad humana para piscinas y estanques.

Dentro de su potencial de escalabilidad se desarrollaron los módulos para la gestión de los trámites de acreditaciones para operadores logísticos, eventos de aglomeración masiva, parques permanentes e itinerantes y shows de pirotecnia; los tres últimos integrados con la Ventanilla única de eventos, sistema a partir del cual se realizará contacto con la ciudadanía ya que en estos trámites, el DAGRD desde sus equipos de seguridad humana y gestión del riesgo para aglomeraciones aporta un concepto mediante el cual las demás dependencias que tienen participación en el trámite emiten sus conceptos y se genera un documento unificado desde el Distrito. Estos módulos se desarrollaron entre 2025 y 2026 y apenas está iniciando su implementación.

Si bien el módulo de establecimientos se encuentra en un estado maduro de desarrollo, el uso de este ha permitido evidenciar oportunidades de mejora y potencial de integración para obtener información valiosa para otros equipos del DAGRD, como lo es el acompañamiento y capacitación y transferencia de conocimiento a los establecimientos de nivel de riesgo ordinario 1 y 2 para la gestión de planes de gestión del riesgo. Por su parte, la gestión del módulo de inspecciones a piscinas y estanques requiere ajustes en el flujo establecido en el desarrollo anterior, esto, debido a que actualmente lo implementado no corresponde con la realidad que se presenta en el qué hacer misional de este servicio.

De manera similar, los módulos de gestión de acreditaciones para operadores logísticos, eventos, parques y pirotecnia, dentro de su fase de implementación pueden requerir cambios, además de que se deben ajustar algunos campos que están pendientes de registro en la ventanilla única y que se requieren para la gestión del trámite en SIGESH.

Asimismo, dentro de la gestión de información se requiere fortalecer el módulo de reportes e informes del sistema, mediante la generación de tableros de control para cada tipo de trámite, con el fin de que se pueda contar con estadísticas claves sobre la gestión de cada uno.

Teniendo en cuenta los cambios en herramientas y procedimientos para la gestión de estos trámites, se requiere incluir un componente de apropiación del sistema dentro de la fase de implementación, mediante el cual se informe, se brinde acompañamiento y capacitación en el uso a todos los actores involucrados en la gestión de éstos, en aras de que sea mucho más fácil la apropiación de la herramienta y la gestión del cambio.

1.2 Bomberos en Línea – BEL

En el año 2025 inició la fase de diseño y desarrollo de los módulos de gestión de novedades de personal, novedades de nómina, novedades de vehículos, novedades locativas y novedades de herramientas, equipos y accesorios, así como el módulo de registro de minuta digital de la guardia de las estaciones y las minutas del Centro de formación y del equipo de seguridad humana. En su mayoría el desarrollo de estos módulos se ejecutó sin novedad e inició la fase de implementación, sin embargo, en los módulos de gestión de novedades de personal, novedades de nómina y minuta del centro de formación se hace necesario realizar algunos ajustes y mejoras, que no estaban contemplados en el contrato inicial y que se requieren para garantizar el adecuado funcionamiento de éstos.

Dentro de los ajustes que se deben realizar al módulo de gestión de novedades de nómina se incluye el refinamiento de los formatos que permitan la integración con SAP, así como la trazabilidad de las novedades y su impacto en las novedades de nómina, tanto para el personal de la tropa como para el personal que apoya actividades en el Centro de formación.

Asimismo, dentro de las oportunidades de evolución del sistema se vio la necesidad de complementar el módulo de minuta del Centro de Formación con el desarrollo de un módulo nuevo denominado “Mapa Humano”, a partir del cual sea posible hacer seguimiento exhaustivo a la formación del personal adscrito al Cuerpo Oficial de Bomberos de Medellín, así como evidenciar las necesidades de actualización o realización de cursos y demás actividades formativas de la carrera bomberil. Dentro de este módulo también se vio la necesidad de refinar el proceso de selección

En la minuta para seguridad humana se requiere la integración con el sistema de información SIGESH, con el fin de poder contar con datos de registro que permitan conocer a partir de los registros realizados en SIGESH, el consolidado de actividades que realiza el equipo de inspectores durante un turno, de manera georreferenciada y clasificada por cada tipo de actividad, trámite o servicio.

En el módulo de novedades de vehículos se requiere la validación de la posibilidad de integración con un aplicativo que está siendo desarrollado por la Secretaría de Suministros y Servicios, esto de cara a que es esta dependencia quien está a cargo de la gestión del parque automotor del Distrito, sin embargo, el DAGRD es quien debe adelantar los procesos contractuales de cara al mantenimiento preventivo, correctivo y reparaciones de los vehículos de emergencias. Dentro de las integraciones de este módulo también se debe validar la posibilidad de integrar con el sistema de información AM, mediante el cual se gestionan las órdenes de trabajo de las reparaciones y mantenimientos del parque automotor.

Para el módulo de gestión de novedades de herramientas, equipos y accesorios se requiere ajustar el desarrollo de acuerdo con las necesidades definidas en el plan de gestión y saneamiento de cartera, en el cual además de incluir el inventario de herramientas de cada estación se debe verificar la posibilidad de asociar cada herramienta al funcionario que la tiene asignada en su cartera. También, se requiere evaluar la posibilidad de realizar la presencia de los elementos de cada vehículo mediante monitoreo a través de chips u otros dispositivos electrónicos, mediante los cuales se pueda validar la presencia o no de elementos en los vehículos cuando salen a atender emergencias y una vez regresan de las mismas.

1.3 Desarrollo del módulo de secretaría de seguridad

Actualmente, la gestión de horas extras, recargos y compensatorios de los servidores públicos de la Secretaría de Seguridad y Convivencia de Medellín se realiza de forma manual, mediante hojas de cálculo, documentos en Word, formularios físicos y correos electrónicos. Cada dependencia administra la información de manera independiente, sin integración entre los procesos ni interoperabilidad con otras áreas.

El registro de las horas laboradas se efectúa en planillas quincenales y mensuales con códigos específicos para cada tipo de hora extra o recargo. Posteriormente, esta información se consolida manualmente para su carga en SAP mediante el archivo SCAT y la transacción ZINFOTIPO_15. Asimismo, los saldos de horas compensatorias se controlan en hojas de cálculo individuales, donde se registran las horas causadas, compensadas, el saldo pendiente, la fecha de prescripción y su estado.

El control de la prescripción de las horas compensatorias, que ocurre tres años después de su causación, se realiza de forma manual y sin alertas automatizadas, lo que aumenta el riesgo de errores y pérdida de trazabilidad. De igual manera, los traslados de saldos entre dependencias se gestionan mediante comunicaciones oficiales.

Finalmente, la solicitud de disfrute de compensatorios se tramita mediante el formulario físico FO-GETH-269, que requiere varias firmas para su aprobación. Todo el proceso, desde la solicitud hasta la actualización del saldo, se ejecuta manualmente y sin trazabilidad digital, dificultando el seguimiento en tiempo real y la validación oportuna de la disponibilidad de horas.

La falta de un sistema integrado para gestionar las horas extras, recargos y compensatorios genera riesgos operativos, jurídicos y administrativos que afectan la eficiencia de la Secretaría de Seguridad y Convivencia. La información dispersa en múltiples archivos de Excel incrementa la probabilidad de inconsistencias, duplicidades y errores en el registro y en la carga de datos a SAP.

Además, la ausencia de alertas para controlar la prescripción de horas compensatorias puede ocasionar la pérdida de estos derechos y generar posibles pasivos laborales. La consolidación manual de información entre dependencias retrasa la toma de decisiones y limita la disponibilidad de información confiable. Finalmente, la falta de una plataforma centralizada dificulta la trazabilidad, las auditorías y la rendición de cuentas ante los organismos de control.

La implementación de un sistema de información web y centralizado para la gestión de horas extras, recargos y compensatorios permitirá automatizar los procesos de registro, seguimiento, solicitud y disfrute de horas compensatorias, eliminando la dispersión de la información y garantizando datos íntegros y disponibles en tiempo real.

El sistema automatizará el cálculo de saldos, el control de la prescripción y los flujos de aprobación, reduciendo tiempos de respuesta, errores manuales y mejorando la trazabilidad de todo el proceso. Además, permitirá generar automáticamente los archivos SCAT para SAP, digitalizar el formulario FO-GETH-269 con firma electrónica, producir reportes consolidados y fortalecer la atención de auditorías. Con ello, se optimizará la gestión del talento humano, promoviendo mayor eficiencia, transparencia y control administrativo.

Teniendo en cuenta el avance en el desarrollo que tiene el DAGRD en el sistema que satisface esta necesidad para el personal de bomberos y que, se adapta a la necesidad planteada por la Secretaría de Seguridad, se requiere el desarrollo de un módulo específico para la Secretaría de seguridad mediante el cual sea posible aprovechar los avances en diseño y desarrollo, además de aunar esfuerzos para potenciar la solución.

1.4 Estrategia de apropiación de los sistemas de información

Atendiendo a las necesidades de divulgación que permitan que los sistemas de información SIGESH y Bomberos en Línea sean conocidos y utilizados por cada uno de los actores involucrados en ellos, se requiere el desarrollo de una estrategia de apropiación, mediante la cual dichos actores comprendan cada sistema y cada uno de los módulos que los componen, así como las necesidades que se busca resolver con cada uno de ellos. Esta estrategia debe comprender:

- **Campañas de socialización:** Presentaciones en eventos, mesas técnicas de GRD, reuniones con grupos de interés específicos, divulgación en medios de comunicación.
- **Material de comunicación:** Infografías, videos tutoriales y boletines informativos sobre cada sistema.
- **Capacitaciones y talleres:** Sesiones prácticas con usuarios clave para garantizar su comprensión y uso.
- **Pruebas de navegación asistidas:** Espacios para que los usuarios exploren el sistema con acompañamiento técnico.
- **Estrategia digital:** Uso de plataformas en línea para la difusión de información, tutoriales y actualizaciones.

La estrategia de divulgación deberá involucrar a entidades públicas, privadas, personal de bomberos, personal del DAGRD y otras dependencias pertenecientes al nivel central del Distrito, comunidad en general, asociaciones gremiales y demás actores de interés para los sistemas.

La estrategia deberá implementarse en concordancia con lo estipulado en el Anexo Lineamientos sobre adquisición, desarrollo, Uso y apropiación de soluciones tecnológicas en la Alcaldía de Medellín, específicamente en el Dominio Uso y Apropiación, el cual contiene los lineamientos específicos para garantizar una divulgación efectiva. Este anexo establece los principios, metodologías, estándares y formatos que rigen para este proceso.

- **Formular el Plan de Gestión del Cambio:** Consiste en incorporar un plan para la gestión del cambio que considere los niveles de adopción del cambio y los efectos o el impacto derivados del proyecto, para que se estructuren las acciones que garanticen la correcta apropiación de parte de los usuarios de la solución implementada y que su utilización sea conforme a los objetivos del proyecto.

El Plan de Gestión del Cambio estará conformado por la matriz de interesados, el plan de comunicación y el plan de formación. El área dueña de la iniciativa de TI (o solución a implementar) se hará cargo de que este plan se formule debidamente con la coordinación del gerente del proyecto y la participación del implementador. El material utilizado para las formaciones (presentaciones, infografías, videos, material de apoyo a las formaciones, entre otros) deberá entregarse de forma digital a la Unidad de Innovación de la SID para que repose en los Centros de Recursos de ApropiaTIC para disponerlo en futuras formaciones, de ser necesario.

- **Realizar seguimiento del Plan de Gestión del Cambio**: El plan de gestión del cambio debe ser evaluado de manera periódica, de forma que pueda medirse su nivel de ejecución y el éxito obtenidos.
- **Medir los resultados:** Para el establecimiento de los resultados se presentan los indicadores en los cuales se apoya la evaluación de la gestión del cambio del proyecto, no obstante, su utilización o pertinencia dependerá de quienes hagan el ejercicio de verificación y de los temas que deseen o requieran visualizar o establecer.

El marco de Gestión del Cambio deberá llevarse a cabo según el Anexo. Dominio Uso y Apropiación, con el uso de los instrumentos Matriz de Interesados.xls, Plan de Comunicaciones.xls, Plan de Formación.xls.

Se debe presentar una estrategia para cada sistema de información de manera separada.

2. Alcance

El alcance de este proyecto abarca el soporte, mantenimiento, actualización y evolución al Sistema de Información de Seguridad Humana, así como el desarrollo e implementación de la segunda fase del sistema de información Bomberos en Línea, verificando la factibilidad de integración de este sistema con el aplicativo SIGAI, el sistema de información AM y el sistema de información SIGESH, y la implementación de la estrategia de apropiación de los sistemas de información, incluyendo la estrategia digital y el plan de gestión del cambio conforme a los lineamientos establecidos en el Distrito.

3. Requerimientos Funcionales

3.1 SIGESH:

3.1.1 Soporte y mantenimiento:

Según lo definido en los Lineamientos sobre adquisición, desarrollo, uso y apropiación de soluciones tecnológicas, para el sistema de información SIGESH, se requiere contar con los

servicios de soporte, mantenimiento preventivo, mantenimiento correctivo y actividades de actualización y optimización a nivel de la estructura del sistema.

De acuerdo con los lineamientos, estas actividades estarán discriminadas de la siguiente manera:

3.1.1.1 Servicio de Soporte para atención de incidentes y solicitudes:

Incidentes	Fallo o error de funcionamiento del aplicativo que debe ser solucionado temporal o definitivamente con alta prioridad para reestablecer el servicio y la afectación a los usuarios.
Solicitudes	Requerimiento de información, inquietud, asesoría, reporte, ajuste de datos o aclaración sobre el funcionamiento del sistema. No se considera un incidente o fallo del sistema. No aplica para nuevos desarrollos o funcionalidades del sistema.

Acuerdos de Nivel de Servicio para el servicio de soporte:

Tipo de Atención	Tiempo máximo de respuesta (primer contacto en horas hábiles)	Tiempo máximo de resolución (solución en horas hábiles)
Incidente de criticidad Alta Cuando se impacta masivamente la utilización del sistema	2 horas	Hasta 8 horas
Incidente de criticidad Baja Cuando se impacta en una funcionalidad puntual y no masiva	8 horas	Hasta 24 horas
Solicitud	8 horas	Hasta 40 horas

La criticidad es asignada por el área que reporta el incidente.

En los tipos de atención se incluirá aquellos relacionados con la seguridad informática de la siguiente manera:

Nivel de criticidad alta: en este nivel el contratista deberá brindar tratamiento, remediación frente a eventos o incidentes de seguridad informática, inestabilidad de funcionalidad que presente el sistema, cuyo impacto sea de criticidad alta. Así mismo, el proveedor deberá

atender los requerimientos relacionados con la identificación de vulnerabilidades, por parte de la entidad o de un tercero y brindar tratamiento y remediación para aquellas vulnerabilidades de criticidad alta.

Nivel de criticidad baja: en este nivel el contratista deberá brindar tratamiento y remediación frente a eventos o incidentes de seguridad informática cuyo impacto sea de criticidad baja. Así mismo, el proveedor deberá atender los requerimientos relacionados con la identificación de vulnerabilidades, por parte de la entidad o de un tercero y brindar tratamiento y remediación para aquellas vulnerabilidades de criticidad baja.

Se debe brindar asistencia técnica frente a fallas de compatibilidad ocasionados por cambio de versiones en los demás componentes del sistema: explorador de internet, sistema operativo, base de datos y seguridad.

3.1.1.2 Mantenimiento preventivo

Brindar mantenimiento Preventivo mediante la revisión permanente del aplicativo en cuanto a funcionalidad, desempeño y estabilidad.

3.1.1.3 Mantenimiento correctivo

- Brindar mantenimiento correctivo presentarse un mal funcionamiento del aplicativo.
- Realizar actualización tecnológica de nuevas versiones y parches de seguridad en las librerías usadas en el aplicativo.

3.1.1.4 Propiedad del Código

- Todo el material desarrollado será propiedad del Distrito de Medellín y deberá ser alojado en el repositorio oficial del servicio.

3.1.2 Componente de Apropiación del Sistema

- **Campañas de socialización:** Presentaciones en eventos, mesas técnicas de GRD, reuniones con grupos de interés específicos, divulgación en medios de comunicación.
- **Material de comunicación:** Infografías, videos tutoriales y boletines informativos sobre cada sistema.
- **Capacitaciones y talleres:** Sesiones prácticas con usuarios clave para garantizar su comprensión y uso.

- **Pruebas de navegación asistidas:** Espacios para que los usuarios exploren el sistema con acompañamiento técnico.
- **Estrategia digital:** Uso de plataformas en línea para la difusión de información, tutoriales y actualizaciones.

La estrategia de divulgación deberá involucrar a entidades públicas, privadas, personal de bomberos, personal del DAGRD y otras dependencias pertenecientes al nivel central del Distrito, comunidad en general, asociaciones gremiales y demás actores de interés para los sistemas.

La estrategia deberá implementarse en concordancia con lo estipulado en el Anexo Lineamientos sobre adquisición, desarrollo, Uso y apropiación de soluciones tecnológicas en la Alcaldía de Medellín, específicamente en el Dominio Uso y Apropiación, el cual contiene los lineamientos específicos para garantizar una divulgación efectiva. Este anexo establece los principios, metodologías, estándares y formatos que rigen para este proceso.

- **Formular el Plan de Gestión del Cambio:** Consiste en incorporar un plan para la gestión del cambio que considere los niveles de adopción del cambio y los efectos o el impacto derivados del proyecto, para que se estructuren las acciones que garanticen la correcta apropiación de parte de los usuarios de la solución implementada y que su utilización sea conforme a los objetivos del proyecto.

  El Plan de Gestión del Cambio estará conformado por la matriz de interesados, el plan de comunicación y el plan de formación. El área dueña de la iniciativa de TI (o solución a implementar) se hará cargo de que este plan se formule debidamente con la coordinación del gerente del proyecto y la participación del implementador. El material utilizado para las formaciones (presentaciones, infografías, videos, material de apoyo a las formaciones, entre otros) deberá entregarse de forma digital a la Unidad de Innovación de la SID para que repose en los Centros de Recursos de ApropiaTIC para disponerlo en futuras formaciones, de ser necesario.

- **Realizar seguimiento del Plan de Gestión del Cambio**: El plan de gestión del cambio debe ser evaluado de manera periódica, de forma que pueda medirse su nivel de ejecución y el éxito obtenidos.
- **Medir los resultados:** Para el establecimiento de los resultados se presentan los indicadores en los cuales se apoya la evaluación de la gestión del cambio del proyecto, no obstante, su utilización o pertinencia dependerá de quienes hagan el ejercicio de verificación y de los temas que deseen o requieran visualizar o establecer.

El marco de Gestión del Cambio deberá llevarse a cabo según el Anexo. Dominio Uso y Apropiación, con el uso de los instrumentos Matriz de Interesados.xls, Plan de Comunicaciones.xls, Plan de Formación.xls.

3.1.3 Ajustes al módulo de inspecciones a establecimientos:

3.1.3.1 Desarrollo del Módulo de plan de gestión del riesgo para establecimientos de autogestión

- **Autodiagnóstico Guiado:** Cuando una empresa ingrese al formulario de SIGESH para hacer su solicitud de inspección, puedan realizar un test de vulnerabilidad e identificar sus escenarios de riesgo más próximos o que se puedan ver enfrentados. Como son empresas más pequeñas el resultado debe de ser dar recomendaciones para estar mejor preparado ante los eventos.
- **Transferencia de Información de Escenarios de Riesgo:** Compartir con las empresas la cartografía e información pública sobre amenazas sectorizadas en el Distrito de Medellín. Ejemplo zonas de inundación, movimientos en masa, esto les permitirá a las empresas de riesgo 1 y 2 alimentar su análisis de vulnerabilidad con datos reales del entorno, alineación directa con SIRMED. Esto se complementa con el test.
- **Fomentar la Ayuda Mutua:** Fomentar que empresas vecinas de riesgo 1 o 2 (ej. locales de un mismo centro comercial o edificios de oficinas) unan esfuerzos para responder de manera conjunta, optimizando los recursos individuales en una respuesta colectiva coordinada, esto se logra poniendo a disposición información sobre los CAM y como es de adherencia voluntaria que simplemente pongan si es de su interés recibir información.
- **Segunda fase integración con SIRMED:** Complementar la integración existente entre SIRMED y SIGESH, agregando campos que permitan al solicitante visualizar información sobre amenazas y riesgos en la zona donde está ubicado el establecimiento, además conocer si existen Comités de ayuda mutua en esta zona.

3.1.3.2 Ajustes a funcionalidades por roles:

- **Rol Ciudadano:**

Tipo de ajuste	Descripción
Mensajes de ayuda	Incluir textos informativos en las casillas de diligenciamiento de la solicitud que guíen al usuario sobre qué información ingresar y cómo hacerlo según su caso (por ejemplo, en la casilla del Dígito de Verificación - DV).
Autocompletado de datos históricos	Al ingresar el NIT o la cédula, el sistema debe traer la información histórica y autocompletar los campos. Asimismo, debe permitir la modificación de datos si es necesario (ej. cambio de dirección). El

	objetivo es que funcione de manera similar al módulo GRA, donde se puede seleccionar una empresa ya registrada y cargar todos sus datos automáticamente para solicitar la inspección.
Resumen previo al envío	Antes de guardar o enviar la solicitud, el sistema debe mostrar un resumen de los archivos cargados y un mensaje de validación para que el ciudadano confirme la información.
Control de duplicidad	Implementar un validador que evite la duplicidad de solicitudes, impidiendo el ingreso de un trámite repetido aun cuando se realicen variaciones menores en el nombre del establecimiento o en la dirección.
Optimización de la gestión mediante precarga de documentos	Optimizar el inicio del trámite mediante la precarga de datos del establecimiento según el NIT o documento ingresado, con opciones para gestionar nuevas sucursales, consultar vigencias y editar información relevante.
Alertas de vencimiento de vigencia del certificado	El sistema debe generar una alerta cuando el establecimiento este próximo a vencer su certificado.

- **Rol Administrador:**

Tipo de ajuste	**Descripción**
Interactividad en informes de estado actual	Al seleccionar el nivel de riesgo, se debe conservar la división por comunas. Adicionalmente, al hacer doble clic sobre una comuna específica, los gráficos deben actualizarse dinámicamente con referencia a la consulta realizada.
Gestión de incidencias de sincronización	Habilitar una opción para que el administrador pueda gestionar y ajustar de forma manual aquellas solicitudes que presenten inconsistencias o problemas de sincronización en los estados de las bandejas
Asignación de roles y permisos a los usuarios del sistema	Contar con una funcionalidad para la asignación de roles y permisos dentro del sistema.
Optimización de la gestión mediante precarga de documentos	Optimizar el inicio del trámite mediante la precarga de datos del establecimiento según el NIT o documento ingresado, con opciones para gestionar nuevas sucursales, consultar vigencias y editar información relevante.

- **Rol inspector:**

Tipo de ajuste	Descripción
Visualización de estado de solicitudes en operativos de seguridad	Visualizar el estado de las solicitudes en operativos que realizan con la PONAL

- Estructuración de gráficos en el módulo de reportes. (Diferentes funcionalidades)

3.1.4 Reestructuración del módulo de inspecciones a piscinas

- Reestructurar el flujo en el módulo de inspecciones a piscinas, de acuerdo con lo establecido en la normativa y procedimientos vigentes.

3.1.5 Ajustes e implementación del módulo de gestión de eventos de aglomeración masiva

- Ajuste de integración con el sistema de información Ventanilla Única, capturando información a través de formularios y documentos requeridos por los equipos del DAGRD para la gestión del trámite.
- Estructuración de gráficos en el módulo de reportes.
- Incluir en el registro de la solicitud del evento, los datos de aforo y otros campos requeridos para la inspección y emisión del concepto.
- Mejorar la visualización de las tablas en cada bandeja mostrando todas las columnas que sean necesarias para entender el trámite; en donde las dos primeras columnas estén bloqueadas y las otras se desplacen al igual que establecimientos (aplica para todos los roles)
- Incluir las plantillas de las notificaciones que sean editables en el rol de administrador al igual que establecimientos.
- Incluir en el rol de administrador la visualización de todos los trámites en cada bandeja y debe haber una opción que diga histórico (histórico de las solicitudes tramitadas al igual que establecimientos).

3.1.6 Ajustes e implementación del módulo de gestión de parques permanentes e itinerantes

- Ajuste de integración con el sistema de información Ventanilla Única, capturando información a través de formularios y documentos requeridos por los equipos del DAGRD para la gestión del trámite.
- Estructuración de gráficos en el módulo de reportes.
- Incluir en el registro de la solicitud los datos de registro de atracciones, aforo, datos del profesional SST que avala el plan de emergencias, y otros campos requeridos para la inspección y emisión del concepto.
- Estructuración de gráficos en el módulo de reportes.
- Ajustar el flujo diferenciado la plantilla cuando el concepto es favorable o desfavorable.
- Mejorar la visualización de las tablas en cada bandeja mostrando todas las columnas que sean necesarias para entender el trámite; en donde las dos primeras columnas estén bloqueadas y las otras se desplacen al igual que establecimientos (aplica para todos los roles)
- Incluir las plantillas de las notificaciones que sean editables en el rol de administrador al igual que establecimientos.
- Incluir en el rol de administrador la visualización de todos los trámites en cada bandeja y debe haber una opción que diga histórico (histórico de las solicitudes tramitadas al igual que establecimientos).

3.1.7 Ajustes e implementación del módulo de gestión de show de pirotecnia

- Ajuste de integración con el sistema de información Ventanilla Única, capturando información a través de formularios y documentos requeridos por los equipos del DAGRD para la gestión del trámite.
- Estructuración de gráficos en el módulo de reportes.
- Ajustar el flujo diferenciado la plantilla cuando el concepto es favorable o desfavorable.
- Incluir en el registro de la solicitud los datos de registro del personal a cargo de la activación de la pirotecnia y otros campos requeridos para la inspección y emisión del concepto.
- Mejorar la visualización de las tablas en cada bandeja mostrando todas las columnas que sean necesarias para entender el trámite; en donde las dos primeras columnas estén bloqueadas y las otras se desplacen al igual que establecimientos (aplica para todos los roles)
- Incluir las plantillas de las notificaciones que sean editables en el rol de administrador al igual que establecimientos.

- Incluir en el rol de administrador la visualización de todos los trámites en cada bandeja y debe haber una opción que diga histórico (histórico de las solicitudes tramitadas al igual que establecimientos).

3.1.8 Ajustes e implementación del módulo de gestión de acreditaciones a operadores logísticos

- Estructuración de gráficos en el módulo de reportes.
- Mejorar la visualización de las tablas en cada bandeja mostrando todas las columnas que sean necesarias para entender el trámite; en donde las dos primeras columnas estén bloqueadas y las otras se desplacen al igual que establecimientos (aplica para todos los roles)
- Incluir las plantillas de las notificaciones que sean editables en el rol de administrador al igual que establecimientos.
- Incluir en el rol de administrador la visualización de todos los trámites en cada bandeja y debe haber una opción que diga histórico (histórico de las solicitudes tramitadas al igual que establecimientos).
- Ajustar en el rol de ciudadano las empresas que están registradas, una tabla que visualice las acreditaciones en cada columna si está acreditada o está en trámite de esta manera el usuario tiene una visual de las acreditaciones que cuenta cada empresa
- Ajustar en cada rol que se pueda visualizar un resumen de la empresa el estado de las acreditaciones que tiene y la que están en trámite.

3.2 Bomberos en Línea

3.2.1 Soporte y mantenimiento:

Según lo definido en los Lineamientos sobre adquisición, desarrollo, uso y apropiación de soluciones tecnológicas, para el sistema de información SIGESH, se requiere contar con los servicios de soporte, mantenimiento preventivo, mantenimiento correctivo y actividades de actualización y optimización a nivel de la estructura del sistema.

Según los lineamientos, estas actividades estarán discriminadas de la siguiente manera:

3.2.1.1 Servicio de Soporte para atención de incidentes y solicitudes:

Incidentes	Fallo o error de funcionamiento del aplicativo que debe ser solucionado temporal o definitivamente con alta prioridad para reestablecer el servicio y la afectación a los usuarios.
Solicitudes	Requerimiento de información, inquietud, asesoría, reporte, ajuste de datos o aclaración sobre el funcionamiento del sistema. No se considera un incidente o fallo del sistema. No aplica para nuevos desarrollos o funcionalidades del sistema.

Acuerdos de Nivel de Servicio para el servicio de soporte:

Tipo de Atención	Tiempo máximo de respuesta (primer contacto en horas hábiles)	Tiempo máximo de resolución (solución en horas hábiles)
Incidente de criticidad Alta Cuando se impacta masivamente la utilización del sistema	2 horas	Hasta 8 horas
Incidente de criticidad Baja Cuando se impacta en una funcionalidad puntual y no masiva	8 horas	Hasta 24 horas
Solicitud	8 horas	Hasta 40 horas

La criticidad es asignada por el área que reporta el incidente.

En los tipos de atención se incluirá aquellos relacionados con la seguridad informática de la siguiente manera:

Nivel de criticidad alta: en este nivel el contratista deberá brindar tratamiento, remediación frente a eventos o incidentes de seguridad informática, inestabilidad de funcionalidad que presente el sistema, cuyo impacto sea de criticidad alta. Así mismo, el proveedor deberá atender los requerimientos relacionados con la identificación de vulnerabilidades, por parte de la entidad o de un tercero y brindar tratamiento y remediación para aquellas vulnerabilidades de criticidad alta.

Nivel de criticidad baja: en este nivel el contratista deberá brindar tratamiento y remediación frente a eventos o incidentes de seguridad informática cuyo impacto sea de criticidad baja. Así mismo, el proveedor deberá atender los requerimientos relacionados con la identificación

de vulnerabilidades, por parte de la entidad o de un tercero y brindar tratamiento y remediación para aquellas vulnerabilidades de criticidad baja.

Se debe brindar asistencia técnica frente a fallas de compatibilidad ocasionados por cambio de versiones en los demás componentes del sistema: explorador de internet, sistema operativo, base de datos y seguridad.

3.2.1.2 Mantenimiento preventivo

- Brindar mantenimiento Preventivo mediante la revisión permanente del aplicativo en cuanto a funcionalidad, desempeño y estabilidad.

3.2.1.3 Mantenimiento correctivo

- Brindar mantenimiento correctivo al presentarse un mal funcionamiento del aplicativo.
- Realizar actualización tecnológica de nuevas versiones y parches de seguridad en las librerías usadas en el aplicativo.

3.2.2 Componente de Apropiación del Sistema

- **Campañas de socialización:** Presentaciones en eventos, mesas técnicas de GRD, reuniones con grupos de interés específicos, divulgación en medios de comunicación.
- **Material de comunicación:** Infografías, videos tutoriales y boletines informativos sobre cada sistema.
- **Capacitaciones y talleres:** Sesiones prácticas con usuarios clave para garantizar su comprensión y uso.
- **Pruebas de navegación asistidas:** Espacios para que los usuarios exploren el sistema con acompañamiento técnico.
- **Estrategia digital:** Uso de plataformas en línea para la difusión de información, tutoriales y actualizaciones.

La estrategia de divulgación deberá involucrar a entidades públicas, privadas, personal de bomberos, personal del DAGRD y otras dependencias pertenecientes al nivel central del Distrito, comunidad en general, asociaciones gremiales y demás actores de interés para los sistemas.

La estrategia deberá implementarse en concordancia con lo estipulado en el Anexo Lineamientos sobre adquisición, desarrollo, Uso y apropiación de soluciones tecnológicas en la Alcaldía de Medellín, específicamente en el Dominio Uso y Apropiación, el cual contiene los lineamientos específicos para garantizar una divulgación efectiva. Este anexo establece los principios, metodologías, estándares y formatos que rigen para este proceso.

- **Formular el Plan de Gestión del Cambio:** Consiste en incorporar un plan para la gestión del cambio que considere los niveles de adopción del cambio y los efectos o el impacto derivados del proyecto, para que se estructuren las acciones que garanticen la correcta apropiación de parte de los usuarios de la solución implementada y que su utilización sea conforme a los objetivos del proyecto.

  El Plan de Gestión del Cambio estará conformado por la matriz de interesados, el plan de comunicación y el plan de formación. El área dueña de la iniciativa de TI (o solución a implementar) se hará cargo de que este plan se formule debidamente con la coordinación del gerente del proyecto y la participación del implementador. El material utilizado para las formaciones (presentaciones, infografías, videos, material de apoyo a las formaciones, entre otros) deberá entregarse de forma digital a la Unidad de Innovación de la SID para que repose en los Centros de Recursos de ApropiaTIC para disponerlo en futuras formaciones, de ser necesario.

- **Realizar seguimiento del Plan de Gestión del Cambio**: El plan de gestión del cambio debe ser evaluado de manera periódica, de forma que pueda medirse su nivel de ejecución y el éxito obtenidos.
- **Medir los resultados:** Para el establecimiento de los resultados se presentan los indicadores en los cuales se apoya la evaluación de la gestión del cambio del proyecto, no obstante, su utilización o pertinencia dependerá de quienes hagan el ejercicio de verificación y de los temas que deseen o requieran visualizar o establecer.

El marco de Gestión del Cambio deberá llevarse a cabo según el Anexo. Dominio Uso y Apropiación, con el uso de los instrumentos Matriz de Interesados.xls, Plan de Comunicaciones.xls, Plan de Formación.xls.

3.2.3 Ajustes e implementación del módulo de nómina

- Realizar ajustes finales al desarrollo para la aprobación masiva de novedades, la validación de horas extras generadas en los equipos del Centro formación y seguridad humana, permitiendo visualizar la trazabilidad de la aprobación de estas y verificando los topes máximos establecidos, así como generar una funcionalidad que permita la supervisión de horas extra.
- Realizar ajustes en el módulo de gestión de novedades de nómina, mediante el cual sea posible la intercomunicación de este módulo con el de novedades de personal y el módulo de minuta del centro de formación.

3.2.4 Desarrollo e implementación de un módulo para la gestión de horas extras, recargos y compensatorios de la Secretaría de Seguridad y Convivencia del Distrito de Medellín

- Verificar la factibilidad del desarrollo e implementación de un módulo para la gestión de horas extras, recargos y compensatorios de la Secretaría de Seguridad y Convivencia del Distrito de Medellín, que permita gestionar de forma centralizada, automatizada y con trazabilidad completa el registro de horas extras, recargos y compensatorios causados, el control de saldos con fechas de prescripción, el flujo digital de solicitudes de disfrute y la generación de archivos de integración con SAP , con el fin de garantizar la eficiencia operativa, la transparencia en la gestión del talento humano y el cumplimiento de las obligaciones laborales con los servidores públicos de la Secretaría de Seguridad y Convivencia.

3.2.5 Ajustes e implementación del módulo del módulo de novedades de personal

- Realizar ajustes finales al desarrollo, posterior a la realización de pruebas e inicio de la fase de implementación con los actores de interés que se ven impactados con la puesta en marcha del sistema.

3.2.6 Ajustes e implementación del módulo de novedades de vehículos

- Realizar ajustes finales al desarrollo, posterior a la realización de pruebas e inicio de la fase de implementación con los actores de interés que se ven impactados con la puesta en marcha del sistema.
- Validar la factibilidad de la integración con el sistema de información SIGAI, de la Secretaría de suministros, buscando que esta dependencia, como dueña del proceso de gestión de vehículos en el Distrito, cuente con información de primera mano respecto a las novedades registradas en los vehículos de emergencias.
- Validar la factibilidad de la integración con el sistema de información AM, mediante el cual se pueda remitir la información de las novedades de vehículos reportadas que requieran la generación de ordenes de trabajo y, de esta manera facilitar la gestión de solicitudes con el contratista a cargo de los mantenimientos y reparaciones de los vehículos.

3.2.7 Ajustes e implementación del módulo locativas

- Realizar ajustes finales al desarrollo, posterior a la realización de pruebas e inicio de la fase de implementación con los actores de interés que se ven impactados con la puesta en marcha del sistema.

3.2.8 Ajustes e implementación del módulo de Herramientas Equipos y Accesorios, de acuerdo con el plan de gestión de cartera, incluyendo la validación de la implementación de un piloto para registro de las HEA´s mediante integración de RFID.

- Reestructurar el módulo de novedades de HEA´s de acuerdo con lo establecido en el plan de gestión y saneamiento de cartera, mediante el cual se busca avanzar hacia una solución que permita el cierre efectivo de los hallazgos que se generaron para el DAGRD a causa de las necesidades de mejora de la gestión de la cartera a cargo de los contratistas.

Con esta reestructuración del módulo se debe poder identificar cada elemento y el funcionario que lo tiene asignado en la cartera.

Además de esto, en este módulo se busca revisar la factibilidad de la implementación de una solución tecnológica mediante la cual se puedan identificar los elementos que se encuentran al interior de los vehículos de emergencias cuando estas salen a realizar las atenciones, asimismo validar que dichas herramientas retornen a la estación posterior a la atención.

3.2.9 Ajustes e implementación del módulo de minuta de guardia

- Realizar ajustes finales al desarrollo, posterior a la realización de pruebas e inicio de la fase de implementación con los actores de interés que se ven impactados con la puesta en marcha del sistema.

3.2.10 Ajustes e implementación del módulo de minuta del centro de formación

- Realizar ajustes finales al desarrollo, posterior a la realización de pruebas e inicio de la fase de implementación con los actores de interés que se ven impactados con la puesta en marcha del sistema.

3.2.11 Ajustes e implementación del módulo de seguridad humana

- Realizar ajustes finales al desarrollo, posterior a la realización de pruebas e inicio de la fase de implementación con los actores de interés que se ven impactados con la puesta en marcha del sistema.
- Integrar el módulo con el sistema de información SIGESH, permitiendo que se pueda generar un informe consolidado de todas las actividades que realiza el equipo con relación a los trámites y servicios gestionados.

3.2.12 Desarrollo del módulo de mapa humano

- Desarrollar el módulo de mapa humano en el cual sea posible contar con la información consolidada frente a la formación del personal del Cuerpo Oficial de Bomberos de Medellín. El desarrollo de este módulo deberá realizarse conforme a las historias de

usuario remitidas por el Departamento Administrativo de Gestión del Riesgo de Desastres.

4 Requerimientos no funcionales

En aras garantizar la operación del sistema en la infraestructura del Distrito se debe cumplir con los lineamientos institucionales "Lineamientos sobre adquisición, desarrollo y uso de las tecnologías de la información y las comunicaciones en la Alcaldía de Medellín" y los entregables de los distintos dominios que allí se relacionan. Isolucion: DE-GTIC Lineamientos sobre Adquisición, Desarrollo y Uso de las TIC en la Alcaldía de Medellín, a continuación, se destacan aspectos claves, no obstante, se anexa el documento completo.

4.1 Dominio de Sistemas De Información

4.1.1 Objetivo

Los lineamientos generales consignados en este dominio pretenden asegurar estándares y buenas prácticas para la adquisición, desarrollo y uso de las tecnologías de la información de cualquier sistema de información para la Alcaldía de Medellín y está dirigido a proveedores, contratistas o funcionarios que participen en la implementación de soluciones de software cualquiera sea su magnitud.

4.1.2 Disposiciones generales

4.1.2.1 Registro de activos

Toda adquisición o desarrollo de sistemas de información o de licencias para su uso, debe ser registrado como activo intangible de la Alcaldía de Medellín a través del equipo de contratación del proyecto.

4.1.2.2 Cesión de derechos patrimoniales

Todos los contratos que contemplen desarrollo, evolución o adquisición de componentes de software deben incluir cláusulas donde las partes acuerden expresamente que los derechos patrimoniales sobre las obras realizadas por el contratista en cumplimiento del objeto del contrato pertenecerán a la entidad, tales como:

- Que el contratista reconozca que la Alcaldía de Medellín es el titular de los derechos patrimoniales de todos los estudios, documentos, software y en general de los productos y obras derivados del contrato, sin límites temporales o territoriales, de conformidad con la normativa vigente. Los derechos patrimoniales corresponden exclusivamente a la

Alcaldía de Medellín para actos de reproducción, comunicación pública, distribución, traducción, adaptación, edición o cualquier otro uso en calidad de titular del derecho.

- El cedente debe garantizar que es propietario de los derechos patrimoniales que cede, y, en consecuencia, garantizar que puede contratar y transferir sus derechos sin ningún tipo de limitación. Por lo tanto, en caso de presentarse cualquier reclamación o acción por parte de un tercero, el contratista asumirá toda la responsabilidad, y saldrá en defensa de los derechos cedidos, exonerando de cualquier responsabilidad a la Alcaldía de Medellín.

En caso de que la Secretaría de Innovación Digital lo solicite y teniendo en cuenta lo dispuesto en el artículo 183 de la Ley 23 de 1982, se debe generar un documento de cesión de derechos patrimoniales, así como la inscripción en el Registro Nacional del Derecho de Autor.
La información básica que debe contener este documento es:

- Información sobre las partes contratantes
- Información del contrato marco con el cual se desarrolla, evoluciona o adquiere el software a ceder o las condiciones para el otorgamiento de una cesión gratuita.
- Descripción del software que se cede
- Ámbito territorial específico al que se circunscribe la cesión del software;
- Alcance de la cesión donde se indique de forma clara y expresa si se transfiere la totalidad de los derechos patrimoniales en todas las modalidades de explotación posibles y conocidas, o si, por el contrario, se reservará la titularidad de algunos derechos de explotación.
- Manifestación de la posible existencia de cargas sobre la titularidad del software
- (como pueden ser prendas, embargos, etc.);
- Información técnica que se deberá facilitar al cedente para el correcto uso del software.

En caso de adquisición de licencias, el contratista deberá entregar a la Alcaldía de Medellín, los certificados de las licencias que sean adquiridas en virtud del contrato y en ellas se deberá facultar expresamente al contratante a la utilización de estas.

4.1.3 Arquitectura de sistemas de información

El propósito es orientar el diseño de cualquier arquitectura de solución bajo parámetros, patrones y atributos de calidad definidos en la Alcaldía de Medellín, asegurando la construcción de sistemas de información con alta calidad técnica, y logrando una apropiación de las tecnologías de punta del mercado acorde a los lineamientos sugeridos por el estado a través de organismos rectores como el MinTIC.

4.1.3.1 Visión general

La arquitectura de la Alcaldía de Medellín cuenta con un componente principal basado en microservicios, el cual describe el diseño de aplicaciones como conjuntos de servicios desplegables de forma independiente, que permiten la optimización funcional de los nuevos sistemas de información, evitando arquitecturas monolíticas y bases de datos centralizadas y únicas.

Información adicional en Anexo 1. Arquitectura de Sistemas de Información

Cualquier sistema de información adquirido o desarrollado para la Alcaldía de Medellín debe implementarse con arquitectura distribuida que permita escalabilidad y capacidad para crecer de forma simple y eficiente de acuerdo con la arquitectura definida en la entidad.

No se admiten sistemas con arquitectura Stand Alone (no distribuidos), en donde todo el software está concentrado en la misma máquina. Es decir que la aplicación, las bases de datos y las conexiones de los controladores residen en la misma PC, que, a su vez, es desde el único lugar donde se lo puede y debe operar.

4.1.3.2 Descripción por componentes

4.1.3.2.1 Desarrollo componentes iniciales: Módulo

Módulo de la plataforma tecnológica, que permite la gestión de plantillas para nuevos desarrollos, con componentes autogenerados, basado en una plantilla con lineamientos de diseño estándar y utilizando patrones de arquitectura.

4.1.3.2.2 Desarrollo API de la lógica basada en Microservicios

Desarrollos unificados de microservicios, donde se tenga la lógica de negocio de la Alcaldía de Medellín y que permita gestionar las peticiones de las aplicaciones. La construcción de un pool de microservicios core con la lógica necesaria para resolver las peticiones desde el backend de las aplicaciones, pasando por el API GATEWAY para consumir uno de los microservicios que se encuentran definidos como Core (Pequeñas instrucciones de código para resolver un mensaje o requerimiento), estos deben resolver una petición o mensaje y enviar la respuesta a la aplicación (Front) que generó el mensaje o petición.

4.1.3.2.3 Implementación de API GATEWAY

Permite generar la correcta distribución y consumo de los microservicios entre las aplicaciones desarrolladas y los microservicios Core del negocio.

Todas las peticiones de consumos de los servicios desde las aplicaciones generadas por medio de las plantillas deben ingresar por medio de una API GATEWAY para su correcta gestión evitando problemas en la conexión persistente de los mensajes hacia los servicios de integración y el Pool de Microservicios Core de la Alcaldía.

Información adicional en: Anexo 2. Características API GATEWAY

4.1.3.3 Ambientes

Los sistemas de información que se requieran implementar desde la distintas Secretarías y/o Direcciones o demás dependencias de la alcaldía, deben estar orientados al proceso de desarrollo en ambientes independientes de Desarrollo, Pruebas y Producción.

Los entornos de desarrollo y pruebas para proyectos internos a través de la Secretaría de Innovación Digital se crearán en Azure DevOps con la previa validación y autorización de la SID.

En el caso que los sistemas de información vayan a ser desarrollados a la medida por un proveedor externo, los ambientes de desarrollo y pruebas deben ser dispuestos contratistas.

Todos los sistemas de información, independiente de su modalidad de implementación, deben ser desplegados, en coordinación con el equipo de DataCenter, en un ambiente de preproducción de la Alcaldía de Medellín para pruebas funcionales y posteriormente en el ambiente productivo para el inicio de la operación.

4.1.3.4 Estructura de Datos

Se deberá propiciar los mecanismos necesarios para centralizar y homogenizar las estructuras de datos de los diferentes sistemas de información, que permita garantizar una única fuente del dato maestro, evitando que se duplique la información en los diferentes sistemas.

Para esto se deberá disponer de un inventario de modelos de datos en el que podrá validar e identificar la disponibilidad de las estructuras de datos actuales.

4.1.4 Almacenamiento

4.1.4.1 Estándares de bases de datos

Con la finalidad de asegurar un buen manejo en el rendimiento de los recursos y; optimización y agilidad en la entrega de la información a través de las aplicaciones, se promueve la utilización de

los siguientes elementos que buscan la unicidad y confiabilidad de la información, al igual que la documentación adecuada de los objetos.

El estándar de base de datos en la Alcaldía de Medellín es el motor PostgreSQL para la implementación de los sistemas de información. En caso de tener otro motor, debe ser justificado y aprobado por la Secretaría de Innovación Digital.

Si el sistema de información que se desarrolla es de tipo gestor de contenidos, se debe usar el CMS WordPress con MariaDB como motor de base de datos.

Cuando se requiera la creación de una instancia de BD se debe realizar a través de la herramienta CSC-Centro de servicios compartidos, y diligenciar los campos que allí se solicitan.

Nota: Las bases de datos que requieran componente geográfico, deberán ser creadas de acuerdo con los lineamientos dados en el capítulo de Implementación de componentes geográficos, y coordinado con el equipo de soporte geográfico de la Alcaldía de Medellín.

4.1.4.1.1 Estructura

Información adicional en: Anexo 3. Descripción nombre de campos/tablas

4.1.4.2 Diccionario de datos

Todos los objetos asociados a las BD deben estar documentados. Cada vez que se realice un cambio a los objetos, éstos deben ser documentados con una breve descripción dentro del mismo objeto adjuntando la fecha del cambio.

Se debe generar y mantener actualizado el diccionario de datos para tener la precisión semántica sobre los datos que se manejan en la base de datos de un sistema de información, evitando diferentes interpretaciones o ambigüedades.

El diccionario de datos se debe generar de acuerdo con las especificaciones del Departamento Nacional de Planeación (DNP) en la "GUÍA PARA LA DEFINICIÓN DE DICCIONARIO DE DATOS DNP"9 que describe los siguientes atributos para tener en cuenta

- Sistema de Información: Corresponde al nombre del sistema de Información.
- Descripción del Sistema de Información: Principalmente tiene que ver con la misión, o mejor, la descripción de los procesos operativos que se manejan.
- Nombre de la Base de datos: Literalmente corresponde al nombre de la base de datos en el DBMS.

- Descripción de la base de datos: En algunos sistemas de información esto se omite, porque solo existe una base de datos, dado que haya más de una, si es necesario describir que tipo de rol cumple cada base de datos para el sistema de información, por ejemplo: i) una base de datos netamente transaccional, y ii) otra que corresponda solo a reportes y/o consulta.
- Tamaño: Tamaño de Bytes de la base de datos.
- Fabricante DBMS: Se debe estipular el nombre de la empresa desarrolladora o fabricante del motor de la base de datos, y su versión.
- Nombre de Tabla: Nombre de cada paquete de datos, este nombre es único en la base de datos.
- Nombre de Campo: Para mayor entendimiento, debe contener el nombre de la columna o elemento de tabla que almacena el valor de cada dato.
- Descripción de Negocio: Este es el campo con más relevancia, dado que debe explicarse en términos de negocio, los valores que se almacenan en cada campo. Más adelante se explica un ejemplo de guía.
- Tipo de Dato; el tipo de dato especifica el dominio de los posibles valores almacenados en el campo

4.1.4.3 Creación de bases de datos

La solicitud para la creación de la base de datos se debe realizar por la herramienta CSC (http://csc.medellin.gov.co/USDKv8) a través de la categoría bases de datos y siempre se debe diligenciar la plantilla con los datos especificados de la DB a crear

4.1.4.4 Variables de enfoque diferencial

4.1.5 Desarrollo e implementación

4.1.5.1 Marcos de referencia de trabajo (Metodología)

La Secretaría de Innovación Digital sugiere adoptar el uso de marcos ágiles para el desarrollo y evolución de sistemas de información. Los requerimientos o necesidades se deben documentar en los artefactos definidos por el marco metodológico adoptado (Impact Mapping, User Story Mapping, Backlog de producto) o en su defecto en el formato de FO-TICS-044 Elicitación de requisitos de Software que se encuentra en Isolucion® (https://bit.ly/3eLqtiD) como insumo inicial del desarrollo.

4.1.5.2 Accesibilidad

Los sistemas de información que estén disponibles para el acceso a la ciudadanía o aquellos que de acuerdo con la caracterización de usuarios lo requieran, deben cumplir con las funcionalidades de accesibilidad que indica la política de Gobierno Digital.

4.1.5.3 Diseño

Se debe realizar un Mockup (prototipo) del portal web que se desea implementar para ser socializado y validado con la Secretaría de Comunicaciones de la Alcaldía de Medellín y antes de iniciar el desarrollo.

Independientemente de si el sitio web que se va a desarrollar estará unificado al portal de la alcaldía o no, se deben seguir los lineamientos gráficos, guía de estilos y de usabilidad definidos por la Secretaría de Comunicaciones.

Se comparten los siguientes enlaces como base para el diseño de los sitios web.

Enlace al sistema de diseño

Enlace con mockup para un home de dependencia - escritorio.

Enlace con mockup para un home de dependencia - mobile.

Enlace con mockup en lorem ipsum para contenido

El diseño de las aplicaciones web debe ser adaptable (Web Responsive Design) para que la apariencia se ajuste al dispositivo que se esté utilizando.

4.1.5.4 Implementación

4.1.5.4.1 Lenguajes de programación

Los lenguajes de programación para desarrollos a la medida en la entidad deben ser interpretados, no compilados.

Se debe usar el patrón Modelo-Vista-Controlador (MVC) usando preferiblemente el entorno NodeJS con el framework AdonisJS para el backend y la biblioteca React para el Frontend.

Para desarrollos que involucren sitios web, se debe usar el sistema de gestión de contenidos (CMS) WordPress y verificar con el equipo de Portales de la alcaldía de Medellín los lineamientos y el manual digital y de identidad que se deben usar y que son necesarios para integrarse al portal

web de la alcaldía: www.medellin.gov.co, el cual ya tiene en cuenta la guía de estilos y usabilidad definida por la Secretaría de Comunicaciones.

Cualquier otro lenguaje o tecnología (PHP, .NET, Python, Laravel, Angular, Joomla, etc.) debe justificarse y concertarse con los arquitectos de software de la Alcaldía de Medellín previo a la contratación de la solución, de manera que puedan validarse los elementos de arquitectura tecnológica que se impactarían. En la Alcaldía de Medellín se aceptan diferentes lenguajes de programación siempre que cumplan con los requerimientos técnicos, de seguridad, soporte, mantenimiento, adaptabilidad y compatibilidad con los sistemas que forman parte de la plataforma tecnológica de la Alcaldía de Medellín. Estos lenguajes deben permitir que se ejecuten en contenedores de Docker.

4.1.5.4.2 Programación

Al programar se deben seguir buenas prácticas. Ver algunas sugerencias:

- Usar Programación Orientada a Objetos (POO)
- Tener en cuenta que la lógica de programación tenga alta cohesión y bajo acoplamiento
- Evitar bloques de control no estructurados.
- Identificar correctamente las variables y su alcance.
- Elegir algoritmos y estructuras de datos adecuadas para el problema.
- Mantener la lógica de la aplicación lo más sencilla posible.
- Las IP no pueden quedar quemadas en el código, se deben hacer referencias a nombres de dominio o variables parametrizables.
- Documentar y comentar adecuadamente el código fuente y en idioma español.
- Limpiar el código fuente final de comentarios y segmentos de código no usados (Clean Code)12.
- Facilitar la interpretación visual del código utilizando reglas de formato de código previamente consensuadas en el equipo de desarrollo.
- Tener en cuenta las matrices de compatibilidad entre lenguajes de programación, sistemas operativos y contenedores de aplicaciones.

Todos los elementos de integración que se requieran implementar deben realizarse con el estándar de API REST con metodología de OpenAPI y Swagger.

Si dentro del análisis de los nuevos sistemas de información existen drivers arquitectónicos o necesidades del negocio que requieran usar otro tipo de tecnologías, estas deberán ser revisadas y aprobadas por la Secretaría de Innovación Digital, antes de iniciar el ciclo de desarrollo.

Se deben mantener actualizados los plugins, librerías y componentes para mejorar el rendimiento y la seguridad de los sistemas.

Para la captura de direcciones se debe realizar de una forma estandarizada mediante el encasillamiento de la estructura que la compone para mantener la uniformidad y consistencia de la información en las bases de datos de la Alcaldía de Medellín.

La estructura del dato de dirección que se almacena en la base de datos corresponde a la concatenación de los componentes de la dirección encasillada

separados por un espacio.

4.1.5.4.3 Aplicaciones móviles

- Las aplicaciones móviles se deben desarrollar para sistema Android y/o iOS y deben ser accedidas desde las respectivas tiendas de aplicaciones.
- El patrón arquitectónico sugerido es una adaptación del patrón MVC
- La comunicación con los servicios se debe hacer a través de HTTPS y con un certificado firmado por una entidad certificadora reconocida ya que algunas plataformas presentan inconvenientes con certificados auto-firmados. Esto presenta relevancia adicional si se incluye la administración de backend dentro del mismo nodo de despliegue del API y se tienen recursos que no son accesibles a través de HTTPS.
- La interfaz de comunicación con los servicios debe ser REST y con formato JSON.
- Las respuestas proporcionadas por los servicios deben devolver un código de estado HTTP acorde al tipo de resultado. Por ejemplo: 200 cuando todo funcionó correctamente y 401 cuando se hace la consulta a un servicio con un token expirado. Esto es requerido ya que es la forma de detectar si una respuesta es satisfactoria o no.

Seguridad

- Se recomienda el uso de claims-based authentication para garantizar el acceso al API del backend. Esto facilita el escalamiento horizontal de la solución y reduce el consumo de recursos de infraestructura.
- Se recomienda, adicional al token jwt asociado al usuario, validar mediante un API Key (por plataforma), el acceso a todos los servicios del API públicos y privados.
- Se debe usar SSL en todas las conexiones al backend.
- Es responsabilidad del backend enviar solo la información disponible de acuerdo con el tipo de usuario que consulta el API. Adicionalmente, si el usuario no tiene acceso a alguno de los servicios o recursos, se debe retornar un error HTTP 401.

Lenguajes de Código Nativo recomendados:

- Java es el lenguaje para escribir código nativo de aplicaciones en Android, es muy estricto y su curva de aprendizaje es muy empinada; aunque, por esto mismo, nos ayuda mucho a mantener las aplicaciones cuando se vuelven más grandes de lo normal.
- Kotlin es una iteración sobre Java creada por el equipo de Google; es un lenguaje menos estricto que Java, pero no tan flexible como JavaScript.
- Swift y Objective-C son los lenguajes para escribir código nativo de aplicaciones en iOS.

Lenguajes de Código multiplataforma recomendados:

- React Native es un puente entre el código nativo y el frontend de la aplicación. Nos permite utilizar JavaScript para crear componentes reactivos que podemos utilizar tanto en Android como en iOS.
- Xamarin es una herramienta muy similar. Pero usa .Net en lugar de JavaScript. Tiene opciones y plugins mucho más avanzados para que no necesitemos escribir código nativo.
- Flutter es una tecnología para diseñar y desarrollar interfaces nativas en iOS y Android usando Dart. También nos permite trabajar con aplicaciones web o de escritorio
- Ionic puede utilizar cientos de elementos de interfaz de usuario predeterminados como formularios, filtros, hojas de acción, vistas de lista, barras de pestañas y menú de navegación en su diseño.

4.1.5.4.4 Políticas para la gestión de tiendas móviles App Store y Google Play

4.1.5.4.5 Componentes geográficos o de georreferenciación

Para los casos en los que el desarrollo haga uso de un componente de mapas, los servidores geográficos disponibles en el datacenter de la Alcaldía de Medellín son:

- Geoserver
- ArcGIS Enterprise

El almacenamiento de información debe realizarse en una base de datos relacional PostgreSQL teniendo en cuenta:

- En caso de uso o administración de algún componente para ArcGIS Enterprise, el almacenamiento permitido es de tipo PG_GEOMETRY (PostGIS Geometry), administrado desde ArcGIS Pro o ArcGIS For Desktop.
- En caso de uso u administración de algún componente exclusivo para Geoserver o QGIS Desktop, el almacenamiento se hará usando la extensión PostGIS.

Las herramientas de consulta, gestión y edición de información geográfica permitidos son:

- QGIS Desktop
- ArcGIS Pro o ArcGIS for Desktop

La implementación de sistemas de información que incorporen componentes geográficos debe seguir los lineamientos SIG definidos por el Departamento Administrativo de Planeación y publicados en el portal de la alcaldía de Medellín en https://www.medellin.gov.co->Temas->Planeación Municipal-> Publicaciones> Estándares e Instructivos SIG.

Para mejorar la calidad de la información capturada por el sistema de información se deben implementar validaciones que permitan controlar los tipos de datos permitidos en cada uno de los campos de los formularios y generando herramientas que brinden facilidad para el registro de estos, como el calendario para campos de fecha, listas desplegables para datos preestablecidos, RadioButton para opciones excluyentes, CheckBox para opciones múltiples.

4.1.5.5 Conexión a base de datos

Con el objetivo de optimizar los recursos de las bases de datos, se debe implementar desde la lógica de desarrollo del sistema de información:

- El uso de Data Sources o creación de pools de conexiones
- El cierre automático de conexiones/sesiones que no estén en uso.

4.1.5.6 Seguridad de aplicaciones

El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) expidió la Resolución 500 de 2021, "por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital".

Esta resolución tiene por objetivo establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI y la guía de gestión de riesgos de seguridad de la información y el procedimiento para la gestión de los incidentes de seguridad digital.

En este sentido se deben seguir las directrices para el dominio de Sistemas de Información indicados en el artículo 13 de la mencionada resolución:

ARTÍCULO 13. Seguridad digital desde el proceso de desarrollo de software. Los sujetos obligados deben integrar la seguridad digital, dentro del ciclo de vida del desarrollo del software para todos los sistemas de información, aplicaciones web y móviles, así como cualquier otro sistema que almacene, transmita o presente información, desde las etapas iniciales como el diseño y el levantamiento de requerimientos, hasta las pruebas de seguridad una vez el software se encuentre en producción, teniendo en cuenta los riesgos asociados a cada sistema de información. Dicho proceso deberá quedar documentado y estar alineado con las normas de responsabilidad demostrada en el tratamiento de datos personales señaladas en la Ley 1581 de 2012, el Decreto 1074 de 2015 y demás normas que las desarrollan, adicionen o modifiquen.

- **Autenticación:** Los sistemas de información deben implementar un mecanismo o módulo de autenticación de usuarios integrado al directorio activo (LDAP) corporativo para servidores públicos y contratistas o integrado al componente UME para el manejo de usuarios externos. Cualquier otro tipo de autenticación deberá ser justificado y aprobado por la Secretaría de Innovación Digital.

En caso de que la solución tenga implementado un módulo de registro de usuarios se debe implementar de tal forma que permita crear una política de contraseñas seguras y haga las validaciones respectivas como velar por que las contraseñas tengan una cantidad mínima de caracteres (se recomienda al menos 8), usando mayúsculas y caracteres especiales. Para los casos en los que el usuario no existe o la contraseña ingresada no le pertenece se debe mostrar un mensaje genérico de Usuario o contraseña incorrecto y otro mensaje genérico que indique si hubo un error general en la aplicación. Es decir, no usar un mensaje específico para cada caso de validación que pueda dar indicios de información de los usuarios.

- **Métodos de seguridad para el control de acceso:** para sistemas de información expuestos a redes externas o de acuerdo con lo definido en las especificaciones funcionales del proyecto que se implementa, se debe restringir el uso de autenticación contra ataques de fuerza bruta por hackers o bots, implementando, entre otros: mecanismos de captcha (Completely Automated Public Turing test to tell Computers and Humans Apart) accesibles o auto detectable, y/o limitar la tasa de intentos de login.

Se debe asegurar que todos los plugins, librerías, temas, etc. que no se usen, se eliminen ya que pueden llegar a ser un punto de entrada para un atacante.

Se debe aplicar metodologías de seguridad tipo OWASP (Open Web Application Security Project) orientadas al análisis de seguridad de aplicaciones Web y el hallazgo de vulnerabilidades para analizar y evaluar los riesgos identificados.

Se debe asegurar que el indicador HttpOnly esté configurado para todas las cookies para evitar el acceso y transmisión de la información de las cookies y el posible secuestro de sesiones por parte de scripts maliciosos.

- **Roles y perfiles:** Se debe tener un esquema de roles y perfiles y su respectiva administración de los privilegios de cada grupo de usuarios del sistema garantizando que los usuarios tengan acceso sólo a las funcionalidades que debe tener.
- **Trazabilidad de las operaciones:** Se debe implementar una trazabilidad de las transacciones que permitan facilitar la identificación, selección y priorización de la información para los procesos de monitoreo, gestión de incidentes y de mejoras. También debe permitir la detección de eventos y excepciones generados por los Sistemas de Información de la entidad. Para más información se puede consultar la guía G.SIS.02 Guía Técnica de Sistemas de Información – Trazabilidad del MinTIC13

Se deben implementar funciones que permitan llevar registro de intentos de ataque, accesos autorizados y no autorizados y demás información que ayude a realizar auditorías de seguridad y proteger el sitio web.

- **Copias de respaldo:** Se debe contemplar un plan de copia de seguridad tanto de las bases de datos críticas como de los componentes de las soluciones en caso de software defectuoso, corrupción de datos, falla de hardware, piratería maliciosa (hacking), error de usuario u otros eventos imprevistos que permita una recuperación rápida y confiable del sistema.
- **Conexiones seguras:** Se deben garantizar conexiones seguras a través del uso de certificados de seguridad, SSL (HTTPS para la confianza de usuarios) y cifrado en la estructura de las peticiones para portales transaccionales, para evitar la manipulación de parámetros en las peticiones.

Se debe ocultar, enmascarar o cambiar las rutas de inicio de sesión, de paneles administrativos y de datos que puedan dar información técnica del sistema tal como versiones, lenguaje, código fuente, scripts, archivos CSS, información de la estructura de la página, plugins, etc.

Se debe configurar correctamente los servidores web, de aplicaciones, equilibradores de carga, etc. para establecer el encabezado ContentSecurity- Policy.

Se debe incluir el encabezado HTTP X-Frame-Options en todas las páginas web devueltas por el sitio si espera que la página esté enmarcada sólo por páginas del mismo servidor (por ejemplo, si es parte de un FRAMESET) usando SAMEORIGIN, de lo contrario, si la página no está enmarcada se debe usar DENY.

4.1.5.7 Calidad del desarrollo de software

Dentro del ciclo de desarrollo e implementación de los sistemas de información de la Alcaldía de Medellín se debe contemplar un ciclo de pruebas que permitan evidenciar la calidad y correcto funcionamiento del software implementado.

Se deben tener en cuenta entonces los siguientes tipos de pruebas aplicables al desarrollo de software:

- **Análisis de seguridad:** Se debe realizar un análisis de seguridad como el análisis estático del código fuente con el objetivo de identificar vulnerabilidades que se encuentra en la programación de las aplicaciones y emitir un informe oficial de los resultados. En todo caso debe definirse un criterio de aceptación de la cantidad y gravedad mínima que se debe garantizar.
- **Pruebas unitarias:** Las pruebas unitarias consisten en aislar una parte del código y comprobar que funciona a la perfección. Son pequeñas pruebas que validan el comportamiento de un objeto y la lógica. Suelen realizarse durante la fase de desarrollo y normalmente las llevan a cabo los desarrolladores, aunque en la práctica, también pueden realizarlas los responsables de QA.14
- **Pruebas de integración:** Las pruebas de integración verifican que los diferentes módulos y/o servicios usados por la aplicación funcionen en armonía cuando trabajan en conjunto.15
- **Pruebas funcionales:** Las pruebas funcionales se centran en los requerimientos de negocio de una aplicación. Se realizan desde el punto de vista del usuario y validan en su totalidad los requerimientos especificados por el usuario e incluso aquellos no especificados u olvidados que afectan el funcionamiento del sistema.
- **Pruebas de rendimiento:** Las pruebas de rendimiento verifican cómo responde el sistema cuando éste se encuentra bajo una alta carga. Son pruebas no funcionales relacionadas al rendimiento de la aplicación y para ejecutarlas se requiere el uso de herramientas que ayuden a simular las condiciones a validar:
- **Pruebas de concurrencia:** Someter al sistema a altas cargas de peticiones para medir y evaluar su desempeño.
- **Pruebas de estrés:** Es un tipo de prueba para encontrar errores debido a la falta de recursos o la competencia por ellos (memoria, espacio en disco, uso de CPU, etc.). Pueden revelar defectos en el sistema que bajo condiciones normales pueden no ser evidentes.
- **Pruebas de volumen:** Somete al sistema a grandes cantidades de datos para determinar que continúe operando correctamente.
- **Pruebas de resistencia:** Somete al sistema durante un determinado tiempo una carga considerable y constante de transacciones.

4.1.5.8 Interoperabilidad

El Distrito de Medellín, en aras de mejorar sus servicios y cumpliendo con la implementación de los habilitadores de la política de gobierno digital, adoptó el "Marco de Interoperabilidad para Gobierno Digital" definido por el MinTIC, el cual se implementa bajo la plataforma X-Road para el intercambio de información con entidades externas de forma segura, eficiente, oportuna y de calidad, facilitando la prestación de trámites y servicios en línea. Con la adopción de esta política la entidad aprovecha la tecnología para mejorar los procesos misionales y prestar

servicios más eficientes y con transparencia hacia los ciudadanos. La Alcaldía de Medellín cuenta con los ambientes de Desarrollo, Pruebas y Producción y la infraestructura necesaria definida por MinTIC para el desarrollo e implementación de servicios a través de la plataforma X-Road como herramienta tecnológica que soporta la interoperabilidad para el intercambio de datos con entidades externas. De acuerdo con lo anterior en todos los proyectos de desarrollo y evolución de sistemas de información y en general en los proyectos en que se requiera interoperar con entidades externas se deben realizar las siguientes actividades:

- Identificar servicios de intercambio de información requeridos con entes externos.
- Identificar y definir los datos a intercambiar
- Identificar las entidades externas con las cuales se intercambiará los datos.
- Solicitar acompañamiento a la Secretaría de Innovación Digital para la articulación con la Agencia Nacional Digital.
- Definir el lenguaje común de intercambio de información.
- Desarrollar los servicios de intercambio de información con protocolos tipo SOAP o REST.
- Validar el cumplimiento del servicio con lineamientos de Agencia Nacional Digital
- Solicitar vinculación al ambiente de QA
- Realizar proceso de pruebas
- Solicitar vinculación al ambiente de Producción
- Tener en cuenta el Marco de interoperabilidad de MinTIC para la implementación de servicios en sus dominios político-legal, organizacional, semántico y técnico.
- Se debe diligenciar en el formato *Anexo Catalogo SI v2.xlsx* el catálogo de servicios de interoperabilidad que son expuestos o consumidos.

NOTA: Para los entregables de los dominios de sistemas de información, por favor remítase a el documento de lineamientos técnicos de la alcaldía DE-GTIC-043LineamientosSIDV4_1.pdf páginas de 48 a la 69.

4.1.5.8 Observaciones para otorgar el aval

Control de cambios: Cualquier implementación, migración, actualización en los ambientes preproductivos y de producción debe surtir las actividades enmarcadas en el proceso de control de cambios definido por la Secretaría de Innovación Digital.

Pruebas de carga y estrés:

- Cantidad de usuarios concurrentes simulados: debe estar alineada con la estimación de usuarios reales que accederán al sistema en -horas pico dependiendo del tipo y criticidad del sistema.

- Tiempos de respuesta esperados: Los tiempos de respuesta de los sistemas deben definirse para operaciones críticas (logín, consultas principales) y no críticas como punto de referencia para medir su rendimiento y tomar las acciones necesarias.

Cobertura de código

La validación de calidad debe contemplar la cobertura mínima de código y la ausencia de vulnerabilidades críticas

Es importante tener en cuenta que más allá del porcentaje, la calidad de las pruebas es clave.

Pruebas de código estático y dinámico

Se debe evidenciar la ejecución de pruebas estáticas y dinámicas de seguridad, según la naturaleza del sistema, así como la gestión de los hallazgos identificados.

No deberán existir vulnerabilidades críticas o de alto impacto sin justificación y tratamiento definido.

Los hallazgos medios o menores deberán estar documentados y, cuando no sean corregidos, contar con la respectiva justificación y plan de remediación.

Se deberán aportar los resultados de las pruebas y las evidencias de gestión de los hallazgos. Se podrán emplear herramientas como SonarQube, OWASP ZAP o Burp Suite, según corresponda.

Pruebas de rendimiento y recuperación

Definir y documentar protocolos o planes de respuesta para escenarios de operación como carga sostenida, la degradación progresiva del servicio, el comportamiento frente a picos inesperados

de demanda o situaciones de estrés, definiendo las acciones, responsables y mecanismos de recuperación ante la materialización de estos eventos.

4.2 Dominio gestión y apertura de datos

4. 2.1 Alcance

Los conceptos y lineamientos definidos por la Secretaría de Innovación Digital en este apartado se debe emplear para la verificación previa al diseño de un modelo de datos (relacional o no relacional). Todas las acciones planteadas en el marco de este dominio está alineadas con las políticas nacionales de datos y tecnología, incluyendo la Ley 1581 de 2012, que constituye el marco general de la protección de los datos personales en Colombia, la Ley de Habeas data 1266 de 2008 y la Ley de transparencia y del derecho de acceso a la información pública 1712 de 2014, la Política Nacional de Gobierno Digital (Decreto 767 de 2022), Decreto 620 de 2020 que establece los lineamientos generales en el uso y operación de los servicios ciudadanos digitales, y la Política Nacional de Explotación de Datos y Big Data contemplada en el CONPES 3920 de 2018.

4.2.2 Términos utilizados en el dominio

Con base en las definiciones adoptadas por el DNP para sus diferentes lineamientos, desde la Secretaría de Innovación Digital se adoptan los siguientes términos y definiciones para el entendimiento del lenguaje utilizado en este dominio.

- **Analítica:** disciplina orientada a analizar datos mediante técnicas científicas y herramientas automatizadas con énfasis en identificar hechos, relaciones, patrones ocultos de comportamiento de variables, correlaciones y tendencias.

- **Analítica descriptiva:** responde preguntas sobre eventos que ya ocurrieron.

Analítica predictiva: identifica la ocurrencia y comportamiento de un evento futuro a través de la predicción de variables específicas, partiendo de los registros históricos de las mismas, así como de otras adicionales.

- **Anonimización:** Definida en el artículo 2.2.3.1.1 del Decreto 1170 de 2015 como el “proceso técnico que consiste en transformar los datos individuales de las unidades de observación, de tal modo que no sea posible identificar sujetos o características individuales de la fuente de información, preservando así las propiedades estadísticas en los resultados”.

- **Conjunto de datos:** Unidad mínima de información sujeta a carga, publicación, transformación y descarga (MINTIC, 2016).

- **Dato personal:** Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la presente ley. Cuando en la presente ley se haga referencia a un dato, se presume que se trata de uso personal. Los datos personales pueden ser públicos, semiprivados o privados. Art. 3, literal e, Ley 1266 de 2008.

- **Datos abiertos:** Son datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos

- **Explotación de datos:** generación de valor social y económico mediante el aprovechamiento de datos para la creación de nuevos bienes, servicios, procesos, así como para el mejoramiento de los existentes.

- **Inteligencia Artificial:** Rama de la ciencia de la computación que busca que las máquinas imiten el comportamiento inteligente para la resolución de problemas. Este campo ofrece los mayores avances en las capacidades técnicas para la explotación de datos. Se sirve de conocimientos de otras disciplinas, como la lingüística, psicología, biología, entre otras. Un paso previo para obtener la inteligencia artificial es el aprendizaje de máquinas.

- **Interfaz de programación de aplicaciones (API - Application Programming Interface):** Conjunto de funciones y procedimientos que opera como una llave de acceso para usar datos entre aplicaciones y servicios web.

- **Internet de las cosas (IoT):** Hace referencia a dispositivos, diferentes a un computador o teléfono móvil, conectados directamente a Internet (v.g., electrodomésticos, ropa, relojes, zapatos, juguetes, edificaciones, dispositivos médicos, entre otros). Estos dispositivos tienen la capacidad de medir fenómenos y generar datos digitales derivados de esta actividad.

- **Interoperabilidad:** Habilidad de transferir y utilizar información de manera uniforme y eficiente entre varias organizaciones y sistemas de información. Corresponde a la capacidad de dos o más sistemas (computadoras, medios de comunicación, redes, software y otros componentes de TI) de interactuar e intercambiar datos de acuerdo con un método definido.

- **Metadatos:** información que describe los datos y permite interpretar el contenido de estos, permitiendo: identificar características para evaluar su calidad y pertinencia para el análisis, rastrear su origen y procesamiento previo e identificar reglas de validación.

4.2.3 Objetivo

Este dominio tiene como propósito establecer los lineamientos y directrices que guiarán la implementación, administración y evolución del Dominio de Gestión de Información y Datos en el marco del Modelo de Gestión y Gobierno de Tecnología de la Información (MGGTI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), su enfoque estará enmarcado en garantizar la gestión integral de los datos como un activo estratégico para las entidades públicas, promoviendo su calidad, seguridad, accesibilidad y uso efectivo.

4.2.6.1 Clasificación de los datos

Gracias a las capacidades del **Big Data**, los datos pueden presentarse en distintos formatos según su origen y estructura, permitiendo una gestión más eficiente y analítica de la información; por ello, entre los formatos más comunes se encuentran los **datos estructurados**, organizados en bases de datos relacionales con formatos como **CSV, JSON y XML**; los **datos no estructurados**, como imágenes, videos, audios y documentos en formatos **PDF, MP4, WAV**; y los **datos semiestructurados**, como logs de servidores y datos de sensores en formatos **NDJSON o YAML**. Esta diversidad de formatos permite al **lago de datos del Distrito** integrar información de múltiples fuentes, habilitando su análisis y explotación para la toma de decisiones basada en datos, en la siguiente tabla se presenta una descripción de cada formato (remítase al documento DE-GTIC-043LineamientosSIDV4_1.pdf paginas 80 a 83)

4.2.6.2 Documentación de los datos

Las dependencias y entidades descentralizadas del Distrito deberán utilizar el formato FO_GTIC-015_Catalogo_Datos en su versión más reciente disponible en Isolucion®, registrando los metadatos necesarios para la gestión en el lago de datos; el diligenciamiento de este instrumento es requisito fundamental para integrar los datos y facilitar su aprovechamiento por parte de la entidad.

4.2.6.3 Establecimiento de políticas de retención

- Se deberán definir periodos de retención para cada tipo de dato, siguiendo lineamientos específicos como los establecidos por el Archivo General de la Nación.

- Se debe garantizar la conservación de datos críticos para el cumplimiento de las funciones misionales y de soporte institucional.

4.2.6.4 Procedimientos para eliminación segura

- Implementar procesos documentados y auditables para la eliminación de datos que incluyan métodos como: o **Sobreescritura**: Eliminación lógica de datos en sistemas digitales. o **Destrucción Física**: Métodos como trituración o incineración para soportes físicos. o **Certificación de Eliminación**: Registro de las actividades de eliminación para garantizar transparencia y cumplimiento normativo.

4.2.6.5 Uso y distribución

- Se deberá controlar el acceso a los datos mediante mecanismos de autenticación y autorización.

- Promover el uso responsable de los datos por parte de los usuarios internos y externos, alineado con las funciones institucionales.

4.2.7 Gobierno de la infraestructura de datos

Todas las dependencias y entidades del Distrito deberán acogerse al modelo de Gobierno de la infraestructura de Datos como un componente estratégico dentro de su gestión institucional, alineándose con las disposiciones del Modelo de Referencia de Arquitectura Empresarial y los lineamientos del sector. Este gobierno busca garantizar el adecuado manejo, calidad, seguridad y uso de los datos, enmarcándose en los objetivos del Dominio de Gestión de Información.

4.2.8 Arquitectura de datos

El propósito principal es garantizar la interoperabilidad, la optimización de recursos y la estandarización tecnológica mediante la adopción de un único motor de base de datos relacionales y un modelo común de almacenamiento y gestión de los datos para su conservación y aprovechamiento.

La estandarización de la arquitectura de datos permitirá:

- **Interoperabilidad:** Facilitar la integración entre sistemas y garantizar la comunicación fluida entre las entidades del Distrito.

- **Reducción de costos:** Evitar redundancias en inversiones tecnológicas, optimizando el uso de recursos presupuestales.
- **Escalabilidad y rendimiento:** Implementar infraestructuras tecnológicas capaces de crecer y responder a las demandas de las entidades y los ciudadanos.
- **Gobernanza y control:** Mejorar la gestión, seguridad y trazabilidad de los datos mediante un enfoque unificado.

Este enfoque, en el marco de una arquitectura de datos consolidada, busca prevenir la adquisición de software con bases de datos que no estén alineadas con la infraestructura operativa estándar definida para las entidades del Distrito. Esta estrategia garantiza:

Homogeneidad Operativa: Todas las dependencias y entidades utilizarán una plataforma tecnológica común, facilitando la integración entre sistemas y reduciendo la complejidad en los procesos operativos.

Reducción de Costos de Infraestructura y Mantenimiento: Al evitar la fragmentación tecnológica y centralizar los esfuerzos en un único motor de bases de datos y modelo de almacenamiento, se optimizan los recursos financieros y se minimizan los gastos asociados a mantenimiento, soporte y licencias.

Simplificación en la Formación del Personal: Unificar herramientas y plataformas permite desarrollar programas de capacitación estandarizados, asegurando que el personal de todas las entidades adquiera las competencias necesarias de manera eficiente y consistente.

Agilidad en la Toma de Decisiones: La consolidación de datos en un sistema centralizado y estandarizado garantiza acceso en tiempo real a información confiable y actualizada, fortaleciendo los procesos de análisis y la toma de decisiones basadas en evidencia.

Lineamientos técnicos

Es de vital importancia que todas las dependencias puedan garantizar los estándares mínimos que aseguren el cumplimiento a los lineamientos, entre estos estándares técnicos se encuentran:

- Todos los sistemas de información adquiridos o desarrollados deben ser compatibles con el motor de bases de datos relacionales y el modelo de almacenamiento definidos por el Distrito.
- Implementar APIs estandarizadas para garantizar la interoperabilidad con los sistemas existentes y futuros.

- Hay que asegurar que los sistemas implementados permitan cumplir con las políticas de gobernanza de datos, como el seguimiento del linaje de datos, la calidad y la trazabilidad.
- Realizar una evaluación de los sistemas de información existentes en las dependencias para identificar redundancias y compatibilidades en las bases de datos.
- Todas las dependencias y entidades procuraran trabajar sobre la misma plataforma, reduciendo complejidades de integración y soporte técnico.

4.2.9 Calidad de datos (remítase al documento DE-GTIC-043LineamientosSIDV4_1.pdf pág. 88 a 90)

4.2.9.1 Importancia de la calidad de los datos

4.2.9.2 Lineamientos para la gestión de la calidad de datos

4.2.9.2.1 Definición de políticas de calidad

- Alinear las políticas de calidad de datos con el **MA-GTIC Manual de Calidad de Datos (MA-GTIC-004)**, priorizando dimensiones clave como completitud, actualidad, conformidad, unicidad y accesibilidad.
- Incorporar estándares nacionales establecidos en el MRAE, que incluyen requisitos de interoperabilidad y arquitectura empresarial.

4.2.9.2.2 Implementación de Procesos de Validación

- Definir procedimientos para la validación de datos en cada etapa del ciclo de vida, desde la captura inicial hasta su almacenamiento y análisis.
- Usar herramientas tecnológicas para la detección y corrección automática de errores en los datos.

4.2.9.2.3 Indicadores de Calidad

- Establecer métricas específicas para medir la calidad de los datos, como:

a) Tasa de completitud: Porcentaje de campos con datos válidos.
b) Tasa de errores: Porcentaje de registros que contienen errores o inconsistencias.
c) Tasa de actualizaciones: Frecuencia con la que se actualizan los datos en sistemas clave.

4.2.9.2.4 Roles y Responsabilidades

- Designar un Administrador de Datos en cada dependencia y entidad, responsable de identificar, definir y clasificar los datos, supervisar su calidad y coordinar acciones de mejora.
- Crear instancias de calidad de datos para supervisar la implementación y el monitoreo de los lineamientos establecidos.

4.2.9.3 Anonimización de datos

4.2.10 Estructuración de los datos

En la estructuración de los datos se deben preparar los archivos que contienen los conjuntos de datos a ser cargados en forma estructurada; este procedimiento solo se debe de aplicar cuando no es posible integrar la fuente primaria, por lo tanto, se deberá estructurar el archivo plano producto de la extracción de los datos, este archivo será el que se integre al lago de datos.

Para realizar dicha estructuración se deberá tener en cuenta las siguientes actividades:

1. Diligenciamiento del archivo a cargar:

- Los valores de los campos deberán cumplir el estándar unicode UTF-8.
- Los datos tipo carácter deben estar en letras minúsculas
- Evitar la inclusión de caracteres especiales.
- Los valores de los campos de tipo fecha se deberán diligenciar con el formato AAAA-MM-DD, si incluye la hora, ésta deberá ser incluida en el formato HH:MM: SS.
- Los valores de campos numéricos con fracciones deberán diligenciarse con. (punto) como separador de decimales.

2. Calidad de los datos:

- La calidad de los datos es responsabilidad de cada una de las dependencias.
- En su estructura no deben contener filas o columnas repetidas.
- Los nombres de los campos deben estar en letra minúscula, evitando la inclusión de caracteres especiales.

3. Generalidades:

En el título de cada conjunto de datos, la primera letra debe de ir en mayúscula, las demás en minúscula. Evitar la inclusión de caracteres especiales.

Para el proceso de estructuración de **información geográfica** deberá cumplir con los lineamientos dados por el Departamento Administrativo de Planeación, los cuales son:

- Estándares básicos de Información Geográfica
- Plantillas para la elaboración de Mapas
- Nombramiento de Objetos en la Geodatabase

Los formatos podrán ser descargado a través de:

https://www.medellin.gov.co/irj/portal/medellin?NavigationTarget=contenido/1075

7-Estandares-e-instructivos-SIG Adicionalmente, se deberá cumplir con:

- DE-GINF Guía para la creación y administración de metadatos
- FO GINF - Diccionario Datos Geográficos
- FO- GINF Catálogo de Objetos Geográficos

Los formatos podrán ser descargados a través de

https://www.medellin.gov.co/Isolucion

4.2.10.1 Estándar de variables unificadas para la construcción de bases de datos

4.2.10.2 Apertura de datos

4.2.11 Plataforma de ciudad inteligente – Fiware

Fiware se constituye en la plataforma del Distrito para la integración, gestión y análisis de los datos generados a través de dispositivos IoT, garantizando su interoperabilidad y aprovechamiento en la toma de decisiones. Fiware permite centralizar datos en tiempo real provenientes de diferentes dispositivos, facilitando su procesamiento y visualización e integración al lago de datos del Distrito y otras plataformas analíticas.

Entre los principales dispositivos IoT que generan datos y que pueden ser integrados a Fiware se incluyen:

- Sensores ambientales (ruido, calidad del aire, temperatura, humedad, etc.).
- Sensores de tráfico y movilidad (aforos vehiculares, semáforosinteligentes).

- Dispositivos de medición de consumo energético y agua.
- Sensores de infraestructura y seguridad (detección de fallas estructurales, incendios o inundaciones).

Para garantizar la correcta integración, las dependencias deben adoptar estándares abiertos de interoperabilidad y estructurar los datos de acuerdo con los modelos de información definidos en Fiware, permitiendo su uso eficiente para la planificación y gestión de la ciudad inteligente.

4.2.12 Disposiciones finales

- El presente documento aparte de ser informativo sirve como base para el diseño y desarrollo de modelos relacionales y no relacionales.
- Todas las bases de datos que se encuentren de forma productiva sin excepción deben cumplir con los puntos aquí consignados

4.2.13 Observaciones para otorgar el aval

Se recomienda la identificación y documentación de los conjuntos de datos generados por la solución, y en particular, se deberá garantizar la utilización del FO_GTIC-015_Catalogo_Datos para el registro de los metadatos requeridos para la gestión de la información en el Lago de Datos, considerando que el documento establece dicho instrumento como requisito fundamental para la integración y aprovechamiento de los datos.

4.3 Dominio infraestructura tecnológica de TI

Este comprende la definición de la arquitectura de la plataforma tecnológica y de los planes de adquisición a partir de los análisis de capacidad, seguridad y de disponibilidad, los cuales recogen las necesidades para soportar los sistemas de información y los servicios tecnológicos.

Dentro de este componente se incluyen todos los elementos de infraestructura tecnológica requeridos para consolidar la plataforma que soporta a los servicios:

- Infraestructura tecnológica: Servidores, equipos de redes y comunicaciones, sistema de almacenamiento, seguridad y backup, data center.
- Hardware y software de oficina: Equipos de cómputo, telefonía, software de productividad.

Para el suministro o adquisición de la infraestructura tecnológica y de los servicios, dependiendo de las necesidades de la organización, deberá seleccionar los componentes de la Arquitectura Tecnológica que más se ajuste a los requerimientos del área.

El proceso de adquisición de la infraestructura tecnológica debe garantizar:

- La compatibilidad con las tecnologías existentes.
- Que el ciclo de vida en el que se encuentra el producto ofrecido esté vigente al menos 5 años (End of Support), con actualizaciones, soporte técnico y suministro de repuestos.
- El proceso de soporte y mantenimiento sea prestado por los mismos fabricantes o proveedores certificados por ellos.
- Que sean productos responsables con el medio ambiente.
- Contar con garantía por parte del fabricante mínimo de 5 años.

A continuación, se describen las características básicas de los diferentes elementos que se contemplan en la arquitectura de la plataforma tecnológica.

4.3.1.2 Plataforma de red LAN

4.3.3 Motores de bases de datos

El motor de base de datos estándar usado para evoluciones e implementaciones de nuevos sistemas de información es PostgreSQL, el uso de otros motores debe ser justificado y aprobado por la Secretaría de Innovación Digital.

4.3.3.1 Desarrollos vs bases de datos

A continuación, se dan las consideraciones y recomendaciones que debe tener presente el equipo de sistemas de información, así como los desarrolladores y responsables de los temas de arquitectura empresarial que requieran utilizar los servicios de bases de datos.

El Distrito de Medellín actualmente cuenta con los siguientes Sistemas de Gestión de Bases de Datos (SGBD) relacionales: PostgreSQL, SQL Server, MariaDB. Para bases de datos no relacionales se cuenta con MongoDB y CrateDB. la versión de implementación de base de datos debe corresponder a la versión disponible o superior con la que cuente el Distrito.

El profesional de enlace de parte de la Secretaría de Innovación Digital hará una lista de chequeo, en donde se solicite lo siguiente:

Consideraciones mínimas para la correcta implementación y uso adecuado del motor de base de datos:

- Cantidad de conexiones estimadas
- Cantidad de sesiones estimadas
- Cantidad de registros
- Uso estimado de recursos de procesamiento y memoria RAM
- La versión de base de datos a implementar
- Resultado de prueba de funcionalidad en ambiente de desarrollo
- Resultado de prueba de stress en ambiente de desarrollo
- implementación de procedimientos almacenados que en lo posible no tenga tantas líneas de código
- Crecimiento estimado de la data en GB por año.

Sin embargo, el éxito para su correcta implementación radica en la adecuada comunicación entre todos los involucrados para dar respuesta a las novedades que se presenten, antes que sean puestas en producción.

El crecimiento estimado de las bases de datos deberá ser informado previamente, antes de ser autorizada la creación de esta, con el fin de estimar los recursos que se deberán asignar a nivel de sesiones, memoria RAM, almacenamiento y hardware, dado que se podrían presentar afectaciones en el rendimiento de las bases de datos existentes.

Los motores de bases de datos instalados en el Distrito de Medellín son transversales; es decir, existen más componentes para su correcto funcionamiento como: red de datos, almacenamiento, seguridad informática entre otros, todos interrelacionados y por tal motivo, es muy importante realizar las verificaciones a todos los niveles al momento de ingreso de nuevos aplicativos o sistemas de información.

Las aplicaciones o sistemas de información deben tener configurado un pool de conexiones que permita controlar el número de sesiones concurrentes hacia la base de datos. De igual manera tener configurado un timeout que cierre las conexiones suspendidas o en estado “idle” que permita el reúso de las conexiones del motor de bases de datos.

4.3.3.2 Uso de software libre y open source

El Distrito de Medellín adopta la implementación y uso de software libre u open source en cada uno de sus frentes como lo son: sistemas operativos, software de uso general o específico,

motores de bases de datos, servidores o contenedores de aplicaciones y lenguajes de programación, cumpliendo con los estándares tecnológicos definidos por la organización, siempre y cuando estos cumplan con los requerimientos técnicos, de seguridad, soporte, mantenimiento, adaptabilidad y compatibilidad con los sistemas que forman parte de la plataforma tecnológica.

Lo anterior indica que cuando se descubran falencias o vulnerabilidades a nivel de seguridad informática o de funcionalidad, se tenga el soporte que pueda dar la solución a lo encontrado con prontitud.

Este tipo de software debe permanecer en sus últimas versiones y contar con un contrato de soporte, que atienda los requerimientos y/o incidentes que puedan presentarse durante su operación y al que pueda hacerse escalamiento por la mesa de servicio de acuerdo con los ANS pactados.

Para la implementación y utilización de software open source se deberán tener en cuenta los siguientes aspectos:

- Aval previo de la Secretaría de Innovación Digital.
- Solicitud con la debida justificación por parte del líder de la dependencia que lo requiere.
- Declaración de libertad para su utilización.
- Documento con las condiciones relativas a derechos y deberes de las partes (proveedor y usuario), bajo las cuales se distribuye el software.
- La solución debe cumplir con las políticas de la Seguridad Informática de la Organización.

4.3.3.2.1 Fundamentos para la adopción del software open source

Se cumple con el decreto 767 de 2022 Política de gobierno digital que en su sección 2, articulo 2.2.9.1.2.1, numeral 2 Innovación publica digital, promueve la adopción de tecnologías basadas en software libre con el fin de fortalecer los procesos de innovación publica digital

4.3.3.2.2 Alcance en el soporte y actualización sobre los componentes open source

La plataforma de infraestructura de TI, sobre la cual corren las aplicaciones será administrada por la Subsecretaría de Servicios de Tecnología de la Información en lo correspondiente a sistemas operativos, motores de bases de datos, servidores, almacenamiento, backups o contenedores de aplicaciones.

Los componentes open source autorizados por la SID, deben contar con contratos de soporte y actualización, que garanticen que estos se mantengan en las últimas versiones y que cuenten con atención de requerimientos de forma oportuna.

4.3.4 Contenedores de aplicaciones

El contenedor de aplicaciones debe cumplir con las matrices de compatibilidad entre lenguaje de programación a utilizar, contenedor de aplicaciones, sistema operativo y base de datos de la infraestructura tecnológica del Distrito. Adicionalmente el tipo de aplicación a implementar (Cliente/Servidor, Aplicación Web, Microservicios).

Todos los contenedores deben contar con contrato de soporte y actualización vigente.

Los contenedores de aplicaciones autorizados son:

- Monolíticas
- Red Hat JBoss EAP
- Microservicios
- Red Hat OpenShift

Notas:

- Aplicaciones actualmente instaladas en contenedores de aplicaciones diferentes a los autorizados, deben ser migradas hacia los contenedores de aplicaciones autorizados que cuentan con soporte.
- Los desarrollos nuevos deben estar sobre los contenedores de aplicaciones autorizados.

4.3.5 Sistemas operativos

Para definir el sistema operativo se debe cumplir con las matrices de compatibilidad entre sistema operativo, contenedor de aplicaciones y base de datos de la infraestructura tecnológica del Distrito. Los autorizados son:

- Windows Server
- Red Hat Linux
- AIX

Los sistemas operativos Windows server y Red Hat Linux están instalados sobre máquinas físicas y virtuales.

El sistema operativo AIX está instalado sobre máquinas Power IBM. Sobre este sistema operativo se encuentra la plataforma SAP y el portal transaccional corporativo en sus ambientes de desarrollo, calidad y producción.

Los servidores, host, appliance, entre otros, de propósito especifico que traen sistema operativo propio, deben contar con contrato de soporte y actualización vigente.

Este tipo de software debe permanecer en sus últimas versiones y contar con un contrato de soporte, que atienda los requerimientos y/o incidentes que puedan presentarse durante su operación y al que pueda hacerse escalamiento por la mesa de servicio de acuerdo con los ANS pactados.

4.3.6 Servidores

En la infraestructura tecnológica del Distrito se tendrán servidores físicos y virtuales, para los servidores virtuales se debe contar con contrato de soporte vigente para el uso del software de virtualización.

4.3.7.1.2 Seguridad

- **Cifrado de Datos:** Asegurarse de que los datos en el almacenamiento tengan opción de cifrado, tanto en reposo como en tránsito, para prevenir accesos no autorizados.
- **Controles de Acceso:** Implementar mecanismos que restrinjan el acceso al almacenamiento según roles y permisos definidos.
- **Cumplimiento Normativo:** Verificar que el almacenamiento cumpla con las normativas legales y estándares del sector.

4.4 Dominio seguridad informática

4.4.1 Objetivo

Generar los lineamientos base, para la aprobación de elementos de seguridad en los nuevos desarrollos de aplicaciones (app) y sistemas de información para la Alcaldía de Medellín.

4.4.2 Contexto

La seguridad informática que ha implementado la Alcaldía de Medellín aborda ante el diseño, contratación e implementación de un proyecto de tecnologías de información diferentes factores, por lo cual la valoración obedece a la inclusión o no de componentes y el cumplimiento de criterios de valor a la hora de la contratación o de la implementación, que pueden afectar la viabilidad técnica de una solicitud de aval.

4.4.3 Casos de uso para estos lineamientos

Con lo anterior se valoran dos casos de uso asociados a diferentes peticiones realizadas por las demás Secretarías y Subsecretarias de la Alcaldía de Medellín:

- Solicitudes de Sistemas de Información

- Solicitudes de Adquisición modificación o remplazo de Infraestructura Tecnológica

4.4.4 Información

Principios para la aprobación de aplicaciones y sistemas de

La Unidad de Seguridad Informática ha definido los principios que son relevantes para el cumplimiento de medidas de seguridad informática, los cuales se listan a continuación:

- Qué la solución adopte la seguridad informática, como un elemento que genera valor y confianza a las partes interesadas.

- Qué la solución adoptada incluye actividades para valorar y mejorar las condiciones de seguridad informática de manera periódica en aras de actuar de conformidad a las necesidades impuestas por los cambios en los contextos internos y externos que afectan las condiciones de seguridad informática

- Qué la solución adoptada incluye actividades para mantenerla actualizada orientadas a mitigar los riesgos asociados a ciberamenazas emergentes en un contexto interno y externo.

- Qué la solución que se adoptada incluya actividades para asegurar la correcta protección en el almacenamiento o transporte de los datos que sean intercambiados, de modo que se minimicen los riesgos asociados a su modificación o acceso no autorizado.

- Qué la solución adoptada incluya actividades para remediar las identificadas y que la expongan a un riesgo por acción interna o externa relacionada con la materialización de una ciberamenaza.

Qué el entorno donde se despliegue la solución ha adoptado políticas y medidas relacionadas con la seguridad informática de los activos de tecnologías de información asociados.

- Qué los acuerdos de nivel de servicio ANS definidos, incluyen el despliegue de acciones y tiempos mínimos para la recuperación de la disponibilidad de la plataforma ante cualquier incidente de seguridad informática presentado.

- Qué los acuerdos de nivel de servicio ANS, incluyen en atención a la detección y valoración de vulnerabilidades de la solución, las acciones y tiempos mínimos para la remediación de la solución tecnológica implementada.

- Que en la solución adoptada y su implementación se vele por la aplicación de políticas, procedimientos y acciones encaminadas a garantizar procesos adecuados de autenticación, autorización y trazabilidad sobre el acceso y uso de la solución.

Desde esa óptica se definen un conjunto de componentes que se sujetan al cumplimiento de unas condiciones y un conjunto de criterios para la realización de su valoración, de la siguiente manera: (remítase a la tabla 11 del documento DE-GTIC-043LineamientosSIDV4_1.pdf)

4.4.5 Entregables

- Matriz de valoración de riesgos de seguridad informática del sistema de información, y de la infraestructura que la soporta.

- Vista de Seguridad informática del Sistema de Información (roles, perfiles, accesos, autenticación, trazabilidad)

- Vista de Seguridad informática de las interoperabilidades del sistema de información (intercambio de datos con otras aplicaciones, almacenamiento, etc)

- Vista de seguridad informática de la infraestructura (Sistema de Información, Bases de Datos, Telecomunicaciones) donde se aloja el sistema de información (Nube, OnPremise) en términos de las capas de seguridad perimetral utilizadas (firewalls, protocolos, acceso remoto)

- Vista de seguridad informática de la protección de los datos (cifrado en reposo, cifrado en tránsito, etc)

- Acuerdo de Nivel de Servicio (Mecanismos para atender y remediar vulnerabilidad de seguridad informática, así como para gestionar incidentes de seguridad informática)

- Condiciones de Prestación del Servicio (Mecanismos para garantizar la disponibilidad de los servicios y la recuperación ante eventualidades o desastres).

4.5 Dominio gestión documental electrónica

4.5.1 Objetivo

Establecer los lineamientos que orientan la Gestión Documental Electrónica (GDE) en la Alcaldía de Medellín, garantizando la autenticidad, integridad, disponibilidad, fiabilidad y preservación digital a largo plazo de los Documentos Electrónicos de Archivo (DEA), en concordancia con el Ciclo Vital del Documento y la normativa archivística vigente en Colombia.

4.5.2 Alcance

Los presentes lineamientos aplican a todas las dependencias, servidores públicos, colaboradores y terceros que generen, administren, tramiten o custodien documentos electrónicos dentro de la Alcaldía de Medellín, en cumplimiento de las funciones administrativas y misionales de la entidad.

4.5.3 Lineamientos Generales

4.5.3.1 El Distrito deberá:

Transición al entorno digital e innovación archivística

- Adoptar progresivamente soportes digitales y electrónicos, reduciendo el uso del papel.

- Priorizar la creación de documentos electrónicos nativos con valor probatorio.

Implementar procesos administrativos digitales alineados con los lineamientos del MINTIC, el Archivo General de la Nación (AGN) y las políticas de transformación digital del Distrito.

- Adoptar la estrategia de Documento Electrónico de Archivo (DEA) y Expediente Electrónico de Archivo (EEA) conforme a los instrumentos archivísticos vigentes (TRD, CCD, PGD, PINAR, etc).

- Implementar procesos de reprografía con valor probatorio para la conversión de documentos análogos a digitales, conforme al Protocolo Distrital de Digitalización.

- Utilizar tecnologías de valor probatorio como firma digital, estampado cronológico longevo y correo electrónico certificado, emitidos a través de un certificador abierto autorizado por ONAC.

- Aplicar tecnologías consolidadas del mercado como facilitadores de la Gestión Documental.

- Fortalecer la modernización archivística del Distrito mediante innovación en procesos, procedimientos y gestión administrativa.

4.5.3.2 Cumplimiento normativo

4.5.4 Ciclo de vida del documento electrónico

4.5.4.1 Captura y producción

4.5.4.2 Trazabilidad

Para garantizar el valor probatorio:

- Toda acción debe quedar registrada en el log de auditoría.

- Deben mantenerse metadatos completos que evidencien origen, gestión y cambios.

- Se conservará un historial de versiones, manteniendo únicamente la versión final como documento de archivo.

- Se aplicarán firmas electrónicas/digitales que garanticen autenticidad e integridad.

- Se deberá registrar la trazabilidad en movimientos inter-archivos (Gestión – Central – Histórico).

4.5.4.3 Consulta

Los sistemas de consulta deben garantizar:

- Integridad y seguridad del documento electrónico.
- Gestión de accesos conforme al nivel de confidencialidad.
- Conservación de metadatos archivísticos y tecnológicos.
- Interoperabilidad con el Sistema de Gestión Documental definido por el Distrito.
- Registro automático de toda visualización o descarga como parte de la trazabilidad.

4.5.4.4 Preservación digital

La preservación digital debe:

- Gestionar la obsolescencia tecnológica mediante migraciones periódicas.
- Mantener metadatos de preservación.
- Contar con copias de seguridad distribuidas geográficamente.
- Aplicar mecanismos de autenticidad y verificación (firma, sello de tiempo).
- Seguir el Plan de Preservación Digital Distrital.

4.5.5 Tecnologías con valor probatorio

Las tecnologías de valor probatorio implementadas en el Distrito de Medellín deben garantizar que los documentos electrónicos mantengan autenticidad, integridad, inalterabilidad, fiabilidad y disponibilidad durante su ciclo de vida, conforme a la Ley 527 de 1999 y el Acuerdo 001 de 2024 del AGN.

Estas tecnologías deben estar integradas al Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA) distrital y ser adoptadas por todas las áreas productoras que generen o administren documentos con valor jurídico o probatorio.

4.5.5.1 Integridad y seguridad

El Sistema de Información o solución automatizada debe:

- Implementar mecanismos criptográficos que garanticen la inalterabilidad del documento desde su creación.
- Usar tecnologías de un certificador abierto autorizado por el Organismo Nacional de Acreditación de Colombia – ONAC**.**
- Registrar automáticamente toda operación realizada sobre el documento en el log de auditoría**,** como parte de la trazabilidad exigida por la normativa archivística.

4.5.5.2 Autenticidad y firma electrónica/digital

Para garantizar la autenticidad documental se debe:

- Usar firmas electrónicas o firmas digitales emitidas por entidades de certificación acreditadas ante ONAC.
- Incorporar sellos cronológicos longevos cuando corresponda.
- Vincular la firma al documento y a sus metadatos para evitar la desasociación entre contenido y autoría.
- Asegurar que la firma sea verificable aun cuando el certificado haya expirado, mediante mecanismos de preservación digital.

4.5.5.3 Vinculación contextual

- Cada documento electrónico debe conservar:
- Su serie, subserie y tipología documental conforme a TRD y CCD.
- Sus metadatos archivísticos, diplomáticos y tecnológicos.
- Su relación con el trámite, proceso o procedimiento administrativo que le da origen.
- Este requisito es indispensable para garantizar la presunción de autenticidad**.**

4.5.5.4 Preservación a largo plazo

4.5.6 Certificados Digitales

El uso de certificados digitales en documentos electrónicos de archivo es obligatorio para garantizar:

- Autenticidad del firmante.
- Integridad del documento.
- No repudio.
- Validez jurídica del acto administrativo.

El Sistema de Gestión Documental Institucional debe gestionar:

4.5.6.1 En la creación y producción

- Uso de certificados digitales emitidos por certificadores autorizados por ONAC.

- Incorporación de firmas en formatos que permitan verificación futura (p. ej., PDF/A).

4.5.6.2 En la gestión y trámite

- Relación inseparable entre documento, firma y metadatos.
- Sellos de tiempo longevos para garantizar vigencia jurídica del documento después del vencimiento del certificado.

4.5.8 Correo electrónico certificado

Un correo electrónico certificado adquiere la calidad de Documento Electrónico de Archivo cuando:

- Hace parte de un trámite administrativo.
- Constituye comunicación oficial interna o externa.
- Contiene evidencia probatoria relevante.

4.5.8.1 Creación

4.5.8.2 Gestión

4.5.8.3 Conservación

4.5.8.4 Disposición final

4.5.9 Firma digital y autenticidad documental

La firma digital es el mecanismo oficial del Distrito para documentos electrónicos de archivo y debe:

- Ser emitida por una entidad acreditada ante ONAC.
- Estar integrada vía API al Sistema de Gestión Docu

4.5.9.6 Requisitos por fase del ciclo vital

4.5.10.1.1 Servidores públicos y contratistas

Los servidores públicos deberán:

- Usar adecuadamente las plataformas tecnológicas oficiales.
- Garantizar la integridad y trazabilidad de los DEA a lo largo del ciclo de vida.
- Respetar las restricciones de uso de firma digital (solo personal autorizado).

La nomenclatura estandarizada facilita la recuperación, preservación y compatibilidad entre sistemas.

4.5.18.1 Reglas generales

- Debe permitir identificar claramente el tipo documental**.**
- Usar Mayúscula Inicial en cada palabra.
- Longitud: entre 5 y 30 caracteres.
- Evitar palabras innecesarias (el, la, de, en, por).
- Evitar siglas desconocidas o no institucionales.

4.5.18.2 Restricciones

- Sin tildes ni caracteres especiales (/, \, %, &, #, ?, etc.)
- Separación mediante guion bajo (_)
- No usar espacios.

Ejemplos válidos:

- Acta_Apertura.pdf o Informe_Seguimiento_20250315.pdf

4.5.18.3 Fechas y Versionamiento

Las fechas deben seguir ISO 8601 (AAAAMMDD)**.** Versiones deben iniciarse con V01, V02, V03… Ej.: V02_Acta_Cierre_20250111.pdf

4.5.18.4 Extensiones

Siempre debe incluirse la extensión del formato (PDF, XML, TIFF, etc.).

4.5.11 Observaciones para otorgar el aval

(i) cumplimiento parcial en la estructuración y almacenamiento documental conforme a las TRD; (ii) incumplimiento en mecanismos de autenticidad e integridad documental por ausencia de

firma digital y estampado de tiempo; (iii) incumplimiento en la incorporación de metadatos de preservación; y (iv) cumplimiento parcial en la formalización del plan de preservación digital a largo plazo: por lo anterior, se recomienda:

Implementar firma digital y mecanismos de integridad documental; reorganizar el expediente conforme a las TRD vigentes; incorporar metadatos obligatorios para los documentos electrónicos; y formular el plan de preservación digital de largo plazo para activos con retención superior a ocho años.

4.6 Dominio uso y apropiación de tic

4.6.1 Antecedentes

La Política de Gobierno Digital (MinTIC, 2022) establece como habilitador Cultura y Apropiación Digital y define para esto, lineamientos orientados a impulsar este objetivo mediante el adecuado involucramiento de los interesados en el desarrollo de los servicios tecnológicos y en su uso y aprovechamiento.

Para tal efecto, la Alcaldía del Distrito de Ciencia, Tecnología e Innovación de Medellín cuenta desde el año 2021con la estrategia de uso y apropiación, ApropiaTIC, donde define acciones y prácticas concretas enfocadas en promover la correcta adopción de los elementos del dominio del cual hay responsabilidad en su ejecución por cada dependencia y unidades o equipos líder/dueño de un proceso, sistema, servicio digital, expresados en el Marco de Referencia Arquitectura de Tecnologías de Información - TI (MinTIC, 2022) de Colombia, a implementación de esta estrategia ayuda a determinar el grado de competencia de las personas para facilitar la adopción de la tecnología de información a partir de lo cual se formulan acciones de formación y difusión con los públicos objetivo y de otro lado, presentar acciones específicas de gestión del cambio que incluyen la planeación, comunicación y divulgación y procesos de mejoramiento continuo e incentivos en la adopción del cambio y esto ocurre desde etapas tempranas de planeación de un proceso o servicio, como parte del desarrollo de habilidades para el aprovechamiento de las soluciones TIC.

La gestión del cambio hace parte de los ámbitos que se gestionan con la implementación de soluciones con componente tecnológico y por eso se incluye en los lineamientos técnicos de la Secretaría de Innovación Digital para proyectos de este tipo y de la cual cada Secretaría es responsable de su cumplimiento.

4.6.2 Lineamientos de uso y apropiación (remítase a la tabla 12 del documento pag 158)

Con la estrategia ApropiaTIC la Secretaría de Innovación Digital se enfoca en definir las rutas de actuación para la promoción y facilitación del buen uso y conocimiento de la innovación digital, la arquitectura empresarial y los servicios digitales de la Alcaldía de Medellín, así como los proyectos con componente tecnológico que los materializan, mediante acciones que promuevan la participación de los grupos de interés y mejoren la cultura de la innovación y la apropiación digital de los usuarios.

El lineamiento MGGTI.LI.UA.02 de Gestión del Cambio se debe incorporar en la implementación de soluciones tecnológicas (vía desarrollo interno, contratación con terceros, adquisición de herramientas comerciales y demás opciones) para garantizar la generación de valor a los públicos objetivo, gestionar el impacto y mejorar el nivel de adopción de los servicios, bienes o productos del proyecto.

La gestión del cambio es responsabilidad del área dueña de la implementación tecnológica, por lo que los recursos necesarios para su planeación, diseño, ejecución y medición deben incluirse en la financiación del proyecto, siendo el gerente que cada Secretaría designa para su proyecto, responsable de su cumplimiento.

4.6.3 Gestión del cambio

La gestión del cambio es un marco para gestionar los efectos de las soluciones tecnológicas (nuevas o mejoradas) que son implementadas en la entidad.

Los cambios en general y, en especial en los aspectos organizativos y de sistemas de información, suelen generar incertidumbre en las personas, motivar expectativas o temores, lo que puede desembocar en un rechazo al servicio o la solución a implementar.

Es por esto por lo que se hace necesario que, en la ejecución de todo proyecto con componente tecnológico, se lleven a cabo una serie de actividades que permitan minimizar el impacto negativo o incertidumbre que el cambio va a provocar en los interesados, el proceso que apalancan en la entidad en general y contribuir al éxito de la puesta en funcionamiento de la solución.

4.6.3.1 Objetivos de la gestión del cambio

- Garantizar lo más oportunamente posible, la adecuada aceptación de los interesados de las soluciones implementadas, a través de acciones de sensibilización y formación que permitan la adaptación de los públicos objetivo y la debida apropiación de la nueva solución.

- Formular un plan de actividades que permita hacer gestión de los interesados en el proyecto, con el fin de disminuir el impacto negativo y la incertidumbre que puedan provocar en los grupos de interés.
- Definir acciones de seguimiento a la ejecución del Plan de Gestión del Cambio.
- Asegurar una adecuada evaluación de los resultados del Plan de Gestión del Cambio Para lograr una buena gestión del cambio, se deben adelantar las siguientes actividades:
- Identificar y socializar oportunamente los efectos del proyecto para prever ajustes requeridos en los procesos, procedimientos o herramientas
- Proveer a los involucrados la formación o entrenamiento requeridos para la mejor utilización del servicio o herramienta que se incorporará al proceso
- Facilitar la adopción del servicio o herramienta de manera que se obtengan rápida y permanentemente los beneficios esperados.

Formulación del Plan de Gestión del Cambio

Todo proyecto de implementación de soluciones tecnológicas deberá incorporar un plan para la gestión del cambio que considere los niveles de adopción del cambio y los efectos o el impacto derivados del proyecto, para que se estructuren las acciones que garanticen la correcta apropiación de parte de los usuarios de la solución implementada y que su utilización sea conforme a los objetivos del proyecto.

El Plan de Gestión del Cambio estará conformado por la matriz de interesados, el plan de comunicación y el plan de formación. El área dueña de la iniciativa de TI (o solución a implementar) se hará cargo de que este plan se formule debidamente con la coordinación del gerente del proyecto y la participación del implementador, así:

4.6.3.2.1 Matriz de interesados

Identifica a todas las personas que tendrán algún grado de involucramiento en el proyecto y que por tanto es importante que lo conozcan y participen en las formas y tiempos se requiere para el éxito del proyecto. Saber quiénes son y qué tipo de influencia tendrán sobre el proyecto es muy importante dado que nos permite Identificar motivaciones y disposiciones para participar y adoptar el cambio.

La matriz de interesados deberá diligenciarse según el formato existente para esta actividad:

La información que debe contener es:

• **Identificación del proyecto:** Nombre, objetivo, identificación del responsable y fecha de elaboración (actualización) de la matriz.

• **Identificación de los interesados:** Registro individual de los involucrados en el proyecto con sus datos de contacto y además con información complementaria que permita identificar

a) Función que la persona o entidad desempeñará en la implementación de la Iniciativa de TI (rol)
b) Si es interno o externo
c) Caracterizar la influencia que tiene dentro del proyecto para el alcance de los objetivos, los beneficios, la toma de decisiones y el éxito general del proyecto, calificando en cada aspecto como alto, bajo o medio,

según aplique:

- **Poder**: Nivel de poder del interesado, orientado a la capacidad que tiene para apoyar estos aspectos en el proyecto:

a) Objetivo
b) Alcance
c) Obtención del Beneficio
d) Toma de Decisiones.

- **Influencia**: Estimación de como puede el interesado puede intervenir en el desarrollo del proyecto:

a) Grado de Influencia (Alto, medio, bajo)
b) Tipo de Influencia (positiva, neutral, negativa)

La Matriz de interesados servirá de base para diseñar las estrategias de comunicación, formación e involucramiento de los interesados.

4.6.3.2.2 Plan de Comunicaciones

Es una herramienta que permite identificar los momentos en los que se hará difusión de lo que está pasando en el proyecto, invitar a los participantes a que ejecuten alguna actividad o tarea – incluido ciclos de formación o hacer pruebas- y finalmente lograr conocimiento y aprobación del proyecto.

En el plan de comunicación se deben incluir los mensajes clave para motivar a las partes interesadas para aceptar y apoyar la transformación, para esto es necesario y útil, haber documentado la matriz de interesados del proyecto.

Para la construcción del plan se debe contar con el acompañamiento del área de comunicaciones de la dependencia que realiza el proyecto, de manera que se aprovechen los canales y estrategias institucionales y se potencien otras herramientas comunicacionales e incluso se promueva la articulación con otras estrategias de comunicación del área dueña del proyecto o de las áreas a las que pertenecen los interesados.

Son responsabilidades de los equipos de comuncaciones, según lo sugerido desde los roles participantes en la estrategia de uso y apropiación sugerida por el MinTIC, las siguientes:

- Participar en la definición de las estrategias de comunicación, divulgación y promoción de los componentes de TI y de los cambios apoyados con tecnología definiendo los mensajes clave, canales y formatos más adecuados de acuerdo con las necesidades identificadas.
- Diseñar los recursos requeridos para divulgar los mensajes clave de las estrategias de comunicación definidas
- Participar en la ejecución de las estrategias de comunicaciones

El plan se formulará con el líder del proyecto utilizando el formato existente para este tema y deberá contener:

Identificación del proyecto: Nombre, objetivo, identificación del responsable y fecha de elaboración (actualización) del plan.

Identificación de las acciones comunicacionales: Se deben presentar de forma clara:

a) **Grupo de interés:** De acuerdo con la identificación de grupos de interés definido en la matriz de interesados en el alcance del ejercicio. Un mensaje puede estar dirigido a distintos grupos de interés.
b) **Zona de influencia/poder:** La intersección de influencia-poder permite definir mensajes para comprometer a las partes interesadas que tienen más influencia y para tratar que las partes interesadas con poder se interesen.
c) **Tipos de Mensajes:** De acuerdo con las necesidades identificadas se puede definir y clasificar los mensajes de acuerdo con su propósito. Ejemplo: mensajes motivadores, mensajes de expectativas, mensajes informativos.
d) **Mensaje:** Es el contenido del mensaje en sí mismo.

e) **Mensajero:** Define quién es el mensajero ideal para emitir el mensaje, de acuerdo con el tipo de mensaje y su propósito. Por ejemplo: en algunos casos se puede requerir que el mensajero tenga un rol de autoridad frente al grupo de interés receptor para generar mayor credibilidad mientras que en otros casos puede ser deseable que el mensaje se comunique entre pares para generar mayor empatía.
f) **Canales de Comunicación:** Identifica los mecanismos que se utilizarán para comunicarse con los grupos de interés y permitir el acceso a la información como reuniones, boletines, píldoras informativas, repositorios, fondos de escritorio etc.
g) **Formato:** De acuerdo con el mensaje y el canal de comunicación se pueden definir recursos de apoyo que faciliten la transmisión del mensaje, ejemplo: flyer, presentación de diapositivas, video, etc.
h) **Etapa y Frecuencia:** Definir de manera general en qué etapa es más adecuado emitir este mensaje y con qué frecuencia o periodicidad.
i) **Cronograma:** Específica las fechas o tiempos de emisión de cada mensaje.

Una vez formulado el plan de comunicaciones será aprobado por la gerencia del proyecto y debe realizarse seguimiento a su ejecución en las reuniones periódicas de seguimiento general del proyecto.

4.6.3.2.3 Plan de Formación

El plan de formación se orienta a que los usuarios conozcan ampliamente como utilizar la solución o aprovechar la nueva implementación, servicio o infraestructura.

El plan permite establecer con claridad la forma en que los usuarios adquirirán las competencias y habilidades que les permitirán aprovechar la implementación de la mejor manera y en él se identifica el orden en que se deben dictar las temáticas, quien debe asistir, el facilitador adecuado para la sesión y los aspectos logísticos para su realización.

El plan de formación incluirá las acciones identificadas para atender las necesidades formativas de los grupos de interés, clasificadas como29:

- **Capacitación**: Formación para entregar conocimientos específicos requeridos. Ejemplo: marcos de referencia, normativas, entre otros.
- **Entrenamiento**: Orientado a desarrollar habilidades y promover comportamientos. Ejemplo: Habilidades de comunicación, liderazgo, gestión de proyectos.

- **Transferencia de Conocimiento**: Espacio para transmitir conocimientos e información y asignar responsabilidades en el contexto específico de la solución o el proyecto. Ejemplo: asignar y entrenar responsables de la gestión de solicitudes
- **Identificación del proyecto:** Nombre, objetivo, identificación del responsable y fecha de elaboración (actualización) del plan.
- **Identificación de las actividades de formación:** Describe en detalle el tipo de actividad a realizar y debe presentar de forma clara:

a) **Tipo de actividad:** Capacitación/Entrenamiento/Transferencia de conocimiento
b) **Grupos de Interés:** Definir a que grupo o grupos de interés se dirige la actividad formativa.
c) **Temática:** Asunto a desarrollar
d) **Objetivo:** De acuerdo con las necesidades identificadas, definir el objetivo académico de la actividad formativa
e) **Contenido**: Especificar los módulos o partes que conforman la actividad formativa
f) **Competencias:**Definir que habilidades, conocimientos ycomportamientos desarrolla o afianza esta actividad formativa
g) **Modalidad:** Las actividades se pueden desarrollar en formato presencial, virtual o híbrido.Audiencia: Grupo de interés al que está dirigida la formación
h) **Duración:** Definir la dedicación en horas que se requieren para cursar la actividad formativa.
i) **Fecha:** Especificación de la fecha en la que se planea realizar la actividad
j) **Instructor:** responsable de la sesión
k) **Estado**: Planeada, ejecutada, postergada.

Toda sesión incluida en el plan de formación deberá incorporar un instrumento debidamente diseñado para la medición del aprendizaje del asistente, de manera que pueda evaluarse posteriormente el grado de asimilación del contenido. Preferiblemente virtual del cual se pueda contar con evidencias y que permita trazabilidad de los resultados.

De igual manera, las sesiones deberán evaluarse en cuanto a nivel de satisfacción del asistentes, como forma de obtención de insumos para la medición posterior de la gestión del cambio.

Una vez formulado el plan de formación será aprobado por la gerencia del proyecto y debe realizarse seguimiento a su ejecución en las reuniones periódicas de seguimiento general del proyecto.

Recomendaciones finales

- El plan de comunicaciones se hará bajo los lineamientos establecidos por el equipo de comunicaciones de la secretaría que ejecuta el proyecto y en lo posible, bajo su acompañamiento.
- Para el desarrollo de cada plan se debe contar con el gerente del proyecto para realizar las convocatorias de formación y promover la asistencia y participación de los usuarios.
- Para cumplir con lo anterior, el enlace de la Secretaría de Innovación Digital apoyará y acompañará en la identificación de las responsabilidades de los diferentes participantes y la planificación de las acciones según el proyecto y la Secretaría.
- Si la ejecución del proyecto se realiza a través de un tercero, deberá incorporarse desde los pliegos la obligación de realizar la gestión del cambio y los aspectos mencionados, como una de las obligaciones del contrato.
- El material utilizado para las formaciones (presentaciones, infografías, videos, material de apoyo a las formaciones, entre otros) deberá entregarse de forma digital a la Unidad de Innovación de la SID para que repose en los Centros de Recursos de ApropiaTIC 30 para disponerlo en futuras formaciones, de ser necesario
- En las actividades de formalización del cierre del proyecto tecnológico (actas de recibo a satisfacción, actas de liquidación de contrato o similares), deberá incluirse información específica sobre el cumplimiento de la gestión del cambio en el mismo.

4.6.3.3 Seguimiento del Plan de Gestión del Cambio

El plan de gestión del cambio debe ser evaluado de manera periódica, de forma que pueda medirse su nivel de ejecución y el éxito obtenidos. Para esa evaluación deben ejecutarse las siguientes tareas:

- **Toma de datos.** Aplicar los instrumentos de recolección de información que se consideren pertinentes.
- **Análisis de resultados.** Elaborar el informe de seguimiento de la gestión del cambio que consolide las mediciones y análisis realizados, así como las conclusiones obtenidas.

Para este seguimiento, se sugiere considerar al menos con los siguientes elementos: (remítase al documento ver tabla 13 pag 173)

Para hacer el seguimiento del Plan de Gestión del Cambio, el gerente del proyecto deberá tener en cuenta las siguientes recomendaciones:

- Utilizar instrumentos de recolección de información, seguimiento y validación de los planes de comunicación y motivación. Estos instrumentos serán conservados digitalmente para su posterior consulta.
- Evaluar las actividades de formación del proyecto y comprobar la eficiencia de estas acciones
- Preparar las acciones a ejecutar a corto plazo.
- Tener en cuenta una periodicidad lo suficientemente corta que asegure una realimentación continua del personal sujeto al cambio.
- Contemplar una muestra que proporcione información desde diferentes puntos de la organización, tener en cuenta a los responsables de la dependencia en todos los niveles.
- Realizar un análisis que permita obtener conclusiones inmediatas.

4.6.3.4 Medición de resultados

Para el establecimiento de los resultados se presentan los indicadores en los cuales se apoya la evaluación de la gestión del cambio del proyecto, no obstante, su utilización o pertinencia dependerá de quienes hagan el ejercicio de verificación y de los temas que deseen o requieran visualizar o establecer.

Los indicadores están orientados a evaluar aspectos diversos de la gestión del cambio y por tanto pueden utilizarse en diferentes momentos de la Implementación (Ver tabla 14 del documento DE-GTIC-043LineamientosSIDV4_1.pdf pag 175)

4.6.4 Observaciones para otorgar el aval

Elaborar y anexar una Matriz de Interesados que clasifique poder e influencia de cada stakeholder, identificando rol, tipo de influencia y estrategia de involucramiento (Numeral 4.6.3.2.1).

Construir un Plan de Comunicaciones detallado que incluya mensajes clave, canales formales e informales, responsables, frecuencia de envíos y cronograma de actividades, según el numeral 4.6.3.2.2.

Diseñar un Plan de Formación que especifique las temáticas, objetivos de aprendizaje, competencia a desarrollar, modalidades (presencial/virtual), duración, cronograma e instrumentos de evaluación del conocimiento, conforme al numeral 4.6.3.2.3.

Definir un conjunto de indicadores cuantitativos y cualitativos (adopción, satisfacción, nivel de participación, eficacia de la formación) y establecer mecanismos periódicos de recolección y análisis de datos, tal como ordena el numeral 4.6.3.4.

Asignar formalmente un Responsable TIC o enlace de la SID encargado del seguimiento del Plan de Gestión del Cambio, con reportes periódicos al Gerente del Proyecto y al acompañante TIC (Numeral 4.6.3.3).

Establecer un cronograma de revisión y actualización periódica del Plan de Gestión del Cambio, con sesiones de retroalimentación y mejora continua, en cumplimiento de los lineamientos del Dominio Uso y Apropiación.

4.7 Transformación digital del distrito a servicios Cloud

4.7.1 Introducción

Transformación Digital del Distrito a Servicios Cloud

En virtud del Decreto 883 de 2020 —artículo 333A—, la Secretaría de Innovación Digital (SID) de la Alcaldía de Medellín es responsable de satisfacer las necesidades de Tecnologías de la Información de los distintos grupos de valor a través de servicios digitales, procesos eficientes y flujos de información seguros, apoyada en prácticas de arquitectura empresarial y seguridad de la información.

Este capítulo establece los lineamientos técnicos para la adopción, implementación y operación de soluciones en la nube de Microsoft Azure. Su propósito es:

- Definir principios, estándares y controles que guíen a las dependencias del Distrito y a sus proveedores en el diseño, migración o despliegue de cargas de trabajo en Azure.
- Proveer directrices para la gestión de datos y la definición de modelos estructurados y no estructurados en entornos cloud, minimizando inconsistencias y riesgos operativos.
- Especificar los requerimientos de seguridad, cumplimiento y continuidad que deberán adoptarse para preservar la confidencialidad, integridad y disponibilidad de la información en la nube.
- Describir la infraestructura de referencia del Distrito en Azure y los dominios de gobierno asociados, garantizando la alineación con la Arquitectura Empresarial y con la Política de Gobierno Digital consignada en el Decreto 1008 de 2018.

Establecer un marco técnico y metodológico que habilite al Distrito para cumplir con las responsabilidades y oportunidades de la nueva categoría de Ciencia, Tecnología e Innovación, según lo dispuesto en la Ley 2286 de 2023, promoviendo ecosistemas tecnológicos, el conocimiento científico y la financiación de emprendimientos de base tecnológica.

El cumplimiento de estos lineamientos será obligatorio para todas las dependencias y contratos que involucren servicios cloud, y constituirá un criterio determinante para la emisión de avales técnicos por parte de la SID. Los proyectos internos liderados por la propia Secretaría estarán exentos de dicho aval, sin perjuicio de su obligatorio ajuste a las disposiciones aquí contenidas

Su aplicación permitirá fortalecer las capacidades institucionales mediante un enfoque cloud-first, potenciando la escalabilidad, la innovación y la eficiencia presupuestal; todo ello orientado a ofrecer mejores servicios digitales a los ciudadanos y a consolidar la transformación digital del territorio.

4.7.2 Principios generales

A continuación, se describen los principios rectores que sustentan la estrategia cloud del Distrito. Estos lineamientos técnicos unifican buenas prácticas internacionales (NIST SP 800-207 Zero Trust, ISO/IEC 27001:2022, CNCF Cloud Native Maturity) con los marcos normativos nacionales de Gobierno Digital. Su aplicación garantiza que toda solución desplegada en Microsoft Azure mantenga consistencia arquitectónica, trazabilidad mediante Infraestructura como Código, cumplimiento integral de seguridad y privacidad por diseño, y observabilidad continua para la toma de decisiones basada en datos operativos.

Se establecen aquí los Lineamientos Técnicos para la Adopción, Implementación y Operación de Soluciones en la Nube de Microsoft Azure para entidades del orden distrital y nacional, priorizando la soberanía del dato, la trazabilidad operativa y la sostenibilidad financiera.

Su propósito es:

- Establecer principios de diseño cloud-first bajo modelos de madurez cloud- native.
- Implementar controles de seguridad y cumplimiento normativo desde el diseño (privacy & security by design).
- Uniformar los criterios para la contratación, despliegue, operación y auditoría de soluciones en Azure.

- Cumplir con la obligatoriedad de estos lineamientos con la política de Transformación Digital Pública establecida en el Decreto 1263 de 2022 del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), así como sus actualizaciones.

4.7.4 Gobierno y roles (RBAC)

La Secretaría de Innovación Digital (SID) es la instancia que revisa y aprueba todo proyecto que se ejecute en la nube del Distrito.

Para que cada equipo tenga claro "quién hace qué", utilizaremos una matriz RACI:

- **R (Responsible)** – Quien realiza la tarea.
- **A (Accountable)** – Quien asume la responsabilidad final y da el visto bueno.
- **C (Consulted)** – Quien es consultado y aporta conocimientos especializados.
- **I (Informed)** – Quien debe mantenerse informado sobre el avance.

Este modelo se aplicará a las principales actividades del proyecto (análisis, diseño, despliegue, pruebas y operación) y permitirá asignar de forma transparente las responsabilidades entre la SID, las áreas usuarias y los proveedores.

4.7.5 Arquitectura de referencia en Azure

La arquitectura que utilizaremos —representada en el archivo **"Despliegue_Azur.drawio.pdf"**— sigue un modelo **hub-and-spoke** muy sencillo de entender:

- **Hub (centro de servicios comunes):** un "punto central" donde residen los servicios compartidos (seguridad, monitoreo, identidad, conectividad) quen ecesitan todos los sistemas.
- **Spokes (zonas de aterrizaje):** tres "ramales" independientes que aíslan los ambientes de **Producción** (lo que ve el ciudadano), o **Calidad / QA** (donde se hacen pruebas), y o **Operaciones / OPS** (herramientas transversales de soporte).

Así logramos que cada entorno esté protegido y separado, mientras seguimos gestionando desde un mismo lugar lo que es común para todos.

Componentes clave del diagrama

- Pasarela de conexión segura a la red del Distrito.

- Firewall y controles de seguridad compartidos.
- Servicios de identidad y acceso (Azure AD).
- Redes virtuales (VNets) separadas para Producción, QA y OPS.
- Almacenamiento y bases de datos según cada entorno.
- Herramientas de monitoreo y registro centralizadas.

En resumen, el hub-and-spoke permite **ordenar, proteger y escalar** la nube del Distrito sin mezclar los ambientes de trabajo, garantizando operaciones seguras y eficientes para usuarios y equipos técnicos.

4.7.6 Seguridad y cumplimiento

La estrategia de Seguridad y Cumplimiento del Distrito se fundamenta en el marco de Zero-Trust y en estándares internacionales como ISO/IEC 27001:2022, NIST SP 800-53 y los Controles CIS para Azure, integrados a las obligaciones nacionales de protección de datos (Ley 1581/2012), ciberseguridad (Ley 1621/2013) y Gobierno Digital (Decreto 620/2020). Bajo este modelo, todos los recursos en Microsoft Azure se rigen por el principio de privilegio mínimo a través de Microsoft Entra ID con MFA y Privileged Identity Management, protección criptográfica con claves administradas en Azure Key Vault y cifrado TLS 1.2 + extremo a extremo.

La postura defensiva se refuerza con Microsoft Defender for Cloud, Microsoft front Door, segmentación de red, Private endpoint, políticas de compliance automatizadas y monitoreo continuo en Microsoft Sentinel para SIEM/SOAR. Estos controles proporcionan visibilidad integral, gestión proactiva de riesgos y evidencia auditada que garantiza el cumplimiento normativo y la resiliencia operativa de las soluciones del Distrito.

Seguridad de la Cadena de Suministro de Software: Se implementarán controles de seguridad exhaustivos para la cadena de suministro de software, incluyendo la vigilancia de vulnerabilidades en librerías de terceros, análisis de dependencias (SCA) y la integridad de los artefactos desde el desarrollo hasta el despliegue.

4.7.10 DevSecOps y calidad del software (remítase al documento DE-GTIC-043LineamientosSIDV4_1.pdf pag 191 a 195)

4.7.11 Requisitos obligatorios para cada despliegue

- **Integración CI/CD** con repositorios Git del Distrito.
- **Pruebas automáticas**: unitarias, integración, carga y seguridad (SAST/SCA).

- **Quality Gates** y escaneos de seguridad superados.
- **Despliegue Canary** con capacidad de *rollback* automático.

4.7.12 Entregables que el equipo debe aportar

- Evidencia de todas las **pruebas automáticas** ejecutadas.
- **Arquitectura firmada** por el Arquitecto Cloud del Distrito.
- **Manual técnico** y **manual de usuario final** actualizados.
- Evidencia de cumplimiento de los **lineamientos de la SID** y de las **pruebas no funcionales** (rendimiento, disponibilidad, seguridad).

Con este modelo DevSecOps aseguramos que las nuevas funcionalidades lleguen a los ciudadanos **rápido, estables y sin exponer la seguridad** del Distrito.

4.7.13 Microservicios y contenedores

A continuación, se establecen las pautas oficiales para el uso de **Azure Red Hat OpenShift (ARO)** y **Azure Container Registry (ACR)** dentro de la nube del Distrito. Estos lineamientos complementan el modelo DevSecOps descrito en la sección 7.7.3 y son de obligatoria aplicación para todos los equipos técnicos.

5.7.13.1.1 Descripción de referencia

ARO es la plataforma empresarial administrada conjuntamente por Microsoft y Red Hat que permite orquestar contenedores con Kubernetes y OpenShift de forma totalmente gestionada, con soporte 24/7 y SLA de nivel empresarial.

5.7.13.1.2 Lineamientos de uso

- **Casos de adopción**

- Utilizar ARO para cargas de misión crítica que requieran alta disponibilidad, escalabilidad automática y gobierno centralizado de políticas.
- Priorizar ARO cuando se necesiten capacidades propias de OpenShift (Operators, Service Mesh, rutas seguras, etc.).

- **Seguridad y cumplimiento**

- Aplicar políticas de seguridad (OpenShift Security Context Constraints) que se alineen con los controles de la SID y el MSPI.
- Habilitar TLS en todas las rutas y certificados administrados con Azure Key Vault.

- **Integración DevSecOps**

- Todos los despliegues deberán provenir de pipelines YAML en Azure DevOps/GitHub Enterprise con pruebas automáticas y quality gates activos.

- **Escalabilidad y costos**

- Configurar escalado automático horizontal (HPA) y vertical (VPA) siguiendo métricas de CPU/memorias definidas por la SID.
- Aplicar etiquetas de costos y políticas de apagado fuera de horario para ambientes de prueba.

5.7.13.2 **Azure Container Registry (ACR)**

5.7.13.2.1 Descripción de referencia

- ACR es el repositorio privado de contenedores donde se almacenan y versionan las imágenes Docker utilizadas por los proyectos del Distrito.

5.7.13.2.2 Lineamientos de uso

1. **Repositorios y versionamiento**

- Crear un ACR dedicado por dominio de negocio (salud, ciudadanía, datos, etc.) para aislar permisos y cumplir la segmentación recomendada.
- Etiquetar las imágenes siguiendo el formato <app>:<major.minor.patch>- <entorno> (ejemplo: ciudadano360:2.3.1-prod).

2. **Seguridad**

- Habilitar autenticación RBAC integrada con Azure AD y exigir uso de identidades administradas para los pipelines.
- Activar escaneo de vulnerabilidades con Microsoft Defender for Containers y bloquear la promoción a producción cuando existan hallazgos críticos.

3. **Disponibilidad y rendimiento**

- Configurar geo-replicación para las regiones donde se desplieguen clústeres ARO/AKS, minimizando la latencia de extracción de imágenes.
- Definir políticas de retención automática para eliminar tags obsoletos y optimizar costos de almacenamiento.

4. **Integración con CI/CD**

- Cada build pipeline debe:

1. Compilar la imagen.

2. Ejecutar análisis SAST/SCA y escaneo de imagen.

3. Publicar en ACR solo si supera los quality gates.

- Los pipelines de despliegue (release) obtendrán la imagen directamente desde ACR con digests inmutables para garantizar trazabilidad.

4.7.13.3 Requisitos transversales

- Documentación: actualizar el "Manual técnico de contenedores" con diagramas de arquitectura, parámetros de despliegue y procedimientos de recuperación.
- Monitoreo: integrar métricas de clúster e imágenes con Azure Monitor y generar alertas sobre fallos de escalado, vulnerabilidades nuevas o uso inusual de red.
- Cumplimiento normativo: evidenciar, en cada release, el cumplimiento de OWASP TOP 10, SAMM, ISO 27034 y las directrices de la SID.

4.7.14 Descripción de componentes de bases de datos

Azure Database for PostgreSQL Flexible Server: Servicio de base de datos relacional totalmente administrado que permite personalizar configuraciones de rendimiento, alta disponibilidad y escalabilidad horizontal. Ideal para aplicaciones empresariales críticas que requieren control detallado sobre versiones de PostgreSQL, configuraciones específicas y eficiencia de costos con pricing flexible (burstable o escalado automático).

Azure SQL Managed Instance (MI): Servicio PaaS completamente administrado que ofrece compatibilidad casi total con SQL Server on-premise, lo que facilita la migración de bases de datos heredadas sin cambios significativos. Incluye características avanzadas como respaldo automático, actualizaciones de seguridad automáticas, alta disponibilidad integrada y soporte para redes privadas con Azure VNet.

Azure Cosmos DB: es un servicio de base de datos NoSQL distribuido global y totalmente administrado, diseñado para ofrecer baja latencia y alta disponibilidad a escala planetaria. Soporta múltiples modelos de datos como documentos, grafos, columnas anchas y claves-valor, además de ofrecer APIs compatibles con MongoDB, Cassandra, Gremlin, Table y SQL (Core).

4.7.15 Descripción de componentes de analítica avanzada

4.7.15.1 Objetivo

Establecer los lineamientos técnicos, metodológicos, éticos y de gobernanza que deben ser tenidos en cuenta para el diseño, desarrollo, implementación y uso de soluciones de analítica de datos e inteligencia artificial (IA) en el Distrito de Medellín.

Esto con el fin de garantizar el uso responsable, seguro, transparente y eficiente de los datos institucionales, apoyando la toma de decisiones basada en evidencia y la transformación digital del territorio.

Estos lineamientos aplican a todas las dependencias del Distrito de Medellín, así como a los proveedores y contratistas que desarrollen o implementen modelos analíticos o soluciones de IA para entidades del gobierno distrital.

4.7.15.2 Disposiciones generales

- Toda iniciativa de analítica de datos o IA debe estar alineada con las estrategias institucionales de transformación digital, gobierno abierto, inclusión social y sostenibilidad.
- Se priorizará el uso de datos abiertos, datos internos estructurados y no estructurados, y la integración de múltiples fuentes de información bajo un modelo federado o centralizado en Azure.
- El tratamiento de datos deberá cumplir con las disposiciones legales sobre protección de datos personales (Ley 1581 de 2012 y demás normativas vigentes).

- Se desarrollarán programas de formación y capacitación continuos para el personal del Distrito en el diseño, desarrollo, implementación y operación de sistemas de inteligencia artificial."
- Se priorizará el uso y la integración con los portales de datos abiertos del Estado, fomentando la reutilización de información pública para el desarrollo de soluciones analíticas y de IA
- La interpretación y explicación de modelos predictivos deben garantizar el principio de transparencia y explicabilidad, especialmente en contextos sensibles (educación, salud, seguridad, entre otros).

4.7.16 Arquitectura de Analítica e IA sobre Azure

La arquitectura institucional para analítica de datos e inteligencia artificial se implementará sobre la nube de Microsoft Azure y contempla los siguientes componentes:

Azure Data Lake Storage Gen2: como repositorio central de datos, organizado bajo una arquitectura medallion (Bronze: datos crudos, Silver: datos transformados, Gold: datos listos para modelamiento o análisis).

Azure Synapse Analytics / Azure Databricks: para procesamiento masivo de datos (ETL/ELT), análisis exploratorio, modelamiento y visualización.

Azure Machine Learning (Azure ML): como plataforma para el entrenamiento, evaluación, versionado y despliegue de modelos predictivos.

Azure Data Factory: como herramienta principal para la interoperabilidad y la ingesta de datos desde múltiples fuentes institucionales y externas.

Azure Purview (Microsoft Purview): para la catalogación, linaje, clasificación y gobierno del dato.

Power BI: para la entrega de visualizaciones interactivas y tableros orientados a la toma de decisiones.

- Azure DevOps: para control de versiones, CI/CD de modelos y automatización de pipelines analíticos.

Lenguajes soportados: Python y R para análisis, modelamiento y desarrollo de

pipelines en Azure ML o Databricks.

Todos los componentes y soluciones de analítica e IA deberán garantizar la interoperabilidad con otros sistemas de información públicos, facilitando el suministro y el intercambio eficiente de información, en concordancia con los principios de Transformación Digital Pública

4.7.16.1 Lineamientos técnicos para proyectos de analítica e IA

- Todos los proyectos deben contar con:

- Especificación del problema.
- Descripción de fuentes de datos y calidad de los mismos.
- Trazabilidad completa del proceso de transformación de datos.
- Documentación del modelo, métricas de evaluación y supuestos.
- Registro de versiones de datasets, modelos y pipelines.

- Se fomentará la evaluación y, cuando sea viable, la adopción de soluciones de software libre y código abierto que se integren con la infraestructura Azure, promoviendo la autonomía tecnológica.
- Los datos deben mantenerse anonimizados o seudoanonimizados cuando se trate de información sensible o personal.
- Se recomienda el uso de notebooks versionados y repositorios centralizados en Azure DevOps o GitHub Enterprise.

4.7.16.2 Lineamientos Éticos

Los proyectos de IA deben cumplir con los siguientes principios:

- ***Transparencia:*** Garantizar explicabilidad en las decisiones automatizadas.
- ***Responsabilidad:*** Asignación clara de responsabilidades sobre los resultados de los modelos.
- ***Seguridad:*** Salvaguardar la integridad de los datos y modelos desplegados.
- ***Consentimiento informado:*** En casos donde se recolecten nuevos datos personales, debe garantizarse el consentimiento del ciudadano.

4.7.16.3 Gobernanza del Dato y de la IA

Todas las soluciones deben estar registradas en el inventario de activos analíticos del Distrito, gestionado por la Secretaría de Innovación Digital.

- El ciclo de vida de los modelos (entrenamiento, pruebas, despliegue, monitoreo) debe quedar documentado y versionado.
- El monitoreo en producción debe incluir alertas por deriva de datos o rendimiento del modelo.
- El acceso a datos y resultados analíticos debe estar gobernado por roles y perfiles definidos, en concordancia con las políticas institucionales de seguridad.

4.7.16.4 Casos de Uso Prioritarios

Se considerarán prioritarios los siguientes tipos de proyectos de analítica e IA:

- Identificación temprana de riesgos sociales (deserción escolar, violencia, pobreza).
- Optimización de recursos y logística de operación distrital.
- Recomendación de programas sociales según perfil ciudadano.
- Segmentación poblacional para campañas de salud pública o participación.

4.7.17 Costos, Gobernanza y Optimización

La gestión de costos y la optimización (FinOps) será una responsabilidad compartida entre los equipos técnicos y financieros, buscando maximizar el valor de la inversión en la nube mediante una cultura de responsabilidad y eficiencia.

4.7.17.1 Operación y Monitoreo

Azure Monitor, Log Analytics y Application Insights son obligatorios para telemetría. Los KPI mínimos incluyen disponibilidad, latencia, costos y alertas de seguridad. Microsoft Sentinel gestionará SIEM/SOAR.

4.7.17.2 Costos y Optimización (Cost Management)

Se etiquetarán recursos con "Cost Managent", Los equipos deberán revisar recomendaciones de Azure Cost Management para validar el consumo y costos actuales de los servicios.

Se establecerán ciclos de revisión periódica de las recomendaciones de Azure Advisor y otras herramientas de optimización para asegurar la mejora continua en la eficiencia del gasto y la configuración de recursos.

5.7.18 Gestión de Cambios

Todo cambio que deba implementarse en la nube del Distrito se tramitará mediante Pull Request en el repositorio oficial y deberá adjuntar los siguientes anexos o evidencias antes de ser aprobado:.

1. **Solicitud de cambio**

- Pull Request con la descripción detallada del cambio y su alcance.

2. **Aval técnico de la SID**

- Documento emitido por la Secretaría de Innovación Digital que valide la pertinencia y viabilidad técnica.

3. **Evidencias de pruebas**

- Pruebas funcionales, técnicas y de seguridad superadas.
- Pruebas unitarias que cumplan los *quality gates* definidos.
- Pruebas de carga y estrés con resultados aceptables.
- Reportes de análisis de código estático y dinámico sin hallazgos críticos.

4. **Documentación de despliegue y operación**

- Manual de despliegue, configuración y operación actualizado.
- Manuales de usuario cuando el cambio impacte funcionalidades visibles.

5 revisión de arquitectura (si aplica)

- Acta o aval del Comité de Arquitectura cuando el cambio tenga alto impacto o modifique componentes críticos.

6 Artefactos de arquitectura y código

- Diagrama de arquitectura actualizado.
- Documento arquitectónico que describa decisiones y patrones utilizados.
- Código fuente alojado en los repositorios oficiales de la Alcaldía de Medellín.

Solo cuando todos los requisitos anteriores estén completos y validados se procederá a la aprobación final y posterior despliegue en el entorno productivo.

4.7.19 Anexo - Despliegue_Azur.drawio.pdf -

4.7.21 Aplicación Obligatoria

Este documento es de cumplimiento obligatorio para todo proyecto de transformación digital o contratación que involucre recursos Cloud del Distrito. Su incumplimiento podrá generar observaciones técnicas, solicitudes de ajuste o rechazo de despliegue por parte de la Secretaría de Innovación Digital.

4.8 Uso y aplicación de la inteligencia artificial – IA

4.8.1 Introducción y marco normativo

El avance acelerado de la Inteligencia Artificial (IA) exige que el Distrito de Medellín establezca un marco claro que equilibre la innovación tecnológica con la protección de los derechos ciudadanos. Estos lineamientos se fundamentan en la hoja de ruta para el desarrollo de la IA en Colombia propuesta por el **MinTIC** y adoptan el estándar internacional **ISO/IEC 42001:2023**. El objetivo es consolidar un Sistema de Gestión de Inteligencia Artificial (AIMS) que sea responsable, ético, transparente y auditable en todas las dependencias de la Administración Distrital.

4.8.2 Lineamientos Éticos para el uso de la IA

El marco ético se estructura en tres pilares: la ética de los datos (procedencia y transparencia), la ética de los algoritmos (lógica y funcionamiento) y la ética de las prácticas (responsabilidad humana y procesos).

4.8.2.1 Transparencia y explicabilidad

La transparencia es una responsabilidad social. La ciudadanía tiene el derecho de conocer de dónde provienen los datos que alimentan los sistemas, cómo se han seleccionado y con qué propósito se utilizan. Los algoritmos, aunque complejos, deben ser comunicados de forma

comprensible, explicando sus alcances, limitaciones y respetando siempre los derechos de autor. En las prácticas en inteligencia artificial es fundamental que se informe de manera clara y accesible sobre quiénes están detrás del desarrollo y uso de estos sistemas, desde los equipos técnicos hasta las personas que toman las decisiones estratégicas. La publicación de manuales de conducta, la promoción del código abierto y la comunicación abierta sobre la intervención humana en el desarrollo de códigos.

4.8.2.2 Privacidad y protección de datos

El respeto absoluto a la privacidad es innegociable. Se debe informar a las personas sobre los propósitos específicos del uso de su información, otorgándoles control sobre sus datos. Queda prohibida la creación de perfiles detallados sin autorización y el uso de datos personales para fines que puedan discriminar o perjudicar a los individuos. Para salvaguardar la privacidad de los usuarios, es necesario establecer procedimientos rigurosos que regulen el manejo de la información. Esto implica desarrollar herramientas para gestionar los riesgos asociados a la privacidad y realizar evaluaciones de impacto antes de implementar nuevas tecnologías.

4.8.2.3 Control humano y supervisión

La IA debe ser entendida como una herramienta que asiste, no que sustituye. La recopilación y tratamiento de datos deben estar bajo supervisión humana. Cualquier sistema de respuesta automática o toma de decisiones críticas debe contar con mecanismos de intervención humana inmediata para asegurar que el juicio y la experiencia de las personas prevalezcan.

4.8.2.4 Seguridad

Es fundamental establecer sistemas de protección robustos que garanticen la confidencialidad e integridad de la información. Se deben implementar evaluaciones de riesgo para analizar las consecuencias de los algoritmos, evitando delegar decisiones que afecten la vida de las personas exclusivamente a sistemas automatizados.

4.8.2.5 Responsabilidad

La responsabilidad es compartida pero clara:

Desarrolladores: Responsables de la calidad del código y la transparencia de los datos.

Usuarios/Implementadores: Responsables de las consecuencias derivadas de la aplicación del sistema.

Nadie puede evadir su responsabilidad alegando autonomía algorítmica.

4.8.2.6 No discriminación y equidad

Para garantizar resultados justos, se deben depurar los conjuntos de datos de cualquier sesgo o prejuicio previo. Es obligatorio monitorear continuamente el desempeño de los modelos considerando factores de género, raza, religión, discapacidad y orientación sexual, promoviendo además la diversidad en los equipos de diseño.

4.8.3 Lineamientos técnicos y de gestión

Siguiendo el estándar internacional (ISO/IEC 42001:2023), el Distrito adopta un enfoque de gestión de calidad y mejora continua.

4.8.3.1 Planificación técnica y gestión de riesgos

Cada proyecto de IA debe identificar riesgos técnicos específicos:

- **Sesgo de Datos:** Uso de conjuntos históricos no representativos.
- **Desviación (Model Drift):** Pérdida de precisión por cambios en el entorno real.
- **Ataques Adversarios:** Manipulación externa mediante inyección de datos alterados.

Definición de Métricas Técnicas: Los objetivos del AIMS deben incluir métricas cuantitativas que se midan y monitoreen automáticamente:

- **Métricas de equidad (Fairness Metrics)**: Medir el desempeño del modelo entre diferentes subgrupos poblacionales (ej. Equal Opportunity o Demographic Parity).
- **Métricas de robustez**: Evaluar la resistencia del modelo a la variación y al ruido en los datos de entrada.
- **Métricas de explicabilidad**: Definir un umbral de confianza o un nivel de contribución mínimo para las características utilizadas en la explicación de las decisiones.

4.8.3.2 Control operacional y ciclo de vida del software

La IA debe integrarse en el ciclo de vida de desarrollo de software convencional, pero añadiendo:

- **Análisis de Linaje de Datos:** Documentación del origen y transformación de los datos.
- **Separación de Entornos:** Estándares de arquitectura (ej. Docker) para garantizar la reproducibilidad entre desarrollo, pruebas y producción.
- **Rollback Automático:** Reversión a versiones estables si las métricas de desempeño caen por debajo de los umbrales definidos.

4.8.3.3 Calidad, integridad y mitigación de sesgos

Se deben utilizar herramientas automatizadas para detectar valores atípicos (*outliers*) e inconsistencias antes del entrenamiento. Es obligatorio aplicar técnicas de anonimización y seudonimización en datos sensibles, además de realizar pruebas de estrés y entrenamiento adversario para asegurar la robustez del sistema.

Para la mitigación de sesgos se deberán aplicar técnicas de pre-procesamiento para equilibrar los conjuntos de datos. Utilizar herramientas de evaluación de equidad (fairness tools) durante la fase de desarrollo para iterar y ajustar el modelo hasta que las métricas de equidad sean aceptables para el contexto.

4.8.4 Mecanismos de transparencia avanzada

La rendición de cuentas técnica requiere herramientas que permitan auditar los resultados de la IA.

4.8.4.1 Herramientas de explicabilidad (LIME y SHAP)

Para decisiones críticas, se deben implementar herramientas de explicabilidad post- hoc como **LIME** (Local Interpretable Model-agnostic Explanations) o **SHAP** (Shapley Additive exPlanations). Estas herramientas permiten entender la contribución de cada variable en un resultado específico, facilitando la confianza del usuario y la detección de sesgos ocultos.

5.8.4.2 Registro de modelos y auditoría (Logging)

- **Registro de modelos (Model Registry):** Actúa como fuente única de verdad para la trazabilidad y gestión del ciclo de vida.
- **Audit Log:** Registro detallado que capture las entradas, la versión del modelo, los parámetros de inferencia y la salida final. Este registro es esencial para procesos de apelación ciudadana e investigación de incidentes.

5. Especificaciones de desarrollo y entregables

5.1 Lineamientos institucionales:

Para los proyectos de componente tecnológico del Distrito se deben seguir las directrices establecidas en los lineamientos emitidos por la Secretaría de Innovación Digital que se encuentran definidas en el documento de LINEAMIENTOS SOBRE ADQUISICIÓN, DESARROLLO Y USO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES EN LA ALCALDÍA DE MEDELLÍN alojado en el sistema de gestión integral del Distrito de Medellín -iSolución- y anexo a este documento, sin embargo a continuación se especifican ciertos ítems clave.

Dominio	Disciplina	Descripción del Entregable
Sistemas de Información	**Al momento de iniciar el proyecto**	Backlog del producto priorizado o lista de requerimientos priorizados.
		Historias de usuarios o Casos de uso.
	Arquitectura de software	Documento de arquitectura del sistema de información
		Catálogo de Sistemas de Información diligenciado incluyendo Microservicios e Integraciones Internas y Externas. (Anexo Catalogo SI)
		Catálogo de Microservicios implementados y Microservicios Core que se usaron (Anexo Catalogo SI v2.xlsx)
		Catálogo de servicios de Interoperabilidad (Anexo Catalogo SI v2.xlsx)
		Catálogo de servicios de integración con aplicaciones internas (Anexo Catalogo SI v2.xlsx)
		Diagrama Modelo entidad relación
		Diccionario de datos de acuerdo con el numeral 2.4.2 de los lineamientos
	Desarrollo	Entrega de código fuente documentado en español y aprobado por el delegado de la Secretaría de Innovación Digital. Este código quedará almacenado en un repositorio de la Alcaldía de Medellín.
	Pruebas	Documento de diseño de pruebas

		Evidencia de pruebas (Unitarias, Funcionales, de integración, de rendimiento)
		Pruebas de rendimiento de requerirse y justificar en caso contrario (Concurrencia, Carga, estrés, entre otros)
	Manuales	Manual de usuario final
		Manual Técnico de parametrización y configuración
		Manual de despliegue
		Se debe entregar la información básica para alimentar el catálogo de sistemas de información de la Alcaldía de Medellín según el instrumento Anexo Catalogo SI v2.xlsx definido por la SID
	Observaciones para otorgar el aval	Control de cambios: Cualquier implementación, migración, actualización en los ambientes preproductivos y de producción debe surtir las actividades enmarcadas en el proceso de control de cambios definido por la Secretaría de Innovación Digital.
		Pruebas de carga y estrés: - Cantidad de usuarios concurrentes simulados: debe estar alineada con la estimación de usuarios reales que accederán al sistema en -horas pico dependiendo del tipo y criticidad del sistema. - Tiempos de respuesta esperados: Los tiempos de respuesta de los sistemas deben definirse para operaciones críticas (logín, consultas principales) y no críticas como punto de referencia para medir su rendimiento y tomar las acciones necesarias.

		Cobertura de código: La validación de calidad debe contemplar la cobertura mínima de código y la ausencia de vulnerabilidades críticas Es importante tener en cuenta que más allá del porcentaje, la calidad de las pruebas es clave.
		Pruebas de código estático y dinámico: Se debe evidenciar la ejecución de pruebas estáticas y dinámicas de seguridad, según la naturaleza del sistema, así como la gestión de los hallazgos identificados. No deberán existir vulnerabilidades críticas o de alto impacto sin justificación y tratamiento definido. Los hallazgos medios o menores deberán estar documentados y, cuando no sean corregidos, contar con la respectiva justificación y plan de remediación. Se deberán aportar los resultados de las pruebas y las evidencias de gestión de los hallazgos. Se podrán emplear herramientas como SonarQube, OWASP ZAP o Burp Suite, según corresponda.
		Pruebas de rendimiento y recuperación: Definir y documentar protocolos o planes de respuesta para escenarios de operación como carga sostenida, la degradación progresiva del servicio, el comportamiento frente a picos inesperados de demanda o situaciones de estrés, definiendo las acciones, responsables y mecanismos de

		recuperación ante la materialización de estos eventos.
Gestión y apertura de datos	**Observaciones para otorgar el aval**	Identificación y documentación de los conjuntos de datos generados por la solución, y en particular, se deberá garantizar la utilización del FO_GTIC-015_Catalogo_Datos para el registro de los metadatos requeridos para la gestión de la información en el Lago de Datos, considerando que el documento establece dicho instrumento como requisito fundamental para la integración y aprovechamiento de los datos.
Gestión documental	**Observaciones para otorgar el aval**	(i) cumplimiento parcial en la estructuración y almacenamiento documental conforme a las TRD; (ii) incumplimiento en mecanismos de autenticidad e integridad documental por ausencia de firma digital y estampado de tiempo; (iii) incumplimiento en la incorporación de metadatos de preservación; y (iv) cumplimiento parcial en la formalización del plan de preservación digital a largo plazo: por lo anterior, se recomienda:
		Implementar firma digital y mecanismos de integridad documental; reorganizar el expediente conforme a las TRD vigentes; incorporar metadatos obligatorios para los documentos electrónicos; y formular el plan de preservación digital de largo plazo para activos con retención superior a ocho años.
Uso y apropiación de las TIC	**Observaciones para otorgar el aval**	Elaborar y anexar una Matriz de Interesados que clasifique poder e influencia de cada stakeholder, identificando rol, tipo de influencia y

		estrategia de involucramiento (Numeral 4.6.3.2.1).
		Construir un Plan de Comunicaciones detallado que incluya mensajes clave, canales formales e informales, responsables, frecuencia de envíos y cronograma de actividades, según el numeral 4.6.3.2.2.
		Diseñar un Plan de Formación que especifique las temáticas, objetivos de aprendizaje, competencia a desarrollar, modalidades (presencial/virtual), duración, cronograma e instrumentos de evaluación del conocimiento, conforme al numeral 4.6.3.2.3.
		Definir un conjunto de indicadores cuantitativos y cualitativos (adopción, satisfacción, nivel de participación, eficacia de la formación) y establecer mecanismos periódicos de recolección y análisis de datos, tal como ordena el numeral 4.6.3.4.
		Asignar formalmente un Responsable TIC o enlace de la SID encargado del seguimiento del Plan de Gestión del Cambio, con reportes periódicos al Gerente del Proyecto y al acompañante TIC (Numeral 4.6.3.3).
		Establecer un cronograma de revisión y actualización periódica del Plan de Gestión del Cambio, con sesiones de retroalimentación y mejora continua, en cumplimiento de los lineamientos del Dominio Uso y Apropiación.
Seguridad Informática		Matriz de valoración de riesgos de seguridad informática del sistema de información, y de la infraestructura que la soporta.

		Vista de Seguridad informática del Sistema de Información (roles, perfiles, accesos, autenticación, trazabilidad)
		Vista de Seguridad informática de las interoperabilidades del sistema de información (intercambio de datos con otras aplicaciones, almacenamiento, etc)
		Vista de seguridad informática de la infraestructura (Sistema de Información, Bases de Datos, Telecomunicaciones) donde se aloja el sistema de información (Nube, OnPremise) en términos de las capas de seguridad perimetral utilizadas (firewalls, protocolos, acceso remoto)
		Vista de seguridad informática de la protección de los datos (cifrado en reposo, cifrado en tránsito, etc)
		Acuerdo de Nivel de Servicio (Mecanismos para atender y remediar vulnerabilidad de seguridad informática, así como para gestionar incidentes de seguridad informática)
		Condiciones de Prestación del Servicio (Mecanismos para garantizar la disponibilidad de los servicios y la recuperación ante eventualidades o desastres).
Protocolo y calidad del dato		Diagrama de arquitectura a nivel de componentes utilizados para el desarrollo de la aplicación como también la comunicación o integración con otros sistemas.
Componente Cloud	**Observaciones para otorgar el aval**	Gestión de identidad y autenticación: se recomienda que tanto SIGESH como Bomberos en Línea evolucionen hacia la integración con Keycloak, o con el servicio institucional de identidad que determine la Secretaría de Innovación Digital, procurando centralizar la autenticación,

		autorización, gestión de usuarios, roles y sesiones. De acuerdo con los lineamientos vigentes, deberá contemplarse igualmente el uso de doble factor de autenticación para usuarios administrativos, privilegiados o que tengan acceso a información sensible o crítica. Gobierno y responsabilidades: durante la etapa inicial de ejecución deberá completarse la matriz RACI del proyecto, identificando claramente los responsables de las actividades de análisis, diseño, desarrollo, despliegue, pruebas y operación, incluyendo los responsables funcionales y técnicos de cada sistema. Los lineamientos cloud establecen la aplicación de este modelo para delimitar las responsabilidades entre la dependencia solicitante, la SID y el proveedor. Gestión de despliegues: para los requerimientos relacionados con creación, configuración, modificación o despliegue de componentes en los ambientes tecnológicos del Distrito, se deberá utilizar el Centro de Servicios Compartidos – CSC, mediante la generación y seguimiento de los respectivos casos de servicio, coordinando las actividades con los equipos técnicos de la Secretaría de Innovación Digital. Durante la ejecución deberán conservarse las evidencias correspondientes a arquitectura, pruebas funcionales y técnicas,

		seguridad, despliegues, documentación y demás entregables establecidos en los lineamientos institucionales y en los documentos contractuales.

5.2 Entregables del proyecto

5.2.1 Generales

Componente	Descripción
Gestión del proyecto	Cronograma general de trabajo conforme a las actividades priorizadas por el DAGRD para el desarrollo del contrato.
	Informe de gestión mensual que dé cuenta de la planeación, gestión, implementación y seguimiento de las acciones de soporte, mantenimiento y mejora del sistema de información de seguridad humana.
Soporte y mantenimiento	Informe de gestión mensual que dé cuenta de la planeación, gestión, implementación y seguimiento de las acciones de soporte, mantenimiento preventivo y correctivo.
	Solución de los incidentes que actualmente se encuentran abiertos debidamente probados y puestos en ambiente de producción del sistema.
Desarrollo	Sistema desplegado en ambiente de preproducción del Distrito de Medellín.
	Sistema desplegado en ambiente de producción del Distrito de Medellín.
	Puesta en producción de las mejoras y evoluciones a los sistemas de información contratadas por el DAGRD.
	Recibo a satisfacción del sistema operando en productivo con los ajustes y mejoras acordadas.

5.2.2 SIGESH

Soporte y mantenimiento	Informe de gestión mensual que dé cuenta de la planeación, gestión, implementación y seguimiento de las acciones de soporte, mantenimiento preventivo y correctivo.
	Solución de los incidentes que actualmente se encuentran abiertos debidamente probados y puestos en ambiente de producción del sistema.
Componente de Apropiación del Sistema	Informes, listados de asistencia y material gráfico de las campañas de socialización.
	Material de comunicación usado en las actividades.

	Listados de asistencia, material fotográfico de las capacitaciones y talleres realizados.
	Listados de asistencia, material fotográfico de las pruebas de navegación asistidas.
	Informe y presentación de las actividades realizadas en la estrategia digital
	Documento del plan de gestión del cambio conformado por la matriz de interesados, el plan de comunicación y el plan de formación, de acuerdo con los lineamientos institucionales.
	Informes de seguimiento plan de gestión del cambio.
	Para cada trámite o servicio gestionado en el aplicativo diseñar un folleto informativo con el proceso actualizado de autogestión, en formato imprimible, para facilitar su socialización con la ciudadanía.
Desarrollo del Módulo de plan de gestión del riesgo para establecimientos de autogestión	Entendimiento de la necesidad y refinamiento de los requisitos técnicos.
	Verificación de la viabilidad de ajustar la integración entre SIGESH y SIRMED, de acuerdo a las necesidades de los ajustes a autogestión
	Historias de usuario
	Diseño de experiencia de usuario (Mockups y prototipos interactivos
	Socialización del módulo y despliegue en pre producción
	Realización de pruebas y ajustes al desarrollo
	Socialización del módulo y despliegue en producción
Ajustes y mejoras al módulo de inspecciones a establecimientos	Ajustes a las funcionalidades del módulo de establecimientos en los roles solicitados, de acuerdo con el listado de priorización remitido por el equipo de trabajo. Ver título 3.2.1.2
Ajustes y mejoras al módulo de inspecciones a piscinas	Reestructuración del módulo de inspecciones a piscinas de acuerdo con los requerimientos funcionales y normativos establecidos incluyendo entendimiento de la necesidad y refinamiento de los requisitos técnicos.
	Socialización del módulo y despliegue en pre producción.
	Realización de pruebas y ajustes al desarrollo.
	Socialización del módulo y despliegue en producción.
	Ajustar los roles para identificar el inspector de piscinas
	Optimizar el diseño del tablero (dashboard) para presentar información relevante y de consulta rápida, integrando enlaces directos que permitan la navegación inmediata al requerimiento específico mediante un clic.
Ajustes e implementación del módulo de	Ajuste de integración con el sistema de información Ventanilla Única, capturando información a través de formularios y documentos requeridos por los equipos del DAGRD para la gestión del trámite.

gestión de eventos de aglomeración masiva	Optimizar el diseño del tablero (dashboard) para presentar información relevante y de consulta rápida, integrando enlaces directos que permitan la navegación inmediata al requerimiento específico mediante un clic.
	Incluir en el registro de la solicitud del evento, los datos de aforo y otros campos requeridos para la inspección y emisión del concepto.
	Incluir las plantillas de las notificaciones que sean editables en el rol de administrador al igual que establecimientos.
	Incluir en el rol de administrador la visualización de todos los trámites en cada bandeja y debe haber una opción que diga histórico (histórico de las solicitudes tramitadas al igual que establecimientos).
Ajustes e implementación del módulo de gestión de parques permanentes e itinerantes	Ajuste de integración con el sistema de información Ventanilla Única, capturando información a través de formularios y documentos requeridos por los equipos del DAGRD para la gestión del trámite.
	Optimizar el diseño del tablero (dashboard) para presentar información relevante y de consulta rápida, integrando enlaces directos que permitan la navegación inmediata al requerimiento específico mediante un clic.
	Incluir en el registro de la solicitud los datos de registro de atracciones, aforo, datos del profesional SST que avala el plan de emergencias, y otros campos requeridos para la inspección y emisión del concepto.
	Ajustar el flujo diferenciado la plantilla cuando el concepto es favorable o desfavorable.
	Incluir las plantillas de las notificaciones que sean editables en el rol de administrador al igual que establecimientos.
	Incluir en el rol de administrador la visualización de todos los trámites en cada bandeja y debe haber una opción que diga histórico (histórico de las solicitudes tramitadas al igual que establecimientos).
Ajustes e implementación del módulo de gestión de show de pirotecnia	Ajuste de integración con el sistema de información Ventanilla Única, capturando información a través de formularios y documentos requeridos por los equipos del DAGRD para la gestión del trámite.
	Optimizar el diseño del tablero (dashboard) para presentar información relevante y de consulta rápida, integrando enlaces directos que permitan la navegación inmediata al requerimiento específico mediante un clic.
	Ajustar el flujo diferenciado la plantilla cuando el concepto es favorable o desfavorable.
	Incluir en el registro de la solicitud los datos de registro del personal a cargo de la activación de la pirotecnia y otros campos requeridos para la inspección y emisión del concepto.

	Incluir las plantillas de las notificaciones que sean editables en el rol de administrador al igual que establecimientos.
	Incluir en el rol de administrador la visualización de todos los trámites en cada bandeja y debe haber una opción que diga histórico (histórico de las solicitudes tramitadas al igual que establecimientos).
Ajustes e implementación del módulo de gestión de acreditaciones a operadores logísticos	Estructuración de gráficos en el módulo de reportes.
	Incluir las plantillas de las notificaciones que sean editables en el rol de administrador al igual que establecimientos.
	Incluir en el rol de administrador la visualización de todos los trámites en cada bandeja y debe haber una opción que diga histórico (histórico de las solicitudes tramitadas al igual que establecimientos).
	Ajustar en el rol de ciudadano las empresas que están registradas, una tabla que visualice las acreditaciones en cada columna si está acreditada o está en trámite de esta manera el usuario tiene una visual de las acreditaciones que cuenta cada empresa.
	Ajustar en cada rol que se pueda visualizar un resumen de la empresa el estado de las acreditaciones que tiene y la que están en trámite.

5.2.3 Bomberos en Línea

Soporte y mantenimiento	Informe de gestión mensual que dé cuenta de la planeación, gestión, implementación y seguimiento de las acciones de soporte, mantenimiento preventivo y correctivo.
	Solución de los incidentes que actualmente se encuentran abiertos debidamente probados y puestos en ambiente de producción del sistema.
Componente de Apropiación del Sistema	Informes, listados de asistencia y material gráfico de las campañas de socialización.
	Material de comunicación usado en las actividades.
	Listados de asistencia, material fotográfico de las capacitaciones y talleres realizados.
	Listados de asistencia, material fotográfico de las pruebas de navegación asistidas.
	Informe y presentación de las actividades realizadas en la estrategia digital
	Documento del plan de gestión del cambio conformado por la matriz de interesados, el plan de comunicación y el plan de formación, de acuerdo con los lineamientos institucionales.
	Informes de seguimiento plan de gestión del cambio.

Ajustes e implementación del módulo de nómina	Realizar ajustes finales al desarrollo para la aprobación masiva de novedades, la validación de horas extras generadas en los equipos del Centro formación y seguridad humana, permitiendo visualizar la trazabilidad de la aprobación de estas y verificando los topes máximos establecidos, así como generar una funcionalidad que permita la supervisión de horas extra.
	Realizar ajustes en el módulo de gestión de novedades de nómina, mediante el cual sea posible la intercomunicación de este módulo con el de novedades de personal y el módulo de minuta del centro de formación.
Desarrollo e implementación de un módulo para la gestión de horas extras, recargos y compensatorios de la Secretaría de Seguridad y Convivencia del Distrito de Medellín	Verificar la factibilidad del desarrollo e implementación de un módulo para la gestión de horas extras, recargos y compensatorios de la Secretaría de Seguridad y Convivencia del Distrito de Medellín, que permita gestionar de forma centralizada, automatizada y con trazabilidad completa el registro de horas extras, recargos y compensatorios causados, el control de saldos con fechas de prescripción, el flujo digital de solicitudes de disfrute y la generación de archivos de integración con SAP , con el fin de garantizar la eficiencia operativa, la transparencia en la gestión del talento humano y el cumplimiento de las obligaciones laborales con los servidores públicos de la Secretaría de Seguridad y Convivencia.
Ajustes e implementación del módulo de novedades de personal	Realizar ajustes finales al desarrollo, posterior a la realización de pruebas e inicio de la fase de implementación con los actores de interés que se ven impactados con la puesta en marcha del sistema.
	Configurar el control de acceso basado en roles (RBAC) para restringir la visualización y edición de la información exclusivamente a las funciones asignadas a cada perfil de usuario.
	Optimizar la interfaz de usuario para mejorar su usabilidad y accesibilidad, integrando herramientas de autoayuda y guías contextuales que faciliten la ejecución de las actividades tanto para el personal bomberil como para los usuarios externos.
	Optimizar el diseño del tablero (dashboard) para presentar información relevante y de consulta rápida, integrando enlaces directos que permitan la navegación inmediata al requerimiento específico mediante un clic.
	Habilitar una funcionalidad de carga masiva mediante archivos de Excel, PDF, Word con plantillas predefinidas, para agilizar el registro y actualización de la información del personal bomberil
	Implementar un perfil de Superadministrador con privilegios de gestión integral sobre roles, configuraciones y asignaciones. Este rol deberá permitir la generación de reportes y ajustes operativos, garantizando en

	todo momento la inalterabilidad de la trazabilidad y la integridad histórica de los trámites.
Ajustes e implementación del módulo de novedades de vehículos	Realizar ajustes finales al desarrollo, posterior a la realización de pruebas e inicio de la fase de implementación con los actores de interés que se ven impactados con la puesta en marcha del sistema.
	Validar la factibilidad de la integración con el sistema de información SIGAI, de la Secretaría de suministros, buscando que esta dependencia, como dueña del proceso de gestión de vehículos en el Distrito, cuente con información de primera mano respecto a las novedades registradas en los vehículos de emergencias.
	Validar la factibilidad de la integración con el sistema de información AM, mediante el cual se pueda remitir la información de las novedades de vehículos reportadas que requieran la generación de ordenes de trabajo y, de esta manera facilitar la gestión de solicitudes con el contratista a cargo de los mantenimientos y reparaciones de los vehículos.
	Configurar el control de acceso basado en roles (RBAC) para restringir la visualización y edición de la información exclusivamente a las funciones asignadas a cada perfil de usuario.
	Optimizar la interfaz de usuario para mejorar su usabilidad y accesibilidad, integrando herramientas de autoayuda y guías contextuales que faciliten la ejecución de las actividades tanto para el personal bomberil como para los usuarios externos.
	Optimizar el diseño del tablero (dashboard) para presentar información relevante y de consulta rápida, integrando enlaces directos que permitan la navegación inmediata al requerimiento específico mediante un clic.
	Habilitar una funcionalidad de carga masiva mediante archivos de Excel, PDF, Word con plantillas predefinidas, para agilizar el registro y actualización de la información de vehículos.
Ajustes e implementación del módulo locativas	Realizar ajustes finales al desarrollo, posterior a la realización de pruebas e inicio de la fase de implementación con los actores de interés que se ven impactados con la puesta en marcha del sistema.
	Configurar el control de acceso basado en roles (RBAC) para restringir la visualización y edición de la información exclusivamente a las funciones asignadas a cada perfil de usuario.
	Optimizar la interfaz de usuario para mejorar su usabilidad y accesibilidad, integrando herramientas de autoayuda y guías contextuales que faciliten la ejecución de las actividades tanto para el personal bomberil como para los usuarios externos.

	Optimizar el diseño del tablero (dashboard) para presentar información relevante y de consulta rápida, integrando enlaces directos que permitan la navegación inmediata al requerimiento específico mediante un clic.
	Habilitar una funcionalidad de carga masiva mediante archivos de Excel, PDF, Word con plantillas predefinidas, para agilizar el registro y actualización de la información.
Ajustes e implementación del módulo de Herramientas Equipos y Accesorios, de acuerdo con el plan de gestión de cartera, incluyendo la validación de la implementación de un piloto para registro de las HEA´s mediante integración de RFID	Se requiere evaluar la viabilidad técnica para la implementación de un sistema de control de inventario automatizado en los vehículos de emergencia mediante tecnología RFID o la tecnología que aplique, con el objetivo de garantizar el alistamiento completo de los equipos en las gavetas previo a la salida a cada atención y ejecutar una validación de retorno al reingreso a la estación, asegurando así la trazabilidad y disponibilidad permanente de los activos; para lo cual solicitamos una propuesta técnica y económica que incluya las especificaciones del hardware, lectores y etiquetas, así como una descripción de la arquitectura de integración con nuestro sistema actual, los tiempos estimados de implementación y el soporte postventa requerido.
	Implementar un módulo de gestión de activos individuales que permita asociar el equipo y herramientas de dotación al perfil de cada bombero, facilitando el seguimiento y control de los elementos bajo su responsabilidad directa.
	Desarrollar un módulo de gestión de inventarios centralizado que permita el control total de los equipos y herramientas, categorizando su ubicación en: personal (asignado a bomberos), estaciones y bodega central. El sistema debe garantizar la trazabilidad de los movimientos, permitiendo registrar y monitorear el historial de préstamos entre estaciones, incluyendo fechas de salida, retorno y estado actual de los elementos.
	Optimizar la interfaz de usuario para mejorar su usabilidad y accesibilidad, integrando herramientas de autoayuda y guías contextuales que faciliten la ejecución de las actividades tanto para el personal bomberil como para los usuarios externos.
	Optimizar el diseño del tablero (dashboard) para presentar información relevante y de consulta rápida, integrando enlaces directos que permitan la navegación inmediata al requerimiento específico mediante un clic.
	Habilitar una funcionalidad de carga masiva mediante archivos de Excel, PDF, Word con plantillas predefinidas, para agilizar el registro y actualización de la información.

Ajustes e implementación del módulo de minuta de guardia	Realizar ajustes finales al desarrollo, posterior a la realización de pruebas e inicio de la fase de implementación con los actores de interés que se ven impactados con la puesta en marcha del sistema.
	El acceso a este módulo estará condicionado al inicio de sesión del bombero desde el equipo asignado a la guardia, habilitándose de manera automática tras la validación de sus credenciales.
	Configurar el control de acceso basado en roles (RBAC) para restringir la visualización y edición de la información exclusivamente a las funciones asignadas a cada perfil de usuario.
	Optimizar la interfaz de usuario para mejorar su usabilidad y accesibilidad, integrando herramientas de autoayuda y guías contextuales que faciliten la ejecución de las actividades tanto para el personal bomberil como para los usuarios externos.
	Optimizar el diseño del tablero (dashboard) para presentar información relevante y de consulta rápida, integrando enlaces directos que permitan la navegación inmediata al requerimiento específico mediante un clic.
Ajustes e implementación del módulo de minuta del centro de formación	Realizar ajustes finales al desarrollo, posterior a la realización de pruebas e inicio de la fase de implementación con los actores de interés que se ven impactados con la puesta en marcha del sistema.
	Desarrollar una interfaz de control para la gestión académica del personal, donde el coordinador pueda consultar perfiles, monitorear la vigencia de certificaciones mediante alertas y gestionar inscripciones a cursos de manera ágil, optimizando el ciclo de actualización de competencias del cuerpo de bomberos.
	Configurar el control de acceso basado en roles (RBAC) para restringir la visualización y edición de la información exclusivamente a las funciones asignadas a cada perfil de usuario.
	Optimizar la interfaz de usuario para mejorar su usabilidad y accesibilidad, integrando herramientas de autoayuda y guías contextuales que faciliten la ejecución de las actividades tanto para el personal bomberil como para los usuarios externos.
	Optimizar el diseño del tablero (dashboard) para presentar información relevante y de consulta rápida, integrando enlaces directos que permitan la navegación inmediata al requerimiento específico mediante un clic.
	Habilitar una funcionalidad de carga masiva mediante archivos de Excel, PDF, Word con plantillas predefinidas, para agilizar el registro y actualización de la información del personal bomberil

Ajustes e implementación del módulo de seguridad humana	Realizar ajustes finales al desarrollo, posterior a la realización de pruebas e inicio de la fase de implementación con los actores de interés que se ven impactados con la puesta en marcha del sistema.
	Integrar el módulo con el sistema de información SIGESH, permitiendo que se pueda generar un informe consolidado de todas las actividades que realiza el equipo con relación a los trámites y servicios gestionados.
	Habilitar una funcionalidad de carga masiva mediante archivos de Excel, PDF, Word con plantillas predefinidas, para agilizar el registro y actualización de la información del personal bomberil
	Configurar el control de acceso basado en roles (RBAC) para restringir la visualización y edición de la información exclusivamente a las funciones asignadas a cada perfil de usuario.
	Optimizar la interfaz de usuario para mejorar su usabilidad y accesibilidad, integrando herramientas de autoayuda y guías contextuales que faciliten la ejecución de las actividades tanto para el personal bomberil como para los usuarios externos.
	Optimizar el diseño del tablero (dashboard) para presentar información relevante y de consulta rápida, integrando enlaces directos que permitan la navegación inmediata al requerimiento específico mediante un clic.
Desarrollo del módulo de mapa humano	Desarrollar el módulo de mapa humano en el cual sea posible contar con la información consolidada frente a la formación del personal del Cuerpo Oficial de Bomberos de Medellín. El desarrollo de este módulo deberá realizarse conforme a las historias de usuario remitidas por el Departamento Administrativo de Gestión del Riesgo de Desastres.
	Entendimiento de la necesidad y refinamiento de los requisitos técnicos.
	Validación y Ajustes a las historias de usuario
	Diseño de experiencia de usuario (Mockups y prototipos interactivos
	Socialización del módulo y despliegue en pre producción
	Realización de pruebas y ajustes al desarrollo
	Socialización del módulo y despliegue en producción

Centro Administrativo Distrital CAD
Calle 44 N° 52-165. Código Postal 50015
Línea de Atención a la Ciudadanía: 604 44 44 144
Conmutador: 604 385 55 55 Medellín - Colombia

CO17/7740