Alcaldía de Medellín
Distrito de
Ciencia, Tecnología e Innovación

LINEAMIENTOS SOBRE ADQUISICIÓN, DESARROLLO, USO Y APROPIACIÓN DE SOLUCIONES TECNOLÓGICAS EN LA ALCALDÍA DE MEDELLÍN

PROCESO
GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

SECRETARÍA DE INNOVACIÓN DIGITAL
DISTRITO ESPECIAL DE CIENCIA TECNOLOGÍA E INNOVACION DE MEDELLÍN

Versión 6.0
Julio 2025

Hoja de autorizaciones

Elaboró:	Revisó:	Aprobó:
Julio 2025	**Julio 2025**	**Julio 2025**
Secretaría de Innovación Digital: Subsecretaria de Ciudad Inteligente -Equipo Sistemas de Información -Equipo Territorio Inteligente -Unidad de Innovación Subsecretaria de Servicios de TI -Unidad de Infraestructura -Unidad de Gestión Documental -Unidad de Seguridad Informática	Secretaría de Innovación Digital: Subsecretaria de Ciudad Inteligente -Equipo Sistemas de Información -Unidad de Innovación Subsecretaria de Servicios de TI	Secretaría de Innovación Digital: Subsecretaria de Ciudad Inteligente -Equipo Sistemas de Información

Control de versiones

Versión	Fecha	Numeral Modificado	Elaboró	Revisó	Aprobó
2	17/06/2022	Subnumerales adicionados: 5.12 - 5.12.1 - 5.12.2 – 5.12.3 y Numeral 9.0 actualizado.	Jaime Rubiel Gil Ossa Lubián Cartagena Durango	Idolfo Delgado Cano	Juan Sebastián González Flórez
3	26/07/2022	Se actualiza: Numeral 3: Dominio Sistemas de Información - Apartados (3.1 - 3.2 - 3.3 - 3.3.1 - 3.3.2 - 3.3.3 - 3.3.4 - 3.4.1 - 3.4.1.1 - 3.4.2 - 3.4.3 - 3.4.4 - 3.5 - 3.5.1 - 3.5.3 - 3.5.4.1 - 3.5.4.2 - 3.5.4.3 - 3.5.4.4 - 3.5.6 - 3.5.7 - 3.6 - 3.6.1.1 - 3.6.1.2 - 3.6.1.3 - 3.6.2.1 - 3.6.2.2 - 3.6.3.1 - 3.6.3.2 - 3.6.4 - 3.6.4.1 y 3.7) Numeral 4: Dominio Protocolo Calidad del Dato – Apartado (4.6) Numeral 8: Dominio Uso y Apropiación – Apartado (8.2.1 – 8.2.1.1)	Denny Ruiz Trujillo Lubián Cartagena Durango Astrid Elena Valencia Ruiz	Idolfo Delgado Cano	Juan Sebastián González Flórez
4	11/10/2023	Se actualiza: Dominio Infraestructura Numeral 5: - Apartados (5.1 - 5.1.1 – 5.1.2 – 5.2 – 5.2 – 5.2.1 – 5.2.2 – 5.2.3 – 5.3 – 5.3.1 – 5.4 – 5.5 – 5.6 – 5.7.1 – 5.7.2 – 5.8 – 5.9 – 5.9.1 – 5.9.2 – 5.9.3 – 5.9.4 – 5.9.5 – 5.9.6) Apartados (5.10 – 5.11 – 5.12) fueron eliminados	Carlos Botero Londoño	Idolfo Delgado Cano	Rivier Hernando Gomez Cuevas

Versión	Fecha	Numeral Modificado	Elaboró	Revisó	Aprobó
		Se actualiza: Dominio sistemas de información Numeral 3: - Apartados (3.4.4) Se actualiza: Dominio Uso y Apropiación Numeral 8: - Apartados (8.1 – 8.2) Apartado (8.3) fue adicionado	Denny Ruiz Trujillo Adilia Lopera Astrid Elena Valencia Ruiz		
5	28/04/2025	Se actualiza: **Dominio sistemas de información** Numeral 2 - Subnumerales ajustados (2.3.1 y 2.5.4.3) **Dominio Territorio Inteligente y Analítica de Datos** Numeral 3 Subnumerales ajustados: 3.1- 3.2 - 3.3 - 3.4 - 3.5 - 3.6 - 3.7 - 3.8 - 3.9 - 3.10 - 3.11 Subnumerales adicionados: 3.8.1 - 3.9.1 - 3.9.2 - 3.12 - 3.13 - 3.14 - 3.15 Subnumerales retirados: 3.4.1 - 3.4.2 - 3.4.3 - 3.4.4 **Dominio de Infraestructura Tecnológica de TI** Numeral 4 Subnumerales ajustados (4.5-4.7-4.7.1-4.8-4.9) Subnumerales adicionados: 4.8.1-4.8.1.1-4.8.1.2-4.8.2-4.9.1-4.9.2 **Dominio Uso y Apropiación de TIC** Numeral 7 Subnumerales ajustados: 7.1-7.2-7.3-7.3.1-7.3.1.1-7.3.1.2-7.4 Subnumerales adicionado: 7.5 Anexos ajustados: Matriz de interesados (actualización del formulario) Plan de Comunicaciones (actualización del formulario) Plan de Formación (actualización del formulario)	Jhon A. Betancur Fredy Emilio Mosquera Lubian Cartagena Durango Carlos Botero Astrid Elena Valencia Ruiz Adilia Lopera Yepes	Idolfo Delgado Cano	Santiago Restrepo Arroyave
6	22/7/2025	Se adiciona: **Capítulo 7** Lineamientos técnicos generales sobre: - Transformación Digital del Distrito a Servicios Cloud	Diana María Ochoa Henao	Idolfo Delgado Cano	Santiago Restrepo Arroyave

INTRODUCCIÓN 10

1. DOMINIO SISTEMAS DE INFORMACIÓN 13

1.1 Objetivo 13

1.2 Disposiciones generales 13

1.2.1 Responsabilidad del proceso contractual 13

1.2.2 Registro de activos 13

1.2.3 Cesión de derechos patrimoniales 14

1.2.4 Soporte y mantenimiento 16

1.3 Arquitectura de sistemas de información 16

1.3.1 Visión general 16

1.3.2 Descripción por componentes 17

1.3.3 Ambientes 19

1.3.4 Estructura de Datos 19

1.4 Almacenamiento 20

1.4.1 Estándares de bases de datos 20

1.4.2 Diccionario de datos 22

1.4.3 Creación de Bases de Datos 24

1.4.4 Variables de Enfoque Diferencial 24

1.5 Desarrollo e implementación 25

1.5.1 Marcos de referencia de trabajo (Metodología) 25

1.5.2 Accesibilidad 26

1.5.3 Diseño 27

1.5.4 Implementación 28

1.5.5 Conexión a Base de datos 37

1.5.6 Seguridad de aplicaciones 37

1.5.7 Calidad del desarrollo de software 42

1.5.8 Interoperabilidad 44

1.5.9 Power Apps 46

1.6 Entregables 46
1.6.1 Proyectos para nuevos desarrollos 46
1.6.2 Proyectos de adquisición 49
1.6.3 Proyectos de servicios de Sistemas de información en la nube (SaaS) 50
1.6.4 Proyectos de renovación de soporte y servicios 51
1.6.5 Elementos de validación 52

2. DOMINIO GESTIÓN Y APERTURA DE DATOS 68
2.1 Alcance 68
2.2 Términos utilizados en el dominio 68
2.3 Objetivo 71
2.4 Datos, Información, Conocimiento 73
2.5 Disposiciones Generales 74
2.6 Gestión del Ciclo de Vida de los Datos 77
2.6.1 Clasificación de los datos 78
2.6.2 Documentación de los datos 82
2.6.3 Establecimiento de Políticas de Retención: 82
2.6.4 Procedimientos para Eliminación Segura: 82
2.6.5 Uso y Distribución: 83
2.7 Gobierno de la infraestructura de Datos 83
2.8 Arquitectura de Datos 83
Cumplimiento de Estándares Técnicos 85
2.9 Calidad de Datos 86
2.9.1 Importancia de la Calidad de los Datos 88
2.9.2 Lineamientos para la Gestión de la Calidad de Datos 88
2.9.3 Anonimización de Datos 90

2.10 Estructuración de los datos 91
2.10.1 Estándar de variables unificadas para la construcción de bases de datos..... 93
2.10.2 Apertura de datos..... 93
2.11 Plataforma de ciudad inteligente – Fiware 94
2.12 Disposiciones finales..... 95

3. DOMINIO INFRAESTRUCTURA TECNOLÓGICA DE TI..... 96
3.1 Equipos de Telecomunicaciones..... 97
3.1.1 Consideraciones generales 97
3.1.2 Plataforma de Red LAN..... 98
3.2 Equipos de cómputo..... 99
3.2.1 Equipos de Cómputo de Escritorio 101
3.2.2 Estación de Ingeniería (WORKSTATION) 104
3.2.3 Equipos de Cómputo Portátiles 107
3.3 Motores de Bases de datos..... 109
3.3.1 Desarrollos vs Bases De Datos 109
3.3.2 Uso de Software libre y Open Source..... 111
3.4 Contenedores De Aplicaciones..... 113
3.5 Sistemas Operativos..... 114
3.6 Servidores 115
3.6.1 Adquisición de Servidores 115
3.6.2 Aprovisionamiento de Servidores 116
3.6.3 Respaldo y Recuperación 117
3.7 Almacenamiento 119
3.7.1 Adquisición..... 119
3.7.2 Uso información no estructurada..... 122
3.7.3 Información estructurada..... 122

4. DOMINIO SEGURIDAD INFORMÁTICA 124

4.1 Objetivo 124

4.2 Contexto 124

4.3 Casos de uso para estos lineamientos 124

4.4 Principios para la aprobación de aplicaciones y sistemas de Información en la Alcaldía de Medellín..... 125

4.5 Entregables 129

5. DOMINIO GESTIÓN DOCUMENTAL ELECTRÓNICA..... 131

5.1 Objetivo 131

5.2 Contexto 131

5.3 Contexto de la Preservación Digital 133

5.3.1 Alcance de la Política de Preservación Digital 134

5.3.2 Principios de la Preservación Digital..... 134

5.4 Lineamientos Técnicos para la gestión documental electrónica 136

5.4.1 Aval Técnico proceso de gestión documental electrónica..... 136

5.4.2 Definir documentos Electrónicos (E.Docs) a preservar..... 137

5.4.3 Gestionar los documentos Electrónicos de archivo (E.Docs)..... 141

5.4.4 Uso de formatos de Archivo para la gestión de documentos de archivo (E.Docs) 143

5.4.5 Integración con Soluciones de Tecnología 144

5.4.6 Autenticidad, Integridad y Fiabilidad de los documentos electrónicos (E-Docs). 149

5.4.7 Procesos de digitalización certificada con finas probatorios. 150

5.4.8 Utilizar Metadatos de preservación..... 154

6. DOMINIO USO Y APROPIACIÓN DE TIC 158
6.1 Antecedentes 158
6.2 Lineamientos de Uso y Apropiación 159
6.3 Gestión del Cambio 161
6.3.1 Objetivos De La Gestión Del Cambio 162
6.3.2 Formulación del Plan de Gestión del Cambio 163
6.3.3 Seguimiento del Plan de Gestión del Cambio 174
6.3.4 Medición de resultados 175
6.4 Anexos 177

7. TRANSFORMACIÓN DIGITAL DEL DISTRITO A SERVICIOS CLOUD 179
7.1 Introducción 179
7.2 Principios Generales 180
7.3 Principios Rectores 182
7.4 Gobierno y Roles (RBAC) 182
7.5 Arquitectura de Referencia en Azure 183
7.6 Seguridad y Cumplimiento 185
7.7 Descripción de componentes del perímetro de red en la nube 187
7.8 Descripción de componentes de acceso seguro a la nube 188
7.9 Componentes para exponer servicios al exterior — 189
7.10 DevSecOps y Calidad del software 190
7.11 Requisitos obligatorios para cada despliegue 191
7.12 Entregables que el equipo debe aportar 191
7.13 Microservicios y Contenedores 191
7.13.1 Azure Red Hat OpenShift (ARO) 192
7.13.2 Azure Container Registry (ACR) 193

7.13.3 Requisitos transversales 194
7.14 Descripción de componentes de bases de datos: 195
7.15 Descripción de componentes de analítica avanzada 196
7.15.1 Objetivo 196
7.15.2 Disposiciones Generales 196
7.16 Arquitectura de Analítica e IA sobre Azure 197
7.16.1 Lineamientos Técnicos para Proyectos de Analítica e IA 199
7.16.2 Lineamientos Éticos 199
7.16.3 Gobernanza del Dato y de la IA 200
7.16.4 Casos de Uso Prioritarios 200
7.17 Costos, Gobernanza y Optimización 201
7.17.1 Operación y Monitoreo 201
7.17.2 Costos y Optimización (Cost Management) 201
7.18 Gestión de Cambios 202
7.19 Anexo - Despliegue_Azur.drawio.pdf - 203
7.20 Glosario de términos técnicos 204
7.21 Aplicación Obligatoria 209

8. GLOSARIO 210

INTRODUCCIÓN

En virtud del Decreto 863 de 2015 de la Alcaldía de Medellín, en su artículo 333A, se indica que la Secretaría de Innovación Digital como dependencia del nivel central, es responsable de :*"Satisfacer las necesidades de servicios de Tecnologías de la información a los diferentes grupos de valor y de interés, a través de servicios digitales, procesos eficientes, flujos de datos e información, y transformación digital del territorio, basados en la innovación y en una gestión enfocada en prácticas de arquitectura empresarial y la Seguridad de la información."*

Basado en lo anterior, este documento contiene los lineamientos que rigen en la Alcaldía de Medellín, para el desarrollo y/o adquisición de sistemas de información (software), que requieran las dependencias para el logro de su misión y el apoyo de sus procesos; plantear las definiciones y estándares, como guía a las diferentes dependencias para el manejo de los datos y el diseño de modelos de datos estructurados y no estructurados, minimizando el impacto negativo de las inconsistencias en los conjuntos de datos generados; facilitar a las dependencias la definición de la infraestructura tecnológica necesaria para desarrollar sus proyectos y; los diferentes aspectos en materia de seguridad informática que deberán ser tenidos en cuenta en lo anteriormente expuesto de este acápite.

De acuerdo al Decreto 1204 de 2020 de la Alcaldía de Medellín, en su artículo 2:

"Toda contratación que conlleve componentes tecnológicos, deben contar con aval técnico que emita la Secretaría de Innovación Digital.". En este orden de ideas todo proyecto de adquisición, desarrollo o evolución de sistemas de información debe realizar el proceso para obtener el aval técnico de la Secretaría de Innovación Digital.

Los lineamientos acá expuestos deberán ser cumplidos por cada una de las dependencias y/o través de sus proveedores con el acompañamiento de la Secretaría de Innovación Digital. Este cumplimiento hará parte de la toma de decisiones para la emisión de los avales técnicos por parte de esta Secretaría y alineado con las políticas de adquisición de bienes y servicios definidas por la Secretaría de Servicios y Suministros y están dirigidos hacia las dependencias que lo solicitan como parte de la incorporación de servicios tecnológicos en la entidad. Es de aclarar que los proyectos propios de la Secretaría de Innovación Digital NO requerirán de aval técnico.

Estos lineamientos están definidos con base la Política de Gobierno Digital, la cual está consignada en el Decreto 767 de 2022 y teniendo en cuenta que la Secretaría de Innovación Digital tiene como función: *"Planear, dirigir, desarrollar, implementar, controlar y mejorar los servicios de tecnologías de la información del Municipio de Medellín con el fin de brindar soluciones óptimas e integrales a los diferentes procesos de la entidad*" establece a través de este compendio las bases para la adecuada gestión y gobierno de las tecnologías de la información y las comunicaciones -TIC en la entidad.

El documento se divide en diferentes dominios basados en componentes que integran la Política de Gobierno Digital, los cuales agrupan los lineamientos a seguir por parte de las diferentes dependencias de la alcaldía y/o los proveedores de éstas, sobre las soluciones a necesidades en materia de tecnologías de la información y las comunicaciones.

Los lineamientos descritos en este documento deben hacer parte de las obligaciones del contratista o proveedor para desarrollos y contrataciones externas y deben quedar explícitos en la documentación del proceso de contratación. Además, todas las implementaciones realizadas al interior de la Alcaldía de Medellín deberán cumplir con lo dispuesto en este documento.

La implementación y cumplimiento de los lineamientos acá descritos, permitirán mejorar las capacidades institucionales mediante el uso adecuado de las TIC y su alineación con las necesidades de la Alcaldía de Medellín, logrando ofrecer de esta forma mejores servicios a los ciudadanos.

1. Dominio Sistemas de Información

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.

1.2 Disposiciones generales

1.2.1 Responsabilidad del proceso contractual

La responsabilidad de los procesos contractuales y de la supervisión para la adquisición, desarrollo, evolución, soporte y/o mantenimiento de los sistemas de información avalados por la Secretaría de Innovación Digital, deben estar a cargo de la secretaría donde el sistema de información es usado para la ejecución de sus procesos misionales.

1.2.2 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.

1.2.3 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 las mismas.

1.2.4 Soporte y mantenimiento

Por lineamientos TIC institucionales, todo sistema de información debe contar con un contrato de soporte, mantenimiento y actualización vigente que garantice su correcta operación en el tiempo.

Las dependencias dueñas del proceso que soporta el sistema de información, deben contemplar los recursos y tramitar un nuevo contrato con antelación a la finalización del mismo para dar continuidad al servicio y el cual debe seguir el proceso de avales internos de la entidad. Toda solución comercial adquirida en el mercado debe incluir dentro del contrato el modo de entrega e implementación del producto y que el proveedor debe realizar el acompañamiento necesario para entregarlo 100% funcional y estable en la infraestructura de la Alcaldía de Medellín.

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.

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 a 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.

1.3.2 Descripción por componentes

1.3.2.1 Desarrollo componentes iniciales: Modulo

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.

1.3.2.2 Desarrollo API de la lógica Alcaldía 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.

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

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 contratista.

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 pre-producción de la Alcaldía de Medellín para pruebas funcionales y posteriormente en el ambiente productivo para el inicio de la operación.

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.

1.4 Almacenamiento

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.

1.4.1.1 Estructura

Definición de las tablas con sus respectivas llaves primarias y llaves foráneas. Los estándares que deben estar asociados a los diferentes objetos son los siguientes:

- El modelo entidad relación debe estar normalizado hasta la tercera forma normal al momento de ser creada en un ambiente productivo, en caso de que por necesidad de la herramienta en la cual está desarrollado el aplicativo no se pueda relacionar la base de datos, se debe justificar en un documento anexo haciendo referencia al porque no se relacionan las tablas, indicando que dicha situación no afectará el rendimiento del servidor.

- Todos los objetos (tablas, campos, procedimientos, paquetes, funciones, vistas) asociados a las BD deben estar documentados, los diferentes motores de BD dentro de su arquitectura permiten documentar los objetos ya sea de forma descriptiva en los campos dispuestos para esta función o a través del mismo código dentro de los procedimientos, paquetes o funciones.

- La documentación debe contener información que describa la funcionalidad del objeto dentro del proceso de una forma básica, clara y concisa de tal forma que cualquier persona que necesite conocer el diccionario de la BD lo pueda entender.

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

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 a 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 a 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.

[9] https://colaboracion.dnp.gov.co/CDTI/Oficina%20Informatica/Sistemas%20de%20informaci%C3%B3n/Gu%C3%ADas%20Formatos%20Plantillas/Gu%C3%ADa%20Definici%C3%B3n%20de%20Diccionario%20de%2 0Datos.pdf

- 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.

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.

1.4.4 Variables de Enfoque Diferencial

De acuerdo a la Política Pública LGBTI de Medellín la cual “se adopta para el reconocimiento de la diversidad sexual e identidades de género y para la protección, restablecimiento, atención y garantía de derechos de las personas lesbianas, gays, bisexuales, transgeneristas, e intersexuales (LGTBI) del Municipio de Medellín”, se determina que todos los sistemas de información del Distrito de Medellín que sean susceptibles de implementar variables de enfoque diferencial, deben incluir la variable sexo, orientación sexual e identidad de género para garantizar una caracterización completa del ciudadano. Por consiguiente, cada dependencia es responsable de validar y gestionar la inclusión de dichas variables en sus sistemas de información.

Las categorías mencionadas anteriormente se definen como:

Sexo: Diagnóstico y asignación médica que se realiza de acuerdo con la anatomía sexual de cada persona. Este dictamen se realiza usualmente con base en los genitales visibles, sin considerar las hormonas, los cromosomas y las gónadas.

Orientación sexual: Hay quienes la denominan como orientación género-afectiva para dar cuenta que, en primera instancia lo que genera a atracción es la expresión

de género y no la anatomía sexual que en la mayoría de los casos no se conoce hasta el encuentro sexual.

Identidad de género: La forma como cada persona vive y experimenta el género de manera que puede corresponder o no con el sexo que le fue asignado/diagnosticado al nacer.

Las diferentes categorías y opciones que los sistemas de información deben incluir específicamente, se encuentran relacionadas en el documento oficial publicado por parte del Departamento Administrativo de Planeación: DE-GINF-021 Estándar de Variables Unificadas Para Codificar y Estructurar Bases de Datos [10] . Este documento debe consultarse directamente en Isolucion, ya que su versión puede cambiar.

1.5 Desarrollo e implementación

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

[10] https://www.medellin.gov.co/Isolucion/BancoConocimiento4AlcaldiaMedellin/3/3389870ec5dd4576a87e217b63964af2/EstandardevariablesparalacaracterizaciondebeneficiariospersonasnaturalesV4.xlsx

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 Isolución (https://bit.ly/3eLqtiD) como insumo inicial del desarrollo.

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.

La política de gobierno digital indica que, de acuerdo con la caracterización de usuarios, ciudadanos y grupos de interés de la entidad, ésta debe garantizar que las páginas, portales y sistemas de información web, con sus respectivos contenidos, cuenten con características técnicas y funcionales que permitan al usuario percibir, entender, navegar e interactuar adecuadamente. Esto también incluye que las personas con discapacidad sensorial puedan acceder de manera autónoma e independiente a dichas páginas, portales y sistemas de información web. Se deben implementar pruebas de accesibilidad y usabilidad con los usuarios, para determinar ajustes a realizar y atributos a incorporar.

Así mismo, la entidad debe garantizar que los contenidos audiovisuales cuenten con audio descripción, subtitulado, transcripción en tiempo real (closed caption) y lengua

de señas. En ese orden, se puede priorizar los contenidos más relevantes, más usados o más demandados por los usuarios.

Para ello, se debe aplicar:

- Norma Técnica de Accesibilidad 5854 disponible en el sitio web del ICONTEC (INCONTEC, s.f.)
- La Guía interactiva de implementación de la NTC 5854 (MinTIC, s.f.)
- La guía de usabilidad disponible en el sitio web de Gobierno Digital (MinTIC, s.f.) [11]

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.

[11] https://estrategia.gobiernoenlinea.gov.co/623/articles-81473_recurso_1.pdf-pág 36

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.

1.5.4 Implementación

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.

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

[12] https://www.freecodecamp.org/news/clean-coding-for-beginners

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.

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 al 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.

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

Pautas y procedimientos para garantizar la seguridad, calidad y legalidad de las aplicaciones del Distrito de Medellín disponibles en las tiendas móviles (App Store y Google Play).

- Política de propiedad intelectual: Proteger los derechos de propiedad intelectual de los desarrolladores y evitar la publicación de aplicaciones que infrinjan derechos de autor, marcas registradas u otros derechos de propiedad intelectual.

- En caso de identificar una posible infracción de propiedad intelectual, se retirará inmediatamente la aplicación de la tienda y se notificará a la dependencia para que actúe según corresponda.
- Política de seguridad y privacidad: Las aplicaciones deben cumplir con estándares de seguridad y privacidad, incluyendo la protección de datos personales de los usuarios, la prevención de malware y la implementación de prácticas de seguridad sólidas, definidas en los lineamientos de la Secretaría de Innovación Digital.
- Política de calidad: Toda aplicación del Distrito de Medellín desplegada en las tiendas móviles debe cumplir los lineamientos de la Secretaría de Innovación Digital, incluyendo requisitos de funcionamiento, usabilidad y estabilidad; esto implica la evaluación de la interfaz de usuario, la ausencia de errores críticos y el rendimiento general de la aplicación.
- Política de actualizaciones y revisión de aplicaciones: Las aplicaciones que se desarrollen y/o actualicen dentro del marco de un contrato o por parte de personal del Distrito de Medellín, deberán haber sido aprobadas por la dependencia propietaria de la misma (esto incluye pruebas funcionales para garantizar el cumplimiento de los requisitos) y notificar a la Secretaría de Innovación Digital que se aprueba su despliegue en tiendas.
- Las aplicaciones móviles que se pretendan desplegar deben ser orientadas hacia las últimas versiones del sistema operativo liberado por los fabricantes. Esto puede incluir requisitos para la corrección o eliminación de vulnerabilidades

de seguridad, mantenimiento de las aplicaciones, así como la compatibilidad con nuevas versiones de sistemas operativos móviles.

- Política de comunicación con los usuarios: Los responsables técnicos y/o funcionales de las aplicaciones deberán responder a las preguntas, comentarios o quejas de los usuarios en la sección de reseñas. Se indicarán los plazos para la resolución de problemas y la disponibilidad de soporte técnico (los establecidos en la Ley 1755 de 2015).
- Política de permisos: Los desarrolladores tendrán acceso y permiso de publicación y/o modificación de las aplicaciones en las tiendas móviles, mientras exista un proyecto o contrato de desarrollo de software, soporte y mantenimiento.
- En caso de incumplimiento de los términos del proyecto o contrato de desarrollo, el Distrito se reserva el derecho de revocar a quien corresponda los permisos de publicación y modificación de las aplicaciones en las tiendas móviles.
- Política de transparencia: Todos los desarrolladores deberán proporcionar información precisa y completa sobre sus aplicaciones, incluyendo detalles sobre la funcionalidad, el propósito, cualquier costo asociado, documentación y código fuente de la aplicación.
- Política de revisión periódica: El equipo encargado de las tiendas virtuales móviles (App Store y Google Play), realizará la revisión periódica de las políticas de las tiendas cada seis meses, con el fin de asegurar que sigan siendo relevantes y efectivas en un entorno tecnológico en constante cambio.

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.

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.

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 a 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 MinTIC[13].

  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.

[13] https://www.mintic.gov.co/arquitecturati/630/w3-article-9263.html

- **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.

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]

[14] https://www.yeeply.com/blog/que-son-pruebas-unitarias

- **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.

[15] https://programacionymas.com/blog/tipos-de-testing-en-desarrollo-de-software

- **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.[16]

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.

16 https://mundotesting.com/etapas-de-pruebas-de-software-etapas-del-testing

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.

1.5.9 Power Apps

El Distrito Especial de Ciencia, Tecnología e Innovación de Medellín, dispone de un conjunto de aplicaciones, servicios, conectores y plataforma de datos a través de MS Power Apps para crear aplicaciones personalizadas que cubran necesidades básicas de las dependencias.

Los lineamientos acerca del alcance, el licenciamiento, las responsabilidades y el gobierno sobre esta plataforma deben consultarse con la Secretaría de Innovación Digital antes de emprender cualquier proyecto sobre esta herramienta.

1.6 Entregables

Todo proyecto de implementación de un Sistema de información debe cumplir con la siguiente documentación de acuerdo al tipo y etapa. Si por algún motivo no es posible entregar uno o varios de los documentos solicitados se deben justificar ante la secretaría de Innovación Digital.

1.6.1 Proyectos para nuevos desarrollos

1.6.1.1 Entregables al solicitar un concepto técnico al equipo de Sistemas de Información

Los entregables mínimos requeridos en un proyecto de desarrollo o evolución de sistemas de información son:

- Oficio de la solicitud del aval
- Documento de especificaciones técnicas
- Diagrama de Proceso
- Documento funcional o de requisitos del sistema de información a desarrollar
- Versión inicial del documento de arquitectura propuesta el cual deberá ser presentado ante el comité de arquitectura de software de la Secretaría de Innovación Digital para su aprobación antes de iniciar el desarrollo.

1.6.1.2 Entregables al momento de iniciar el proyecto

Los entregables mínimos requeridos en un proyecto de desarrollo o evolución de sistemas de información para la disciplina de Requisitos son:

- Impact Mapping (Opcional)
- User story Mapping
- Backlog del producto priorizado o lista de requerimientos priorizados.
- Historias de usuarios o Casos de uso.

1.6.1.3 Entregables al momento de terminar el proyecto

Los entregables mínimos requeridos en un proyecto de desarrollo o evolución de sistemas de información para la disciplina de Arquitectura de software son:

- Documento de arquitectura del sistema de información.
- 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 al numeral 3.4.2 definido en este documento

Los entregables mínimos requeridos en un proyecto de desarrollo o evolución de sistemas de información para la disciplina de Desarrollo son:

- 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.

Los entregables mínimos requeridos en un proyecto de desarrollo o evolución de sistemas de información para la disciplina de Pruebas son:

- Documento de diseño de pruebas
- Evidencia de pruebas
- Pruebas de rendimiento de requerirse y justificar en caso contrario (Concurrencia, Carga, estrés, entre otros)

Los Manuales mínimos requeridos en un proyecto de desarrollo o evolución de sistemas de información son:

- 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. (Información del Sistema para el Catálogo de Sistemas de información)

1.6.2 Proyectos de adquisición

1.6.2.1 Entregables al momento de solicitar un concepto técnico al Equipo de Sistemas de Información

Los entregables mínimos requeridos en un proyecto adquisición de sistemas de información son:

- Oficio de la solicitud del aval
- Documento de especificaciones técnicas
- Diagrama de Proceso
- El documento de arquitectura de la solución el cual deberá ser presentado ante el comité de arquitectura de la Alcaldía de Medellín para su aprobación antes de la implementación.
- Se deben entregar las especificaciones técnicas de infraestructura mínima requerida para el correcto despliegue y funcionamiento del sistema adquirido (servidores, memoria, almacenamiento, etc)

1.6.2.2 Entregables al momento de implementar la adquisición

Los entregables mínimos requeridos en un proyecto de desarrollo o evolución de sistemas de información para la disciplina de Arquitectura de software son:

- Documento de arquitectura del sistema de información actualizado.
- Diagrama Modelo entidad relación
- Diccionario de datos de acuerdo al numeral *3.4.2* definido en este documento

Los Manuales mínimos requeridos en un proyecto de desarrollo o evolución de sistemas de información son:

- 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*. (Información del Sistema para el Catálogo de Sistemas de información)

1.6.3 Proyectos de servicios de Sistemas de información en la nube (SaaS)

1.6.3.1 Entregables al momento de solicitar un concepto técnico al equipo de Sistemas de Información

Los entregables mínimos requeridos en un proyecto de sistemas de información en la nube son:

- Oficio de la solicitud del aval
- Documento de especificaciones técnicas
- Diagrama de Proceso.

1.6.3.2 Entregables al momento de habilitar el servicio

Los entregables mínimos requeridos en un proyecto de sistemas de información en la nube (SaaS) son:

- Manual de usuario final
- Manual Técnico de parametrización y configuración
- 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*. (Información del Sistema para el Catálogo de Sistemas de información)
- Plan de respaldo de la información en la infraestructura de la Alcaldía de Medellín.

1.6.4 Proyectos de renovación de soporte y servicios

1.6.4.1 Entregables al momento de solicitar un concepto técnico al equipo de Sistemas de Información

Los entregables mínimos requeridos en un proyecto de renovación de soporte o servicios de sistemas de información son:

- Oficio de la solicitud del aval
- Documento de especificaciones técnicas

- Análisis de alternativas de solución: Se debe entregar un análisis de otras herramientas al interior de la entidad o en el mercado que pudieran reemplazar la solución actual con mejoras técnicas y/o económicas o justificar la continuidad del sistema actual. Esto buscando modernizar la arquitectura y las aplicaciones de la entidad.
- Diagrama de Proceso
- El documento de arquitectura de la solución
- Diagrama Modelo entidad relación
- Diccionario de datos de acuerdo al numeral “Diccionario de datos” definido en este documento
- 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*. (Información del Sistema para el Catálogo de Sistemas de información)

1.6.5 Elementos de validación

Dependiendo de la modalidad de desarrollo y/o adquisición del sistema de información (Desarrollo a la medida, Evolución de un sistema existente, Adquisición), se deberán tener en cuenta en los documentos contractuales los siguientes criterios de valoración y si el criterio genera un entregable, se debe hacer llegar al equipo de Sistemas de Información.

Los elementos de validación, así como los lineamientos de este dominio, deben quedar por escrito de manera explícita en los documentos contractuales para cualquier tipo de contratación que se vaya a realizar.

A continuación, se enumeran los criterios que se deben tener en cuenta al desarrollar o adquirir un Sistema de información. Según la modalidad, se debe tener solamente en cuenta el elemento de validación con el símbolo X. Cada ítem debe tener una evidencia y su respectiva justificación en caso de no cumplir con la validación.

Elemento de validación	Desarrollo (Ver Definiciones clave)	Evolución (Ver Definiciones clave)	Adquisición (Ver Definiciones clave)
Validar si la necesidad puede ser resuelta con alguno de los sistemas actuales de la Alcaldía de Medellín.	X		X
Analizar si la infraestructura tecnológica de la Alcaldía de Medellín es suficiente para soportar la implementación del sistema de información.	X	X	X
Identificar y describir el método de integración (Webservices, API Rest, Microservicios, XROAD, etc.) con sistemas internos y externos y las entidades con las cuales se va a interoperar.	X	X	X
Analizar y validar el esquema de licenciamiento necesario para el funcionamiento del Sistema de Información, indicando el modelo de licenciamiento, la cantidad de licencias, la forma de renovación y los costos.		X	X
Contemplar los recursos necesarios para un contrato de soporte, mantenimiento y actualización post-implementación que permita la correcta operación del sistema en el tiempo.	X	X	X
Identificar e informar al equipo de Sistemas de información los responsables técnico y funcional del sistema de información por parte de la Alcaldía de Medellín (Nombre, Cargo y Correo electrónico). Preferiblemente deben ser funcionarios de carrera administrativa.	X	X	X

Tabla 1.Elementos de Validación

Los siguientes elementos deben ser incluidos en los documentos técnicos o estudios previos del proceso contractual de acuerdo a la pertinencia	**Desarrollo**	**Evolución**	**Adquisición**
El sistema de información debe estar diseñado con arquitectura distribuida que permita escalabilidad y capacidad para crecer de forma simple y eficiente de acuerdo a la arquitectura definida por la Alcaldía de Medellín	X	X	X
La implementación del sistema de información se debe basar en Microservicios y hacer uso de los servicios Core de la arquitectura definida en la Alcaldía de Medellín.	X	X	
Las aplicaciones Web deben funcionar correctamente en diferentes navegadores. Por lo menos se debe garantizar un correcto funcionamiento en el sistema operativo Windows y navegador Google Chrome que son los usados por defecto en la administración Distrital.	X	X	X
El sistema de información debe estar diseñado de acuerdo a los lineamientos definidos por la Secretaría de Comunicaciones. Para portales web de cara a la ciudadanía es de obligatorio cumplimiento.	X	X	
Para el desarrollo de Sistemas de información a la medida, el proveedor es responsable de los ambientes de desarrollo y de de pruebas para usuarios finales de la Alcaldía. Cualquier excepción a este criterio debe ser validado técnicamente con la Secretaría de Innovación Digital. Para sistemas de información adquiridos, en la Alcaldía de Medellín dispone del ambiente de pruebas.	X	X	X
El proveedor debe realizar acompañamiento en la instalación y puesta en producción del Sistema de información de acuerdo al procedimiento definido por la Secretaría de innovación digital.	X	X	X
Se debe definir un tiempo de garantía y estabilización del sistema de información.	X	X	X
El sistema de información debe contener los siguientes factores de seguridad de acuerdo a la pertinencia: • El control de acceso al sistema debe estar integrado al LDAP o UME • Manejo de roles y perfiles • Trazabilidad de transacciones de los usuarios en el sistema • Control de acceso malicioso o de bots (Captcha) • De acuerdo al tipo y sensibilidad de la información que se maneje en el sistema se debe contemplar doble factor de autenticación.	X	X	X

Los siguientes elementos deben ser incluidos en los documentos técnicos o estudios previos del proceso contractual de acuerdo a la pertinencia	Desarrollo	Evolución	Adquisición
La base de datos debe ser implementada en PostgreSQL en la versión soportada por la Alcaldía de Medellín. En caso de ser necesario el uso de otro motor debe ser justificado y validado técnicamente con la Secretaría de Innovación Digital.	X	X	X
El sistema de información debe estar implementado en servidor de aplicaciones JBoss, en la versión soportada por la Alcaldía de Medellín. En caso de ser necesario el uso de otro servidor debe ser justificado y validado técnicamente con la Secretaría de Innovación Digital.	X	X	X
El sistema de información debe operar sobre los sistemas operativos soportados por la Alcaldía de Medellín: Windows Server y Red Hat Linux.	X	X	X
Si el Sistema de Información es de tipo “Gestor de contenidos” se debe usar WordPress como herramienta de implementación y MariaDB como motor de Base de datos. En caso de ser necesario el uso de otro gestor de contenidos o Base de Datos, debe ser justificado y validado técnicamente con la Secretaría de Innovación Digital.	X	X	
Se debe definir un plan de capacitación y entrenamiento que permita el uso y apropiación del Sistema de Información en la Alcaldía de Medellín	X	X	X
Se deben incorporar dentro del contrato cláusulas de cesión de derechos patrimoniales a favor de la Alcaldía de Medellín.	X	X	
Si el sistema almacena información de caracterización de usuarios (variables demográficas, geográficas, de comportamiento), se deben contemplar las variables de enfoque diferencial (Sexo, Etnia, Orientación Sexual e Identidad de género)	X	X	X
Si se contempla integraciones con sistemas externos se debe usar la plataforma de interoperabilidad XROAD como herramienta dispuesta por el gobierno nacional para este efecto, en caso de no usar XROAD se debe justificar.	X	X	

Tabla 2.Elementos a incluir en el proceso contractual

Recomendaciones a tener en cuenta para la contratación de servicios SAAS
Analizar y definir el plan de contingencia para que la operación que soporta el Sistema de Información en la nube pública, no sufra afectaciones en caso de no darse continuidad al servicio.
Definir y acordar con el proveedor un plan de continuidad del servicio teniendo en cuenta que los procesos de contratación de las entidades públicas no siempre coinciden con las fechas de terminación de la suscripción de los servicios.
Analizar y definir el esquema de licenciamiento necesario para el funcionamiento del Sistema de Información. (Modelo de licenciamiento, cantidad, forma de renovación, Costos)
Analizar y definir la necesidad de adquirir un servicio adicional de cifrado de datos para mejorar la seguridad de acceso a estos.
Se debe definir un plan de respaldo, recuperación de datos y acceso a la información vía ETL o Servicios de integración de forma periódica, estructural y automática en infraestructura de la Alcaldía de Medellín. Definir la estructura de información a ser almacenada en el centro de datos de la Alcaldía de Medellín.
Se debe especificar que el proveedor realizará el borrado de la información del servidor en la nube cuando finalice la relación contractual y se haya entregado satisfactoriamente el respaldo a la Alcaldía de Medellín.
Realizar validación con el área de infraestructura de Innovación Digital, para el acceso concurrente al servicio de acuerdo a la cantidad de usuarios y la capacidad del canal de Internet de la Alcaldía de Medellín.
Definir tiempos y procedimientos para los procesos de mantenimiento y actualización de la plataforma en la nube de tal forma que se minimice la afectación de la operación del servicio.
Establecer el tiempo de restauración del servicio y los datos en caso de alguna eventualidad que afecte la operación de este.
Incorporar dentro del contrato cláusulas, términos y condiciones específicas para el tratamiento de datos y solicitar una certificación de seguridad que avale que el proveedor está adherido a algún sello de confianza o código de conducta dentro de los certificados internacionales. Debe garantizarse expresamente que no se utilizarán los datos para otra finalidad que no tenga relación con los servicios contratados.
Tener en cuenta la región geográfica donde estarán alojados los servicios y la información y analizar las políticas gubernamentales del territorio para preservar la confidencialidad e integridad de los datos de la entidad.

Tabla 3.Recomendaciones para la Contratación

ANEXO 1. Descripción técnica Arquitectura de Sistemas de Información

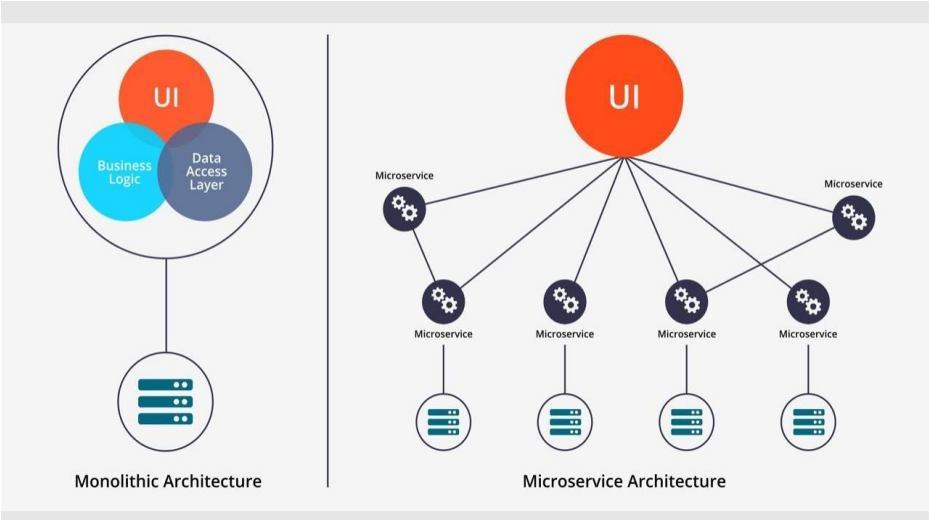


Ilustración 1.Arquitectura Monolítica vs Arquitectura de Microservicios

La arquitectura basada en microservicios es un enfoque para desarrollar una sola aplicación como un conjunto de pequeños servicios, cada uno ejecutándose en su propio proceso y comunicándose con mecanismos ligeros como API HTTP. Estos servicios se basan en capacidades empresariales y se debe implementar de forma independiente mediante una infraestructura tecnológica de despliegue completamente automatizado apto para la integración y despliegue continuo de las aplicaciones.

Existe un mínimo de gestión centralizada de estos servicios, que pueden construirse en diferentes lenguajes de programación y utilizar diferentes tecnologías de almacenamiento y procesamiento.

En esta arquitectura estará presente un API Gateway que gestionará las llamadas entre cada uno de los recursos que exponen colecciones de datos, del lado de la exposición de servicios externos y microservicios internos.

Consecuentemente y con el fin de lograr una arquitectura ideal donde se puedan reusar componentes, se está trabajando en la definición e integración de varios servicios transversales tales como repositorios, notificaciones, mensajerías, seguridad, manejo de trazabilidad, gestión documental, agentes de tareas automáticas, componentes o servicios de monitoreo o estado de salud de las aplicaciones o plataforma.

A continuación, se presenta la visión de arquitectura gráficamente:

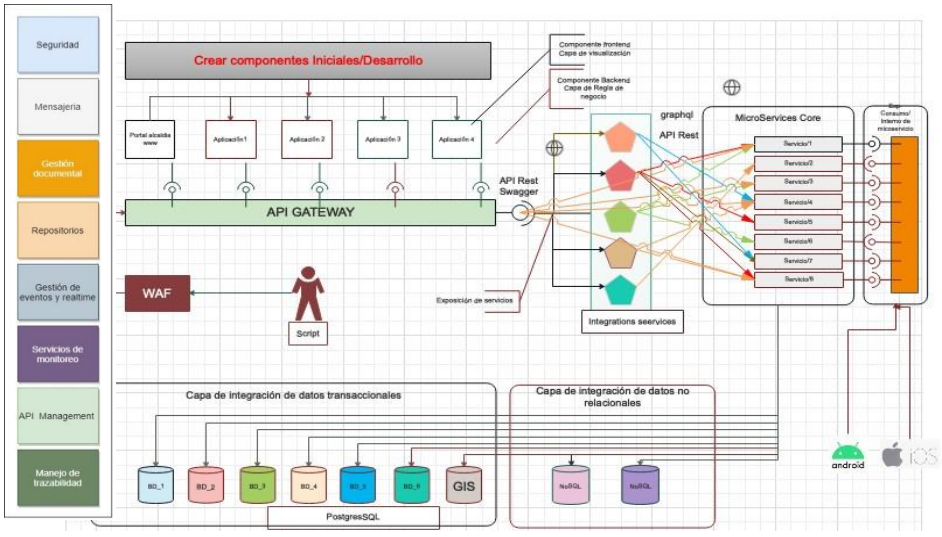


Ilustración 2.Visión de Arquitectura

Como complemento a la visión planteada, se tiene el Micro Frontend que extiende el concepto de microservicios al mundo del frontend dividiendo una aplicación web en módulos independientes y desplegables de forma autónoma. Cada micro frontend es desarrollado, probado y mantenido por equipos separados, utilizando tecnologías y Frameworks distintos si es necesario. La integración se realiza en el navegador mediante técnicas como Iframes, Web Components, Single-SPA o Module Federation en Webpack.

La tendencia actual es crear una aplicación de navegador potente y rica en características, también conocida como “single page app”, que se asiente sobre una arquitectura de microservicios. Con el tiempo, la capa de frontend, a menudo desarrollada por un equipo independiente, crece y se vuelve más difícil de mantener. Eso es lo que llamamos una Interfaz Monolítica.[17]

La idea detrás del Micro Frontend es pensar en un sitio web o aplicación web como una composición de características que son creados y mantenidos por equipos diferentes; cada equipo tiene un área de negocio definida o misión de la que se preocupa y se especializa. Un equipo es Cross Functional y desarrolla sus características End-to-End, desde la base de datos hasta la interfaz de usuario.

[17] https://micro-frontends-es.org/

Sin embargo, esta idea no es nueva, en el pasado se llamaba Integración de Frontend para Sistemas Verticales o Sistemas auto-contenidos. Pero Micro Frontends es claramente un término más amigable y menos voluminoso.

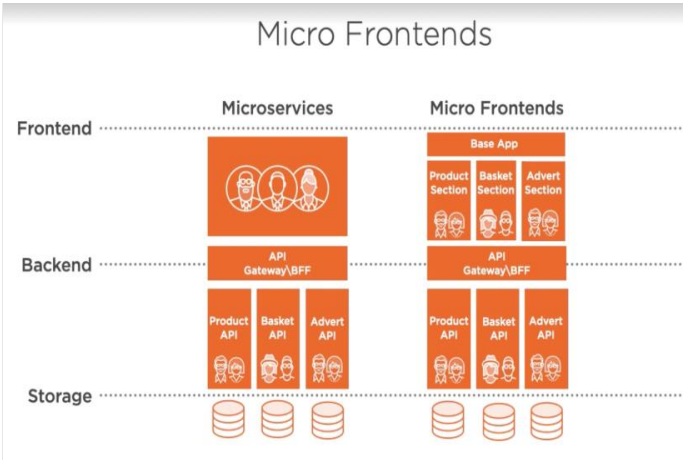


Ilustración 3. Microservicios Vs Micro Frontends

ANEXO 2. Características API GATEWAY

- **Persistencia:** Capa de persistencia transaccional desde los microservicios a las bases de datos.

- **Repositorios:** son sitios centralizados donde se almacena y mantiene información digital, habitualmente bases de datos o archivos informáticos, estos datos almacenados en un repositorio pueden distribuirse a través de una red informática, como Internet, o de un medio físico, como un disco compacto. Pueden ser de acceso público o estar protegidos y necesitar de una autentificación previa.

- **API management:** los procesos de distribución, control y análisis de las API que conectan las aplicaciones y los datos en toda la empresa y en las distintas nubes. Su objetivo es permitir que las empresas que generan API o que utilizan las de otras organizaciones supervisen la actividad y garanticen que se satisfagan las necesidades tanto de los desarrolladores como de las aplicaciones que utilizan dichas API.

- **Mensajería:** La comunicación entre microservicios tiene que ser eficiente y sólida. Con una gran cantidad de pequeños servicios interactuando para realizar una sola transacción.

- **Seguridad:** es el proceso de prevenir y detectar el uso no autorizado de un sistema informático. Implica el proceso de proteger contra intrusos el uso de nuestros recursos informáticos con intenciones maliciosas o con intención de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente.

- **Gestión de eventos y realtime:** Una arquitectura orientada por eventos, usa eventos para desencadenar y comunicarse entre servicios desacoplados y es común en aplicaciones modernas creadas con microservicios. Un evento es un cambio de estado o una actualización, puede tener un estado o puede ser un identificador de una notificación. Los gestores de eventos tienen tres componentes clave: productores de eventos, enrutadores de eventos y consumidores de eventos. Un productor publica un evento en el enrutador, que filtra y envía los eventos a los consumidores. Los servicios al productor y los servicios al consumidor están desacoplados, lo que permite escalarlos, actualizarlos e implementarlos de forma independiente.

- **Manejo de trazabilidad:** La auditoría de los Sistemas de Información contempla el estudio, revisión y valoración de todos los elementos (o parte de ellos) de los sistemas automáticos de procesamiento de la información, incluyendo operaciones no automáticas relacionadas con ellos y su interfaz correspondiente. Permite el almacenamiento, consulta y análisis de los registros que deja las transacciones realizadas por los usuarios y los procesos automáticos en las aplicaciones y bases de datos.

- **Gestión documental:** Sistema que permite almacenar, administrar y controlar el flujo de documentos electrónicos dentro de una organización con funcionalidades de radicación, indexación, búsqueda, asignación, consulta, descarga, transferencia, colaboración en línea, control de versiones, orquestación de flujos de trabajo, aprobaciones, alertas y notificaciones.

- **Servicios de monitoreo:** Control y supervisión del desempeño y disponibilidad de los servicios y aplicaciones, análisis y gestión de logs, registro de alarmas y gestión de incidentes, cálculo de indicadores operacionales.

ANEXO 3 – Descripción nombre de campos/tablas

Las tablas deben ser nombradas con descripciones nemotécnicas que hagan relación a su contenido de la siguiente forma:

TBL_NOMBRETABLA; donde **TBL** indica que la estructura es una tabla y **NOMBRETABLA** es una cadena descriptiva asociada al contenido.

Ejemplo: TBL_INFEMPLEADO.

Los nombres de los campos asociados a las tablas deben ser nombrados con descripciones nemotécnicas que hagan relación a su contenido de la siguiente forma: **TAB_NOMBRECAMPO;** donde **TAB** indica las tres primeras letras del nombre de la tabla y **NOMBRECAMPO** es una cadena descriptiva asociada al contenido. Ejemplo: Si la tabla se llama **TBL_INFEMPLEADO**, los nombres de los campos podrían quedar así **INF_CEDULA, INF_NOMBRES, INF_DIRECCION, etc.**

Los procedimientos almacenados deben ser nombrados con descripciones nemotécnicas que hagan relación a su funcionalidad en la BD de la siguiente forma: **SPR_NOMBREPROC**; donde **SPR** indica que la estructura es un procedimiento almacenado y **NOMBREPROC** es una cadena que hace relación a la funcionalidad que este realiza dentro de la BD. Ejemplo: SPR _GENESTADOS.

Los paquetes deben ser nombrados con descripciones nemotécnicas que hagan relación a su funcionalidad en la BD de la siguiente forma: **PKG_NOMBREPKG**; donde **PKG** indica que la estructura es un paquete y **NOMBREPKG** es una cadena

descriptiva que hace relación a la funcionalidad que este realiza en la BD. Ejemplo: PKG _CONSOLIDADO.

Las vistas deben ser nombradas con descripciones nemotécnicas que hagan relación a su funcionalidad en la BD de la siguiente forma: **VW_NOMBREVW**; donde **VW** indica que la estructura es una vista y **NOMBREVW** es una cadena descriptiva que hace relación a la funcionalidad que esta realiza en la BD. Ejemplo: VIW _CONSESTADOS.

Los triggers deben ser nombrados con descripciones nemotécnicas que hagan relación a su funcionalidad en la BD de la siguiente forma: **TRG_NOMBRETRG**; donde **TRG** indica que la estructura es una triggers y **NOMBRETRG** es una cadena descriptiva que hace relación a la funcionalidad que este realiza en la BD. Ejemplo: TRG_CREAREGINV.

Las funciones deben ser nombradas con descripciones nemotécnicas que hagan relación a su funcionalidad en la BD de la siguiente forma: **FUN_NOMBREFUN**; donde **FUN** indica que la estructura es una función y **NOMBREFUN** es una cadena descriptiva que hace relación a la funcionalidad que esta realiza en la BD. Ejemplo: FUN_HABILES.

Las vistas materializadas o geográficas deben utilizar un prefijo de acuerdo con el tipo: vista geográfica (geographic view): **vwg_nombrevistageografica**, vista materializada (materialized view): **vwm_nombrevista**. A continuación del prefijo que identifica la vista utilizar un nombre que represente la información que se va a mostrar (p.e. **vwg_accidente_transito**).

Los nombres de objetos en base de datos PostgreSQL, deberán estar en minúscula y no pueden exceder un tamaño de 30 caracteres.

Anexo 4. Direcciones encasilladas

La siguiente tabla describe la estructura para el manejo de las direcciones encasilladas:

NOMBRE CAMPO	TIPO DATO	DESCRIPCIÓN
DEPARTAMENTO	Texto	Campo tipo lista que determina el departamento al cual pertenece la dirección. Por defecto se debe preseleccionar “Antioquia”.
MUNICIPIO	Texto	Campo tipo lista que determina el municipio al cual pertenece la dirección. La lista se debe cargar de acuerdo al departamento seleccionado. Por defecto se debe preseleccionar "Medellín".
COMUNA	Texto	Campo tipo lista que determina la comuna o corregimiento de acuerdo al municipio seleccionado. En el caso de Medellín, se compone de 16 comunas y 5 corregimientos. Si el municipio seleccionado no contempla comunas en su estructura, se debe cargar el nombre del municipio.
BARRIO	Texto	Campo tipo lista que determina el barrio de acuerdo a la comuna seleccionada.
TIPO DE VÍA	Texto	Campo tipo lista que corresponde a la abreviatura del tipo de vía principal. Puede ser: Calle (CL), Carrera (CR), Circular (CQ), Transversal (TV), Diagonal (DG).
NÚMERO DE VÍA	Número	Número de la vía principal. Los valores posibles son desde el 1 hasta el 999 omitiéndose los ceros (0) a la izquierda.
APÉNDICE VÍA	Texto	Campo tipo lista con el apéndice de la vía principal (si existe). Pueden ir letras hasta la A hasta la H y sus posibles combinaciones máximo de dos literales. Ej. A, B, AA, DD, … hasta HH.

NOMBRE CAMPO	TIPO DATO	DESCRIPCIÓN
ORIENTACION VÍA	Texto	Campo tipo lista con el direccionamiento u orientación de la vía principal (si existe). Puede ser: • Sur, para las calles. • Este, para las carreras. Los direccionamientos Este y Sur son excluyentes, es decir, no existe la combinación de direccionamientos Calle con Este ni Carrera con Sur en la división político-administrativa de la Alcaldía de Medellín.
NÚMERO DE CRUCE	Número	Número de la vía que cruza la vía principal. Los valores posibles son desde el 1 hasta el 999 omitiéndose los ceros (0) a la izquierda.
APÉNDICE CRUCE	Texto	Campo tipo lista con el apéndice de la vía del cruce (si existe). Pueden ir letras hasta la A hasta la H y sus posibles combinaciones máximo de dos literales. Ej., A, B, AA, DD, … hasta HH.
ORIENTACIÓN CRUCE	Texto	Campo tipo lista con el direccionamiento u orientación del cruce (si existe). Puede ser: • Sur, para las calles. • Este, para las carreras. Los direccionamientos Este y Sur son excluyentes, es decir, no existe la combinación de direccionamientos Calle con Este ni Carrera con Sur en la división político-administrativa de la Alcaldía de Medellín.
NÚMERO	Número	Corresponde a la distancia, en la vía principal, a partir del cruce. Los valores posibles son desde el 1 hasta el 999 omitiéndose los ceros (0) a la izquierda.
COMPLEMENTO	Texto	Campo abierto para complementar la dirección principal. Ej. Edificio, Manzana, Lote, Unidad, Bloque, Interior, Apto, etc.

Tabla 4.Estructura para el manejo de las direcciones encasilladas

2. Dominio Gestión y Apertura de Datos

2.1 Alcance

Los conceptos y lineamientos definidos por la Secretaría de Innovación Digital en este apartado se deben 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 están 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.

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.

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.

Para cumplir con los objetivos de la entidad y buscar una gestión integral de los datos, se establecen los siguientes principios fundamentales:

- Los datos deben ser precisos, completos, consistentes, actualizados y relevantes.

- La información es un activo clave que debe ser gestionado con la misma prioridad que otros recursos críticos de la organización.

- Los datos deben estar alineados a los procesos.

- Los datos deben estar integrados y ser accesibles de manera unificada entre diferentes sistemas y entidades.

- La gestión de datos debe ser transparente, con roles y responsabilidades claramente definidos para garantizar la rendición de cuentas.

- La información y datos deberá ser manejada con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros.

- Los datos deben estar protegidos evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, garantizando el cumplimiento normativo en privacidad de datos personales.

- Los datos deben ser utilizados de manera ética, respetando los derechos de los titulares y el propósito para el cual fueron recolectados.

- La información debe ser accesible para todos los actores autorizados, asegurando que los datos estén disponibles en formatos utilizables para usuarios técnicos y no técnicos.

- La gestión de los datos debe habilitar la toma de decisiones y la innovación mediante el uso de tecnologías avanzadas como analítica de datos, inteligencia artificial y machine learning.

- Los datos deben gestionarse de forma integral durante todo su ciclo de vida, desde su creación hasta su archivado y eliminación definitiva.

- La gestión de información debe estar orientada a generar valor público, optimizando la prestación de servicios, fomentando la transparencia y empoderando a los ciudadanos.

- Los recursos necesarios para la gestión y el aprovechamiento de los datos deben procurarse de acuerdo con los parámetros y directrices de la entidad para la estructuración de necesidades y gestión de las adquisiciones.

2.4 Datos, Información, Conocimiento

Para garantizar una comprensión homogénea en todas las dependencias del Distrito sobre la gestión de datos, es fundamental establecer una diferenciación clara entre los conceptos de Dato, Información y Conocimiento, en concordancia con normativas nacionales e internacionales que sean reconocidos en la entidad, así:

Los datos son la representación primaria de variables cualitativas y cuantitativas que son almacenables, transferibles, pueden ser visualizadas, controladas y entendidas. Los datos que se perciben por los sentidos humanos, de manera continua y sin interrupciones, se denominan analógicos. Cuando son interpretados mediante codificación binaria, se trata de datos digitales. Estos últimos pueden generarse de dos maneras: por la interacción de personas con sistemas,

herramientas y servicios digitales o automáticamente por programas de software y dispositivos de hardware que los capturan (DNP, 2018).

La recolección, almacenamiento y procesamiento de datos da lugar a la información, de la cual es posible obtener conocimiento. La disponibilidad de inmensas cantidades de datos digitales, unido a la capacidad para aprovecharlos mediante técnicas cada vez más sofisticadas, es lo que permite la creación de bienes, servicios, procesos, el mejoramiento de los existentes y la toma de mejores decisiones (DNP, 2018). De acuerdo con la organización y almacenamiento de los datos digitales, estos pueden clasificarse en estructurados, No estructurados y Semiestructurados.

En consecuencia, la Secretaría de Innovación Digital promoverá el uso adecuado de estos conceptos en todas las dependencias del Distrito, asegurando su alineación con estándares internacionales y normativas nacionales vigentes.

2.5 Disposiciones Generales

Para que las entidades y dependencias de la Alcaldía cumplan con los principios establecidos y aborden eficazmente la gestión de los datos y la información, es necesario implementar disposiciones generales que alineen sus procesos, estructuras y tecnología con los objetivos estratégicos de la entidad en la estrategia de *datos abierto*, logrando que las disposiciones busquen garantizar una gestión eficiente, ética y segura de los datos y la información.

Por lo anterior, estas disposiciones buscan garantizar una gestión eficiente, ética y segura de los datos, debido a ella, se deberá tener en cuenta para su cumplimiento:

- Que cada dependencia debe asignar un enlace con el cual se pueda coordinar la gobernanza y gestión de los datos, el cual preferiblemente debe ajustarse al siguiente perfil:
  - Ser vinculado
  - Pertenecer al nivel profesional
  - Demostrar un buen conocimiento de los sistemas de información, las bases de datos y los procesos responsabilidad de su dependencia.
- Cada dependencia debe contar con un **Administrador de datos** para velar por la disponibilidad, calidad y el linaje de los datos.
- Se debe hacer una adecuada gestión de la seguridad, la calidad y la privacidad de los datos y la información.
- Se debe contar con indicadores clave y controles para evaluar y mejorar la calidad de los datos en cada dependencia.
- Hacer uso de estándares abiertos para garantizar la integración de datos entre dependencias.
- Capacitar a los empleados sobre manejo ético, calidad y seguridad de los datos.
- Todas las dependencias deben adoptar herramientas compatibles con la arquitectura de datos definida por la Alcaldía.

- Cumplir con la **Ley 1581 de 2012** y el **Decreto 1377 de 2013** en el manejo de información personal, así como 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.

- Adoptar controles como encriptación, autenticación multifactor y monitoreo constante.

- Implementar estrategias para garantizar la continuidad operativa en caso de incidentes.

- Garantizar la conexión desde las fuentes primarias (bases de datos, archivos planos primarios, etc.) con el lago de datos de la entidad (Entiéndase por conexión los permisos, usuarios, reglas de firewall, configuraciones de red, entre otros; que permitan la ingesta de datos por parte del lago de datos de la entidad).

- Cada dependencia contará con un espacio de almacenamiento al interior del lago de datos, capacidad habilitada por la Secretaría de Innovación Digital para realizar procesos de autoservicio de analítica (descriptiva, predictiva y prescriptiva).

- Las dependencias deberán hacer uso de los formatos, documentos y guías que se encuentren en Isolucion relacionadas con: La definición de variables (DE-GINF-021 Estándar de Variables Unificadas Para Codificar y Estructurar Bases de Datos"), y los demás que se generen para el mejoramiento de la calidad, el aprovechamiento y la visualización de los datos.

La Secretaría de Innovación Digital propende por la alienación de la gestión de los datos y la información a los siguientes subdominios de acuerdo con el Modelo de Gestión y Gobierno de Tecnologías de la Información -MGGTI-:

2.6 Gestión del Ciclo de Vida de los Datos

La gestión del ciclo de vida del dato es un proceso indispensable para alcanzar el aprovechamiento de los datos dispuestos en la infraestructura de datos del Estado. El ciclo de vida de los datos está integrado por diferentes fases como se muestra en la figura:



*Figura **3.**1.* Ciclo de vida del dato *de los datos*

Fuente: Elaboración propia basada en Ciclo de Vida definido por Mintic DAMA y PNID

Todas las dependencias y entidades del distrito deben identificar y categorizar los datos según sean públicos, semiprivados, sensibles, y que sobre ellos se pueda hacer aprovechamiento mediante el uso, para brindar un valor estratégico a la entidad, en concordancia con marcos legales y normativos colombianos como la Ley 1581 de 2012, el Decreto 1377 de 2013, y las directrices de gobernanza de datos del MinTIC, dicho proceso debe estar alineado con las siguientes acciones:

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

Estructurado	Están organizados conforme a un modelo o esquema. Se almacenan en forma tabular y algunas veces su estructura también incluye la definición de las relaciones entre ellos. Típicamente están representados en bases de datos que hacen parte del funcionamiento de sistemas de información.
No estructurado	Su organización y presentación no está guiada por ningún modelo o esquema. En esta categoría se incluyen, por ejemplo, las imágenes, texto, audios, contenidos de redes sociales, videos.
Semiestructurado	Su organización y presentación tiene una estructura básica (etiquetas o marcadores), pero no tiene establecida una definición de relaciones en su contenido. En esta categoría se incluyen contenidos de e-mails, tweets, archivos XML.

Tabla 4.5. Clasificación de los datos según su formato
Fuente: DNP

Los datos pueden clasificarse según criterios orgánicos en tres categorías: públicos, accesibles sin restricciones; privados, con acceso controlado por normativas; y cualitativos, que se dividen en personales (vinculados a individuos) e impersonales (sin identificación directa). Esta clasificación es clave para su gestión y protección.

Criterio orgánico: sujeto que genera el dato	Público	Datos producidos o recolectados por una entidad pública, que ejerce funciones públicas o presta un servicio público (p. ej. cantidad de contratos suscritos, listado de funcionarios de una entidad).
	Privado	Datos producidos o recolectados por un particular (empresa, ciudadano, academia). Como las notas de los estudiantes o la historia laboral de los empleados de una empresa
Criterio cualitativo: variables representadas	Personal	Datos que describen características que permiten identificar a una persona (p. ej. fecha de nacimiento, estatura, etc.).
	Impersonal	Datos que no permiten la individualización de una persona o se refieren a fenómenos que acaecen (p. ej. temperatura en un día, cantidad de vehículos que transitan por una calle, etc.).

Tabla 5.6. Tipologías de los datos
Fuente: DNP

En Colombia, los datos se clasifican por su nivel de sensibilidad en diferentes categorías: entre ellas encontramos datos públicos, accesibles sin restricciones; datos semiprivados, que requieren autorización para su uso, como información financiera; y datos sensibles, que incluyen información biométrica, de salud o política, y requieren mayor protección. Esta clasificación garantiza el adecuado manejo y seguridad de la información, en la siguiente tabla se ilustran las diferentes categorías existentes en el marco jurídico.

Clasificación	Descripción
Sensible	Afecta la intimidad y puede generar discriminación
Privado	Naturaleza íntima, solo es relevante para su titular
Semiprivado	Corresponde a aquella que, teniendo protección legal, es posible, para una entidad pública, ponerla a disposición de otra entidad pública, pero solamente para efectos de las tareas misionales que, en virtud de la ley, se le han otorgado a la entidad solicitante de la información. Ellos compilan información personal, que tiene el carácter de reservada, pueden ser compartidos en virtud de las funciones legales de cada entidad pública bajo estrictos protocolos de seguridad que garanticen su reserva y divulgación no autorizada.
Público	No pertenece a las tipologías anteriores o es definido por la ley
Abierto	Primario o sin procesar, en formatos estándar e interoperables, libre y sin restricciones. Puede ser usado y reutilizado
Clasificado	Puede generar daños a la intimidad, vida, salud o seguridad de una persona; o a los secretos comerciales, industriales y profesionales
Reservado	Acceso prohibido por la Constitución o la Ley

Tabla 6.7. Tipos de datos según su nivel de sensibilidad
Fuente: DNP

- Los datos abiertos del Distrito deben ser publicados en Medata, el portal oficial de datos abiertos del distrito, garantizando su disponibilidad, accesibilidad y reutilización por parte de ciudadanos, academia y sector privado, lo que permite mejorar la eficiencia la transparencia, la participación ciudadana y

fomentar la innovación, en línea con la Política de Gobierno Digital y los estándares nacionales de datos abiertos.

- Publicar en Medata asegura que la información esté estructurada bajo formatos abiertos y compromete a las todas las dependencias del Distrito a mantenerla actualizada, para facilitar su aprovechamiento para la toma de decisiones y el desarrollo de soluciones basadas en datos.
- Para autorizar la circulación de datos semiprivados, los responsables de datos de las dependencias deben:
- Verificar que se trata de datos semiprivados conforme a la clasificación y orientación contenida en esta guía.
- Verificar que el solicitante es una entidad pública y que el funcionario responsable, lo es de acuerdo con sus funciones legalmente asignadas mediante el manual de funciones de la entidad.
- Verificar que la información solicitada, corresponde al ejercicio de las funciones misionales de la entidad (Por ejemplo, no sería lógico que el Ministerio de Agricultura, solicite la base de datos de los pacientes portadores de VIH, pues esa temática no le corresponde dentro de sus áreas misionales)
- Asegurarse que la entidad que recibe la información garantizará la confidencialidad y reserva de esta, para lo cual se recomienda suscribir un documento de compromiso con la entidad receptora de la información.
- Entregar la información con todos los protocolos de seguridad y encriptaciones que garanticen su protección y no divulgación.

- En todos los casos, es necesario que la dependencia, antes de entregar o publicar los datos o la información, efectúe la clasificación y análisis de esta, para verificar que datos se pueden publicar, y cuáles no, conforme a la normatividad vigente.

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.

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.

2.6.4 Procedimientos para Eliminación Segura:

- Implementar procesos documentados y auditables para la eliminación de datos que incluyan métodos como:

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

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.

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.

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 basada en evidencia.

Cumplimiento de Estándares 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.

2.9 Calidad de Datos

La calidad de los datos es un componente crítico para garantizar que la información utilizada en los procesos operativos y estratégicos de las entidades del Distrito sea confiable, precisa y adecuada para soportar la toma de decisiones.

Por lo anterior, es de vital importancia que mediante el presente capítulo establece lineamientos específicos para la gestión de la calidad de los datos, alineados con los principios del Modelo de Referencia de Arquitectura Empresarial (MRAE) del Mintic y el MA-GTIC- Manual de Calidad de Datos (que puede ser consultado en Isolucion[19] sea marco de referencia para orientar las decisiones relacionadas con la gestión de las actividades de calidad de datos, y las guías específicas que deben ser adoptadas por las dependencias y entidades del Distrito.

[19] MA-GTIC - Manual de Calidad del Dato

En el flujo de procesos para el uso y gestión de los datos dentro de la organización, en la fase de preparación de los datos, se debe realizar la evaluación de calidad de los datos, después de catalogar los datos, lo cual se realiza en la fase de Entendimiento de los Datos, como se muestra en el siguiente gráfico:

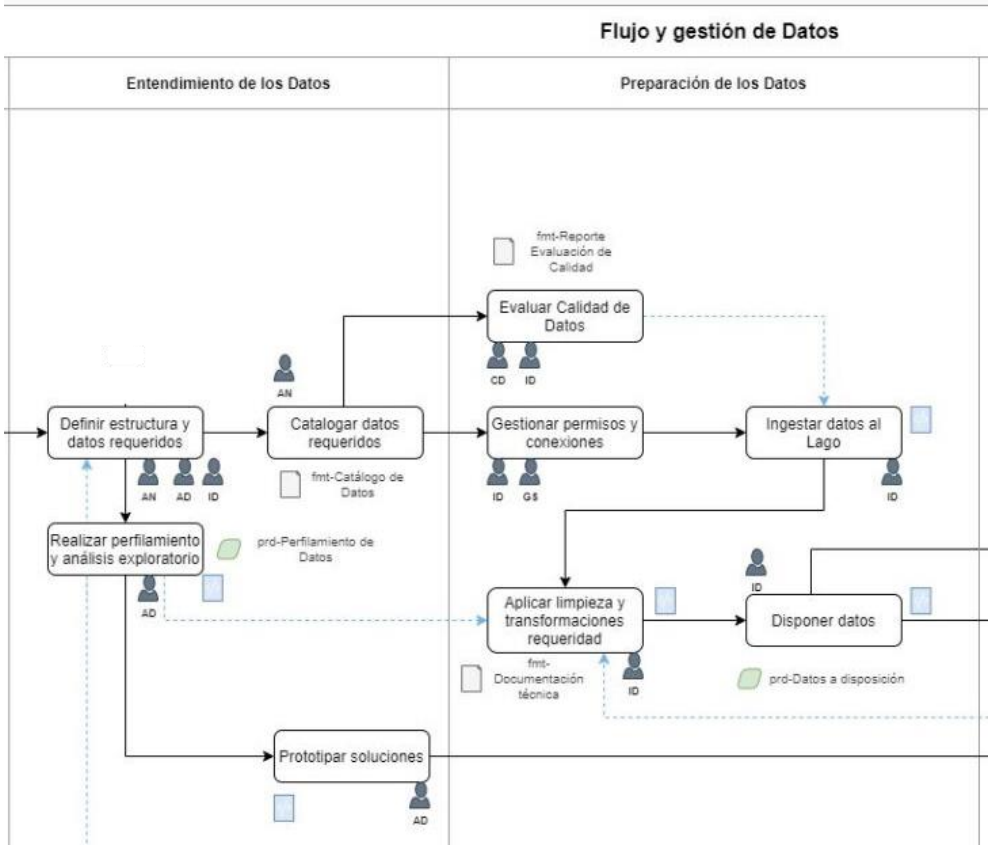


Figura 7.2. Fases de Entendimiento y Preparación en el Diagrama de Flujo y Gestión de Datos

2.9.1 Importancia de la Calidad de los Datos

La calidad de los datos asegura que la información que va a ser aprovechada sea seleccionada por cada dependencia atendiendo a los principios de:

- **Precisión**: representa correctamente los fenómenos que describe.
- **Completitud**: contiene toda la información requerida para su propósito.
- **Consistencia**: es coherente a lo largo de diferentes sistemas y procesos.
- **Actualidad**: refleja la información más reciente disponible.
- **Accesibilidad**: es fácil de obtener y utilizar por los usuarios autorizados.

Estos principios son fundamentales para el diseño y funcionamiento de sistemas de información interoperables, la generación de valor público y el cumplimiento de las políticas de datos del Distrito.

2.9.2 Lineamientos para la Gestión de la Calidad de Datos

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.

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.

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.

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.

2.9.3 Anonimización de Datos

La anonimización de datos es un proceso fundamental para proteger la privacidad de las personas, garantizando el cumplimiento de normativas como la Ley 1581 de 2012 en Colombia y el Reglamento General de Protección de Datos (GDPR) en el caso europeo.

La finalidad de la anonimización es impedir que, a partir de un dato o de una combinación de éstos, se logre identificar sujetos individuales ya sean individuos, empresas o establecimientos, u otro tipo de unidades de observación en un archivo de microdatos (Morales, 2017: 5).

Según la "Guía para la anonimización de bases de datos en el Sistema Estadístico Nacional" [20] publicada en 2018, la gestión del proceso de anonimización de una base de datos se encuentra compuesto por seis etapas que son: i) Revisiones previas; ii) Análisis de riesgos de identificación de las fuentes de información; iii) Identificación y selección de técnicas de anonimización; iv) Análisis de viabilidad del proceso, v) Aplicación de técnicas de anonimización, y vi) Evaluación de resultados del proceso.

[20] https://www.dane.gov.co/files/sen/registros-administrativos/guia-metadatos.pdf

La guía citada en el párrafo anterior contempla el proceso de anonimización, el cual debe ser seguido por las dependencias y entidades del distrito cuando se requiera según la sensibilidad de los datos, Implementar estas técnicas permite compartir información de manera segura, fomentando la innovación y el uso de datos abiertos sin vulnerar la privacidad. Este proceso se debe realizar con los datos que se pretendan compartir o publicar en el portal de datos abiertos Medata.

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/10757-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

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

La alcaldía cuenta con el documento específico en la plataforma *isolucion* "DEGINF Estándar de Variables Unificadas Para Codificar y Estructurar Bases de Datos" (Cód. DE-GINF-021), este documento se debe utilizar para realizar la estandarización de variables en todas las bases de datos de la entidad.

2.10.2 Apertura de datos

Todas las dependencias y entidades del Distrito deben disponer los datos clasificados como abiertos en Medata, el portal oficial de datos abiertos, como la plataforma para la publicación y actualización de la información de acceso público, garantizando su disponibilidad, transparencia y reutilización por parte de ciudadanos, academia y sector privado.

Es fundamental asegurar la calidad de los datos publicados, cumpliendo con los principios de precisión, completitud, consistencia y actualidad. En particular, el

criterio de actualidad exige que los conjuntos de datos reflejen la información más reciente disponible, evitando rezagos que afecten su utilidad para la toma de decisiones y el desarrollo de soluciones innovadoras.

Las dependencias deberán establecer procesos de actualización periódica según la naturaleza de los datos, definiendo frecuencias de publicación claras y asegurando que la información en Medata se mantenga vigente y alineada con los estándares de calidad definidos en la Política de Gobierno Digital y la Guía Nacional de Datos Abiertos.

La apertura de datos en el distrito debe seguir los lineamientos establecidos por la entidad, especialmente en lo referente a seguridad y privacidad de los datos, estructuración y anonimización de la información.

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, semáforos inteligentes).
- 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.

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.

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.

3.1 Equipos de Telecomunicaciones

Los equipos de telecomunicaciones comprenden las redes cableadas, redes inalámbricas, radio enlaces y telefonía. A continuación, se describe el detalle:

3.1.1 Consideraciones generales

- Para desarrollos o soluciones que vayan a ser publicados hacia Internet o requieran ser consultados por funcionarios en sedes externas, se debe cuantificar el ancho de banda requerido por usuario, con el fin de dimensionar si los canales actuales son suficientes o se deben ampliar. El responsable de las aplicaciones y sistemas de información nuevos debe informar al equipo de Telecomunicaciones de la Unidad de Infraestructura de TI, los requerimientos y necesidades de ancho de banda, basados en herramientas técnicas de consumo del aplicativo que se vaya a publicar.
- Se debe cuantificar la concurrencia de usuarios, ya que esto afecta la capacidad de los canales. Si por crecimiento o adecuaciones en sedes, se requiere adquirir switches, la marca debe ser la misma de los switches de core, de 24 o 48 puertos según la necesidad, con su respectivo cable de stack

en caso de que sea más de un switch. Se debe cumplir con los lineamientos de conectividad y seguridad exigidos por T.I.

Si se requiere adquirir AP (Access -Points, Puntos de acceso inalámbrico) para conexión WIFI, se deben adquirir las mismas marcas que se tienen instaladas en la infraestructura existente, con su respectiva licencia.

Si se requiere adquirir teléfonos, deben ser de la misma marca del servidor de telefonía con que cuente la entidad, con su respectiva licencia.

3.1.2 Plataforma de Red LAN

La Alcaldía de Medellín tiene una red **LAN** (Local área Network, Red de área local) la cual permite la comunicación entre el usuario final y las diferentes aplicaciones (correo, impresión, internet, sistemas de información, SAP, intranet, etc.).

Para la adquisición e instalación de los dispositivos de Red LAN (Switches de CORE, Acceso, Borde y Access Point) se debe tener en cuenta la compatibilidad con la infraestructura de la red LAN existente en la Alcaldía; cumpliendo con los estándares de conectividad a nivel de protocolos de enrutamiento, vlans, troncales entre otros y que se puedan integrar con otras marcas de otros fabricantes.Telefonía IP (Avaya)

El Distrito de Medellín cuenta con una red de telefonía que consta de dispositivos que prestan los servicios de telefonía IP, los cuales permiten que las comunicaciones se encaminen de manera adecuada, entre las diferentes sedes de la Alcaldía y el Concejo de Medellín.

Los servicios proporcionados por la plataforma de telefonía son:

- Telefonía IP, buzón de voz.
- Tarificación de llamadas.
- Call Center.
- Conferencia.
- Hunt groups
- Ivr

3.2 Equipos de cómputo

Los elementos de cómputo a adquirir deben garantizar el cumplimiento de las especificaciones mínimas definidas y adoptadas por la Secretaría de Innovación Digital.

Para todos los elementos de cómputo deberá adquirirse pre-instalado el Sistema Operativo avalado por la Unidad de Infraestructura tecnológica y dicha información deberá ser detallada de manera explícita en la factura de compra o documento equivalente.

Para cada elemento deberá pactarse cinco (5) años de garantía, certificados por el fabricante del equipo y verificable desde la página web del fabricante.

El ciclo de vida en el que se encuentra el producto ofrecido debe estar vigente al menos 5 años (end line), con actualizaciones, soporte técnico y suministro de repuestos.

Para cada equipo se deberá anexar la ficha técnica, donde se debe especificar de manera explícita que al equipo se le realizaron las pruebas de rendimiento, mediante ejecución del Benchmark Pc Mark (o la que defina la Tienda Virtual del Estado Colombiano) y aplicando el protocolo de pruebas de rendimiento definido en cómputo.

Para el Benchmark se tiene definido un porcentaje de error de hasta el 3% por debajo del umbral definido en las condiciones para el procesador, descrita en el numeral 1.2.1 de este documento.

Siendo consecuentes con las políticas del ministerio del medio ambiente y en cumplimiento de la Agenda 21 “políticas para el desarrollo sostenible del planeta”, el fabricante deberá acreditar la certificación de las normas Energy Start, Epeat Gold.

Para cada máquina que requiera ser conectada a la red de datos corporativa se deberá contar con la disponibilidad (adquiridas o por reposición) de las licencias de ofimática: **Office LTSC Standard, Windows Server - 1 Device CAL,** estas deben venir a nombre del Distrito de Medellín. Si se va a utilizar correo Exchange se debe acreditar la disponibilidad de la licencia de **CAL Exchange Server.** De no contar el Distrito con estas licencias, la dependencia deberá asumir la compra de estas.

Una vez adquiridos los elementos de cómputo mediante los diferentes procesos contractuales y después de realizado el proceso de marcación por la Unidad de Bienes Muebles, se deben ingresar a línea base de activos de TI, a través de una solicitud al CSC (Centro de Servicios Compartidos), por parte de líderes,

subsecretarios, secretarios, directores, alcalde o en su defecto el supervisor del contrato.

3.2.1 Equipos de Cómputo de Escritorio

CONDICIONES	
Garantía	Cinco (5) años para el equipo certificada por el fabricante, obligatoria con la entrega del equipo. Debe ser verificable en la página web del fabricante.
Certificado	Se solicita certificación del fabricante que indique que el proponente es canal autorizado de la marca y/o estar certificado por el fabricante.
Energía y Estándares – Obligatorios	Energy Star 7.0 o superior
	TPM 2.0 Discreto/ Físico
	EPEAT
Cables	Los equipos deben venir con todos los cables necesarios para su correcto funcionamiento.
USB Tipo C	Si el equipo a ofertar tiene todos los puertos USB TIPO C se debe entregar un adaptador a USB convencional.
Software Sistema Operativo	Última versión de Windows Profesional 64-bits OEM en español. El proveedor debe certificar en la factura que los equipos adquiridos tengan instalado el sistema operativo Windows.
Gestión de procesamiento	Sí

CONDICIONES	
Forma de entrega	El proveedor entregará los elementos contratados en los sitios definidos por la entidad y asumirá los costos del transporte de los mismos.
Marca	Registrada internacionalmente
Forma o tipo de chasís	All-in-One / Todo en uno no modular.
Línea	Corporativa
Procesador	La fecha de lanzamiento o introducción al mercado del procesador debe estar dentro de los 18 meses anteriores a la suscripción del contrato y el umbral de rendimiento PCMARK 10, mínimo de 5500, con un mínimo de 20 cores y 28 hilos, frecuencia base performance mínimo de 3,4 GHz, cache 33 MB
Memoria RAM	DDR4 a 3200 MHz o superior, con 2 ranuras intercambiables que permitan crecimiento, mínimo a 32 GB.
	1 x 16 GB
Almacenamiento	Disco Duro de 500 GB SSD M.2 PCIe o superior
Multimedia	Conectores auriculares y micrófono de 3,5 mm independiente o en combo y parlante o altavoz interno mono o estéreo.
Conectividad	Red Inalámbrica: Tarjeta de red inalámbrica PCI interna sin antena externa, protocolo 802.11 AC 2X2 y Bluetooth 5.0 o superior.
	Ethernet (RJ-45) 10/100/1000 integrada con compatibilidad nativa de IPv6 en coexistencia con IPv4.

CONDICIONES	
Puertos	Mínimo 2 Puertos USB libres tras conectar teclado y mouse.
	Mínimo 1 Puerto de video libre
Cámara web y micrófono integrados	Cámara Web integrada de 720p de alta definición y Micrófono integrado
Fuente de alimentación	Los equipos de cómputo deben contar con fuente de poder interna con capacidad de soporte estable a la configuración final requerida, mínimo 85% de rendimiento al 50% de carga.
Monitor	Monitor LED IPS, VA, PVA, MVA, TFT, FULL HD antirreflejos con ajuste de inclinación y altura ajustable. La resolución mínima del monitor debe ser FHD para 23.8” y 27”
Periféricos	Teclado en español con cable, conexión USB y teclado numérico a prueba de salpicaduras o derrame de líquidos, de la misma marca del equipo A prueba de salpicaduras o derrame de líquidos.
	Mouse con cable con conexión USB con sensor óptico, debe tener 2 botones y scroll , de la misma marca del equipo.

Tabla 8.Condiciones Generales para Adquisición de Equipos de Escritorio

3.2.2 Estación de Ingeniería (WORKSTATION)

CONDICIONES	
Garantía	Cinco (5) años para el equipo certificada por el fabricante, obligatoria con la entrega del equipo. Debe ser verificable en la página web del fabricante.
Certificado	Se solicita certificación del fabricante que indique que el proponente es canal autorizado de la marca y/o estar certificado por el fabricante
Energía y Estándares – Obligatorios	Energy Star 7.0 o superior
	TPM 2.0 Discreto/ Físico
	EPEAT
Cables	Los equipos deben venir con todos los cables necesarios para su correcto funcionamiento.
USB Tipo C	Si el equipo a ofertar tiene todos los puertos USB TIPO C se debe entregar un adaptador a USB convencional.
Software Sistema Operativo	Última versión de Windows Profesional for Workstation 64-bits OEM en español. El proveedor debe certificar en la factura que los equipos adquiridos tengan instalado el sistema operativo Windows.
Gestión de procesamiento	Sí

CONDICIONES	
Forma de entrega	El proveedor entregará los elementos contratados en los sitios definidos por la entidad y asumirá los costos del transporte de los mismos.
Marca	Registrada internacionalmente
Forma o tipo de chasís	Torre
Línea	Corporativa
Procesador	La fecha de lanzamiento o introducción al mercado del procesador debe estar dentro de los 18 meses anteriores a la suscripción del contrato y el umbral de rendimiento PCMARK 10, mínimo de 6500
Memoria	Memoria RAM de 32 GB o superior
	Con corrección de errores - ECC
Tarjeta de video	Discreta o independiente 5GB o superior.
Almacenamiento	1 Disco duro de 500 GB o superior SSD para Sistema Operativo y 1 Disco Duro 1 TB tipo SATA para Datos.
	Unidad de DVD/CD +/- R RW min 8X. Interna
Monitor	Mínimo de 27” de tecnología LED IPS o VA o PVA o MVA, antirreflejo con ajuste de inclinación, altura ajustable y resolución mínimo FULL HD
	FHD de 1920 x 1080 @60Hz o superior.
Video	Integrado, mínimo de 2GB independiente de la memoria RAM.

CONDICIONES	
Conectividad	Gigabit Ethernet integrada. Compatibilidad nativa con IPv6 y en convivencia con IPv4, con Wake On Lan activado.
Multimedia	Conectores auriculares y micrófono de 3,5 mm independiente o en combo y parlante o altavoz interno mono o estéreo.
Fuente de poder	Fuente de poder interna con capacidad de soporte estable a la configuración final requerida, mínimo 85% de rendimiento al 50% de carga. Debe dar cumplimiento a la Certificación 80 PLUS.
Puertos	Mínimo 4 puertos USB libres tras conectar teclado y mouse
	Mínimo un puerto de video libres tras conectar el monitor.
Periféricos	Teclado en español con cable con conexión USB, con teclado numérico a prueba de salpicaduras o derrame de líquidos, de la misma marca del equipo.
	Mouse con cable con conexión USB con sensor óptico, debe tener 2 botones y scroll , de la misma marca del equipo.

Tabla 9.Condiciones Generales para Adquisición de Estación de Ingeniería (WORKSTATION)

3.2.3 Equipos de Cómputo Portátiles

CONDICIONES	
Garantía	Cinco (5) años para el equipo certificada por el fabricante, obligatoria con la entrega del equipo. Debe ser verificable en la página web del fabricante.
Certificado	Se solicita certificación del fabricante que indique que el proponente es canal autorizado de la marca y/o estar certificado por el fabricante.
Energía y Estándares – Obligatorios	Energy Star 7.0 o superior
	TPM 2.0 Discreto/ Físico
	EPEAT
Cables	Deben ser suministrados todos los cables necesarios para el correcto funcionamiento del equipo.
USB Tipo C	Si el equipo a ofertar tiene todos los puertos USB TIPO C se debe entregar un adaptador a USB convencional.
Sistema Operativo	Última versión de Windows Professional 64-bits OEM en Español. El proveedor debe certificar en la factura de venta que los equipos adquiridos tengan instalado el sistema operativo en la última versión de Windows Professional 64-bits OEM en Español.
Gestión de procesamiento	Sí
Forma de entrega	El proveedor entregará los elementos contratados en los sitios definidos por la entidad, y asumirá los costos del transporte de los mismos.
Marca	Registrada internacionalmente.

CONDICIONES	
Forma o tipo de chasís	Liviano
Línea	Corporativa
Procesador	La fecha de lanzamiento o introducción al mercado del procesador debe estar dentro de los 18 meses anteriores a la suscripción del contrato y el umbral de rendimiento PCMARK 10, mínimo de 5300, mínimo 16 cores y 24 hilos, frecuencia turbo máxima a partir de 4,7 GHz, cache 30 MB o superior
Memoria RAM	DDR4 a 3200 MHz o superior, con 2 ranuras intercambiables que admiten crecimiento mínimo hasta 32 Gb o soldada con el total de crecimiento (32 Gb)
	1 x 16 GB o superior
Almacenamiento	Disco Duro de 500 GB SSD M.2 PCIe o superior
Monitor	Pantalla de alta definición, iluminada y antirreflejo. Resolución soportadas 1366 x 768 o 1280 x 800 o superior
Puertos	Mínimo 3 puertos USB
	Mínimo 1 puerto de video
Multimedia	Conectores auriculares y micrófono de 3,5 mm independiente o en combo y parlante o altavoz interno mono o estéreo.
Conectividad	Red Inalámbrica: Tarjeta de red inalámbrica PCI interna sin antena externa, protocolo 802.11 ax 2X2 y Bluetooth 5.0 o superior.
	Ethernet (RJ-45) 10/100/1000 o Ethernet mini RJ-45 integrado, con Compatibilidad nativa de Ipv6 en coexistencia con Ipv4. Se exceptúa este puerto en los portátiles de 13”
	Teclado incorporado idioma español y teclado externo adicional en español de la misma marca del equipo con conector USB.

CONDICIONES	
Periféricos	Mouse óptico con 2 botones y botón Scroll con conector USB de la misma marca del equipo.
Cámara web y micrófono integrados	Cámara web integrada de 720p HD y micrófono integrado

Tabla 10.Condiciones Generales para Adquisición de Portátiles

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.

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.

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.

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

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.

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.

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.

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.

3.6.1 Adquisición de Servidores

La adquisición de servidores debe cumplir con los siguientes lineamientos:

- Todo servidor que se vaya a adquirir debe provenir de fabricantes de marcas reconocidas a nivel mundial y con soporte en Colombia
- Tener garantía de fábrica de al menos 5 años.
- El sistema operativo debe estar licenciado y autorizado por la Unidad de Infraestructura Tecnológica de TI
- Deben ser raqueables.
- Deben tener redundancia a nivel de la alimentación eléctrica, ventilación y conexiones de red.
- Las conexiones a la red deberán ser a través de tarjetas ópticas
- Deben tener redundancia en tarjetas HBA
- Debe incluir el cableado de acuerdo al estándar del Distrito de Medellín
- Debe soportar el protocolo IP v6

Revisar la parte frontal al pasillo frio y la trasera al pasillo caliente.

3.6.2 Aprovisionamiento de Servidores

Para la provisión de servidores se requiere definir con antelación el tipo de servidor que se necesita; esto es, si requiere ser físico o puede ser virtual.

Adicional a lo anterior, se requiere definir lo siguiente:

- Sistema Operativo requerido para la implementación.
- Número de cores o procesadores requeridos
- Determinar la capacidad de memoria RAM que se necesita
- Almacenamiento requerido

Teniendo en cuenta el tipo de aplicación, bases de datos, contenedor de aplicaciones, entre otros, se debe contar con el licenciamiento adecuado, en caso de ser necesario.

Si se trata de software open source, se debe tener en cuenta contar con el contrato de soporte.

Si los requerimientos están por fuera de las capacidades existentes en la infraestructura de TI, se debe solicitar su revisión a la Unidad de Infraestructura Tecnológica.

3.6.3 Respaldo y Recuperación

3.6.3.1 Adquisición de plataforma de backup

Los dispositivos y software para la plataforma de backup deben cumplir con los siguientes lineamientos:

3.6.3.2 Dispositivos

- Todo dispositivo de almacenamiento que se vaya a adquirir debe provenir de fabricantes de marcas reconocidas a nivel mundial y con soporte en Colombia
- Tener garantía de fábrica de al menos 5 años.
- El sistema operativo debe estar licenciado por 5 años
- Deben tener redundancia a nivel de la alimentación eléctrica, ventilación y conexiones de red.
- Las conexiones a la red deberán ser a través de tarjetas ópticas
- Se debe tener en cuenta la compatibilidad con la infraestructura de la red LAN existente en la Alcaldía
- Debe tener almacenamiento inmutable, es decir, almacenamiento que protege los datos almacenados evitando cualquier cambio o alteración durante un periodo determinado o indefinido.
- Debe manejar protocolo de deduplicación que permite la consolidación de datos que busca grandes bloques de datos redundantes (normalmente de 4 KB o más) y los guarda una sola vez, independientemente del número de

copias que haya de los mismos. Un «puntero» hace referencia a los bloques de datos originales, en vez de almacenar los datos de nuevo.

- Debe ser escalable, que permita una fácil expansión, migración y crecimiento durante al menos 5 años.
- Debe tener una arquitectura de seguridad multicapa para protegerse contra múltiples vectores de ataque.

3.6.3.3 Software para backup

- Debe soportar e integrarse con los diferentes motores de bases de datos que estén aprobados por la Alcaldía
- Debe contar con funcionalidades para análisis de malware
- Debe tener integración con máquinas virtuales
- Debe permitir realizar copias de datos almacenados en la nube
- Debe permitir realizar copias de datos de la plataforma Office 365
- Debe contar con la funcionalidad de réplica de backups y manejar diferentes tipos de dispositivos como destino de las copias, es decir, librerías de cintas, nube publica, nube privada, almacenamiento NAS, almacenamiento SAN.

3.6.3.4 Uso de la plataforma de backup

Para poder que la información de aplicaciones, bases de datos, datos no estructurados, entre otros, queden incluidas en las políticas de backup deben ser explícitamente solicitadas a través de la herramienta de gestión de casos del centro de servicios compartidos.

En la medida que los recursos lo permitan se deberá respaldar la información con frecuencias diarias, semanales, quincenales y mensuales.

Para los requerimientos de respaldo dentro de las políticas de backups de los datos se debe especificar:

- Frecuencia sugerida para el respaldo
- Tipo de información a respaldar (datos estructurados o datos no estructurados).
- Para el backup de bases de datos, definir si se requiere online
- Definir si se requiere de un horario especial para la ejecución del backup
- Definir el tiempo sugerido de retención para la información respaldada
- Definir el nombre del servidor y su dirección IP.
- Definir el nombre de la aplicación a la que se le realizará el backup
- En caso de que la información a respaldar sea de una ruta específica se debe informar la ruta completa.

3.7 Almacenamiento

3.7.1 Adquisición

Para la adquisición e instalación de los dispositivos de almacenamiento (storage) se deben tener en cuenta las siguientes consideraciones técnicas:

3.7.1.1 **Generales**

- **Escalabilidad:** Debe ser escalable, que permita una fácil expansión, migración y crecimiento durante al menos 5 años.

- **Compatibilidad:** Verificar la compatibilidad en los elementos de almacenamiento con los sistemas existentes, tanto en hardware como en software.
- **Redundancia y Seguridad de Datos:** Considerar opciones que ofrezcan redundancia de datos, copias de seguridad automáticas o replicaciones.
- **Latencia y Tiempo de Respuesta:** Garantizar que el almacenamiento seleccionado ofrezca tiempos de acceso acordes a las necesidades del negocio.

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.

3.7.1.3 Sostenibilidad y Eficiencia Energética

Considerar soluciones de almacenamiento con un enfoque sostenible, que reduzcan el consumo de energía y minimicen el impacto ambiental.

3.7.1.4 Disponibilidad y Fiabilidad

- **Alta Disponibilidad:** Priorizar soluciones que ofrezcan redundancia para evitar interrupciones en caso de fallos.

- **Recuperación ante Desastres:** Incluir opciones de recuperación de datos ante desastres (DRP) que contemple copias de seguridad externas y otros mecanismos de recuperación rápida.

3.7.1.5 Soporte, garantía y Mantenimiento

- **Soporte Técnico:** Asegurarse de que la solución de almacenamiento venga con opciones adecuadas de soporte técnico, mantenimiento y actualizaciones.
- **Facilidad de Administración:** Seleccionar sistemas con interfaces de gestión intuitivas y automatización para facilitar su administración.
- **Garantía:** Tener garantía de fábrica de al menos 5 años.

3.7.1.6 Monitorización y Gestión de Rendimiento

- Incluir opciones que permitan implementar herramientas para monitorear el uso del almacenamiento, identificar cuellos de botella y optimizar el rendimiento.

3.7.1.7 Planificación de Despliegue

- Planificar la instalación, configuración, y migración de datos minimizando interrupciones al negocio.
- Asegurar temas de migración con el proveedor en temas de actualización y nuevos equipos.

3.7.1.8 Evaluación de Soluciones en la Nube pública o privada

- **Elasticidad:** Evaluar las opciones de almacenamiento en la nube en función de la elasticidad, que permite ajustar dinámicamente el espacio según las necesidades.
- **Seguridad en la Nube:** Asegurarse de que los proveedores en la nube ofrezcan medidas de seguridad robustas y cumplimiento normativo.

3.7.2 Uso información no estructurada

La entidad cuenta con una plataforma de almacenamiento tipo NAS (*Network Attached Storage)*, la cual es una solución que tiene capacidad para manejar grandes volúmenes de información que permite gran número de usuarios conectados a la red en forma concurrente, aplicando políticas y lineamientos que ayudan a almacenar, organizar, centralizar y dar acceso a los datos almacenados en ella, según las solicitudes de los líderes y directivos.

Se tienen definidos los lineamientos para su uso en el documento **DE-GTIC-027** Directrices para el Almacenamiento de la Información Corporativa en el Repositorio Oficial publicado en la plataforma de documentación de calidad de la institución.

3.7.3 Información estructurada

La entidad cuenta con una red de almacenamiento SAN (Storage Attached Network), se trata de una arquitectura completa que agrupa los siguientes elementos.

- Una red de alta velocidad de canal de fibra o iSCSI.

- Un equipo de interconexión dedicado
- Elementos de almacenamiento de red

Esta red de almacenamiento dedicada permite a los servidores y dispositivos de almacenamiento compartir datos a través de una conexión segura de alta velocidad y permite manejar grandes cantidades de datos con acceso rápido y seguro.

La SAN proporciona alta velocidad de procesamiento de entrada/salida y baja latencia características que son necesarias para las bases de datos de las aplicaciones transaccionales. Estas bases de datos contienen datos de misión crítica que requieren un alto rendimiento y disponibilidad.

La SAN también soporta la plataforma de virtualización en la que ejecutan diferentes sistemas operativos y aplicaciones.

4. Dominio Seguridad Informática

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.

4.2 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.

4.3 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 Principios para la aprobación de aplicaciones y sistemas de Información en la Alcaldía de Medellín

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 e 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:

No.	Criterio	Riesgo	Controles Deseados
1	Control de Acceso	Acceso no autorizado a la información que procesa la solución debido a una inadecuada gestión de controles de acceso	La solución define e implementa un mecanismo para garantizar que solo las personas autorizadas acceden a ellas como cuentas de usuario, asignación de contraseñas seguras, cuentas de usuario con vigencias limitadas en tiempo o a condiciones del contexto.
2	Autenticación de Usuarios	Acceso no autorizado a la información que procesa la solución debido a una inadecuada gestión de controles de acceso	La autenticación de usuarios, en caso de ser para servidores públicos y contratistas de la entidad, debe realizarse contra el directorio de autenticación corporativo a través de mecanismos seguros. La autenticación de usuarios, en casos de ser ciudadanos o personal externo a la entidad, debe realizarse frente a la solución de gestión de identidades adoptado en la organización para tal fin. En caso de que una solución esté alojada en un lugar externo a la organización y requiera utilizar los servicios de autenticación de la organización, debe utilizar mecanismos seguros, debidamente aprobados y validados por la secretaría de innovación digital. Para la autenticación se debe implementar un sistema de validación para determinar cuándo el usuario es no humano y evitar robots y spambots. Ejemplo: Captcha, reCaptcha

No.	Criterio	Riesgo	Controles Deseados
3	Gestión de roles de usuario	Acceso no autorizado a la información que procesa la solución debido a una inadecuada gestión de controles de acceso	Según la complejidad de la solución, siempre que sea posible se recomienda contar con esquema de roles de usuarios, debidamente validado por el propietario de la solución, de forma que se evite que usuarios accedan a funcionalidades que les estén autorizadas.
4	Cifrado de datos	Interceptación de los datos en tránsito o acceso a los datos almacenados debido a una inadecuada gestión de protección de los datos	Siempre que se realice transmisión de datos que la organización pudiera considerar sensibles, la transmisión debe hacerse a través del uso de algoritmos criptográficos en sus últimas versiones. De igual manera, en atención al almacenamiento de datos que la organización pudiera considerar sensibles, se deberán incluir actividades para asegurar de que no puedan ser accedidos para alguien no autorizado.
5	Protección contra código malicioso	Destrucción o daño de los datos almacenados debido a una inadecuada protección ante código malicioso.	La adquisición de la solución en caso de ser necesario, debe considerar adquirir las licencias que se requieran para la protección frente a código malicioso.
6	Protección frente a vulnerabilidades	Afectación a la confidencialidad, integridad o disponibilidad debido a una inadecuada protección frente a las vulnerabilidades de infraestructura o de aplicaciones	La solución define e implementa las acciones que se requieren para gestionar las vulnerabilidades conocidas, realizando las remediaciones necesarias.

No.	Criterio	Riesgo	Controles Deseados
7	Seguridad de servicios de las aplicaciones en redes públicas	Afectación a la confidencialidad, integridad o disponibilidad debido a una inadecuada protección del uso de servicios sobre redes públicas	La solución define e implementa las acciones para asegurar que todos los servicios que requieren de algún acceso a una red externa a la corporativa se realizan mediante protocolos seguros y debidamente cifrados.
8	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Afectación a la confidencialidad, integridad o disponibilidad debido a una inadecuada atención o soporte a la solución	La solución define e implementa las acciones para asegurar que la solución contará con un soporte permanente garantizando las actualizaciones necesarias, unos acuerdos de nivel de servicios para la atención y remediación frente a eventos o incidentes de seguridad informática que puedan impactar los servicios de la organización.
9	Protección de Registros de Operación		Se recomienda que la solución defina e implemente una adecuada gestión de la trazabilidad de las acciones realizadas por los usuarios y que se asegure para su utilización en

Tabla 11.Componentes para la valoración de Riesgos

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).

•

5. Dominio Gestión Documental Electrónica

5.1 Objetivo

Definir los lineamientos para la gestión de documentos electrónicos, que permitan una preservación digital a largo plazo de todos los documentos generados o gestionados en los diferentes procesos de la Alcaldía de Medellín.

5.2 Contexto

En la Alcaldía de Medellín estamos enfrentados a un proceso de transición del papel físico o análogo a los soportes electrónicos y digitales, estos procedimientos contribuirán a una mejor gestión administrativa aportando eficiencia y eficacia para la Gestión Documental Electrónica de archivo, aportando de manera significativa la reducción del papel físico y realizando la pasarela a un ambiente electrónico donde se utilizarán tecnologías de valor probatorio para dar cumplimiento normativo, técnico, jurídico, tecnológico alineado con los marcos de referencia definidos por el MINTIC y el Archivo General de la Nación.

El marco del Proyecto de la Modernización de la Gestión Documental Electrónica para la Alcaldía de Medellín, se definieron las estrategias que permitirán la estandarización y normalización del ciclo de Vida de los Documentos Electrónicos, el cual va desde la captura digital, la producción, la trazabilidad y la consulta que asegure la Autenticidad, Integridad y preservación de los documentos a lo largo plazo, utilizando plataformas tecnológicas con carácter probatorio y de no repudio, contando certificados digitales, estampado de tiempo longevo, correo electrónico

certificado, a través de un certificador externo registrado en el ONAC (Organismo Nacional de Acreditación en Colombia).

En el mundo digital y debido al continuo desarrollo de las tecnologías de la información y la comunicación, la firma digital se ha convertido en el procedimiento base para la autenticidad y dar valor probatorio a los documentos electrónicos. En todos los países del Mundo, del cual Colombia no es ajeno se establecido el valor probatorio en los procesos administrativos en las entidades del estado donde los documentos electrónicos han sido tenidos como pruebas validas dentro del proceso jurídicos o judiciales en Colombia, por ser un documento en línea reconocido con el mismo valor y validez probatoria que el documento público entre las partes y ante el tercero. El desarrollado de acuerdo con la pandemia por el Covid19 bajo el Decreto 806 de 2020 y el Decreto 491 de 2020, y demás normas vigentes han habilitado mayormente el uso de la Gestión Documental Electrónica para que sean tenidos como medio de prueba cuando cumplen con los atributos de ser autentico, fiable, íntegro y usable o disponible.

Con la Ley 527 de 1997 se instituye por primera vez la eficacia de la introducción de los actos administrativos por medios electrónicos como los correos electrónicos para así proveer la etapa de notificación. Además, establece en el artículo 5 que no se debe negar efecto jurídico, así como la validez a los documentos electrónicos por el simple hecho de ser mensaje de datos. (Ley 527/97, 1997). Dicha normatividad, plantea que los mensajes de datos tienen fuerza y valor probatorio, por lo que no puede negarse por estar en un medio diferente al que usualmente es aportado un documento o información.

Además, establece en el capítulo segundo “aplicación de los requisitos jurídicos de los mensajes de datos” artículo décimo, una muestra fundamental expresando que el mensaje de datos puede ser utilizado como prueba, y su poder probatorio es la prueba que brindan las disposiciones del Capítulo 13, Sección 3, Capítulo 8 del Tomo II de la Ley de Procedimiento Civil. (Ley 527/99, 1999). En consecuencia, el mensaje de datos es admitido como medio de prueba y su fuerza probatoria es la otorgada por el Código de Procedimiento Civil, hoy derogado por la Ley 1564 de 2012 “Código General del Proceso”. Por otro lado, la Ley 1437 de 2011 “Código de Procedimiento Administrativo y de lo Contencioso Administrativo” establece en el capítulo IV artículo 53 que los trámites administrativos se realizan por vía electrónica.

En este sentido, garantizar un contacto equitativo con la autoridad competente, esta debe garantizar que existen mecanismos adecuados para el libre acceso a los medios electrónicos o permitir el uso alternativo de otros programas. (Ley 1437/11, 2011) Es por ello por lo que, la Ley 1437 de 2011 correlaciona los avances obtenidos con la Ley 527 de 1999 en materia de las tecnologías de la información y también regula aspectos en materia tecnológica como la firma digital y sus clases. Marco Jurídico Analítico Regulación Nacional.

5.3 Contexto de la Preservación Digital

La preservación de los documentos y archivos electrónicos tiene como finalidad la conservación y preservación de cualquier tipo de información, independientemente del medio o tecnología con la cual se haya elaborado.

En el entorno digital a diferencia del mundo análogo del papel, para desarrollar un plan de preservación digital a largo plazo, es necesario que los componentes del documento electrónico deben mantener las características de autenticidad, integridad, confidencialidad, inalterabilidad, fiabilidad, interpretación, comprensión y disponibilidad a través del tiempo y deben reflejar la forma contextual, su producción a través de la aplicación de principios documentales (Procedencia y Orden Original), y obedecer a los tiempos de retención documental establecidos en las Tablas de Retención Documental.

5.3.1 Alcance de la Política de Preservación Digital

La Política de Preservación Digital a Largo Plazo y el Plan de Preservación Digital a Largo Plazo son aplicables en todas las dependencias de la Alcaldía de Medellín que producen, tramitan y reciben documentos en medios digitales y que la disposición final definida en las TRD es mayor a 8 años.

5.3.2 Principios de la Preservación Digital

A continuación, se definen los principios de Preservación Digital adoptados por la Alcaldía de Medellín, según el acuerdo 006 de 2014 “Por medio del cual se desarrollan los artículos 46, 47 y 48 del Título XI “Conservación de Documentos” de la Ley 594 de 2000:

Principio de Integridad: Asegurar que el contenido informativo, la estructura lógica y el contexto no se han modificado ni se ha afectado el grado de fiabilidad ni la autenticidad del documento original.

Principio de Equivalencia: Modificar, cuando sea necesario, la forma tecnológica sin alterar el valor de certeza de los documentos, como una medida para enfrentar la obsolescencia tecnológica y para garantizar el acceso a la información.

Principio de Economía: Aplicar procesos, procedimientos, métodos y técnicas de preservación viable, práctica y apropiada para el contexto de los documentos, de tal modo que se asegure la sostenibilidad técnica y económica de la preservación digital.

Principio de Actualidad: Evolucionar al ritmo de la tecnología y utilizar los medios disponibles en el momento actual para garantizar la preservación de los documentos en el futuro. Esto significa que en un sistema de preservación digital debería mantener la capacidad de evolucionar, de ajustarse a los cambios dimensionales y añadir nuevas prestaciones y servicios.

Principio de Cooperación: Reutilizar y compartir soluciones ya existentes y desarrolladas de forma conjunta con otros archivos digitales, especialmente las relacionadas con los procesos que pueden ser gestionados de forma centralizada.

Principio de Normalización: Generar lineamientos y herramientas basadas en normas, estándares y buenas prácticas, como apoyo a la gestión y preservación de los documentos digitales.

5.4 Lineamientos Técnicos para la gestión documental electrónica

La secretaría de Innovación Digital define los lineamientos los cuales son de uso obligatorio para las diferentes áreas productoras o generadoras de información documental en la Alcaldía de Medellín.

5.4.1 Aval Técnico proceso de gestión documental electrónica

Para el desarrollo de proyectos a nivel de la Gestión Documental Electrónica, estos deberán contar con un aval técnico por parte del Equipo de Gestión Documental, quien dará las recomendaciones y sugerencias a incluir en los proyectos que involucren generación de contenido documental de Archivo.

El alcance del Aval Técnico incluye los procesos de digitalización certificada con valor probatorio, para los cuales las dependencias deberán entregar el Protocolo de Digitalización a utilizar para su verificación.

Los procesos que incluyan a través de los Sistemas de Información y que genere documentos de archivo ya sea con la representación gráfica a través de .PDF o generación de diferentes contenidos como imágenes, videos, audios, planos, deberán generar las integraciones que sean necesarias para que pueda realizar una interoperabilidad con el Sistema

de Gestión Documental Electrónica de tal forma que los procesos de captura, gestión, almacenamiento y publicación quede integrado al expediente electrónico, dando cumplimiento a las estructura archivística ajustada a la TRD para la dependencia, de tal forma que se aseguren los atributos de **autenticidad, fiabilidad, integridad, usabilidad o disponibilidad** para que tenga validez sin necesidad de imprimir los documentos

5.4.2 Definir documentos Electrónicos (E.Docs) a preservar

Para lograr implementar la política de preservación digital, la primera actividad a realizar es la identificación de la información de archivo que se debe preservar, ya que *NO* todos los documentos deben surtir este tipo de procedimientos. Por ***documento de archivo*** se entiende el registro producido o recibido por la Alcaldía de Medellín en razón de sus actividades o funciones.

Con el fin de dar un mejor entendimiento para las áreas productoras y de gestión a continuación se describe la estructura de documentos adoptadas para la Alcaldía de Medellín:

- ***Documento de archivo****:* Registro de información producida o recibida por la Alcaldía de Medellín en razón de sus actividades o funciones.

- **Documento activo*:*** Aquel con valores primarios [21] cuyo uso es frecuente.
- **Documento de apoyo**: Documento generado por la misma oficina o por otras oficinas de la Alcaldía de Medellín, que no hace parte de sus series documentales, pero es de utilidad para el cumplimiento de sus funciones.
- **Documento esencial:** Documento necesario para el funcionamiento de la Alcaldía de Medellín y que, por su contenido informativo y testimonial, garantiza el conocimiento de las funciones y actividades del mismo, aun después de su desaparición, por lo cual posibilita la reconstrucción de la historia institucional.
- **Documento electrónico de archivo (e-docs):** Registro de la información generada, recibida, almacenada, y comunicada por medios electrónicos, que permanece en estos medios durante su ciclo vital; es producida por un servidor público de la Alcaldía de Medellín. o persona o entidad que presta los Servicios para la Administración Municipal, que en razón de sus actividades y debe ser tratada conforme a los principios y procesos archivísticos.
- **Documento facilitativo**: Documento producido en cumplimiento de funciones idénticas o comunes en todas las entidades.
- **Documento histórico:** Documento único que por su significado jurídico o autográfico o por sus rasgos externos y su valor permanente para la dirección

[21] Valores Primarios: Es el que tienen los documentos mientras sirven a la institución productora y al iniciador, destinatario o beneficiario del documento, es decir, a los involucrados en el tema o en el asunto. Definición de los tipos de documentos tomada de la Fuente de Información del Archivo General de la Nación en sus diferentes documentos técnicos.

del Estado, la soberanía nacional, las relaciones internacionales o las actividades científicas, tecnológicas y culturales, se convierte en parte del patrimonio histórico.

- **Documento inactivo:** Documento que ha dejado de emplearse al concluir sus valores primarios.
- **Documento misional**: Documento producido o recibido por una institución en razón de su objeto social.
- **Documento original:** Fuente primaria de información con todos los rasgos y características que permiten garantizar su autenticidad e integridad.
- **Documento público:** Documento otorgado por un funcionario público en ejercicio de su cargo o con su intervención.

Para el cumplimiento de este lineamiento las diferentes áreas de la Alcaldía de Medellín debe tener como base teniendo en cuenta la Tabla de Retención Documental actualizadas para el área organizacional y actualizadas para el soporte electrónico como el instrumento archivístico en el cual se refleja la Valoración Documental, identificando los valores primarios y secundarios de cada una de las series y subseries documentales producidas por cada dependencia de la Alcaldía de Medellín, se debe tener en cuenta la definición de sus tiempos de retención y los procedimientos de disposición final correspondientes.[22]

[22] Tomado Programa de Gestión Documental PGD – de la Alcaldía de Medellín

Será responsabilidad de cada área productora el análisis y selección de las series a preservar a largo plazo aplicando el criterio establecido de tiempo de retención mayor a ocho (8) años teniendo como base la TRD actualizada y generar el Pla de Preservación documental con los responsables y plan de acción, el cual deberá ser entregado al Equipo de Gestión Documental para el seguimiento y asegurar el cumplimiento del plan de preservación documental específico, este plan tendrá el acompañamiento técnico del equipo de Gestión documental para definir los tipos de tecnología digital a incluir según el tipo de información y soporte en el que se encuentre la información los cuales van desde planes de migración, emulación, replicado o refreshing, este plan se debe alinear con las políticas de seguridad de la información de la Alcaldía de Medellín, en el plan específico por entidad productora debe especificarse:[23]

Contexto de la preservación, identificación de medios de almacenamiento y formatos digitales; evaluación de los aspectos técnicos, riesgos y diferentes estrategias de preservación; resultados de la evaluación realizada; estrategia de preservación seleccionada incluida la decisión con su justificación; funciones y responsabilidades para el plan de preservación y su seguimiento; presupuesto para la formulación y ejecución.

[23] Estas actividades de la preservación especifican para la preservación de los documentos específicos para lo cual el equipo de Gestión Documental Electrónica está prestando las asesorías respectivas.

En caso de requerir presupuesto para la implementación, serán responsabilidades de las áreas productoras en coordinación con la Secretaría de Innovación Digital.

5.4.3 Gestionar los documentos Electrónicos de archivo (E.Docs)

Un *Documento electrónico de archivo (e-docs)* es un registro de la información generada, recibida, almacenada, y comunicada por medios electrónicos, que permanece en estos medios durante su ciclo vital, es producida por un servidor público de la Alcaldía de Medellín, persona o entidad que presta los Servicios para la Administración Municipal, que en razón de sus actividades y debe ser tratada conforme a los principios y procesos archivísticos.

Se pueden producir y/o capturar en cualquier formato electrónico, asegurándose que se trate de formatos sin obsolescencia tecnológica o que estén en desuso, por tal motivo el Equipo de Gestión Documental Electrónico definió los formatos autorizados de acuerdo con el contenido.

Los archivos producidos deben quedar almacenados en la Unidad que haya sido definida por la Secretaría de Innovación y debe ser estructurada de acuerdo a lo definido en la tabla de Retención Documental en las series, subseries y tipos documentales.

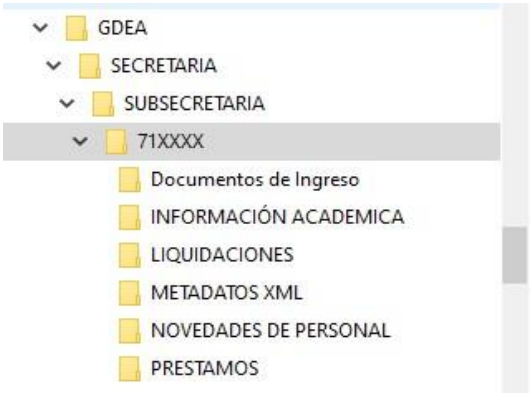
Los documentos integrados de una aplicación a otra, deberán ser únicos, y no se permite la duplicación de archivos en diferentes unidades de almacenamiento, cada archivo electrónico debe generar un hash que lo identifique como único, las demás

aplicaciones deben referenciar y llamar el mismo archivo electrónico, se prohíben copias de archivos.

El equipo de Gestión Documental Electrónica definirá en la Unidad de Almacenamiento la estructura de carpetas a utilizar, de igual forma se realizarán mesas de trabajo para definir la estructura de archivo definitiva la cual sea un reflejo de la TRD y donde cada servidor público debe almacenar la información debidamente clasifica en su formato final y en los formatos electrónicos definidos.

Los servidores y servidoras públicos de la Alcaldía de Medellín en el ejercicio de sus funciones actividades y conforme a los principios y procesos archivísticos, en el proceso de gestión de los documentos y a lo largo del ciclo de vida de los documentos se van elaborando documentos de apoyo o anexos que se pueden convertir en la versión definitiva, esta versión es la que debemos guardar con la estructura documental definida por el Equipo de Gestión Documental.

A continuación, un ejemplo de estructura:



En cada carpeta van los documentos en los formatos definidos según el Anexo 1 FORMATOS DEFINIDOS PARA LA PRESERVACION DIGITAL.

Los archivos deben tener nombres que identifiquen el tipo documental, la inicial en Mayúscula, separados por guion bajo, que den claridad el contenido. Se entregará a cada área productora los estándares a realizar en las mesas de trabajo con el equipo de Gestión Documental Electrónica.



Pueden generar un documento electrónico en diferentes versiones, pero solamente se preservará la versión final de este, las versiones anteriores se tomarán como documentos de apoyo que no son susceptibles a preservar y son susceptibles a eliminación por el productor documental.

5.4.4 Uso de formatos de Archivo para la gestión de documentos de archivo (E.Docs)

El equipo de Gestión Documental de la Secretaría de Innovación establece los tipos de formatos a utilizar por las diferentes soluciones tecnológicas de la Alcaldía de Medellín, los cuales son de uso obligatorio para la generación de documentos para

todas las dependencias para los nuevos procesos a realizar y para los documentos creados con anterioridad a la publicación del este documento, deberá definir el plan de migración de estricto cumplimiento para la estandarización, los cuales deberán entregar en el mes de junio de 2021 y en coordinación con el Equipo de Gestión Documental Electrónico iniciar la ejecución.

Los formatos de archivos definidos que permiten la preservación digital en el tiempo, y que han sido definidos por Ministerio de las TIC en la G.Inf.08 Guía para la gestión de documentos y expedientes electrónicos y que la Secretaría de Innovación Digital adopta como exigencia para todas las dependencias de la Alcaldía de Medellín.

5.4.5 Integración con Soluciones de Tecnología

Los nuevos desarrollos de Soluciones de tecnología deben adoptar los formatos de archivos establecidos por el Equipo de Gestión Documental Electrónico, de acuerdo con los tipos de representación gráfica a nivel de .pdf, o sonido, mapas, de acuerdo con el Anexo 1 FORMATOS DEFINIDOS PARA PRESERVACION DIGITAL, en el cual se definen para la Alcaldía de Medellín los formatos a utilizar para los documentos electrónicos de archivos, el anexo agrupa por tipos de contenidos, donde se definen las características técnicas, el tipo de extensión, el estándar referenciado si es para difusión de la información para la preservación a largo plazo de los archivos.

Los contenidos definidos y de uso estricto cumplimiento para las soluciones tecnológicas en la Alcaldía de Medellín se agrupan en los siguientes contenidos de los archivos[24]:

- Contenido Genérico.
- Contenido de imagen.
- Contenido de audio.
- Contenido de video.
- Contenido Geoespacial.
- Formato de compresión.
- Base de Datos.
- Páginas Web.
- Correo Electrónico.

Ver anexo 1: Anexo 1 Formatos Definidos Para La Preservación Digital.

En caso de que las áreas productoras reciban documentos electrónicos de archivo soportados en formatos propietarios estos deberán ser convertidos a los formatos definidos por la Secretaría de Innovación Digital, a formatos con reconocimiento

[24] Los contenidos de archivo se estarán actualizando en las próximas versiones de lineamientos liberadas.

OCR (PDF/A) o el formato que aplique de acuerdo con en el Anexo *1 Formatos Definidos Para La Preservación Digital.*

5.4.5.1 Correo Electrónico (E-MAIL)

El correo electrónico es considerado documento electrónico siempre que sea utilizado como una comunicación oficial interna o externa o haga parte de un trámite en el cumplimiento de las funciones de la Alcaldía de Medellín, por tanto:

Se debe usar el correo Institucional para el desarrollo de las funciones corporativas, en cual no requiera evidencia de envío, entrega y apertura.

Se debe usar los Servicios de correo electrónico certificado en uso de la comunicaciones externas (dominio diferentes a @medellin.gov.co), este servicio permite realizar un tracking al correo enviado, donde se indicara entre otros atributos, la IP desde donde se envía el correo, la IP del buzón del destinatario, fecha y hora de envío, fecha y hora de llegada a la bandeja de correo del destinatario, hora y fecha apertura del archivo, todos estos procedimientos quedan registrado en el acta de entrega que realiza el certificador de confianza.

Los correos electrónicos certificados deben salir de las cuentas de los funcionarios que tengan autorizado el firmado digital, el estampado de tiempo de los documentos de acuerdo a lo definido por el Equipo de Gestión Documental Electrónico. Este es el tratamiento que se debe realizar para las comunicaciones oficiales externas y aquellos correos que se constituyan como un documento de archivo, para el caso de la Gestión Documental se deben enviar a través del Sistema de Gestión

Documental para que este quede radicado y hace parte de la gestión de respuesta quedando integrado a la gestión del trámite o Servicio para el Ciudadano.

Al igual que los documentos electrónicos, los emails pueden ser archivados atendiendo los cuadros de clasificación y tablas de retención documental.

La impresión en papel o una captura de pantalla no reemplaza el correo original en su formato nativo, razón por la cual el Equipo de Gestión Documental No avala este tipo de prácticas, ya que esta operación pierde entre otros datos relacionados con la producción y transmisión del mensaje.

5.4.5.2 Plataformas de Comunicación por Internet

Si bien es cierto que, con la situación actual de pandemia, las entidades públicas y en nuestro caso la Alcaldía de Medellín habilitaron múltiples canales de comunicación como son los chats (mensajería instantánea), video chat, video conferencias, redes sociales, es importante tener en cuenta los siguientes lineamientos desde la Gestión Documental Electrónica.

5.4.5.3 Chat (mensajería instantánea)

Los chat, video chat o similares NO se constituyen como documentos electrónicos de archivo por no contar con los mecanismos para su captura y gestión que permita garantizar su Autenticidad, integridad, fiabilidad y disponibilidad, ni su preservación.

Las impresiones en papel o .pdf o las capturas de pantalla de los chats, no se constituyen como documentos electrónicos de archivo y no reemplazan el chat en su forma nativa.

5.4.5.4 Videoconferencias

Las video conferencias, video llamadas o similares pueden considerarse como documentos electrónicos de archivo, siempre y cuando se incluya en la estructura archivística y sea parte del tipo documental, guardándolo en el formato definido den el Anexo 1, para asegurar su preservación digital.

Las grabaciones pueden ser consideradas como documentos de archivo si son capturas en su formato original, para lo cual se debe descargar indicando los metadatos y cuidando de las normas de protección de datos personales y las autorizaciones requeridas en caso de grabar video conferencias.

5.4.5.5 Redes sociales

El uso de redes sociales NO se considera documentos electrónicos de archivo por no contar con los mecanismos para su captura y gestión que permita garantizar su Autenticidad, integridad, fiabilidad y disponibilidad, ni su preservación.

Las impresiones en papel o .pdf o las capturas de pantalla de los chats, no se constituyen como documentos electrónicos de archivo y no reemplazan el chat en su forma nativa.

5.4.6 Autenticidad, Integridad y Fiabilidad de los documentos electrónicos (E-Docs).

El Valor Probatorio de un documento de archivo permite identificar los atributos para que tengan validez, como se define en la Norma Técnica Colombiana NTC-

ISO 30300 conocida también como “Información y Documentación. Sistemas de Gestión para Registros. Fundamentos y Vocabulario” el cual forja las características de la Ley General de Archivos del Estado y la Norma Técnica Colombiana ISO-15489-1. Así entonces, las características fundamentales que debe poseer un documento de archivo son los siguientes**: autenticidad, fiabilidad, integridad, usabilidad o disponibilidad**, los cuales se deben garantizar mediante el uso de los ELEMENTOS DE VALOR PROBATORIO entre los cuales se encuentran la firma electrónica, la firma digital, el estampado de tiempo longevo, el correo electrónico certificado, el código de verificación y marcas de agua.

La Secretaría de Innovación Digital establece el uso de tecnologías de valor probatorio para 386 funcionarios de tipo administrativo los cuales están autorizados para el uso de esta tecnología. Los servidores autorizados para los elementos de valor probatorio son: Secretarios de despacho, subsecretarios de despacho, directores administrativos, subdirectores administrativos, líderes de programa, líderes de proyecto, inspectores de categoría especial de la secretaría de Movilidad e inspectores de policía y/o aquellas personas con vinculación a la alcaldía de Medellín, que en uso de sus funciones requiera el uso de esta tecnología. Es importante aclarar que no se autoriza esta tecnología para personal contratista.

El uso de la tecnología de valor probatorio debe ser a través de formatos electrónicos predefinidos en el sistema de gestión documental, y de manera integrada 4 elementos, que ya se han mencionado anteriormente, igualmente se define que los documentos de archivo solo deben contener una (1) sola firma, el cual lo debe realizar el servidor público de mayor rango.

El Sistema Actual de Gestión Documental Mercurio se cuenta con los desarrollos para el fortalecimiento de la seguridad de la información, el cual se encuentra implementado la firma digital, el estampado de tiempo longevo y el correo electrónico certificado en la Serie Comunicaciones Oficiales, para la generación de las respuestas oficiales que se enviadas a los ciudadanos y a las comunicaciones internas, las comunicaciones recibidas, la generación de normas y procesos de certificación para los procesos de Digitalización.

5.4.7 Procesos de digitalización certificada con finas probatorios.

La digitalización de documentos se establece como el proceso tecnológico y archivístico, por medio del cual se convierte, un documento de archivo que se produce en soporte análogo, físico o papel, a una imagen digital del documento de archivo.

La Ley 594 de 2000, en su Art. 19, establece que las entidades podrán incorporar tecnologías de avanzada en la administración y conservación de sus archivos, empleando cualquier medio técnico, electrónico, informático, óptico o telemático, siempre y cuando se cumpla con los requisitos de organización archivística de los documentos, teniendo en cuenta aspectos como la conservación física, las

condiciones ambientales y operacionales, la seguridad, perdurabilidad y reproducción de la información contenida en estos soportes, así como el funcionamiento razonable del sistema.

De acuerdo con esta Ley, técnicas reprográficas como la digitalización, pueden ser aplicadas a cualquier tipo de documento, siempre y cuando estos procesos respondan a una decisión basada en la política de gestión documental de la Alcaldía de Medellín y se desarrollen de conformidad con el Programa de Gestión Documental -PGD- Aprobado en sus procesos y procedimientos, en cumplimiento de la normativa legal y estándares vigentes en materia de archivos, de tal manera que pueda atribuirse valor probatorio a los documentos.

Además de estos aspectos, el valor probatorio de la digitalización depende de los procesos de calidad de las imágenes y que éstas conserven sus atributos de autenticidad, fiabilidad, usabilidad, accesibilidad y perdurabilidad, que le otorguen la fuerza probatoria del original, de tal manera que cuando se requiera una copia ésta represente los atributos del documento físico; también se debe utilizar las herramientas definidas para los procesos de digitalización.

El proceso de digitalización implica que, para llevar los documentos de archivo del ámbito físico al ámbito digital, se debe realizar bajo las características integrales propias de la archivística y gestión documental, con base en la normatividad nacional y distrital, que conlleva la implementación de buenas prácticas para el uso racional de los recursos, entendiendo que la política “Cero Papel” no es sólo una actividad tecnológica, sino que se requiere la integración de los recursos humanos,

técnicos y tecnológicos adecuados, que se armonicen con los objetivos que señala la Directiva Presidencial 04 de 2012, los cuales son: optimizar, racionalizar, simplificar y automatizar los procesos de la entidad, aplicando de forma correcta la disciplina archivística y la gestión documental, para garantizar la protección del patrimonio documental digital.

Es indispensable advertir que la digitalización e indexación de la documentación de archivo, está regulada desde la Secretaría de Innovación Digital, por lo tanto los proceso de digitalización que se quieran adelantar en las diferentes áreas deberán solicitar el acompañamiento del Equipo de Gestión Documental Electrónica.

La herramienta tecnológica a utilizar para cualquier proceso de Digitalización in house o out house, será el Visor Documental 360. La parametrización de los flujos documentales se realizará con la asesoría del Equipo de Gestión Documental Electrónico.

En el visor documental 360 se deberá cumplir cada una de las etapas definidas como son desde el ingreso FUIDE, el alistamiento, la digitalización, el control de calidad 1, control de calidad 2, control de calidad 3, certificación y carga a la herramienta definidas por el equipo de Gestión Documental Electrónica de la Alcaldía de Medellín, como se muestra en la siguiente gráfica:

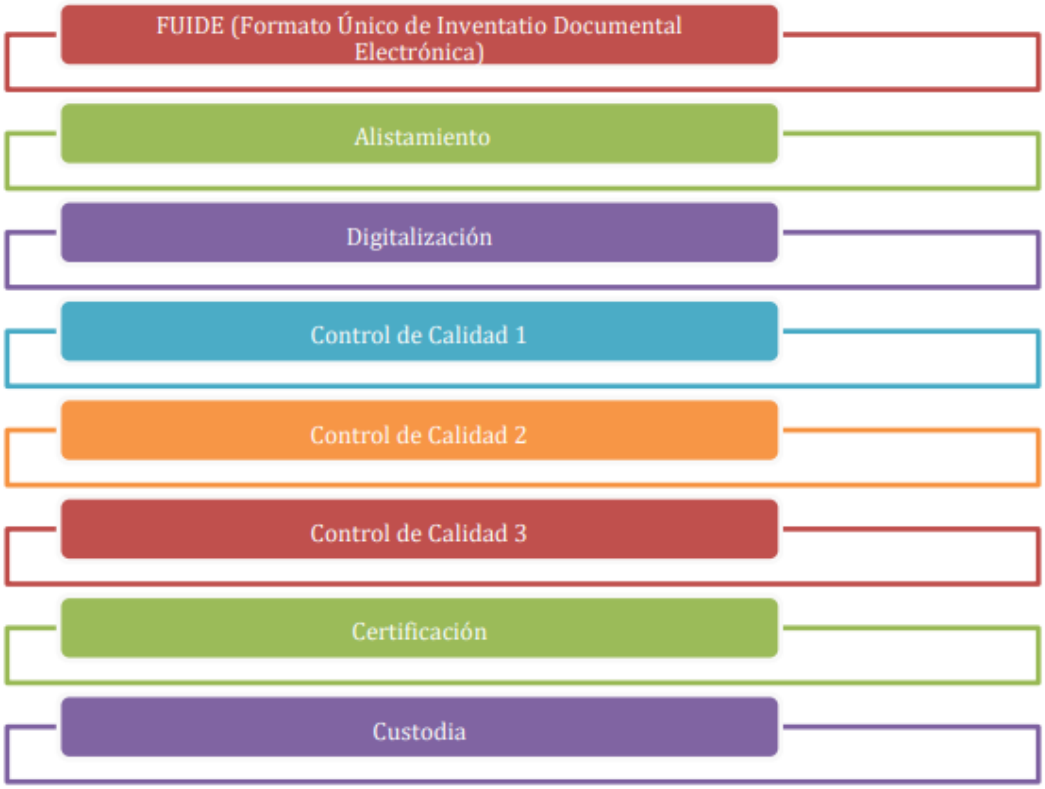


Ilustración 8. Etapas Definidas FUIDE

Se utilizará el software de Visor Documental 360 con el fin de realizar un seguimiento diario del proyecto, mostrando los avances en cada una de las etapas del proyecto de Digitalización Certificada.

5.4.8 Utilizar Metadatos de preservación.

De acuerdo con lo señalado en la norma UNE-ISO 23081-1, los metadatos son "*Información estructurada o semi estructurada que posibilita la creación, registro, clasificación, acceso, conservación y disposición de los documentos a lo largo del tiempo"*. Los metadatos se consideran desde el contexto mismo en el que se crea o produce la información, hasta las características técnicas, en el cual fue originado o convertido, de tal manera que permita su acceso preservación y transferencia. Se deben incluir entre 2 y 10 metadatos descriptivos según las características de los documentos y la estructura *Dublin Core Initiativa* correspondiente a 5 elementos de metadatos descriptivos obligatorios y 10 elementos de metadatos descriptivos optativos.

Estructura *Dublin Core Initiativa*[25]

Tanto los documentos electrónicos de archivo como sus expedientes necesitan la asignación de metadatos mínimos obligatorios siguiendo la norma ISO 23081, DUBLIN CORE y METS.

A continuación, se presenta la estructura mínima de metadatos que deben contener tanto los expedientes como los documentos que los conforman para su identificación, autenticación y contextualización:

[25] Tomado de la Guía para la Gestión de Documentos y Expedientes Electrónicos G.INF.07, Ministerio de Tecnologías de información y las comunicaciones MINTIC. Noviembre de 2017

DUBLIN CORE[26]					
No.	**Nombre**	**Estructura XML / Etiqueta**	**Obligatoriedad**		**Descripción**
1	Título	<Title>	O	Elemento obligatorio	Normalmente el título será el nombre por el que se conoce formalmente el recurso (expediente)
2	Autor	<Creator>	O	Elemento obligatorio	Autor personal o entidad responsable del contenido del recurso (expediente)
3	Fecha	<Date>	O	Elemento obligatorio	Fecha clave del recurso (creación del expediente)
4	Materia	<Subject>	Opt	Elemento Optativo	Descriptores o palabras claves que definen el tema del que trata el recurso (expediente)
5	Editor	<Publisher>	Opt	Elemento Optativo	Editor del Recurso
6	Tipo de Recurso	<Type>	Opt	Elemento Optativo	Naturaleza del contenido (artículo, tesis, ponencia, etc.).
7	Descripción	<Description>	Opt	Elemento Optativo	Resumen del recurso
8	Colaborador	<Contributor>	Opt	Elemento Optativo	Personas o entidades colaboradoras en el contenido del recurso.
9	Formato	<Format>	O	Elemento obligatorio	Formato del recurso (tamaño, duración, software, hardware necesario para su reproducción, etc.).
10	Fuente	<Source>	Opt	Elemento Optativo	Recurso relacionado del cual se deriva el recurso que se describe
11	Derechos	<Rigths>	Opt	Elemento Optativo	Derechos de autor que afectan al recurso (copyright, IPR, etc.).
12	Identificación	<Identifier>	Opt	Elemento Optativo	Referencia unívoca de identificador del recurso (ISBN, URL, DOI, etc.).
13	Idioma	<Language>	Opt	Elemento Optativo	Idioma en el que esta expresado el recurso
14	Relación	<Relation>	O	Elemento obligatorio	Otro recurso relacionado con el que se describe (referencia cruzada)
15	Cobertura	<Coverage>	Opt	Elemento Optativo	Periodo de tiempo o lugar geográfico sobre los que trata el recurso.

[26] Ht10tp://dublincore.org/

Para desarrollar el proceso de indexación o descripción documental se deben tener en cuenta las pautas o estándares establecidos tanto por el Archivo General de la Nación como de la Secretaría de Innovación Digital.

Se debe tener en cuenta el *Formato Único de Inventario Documental*, en el cual se registra la información que corresponde a los expedientes generados y administrados por cada archivo de gestión, en cada dependencia y que luego son transferidos al Archivo Central, que por lo general son los que se encuentran en soporte físico, aunque el formato de inventario es transversal a cualquier soporte. Esta herramienta brinda datos fundamentales para avanzar en el proceso de descripción.

Para la identificación de los metadatos de cada uno de los documentos electrónicos de archivo se deberá pedir el acompañamiento del equipo de Gestión Documental Electrónica.

Cuando se cumpla el tiempo de retención en archivo central o culminado el trámite o cerrado el expediente electrónico se deberá realizar la conversión de todos los tipos documentales que integran el expediente para garantizar la preservación a Largo Plazo, cada entidad generadora podrá utilizar los formatos longevos definidos en el **Anexo Formatos definidos para la preservacion digital.pdf**. (Formatos de archivo de uso común)

Una vez analizada la serie o colección a preservar se deberá seleccionar la estrategia técnica para la preservación digital la cual deberá estar soportada, documentada y justificada de acuerdo con los requisitos de preservación de los

documentos, las estrategias a utilizar definidas por la Secretaría de Innovación Digital son:

- **Migración:** Cambio a nuevos formatos/plataformas (hardware y software) o nuevos medios.
- **Emulación:** Recreación en sistemas computacionales actuales del entorno software y hardware para permitir la lectura de formatos obsoletos.
- **Replicado:** Copias de la información digital establecidas según la política de seguridad de la información de la entidad.
- **Refreshing:** Actualización de software o medios.

Para realizar las técnicas mencionadas las áreas productoras o responsables de la administración municipal, contarán con la asesoría del equipo de gestión documental y su implementación con el equipo de infraestructura.

6. Dominio Uso y Apropiación de TIC

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.

6.2 Lineamientos de Uso y Apropiación

Conforme a lo descrito para el dominio en las guías oficiales del MinTIC, los lineamientos para uso y apropiación de las TIC son los siguientes[27]:

Identificación del Lineamiento	Descripción
MGGTI.LI.UA.01 Estrategia de Uso y Apropiación de TI	La Dirección de Tecnologías y Sistemas de la Información, o quien haga sus veces, es la responsable de definir la estrategia de uso y apropiación de los componentes de TI.
MGGTI.LI.UA.02 Gestión del cambio	La dirección de Tecnologías y Sistemas de la Información, o quien haga sus veces, es la responsable de elaborar una estrategia de gestión del cambio cada vez que se despliegue o adquiera un nuevo sistema de información, solución o aplicación de software en la Entidad.
MGGTI.LI.UA.03 Plan de Formación	La Dirección de Tecnologías y Sistemas de la Información, o quien haga sus veces, es la responsable de articularse con los responsables de la entidad y asegurar que el plan de

[27] MGGTI.G.UA - USO Y APROPIACIÓN DE TI – MinTIC 2023

Identificación del Lineamiento	Descripción
	formación de la institución incorpore adecuadamente el desarrollo de las competencias internas requeridas en TI.
MGGTI.LI.UA.04 Evaluación del nivel de adopción de TI	La Dirección de Tecnologías y Sistemas de la Información, o quien haga sus veces, debe contar con indicadores de uso y apropiación para evaluar el nivel de adopción de la tecnología y la satisfacción en su uso, lo cual permitirá desarrollar acciones de mejora y transformación.
MGGTI.LI.UA.05 Plan de capacitación y entrenamiento sobre los sistemas de información	La Dirección de Tecnologías y Sistemas de la Información, o quien haga sus veces, debe realizar constantemente capacitación y entrenamiento funcional y técnico a los grupos de interés, para fortalecer el uso y apropiación de los componentes de TI disponibles.

Tabla 12. Lineamientos para el Uso y Apropiación de las TIC - MinTIC 2023

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.

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.

"*El proceso de adaptación a nuevas tecnologías y componentes de TI es diferente para cada persona. Algunas personas pueden valorar la certeza y evitar los riesgos de lo desconocido, mientras que otros se pueden sentir motivados por la posibilidad de la experimentación y la novedad. Estas últimas, que están espontáneamente inclinadas a aprender, pueden sentirse motivados al ser reconocidos como agentes, líderes de cambio,*

mientras que para los más reticentes pueden encontrar confianza al identificar a quién seguir, consultar o inclusive imitar."[28]

Es por esto 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.

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.

[28] MGGTI.G.UA – Uso y Apropiación de TI MinTIC 2023

- 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.

6.3.2 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:

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:

Alcaldía de Medellín

Secretaría de Innovación Digital
Estrategia de Uso y Apropiación de TIC
Gestión del Cambio de Proyectos Informáticos

Proyecto	
Objetivo	
Responsable	
Fecha	

Matriz de Interesados

LISTA DE INTERESADOS						PODER/ INFLUENCIA					
Nombres y Apellidos	Cargo	Dependencia	Correo electrónico	**Rol y/o Función en el proyecto** Rol: Función que la persona o entidad desempeñará en la implementación de la Iniciativa de TI	**INTERNO / EXTERNO** **Interno:** servidor/ contratista del Distrito **Externo:** Proveedor, Empresas Outsourcing, Entidad Adscrita y/o	Objetivo	Alcance	Obtención del Beneficio	Toma de Decisiones	Grado de Influencia	Tipo de Influencia

Ilustración 8.Formato de Matriz de Interesados - Gestión del Cambio Proyectos Informáticos

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.

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.

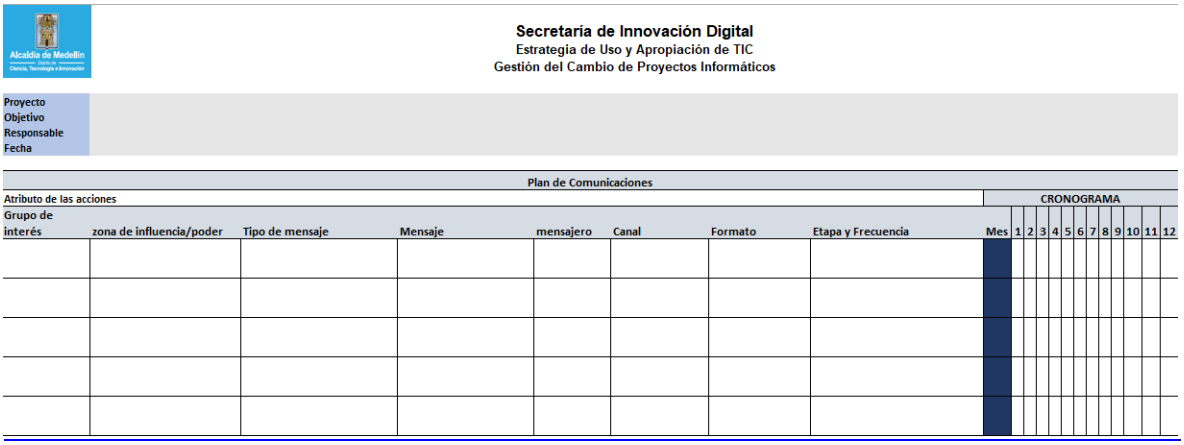
Para la construcción del plan se debe contar con el acompañamiento del área de comunicaciones de la dependencia que realiza el proyecto, de manera que se aprovechen los canales y estrategias institucionales y se potencien otras herramientas comunicacionales e incluso se promueva la articulación con otras 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:



Secretaría de Innovación Digital
Estrategia de Uso y Apropiación de TIC
Gestión del Cambio de Proyectos Informáticos

Proyecto
Objetivo
Responsable
Fecha

Plan de Comunicaciones																							
Atributo de las acciones								CRONOGRAMA															
Grupo de interés	zona de influencia/poder	Tipo de mensaje	Mensaje	mensajero	Canal	Formato	Etapa y Frecuencia	Mes	1	2	3	4	5	6	7	8	9	10	11	12			

Ilustración 9. Formato de Plan de Comunicaciones - Gestión del Cambio Proyectos Informáticos

- 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.

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 como[29]:

[29] MAE.G.UA - USO Y APROPIACIÓN DE LA PRÁCTICA DE AE

- **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 en el sistema de información.

El plan de formación deberá conformarse según el formato existente para tal fin en el cual se incluirán los siguientes elementos:



Secretaría de Innovación Digital
Estrategia de Uso y Apropiación de TIC
Gestión del Cambio de Proyectos Informáticos

Proyecto
Objetivo
Responsable
Fecha

Plan de Formación

No	Tipo de Actividad	Grupo de interés	Temática	Objetivo	Contenidos	Competencias	Modalidad Virtual /Presencial	Duración	Fechas	Instructor	Estado
1											
2											
3											
4											
5											
6											
7											

Ilustración 10.Formato de Plan de Formación - Gestión del Cambio Proyectos Informáticos

- **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 y comportamientos desarrolla o afianzaesta 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.

[30] Banco de Recursos ApropiaTIC: https://medellingovco.sharepoint.com/sites/BancoDeRecursosApropiaTIC?locale=es-es

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:

ENTRADAS	• Documentación Proyecto a implantar • Matriz de interesados • Plan de comunicaciones • Plan de formación
SALIDAS	• Evaluación plan de gestión del cambio • Resultado Indicadores
PARTICIPANTES	• Equipo directivo del proyecto • Secretaría de Innovacion Digital • Equipo de Formación y Capacitación de la Subsecretaría de Gestión Humana • Equipo de Comunicaciones • Áreas involucradas en el proyecto

Tabla 13.Entradas y salidas para el seguimiento Gestión del Cambio Proyectos Informáticos

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.

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[31]:

Aspecto	Indicador	Descripción	Fórmula
Grado de implementación	Ejecución del plan de comunicación	Mide la ejecución de las actividades planeadas en el plan de comunicaciones	Número de actividades ejecutadas/ Número de actividades planeadas
	Ejecución del plan de formación	Mide la ejecución de las actividades planeadas en el plan de formación	Número de actividades ejecutadas/ Número de actividades planeadas
	Cobertura de plan de formación	Mide el porcentaje de personas involucradas en los cambios que recibe efectivamente actividades de formación.	Cantidad de personas capacitadas/ Cantidad de personas involucradas
	Asistencia al plan de formación	Mide la asistencia efectiva a las actividades y permite inferir la efectividad de las actividades de convocatoria y el interés en la formación.	Cantidad de asistentes efectivos/ Cantidad de convocados

[31] Tomados de la MGGTI.G.UA Guía del Dominio de Uso y Apropiación de TI – MinTIC 2023

Aspecto	Indicador	Descripción	Fórmula
Grado de cumplimiento de logros	Nivel de satisfacción	Mide si el programa de formación cumplió con las expectativas de aprendizaje de las personas involucradas	Suma de nivel de evaluación de satisfacción/ cantidad de personas evaluadas
	Nivel de aprendizaje	Mide la retención de aprendizaje, así como las nuevas habilidades adquiridas con base a la participación de la capacitación.	Suma de nivel de evaluación de conocimientos/ cantidad de personas evaluadas

Tabla 14.Indicadores para medición de resultados Gestión del Cambio

Una vez medidos los resultados, los responsables de las áreas y proyectos podrán ajustar sus planes comunicacionales o formativos, según sea aplicable, para obtener los niveles de conocimiento, aprovechamiento y apropiación que se requieran para cumplir con la generación de valor para los interesados.

6.4 Anexos

Matriz de Interesados.xls

Plan de Comunicaciones.xls

Plan de Formación.xls

7. Transformación Digital del Distrito a Servicios Cloud

7.1 Introducción

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.

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.

7.3 Principios Rectores

Principio	Descripción
Cloud-First	Toda solución deberá priorizar servicios administrados (PaaS/SaaS) sobre IaaS.
Zero Trust	Autenticación multifactor, acceso mínimo, control continuo de identidades y dispositivos.
Cumplimiento Normativo	Integración con políticas de datos personales, ciberseguridad, transparencia y auditoría.
Automatización	Todo recurso debe ser aprovisionado mediante Infraestructura como Código (IaC).
Observabilidad	Monitoreo activo, trazabilidad operativa, dashboards unificados y alertas basadas en reglas.

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.

Rol	Responsable	Responsabilidades Clave	Dependencia
Product Owner(PO)	Líder de proceso	Responsable de definir los requerimientos y prioridades del negocio.	Dependencia solicitante
Cloud Architect	Arquitecto de la SID	Encargado de validar la arquitectura, estándares, aval técnico.	SID
DevSecOps	Fábrica de software externo	CI/CD, IaC, pruebas de seguridad	Proveedor / SID
Security Officer	Equipo de Seguridad	Políticas de Zero-Trust, cumplimiento	SID – Seguridad Informática
Infraestructure Officer	Equipo de infraestructura	Gestionar los dispositivos de red	Red – e infraestructura Cloud

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) que necesitan todos los sistemas.

- **Spokes (zonas de aterrizaje):** tres “ramales” independientes que aíslan los ambientes de
    - **Producción** (lo que ve el ciudadano),
    - **Calidad / QA** (donde se hacen pruebas), y
    - **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.

Dominio	Servicio Azure Recomendado
Red perimetral	Azure Firewall Premium, Azure DDoS Protection
Acceso seguro	Azure Bastion, Just-In-Time, Azure Private Link
Exposición de servicios	Application Gateway + WAF, Azure Front Door, API Management
Microservicios	Azure Kubernetes Service (AKS), Azure Red Hat OpenShift (ARO)
Bases de datos	PostgreSQL Flexible Server, Azure SQL MI, Cosmos DB
Analítica avanzada	Azure Synapse, Data Lake Gen2, Azure Databricks
Observabilidad	Azure Monitor, Log Analytics, Application Insights, Microsoft Sentinel
DevSecOps	Azure DevOps, Terraform/Bicep, GitHub Enterprise

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.

Control de Seguridad	Implementación Azure
Seguridad de la Cadena de Suministro	Escaneo SCA, Verificación de firmas de imágenes, Integración con herramientas de seguridad en pipelines CI/CD
Identidad y acceso	Azure Entra ID, MFA, Privileged Identity Management (PIM)
Cifrado en reposo	Azure Key Vault con Customer Managed Keys (BYOK/CMK)
Cifrado en tránsito	TLS 1.2 o superior, cifrado extremo a extremo
Respaldos y recuperación	Backup GRS, Azure Backup Vault, Azure Site Recovery
Cumplimiento legal	Clasificación de datos, tagging DE-GINF-021
Auditoría continua	Microsoft Defender, Azure Policy, Microsoft Sentinel (SIEM)

7.7 Descripción de componentes del perímetro de red en la nube

Componente	¿Qué hace?	¿Por qué es importante?
Azure Firewall Premium	Es un “guardián” en la entrada de la red. Revisa todo el tráfico y aplica reglas finas (por nombre de dominio, puertos o tipos de amenaza). Incluye inspección TLS, filtrado web y detección-prevención de intrusos (IDPS).	Mantiene fuera a atacantes y bloquea conexiones sospechosas antes de que lleguen a las aplicaciones del Distrito.
Azure DDoS Protection (Premium)	Detecta y frena ataques de Denegación de Servicio Distribuida (DDoS) que buscan saturar los sistemas. Ajusta sus umbrales de forma automática y responde en segundos cuando nota un pico anómalo de tráfico.	Garantiza que los servicios críticos sigan disponibles para los ciudadanos, aun bajo intentos masivos de bloqueo.
Network Security Groups (NSG)	Son “listas de control” que dicen qué tipo de tráfico puede entrar o salir de cada red o servidor (por puerto, protocolo y dirección).	Permiten segmentar los entornos (Producción, QA, OPS) y aplicar el principio de **menor privilegio**: solo el tráfico estrictamente necesario está permitido

En conjunto, estos tres componentes crean una barrera multicapa que protege la infraestructura del Distrito contra accesos no autorizados, ataques de saturación y tráfico malicioso, mientras mantienen las comunicaciones legítimas seguras y fluidas.

7.8 Descripción de componentes de acceso seguro a la nube

Componente	¿Qué hace?	Beneficio para el usuario final
Azure Bastion	Permite conectarse por RDP o SSH a las máquinas virtuales **desde el navegador** sin exponer direcciones IP públicas. Funciona totalmente dentro del portal de Azure y cifra la sesión de extremo a extremo.	Acceso remoto fácil y seguro—desde la oficina o desde cualquier lugar del mundo—sin abrir puertos que puedan ser atacados.
Just-In-Time (JIT) VM Access	Habilita el acceso a las VMs **solo por el tiempo estrictamente necesario**. Un administrador solicita la conexión y Azure abre el puerto indicado (RDP/SSH) durante un intervalo limitado; luego lo cierra automáticamente.	Reduce el riesgo de intrusiones, porque los puertos sensibles permanecen cerrados el 99 % del tiempo.
Azure Private Link	Conecta servicios PaaS (Azure SQL, Storage, etc.) a través de **direcciones IP privadas** dentro de la red del Distrito. Todo el tráfico viaja por la red interna de Microsoft, sin pasar por internet pública.	Añade una capa extra de seguridad (sin endpoints públicos) y baja la latencia al mantener el tráfico “dentro de casa”.

En conjunto, estos componentes simplifican el trabajo diario de los equipos técnicos y, a la vez, protegen los sistemas del Distrito contra accesos no autorizados y ataques a puertos expuestos.

7.9 Componentes para exponer servicios al exterior —

Componente	¿Qué hace?	Ventaja práctica
Application Gateway v2 + WAF	Es un balanceador de carga "inteligente" (capa 7) que dirige el tráfico según la URL o el nombre del sitio. Trae un **Firewall de Aplicaciones Web (WAF)** incorporado que bloquea los ataques más comunes (OWASP Top 10).	Envía a cada usuario al servicio correcto y, al mismo tiempo, protege las aplicaciones de inyecciones SQL, scripts maliciosos y otras amenazas.
Azure Front Door	Plataforma global de entrega (CDN) que ubica copias del contenido en múltiples regiones. Usa enrutamiento inteligente y acelera el tráfico HTTPS. Integra WAF, geobloqueo y mantiene la sesión del usuario (afinidad).	El ciudadano accede al portal desde cualquier país y la página responde rápido y segura, incluso durante picos de demanda o ataques.
API Management	"Puerta principal" para las API del Distrito. Controla quién puede usarlas, aplica reglas de seguridad (OAuth 2.0, Azure AD), versiona y supervisa el consumo. Se puede extender a entornos on-premise con gateways híbridos.	Facilita abrir datos y servicios de forma ordenada, medible y segura, impulsando integraciones con terceros sin exponer directamente los sistemas internos.

En conjunto, estos tres servicios permiten publicar aplicaciones web y API hacia internet con alto desempeño, protección frente a amenazas y un control granular sobre el acceso de usuarios y desarrolladores.

7.10 DevSecOps y Calidad del software

El Distrito usa un enfoque **DevSecOps**, que combina **Desarrollo (Dev)**, **Seguridad (Sec)** y **Operaciones (Ops)** para que la calidad y la protección del software se verifiquen desde el primer día y de forma automática.

Paso del ciclo	¿Qué sucede?	Beneficio
Código y artefactos únicos	Todo (código fuente, scripts de infraestructura, contenedores, paquetes) vive en **un solo repositorio Git** (Azure DevOps o GitHub Enterprise).	Trazabilidad total: sabemos qué versión está en cada ambiente.
Pipelines automáticos (CI/CD)	Un pipeline YAML compila, prueba y despliega el software cada vez que hay un cambio.	Entregas rápidas y repetibles, sin tareas manuales.
Pruebas continuas	Se ejecutan pruebas unitarias, de integración, de carga y de seguridad (SAST/SCA, escaneo de imágenes).	Detectamos errores y vulnerabilidades antes de llegar a producción.
Quality Gates	El pipeline se detiene si no se cumplen métricas mínimas (cobertura de pruebas, “cero” vulnerabilidades críticas, etc.).	Solo se publica código confiable y seguro.
Despliegue Canary	El nuevo código llega primero a un pequeño porcentaje de usuarios; si todo marcha bien, se expande al resto. Reversión automática si aparece un fallo.	Actualizaciones sin interrupciones y con riesgo mínimo.

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.

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.

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.

7.13.1 Azure Red Hat OpenShift (ARO)

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.

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**
  -
- **Escalabilidad y costos**

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

7.13.2 Azure Container Registry (ACR)

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.

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.

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.

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 globalmente 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).

7.15 Descripción de componentes de analítica avanzada

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.

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).

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

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.

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.

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.

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.

7.17 Costos, Gobernanza y Optimización

Elemento de Gestión	Práctica Recomendada
Etiquetado de recursos	Campos: "CostCenter", "Environment", "Owner", "App"
Límites de gasto	Reglas de alerta en Azure Budgets + notificaciones proactivas
Reporting financiero	Power BI conectado a Azure Cost Management y Log Analytics
Buenas prácticas FinOps	Revisión mensual de Azure Advisor, reducción de recursos ociosos

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.

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.

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.

Práctica	Implementación
Etiquetado	**CostManagement**
Recomendaciones	**Uso de Azure Cost Management y seguimiento a consumos**
Alertas de umbral	**Notificaciones cuando el gasto supere 80 % del presupuesto mensual**
Reporting	**Dashboard Power BI con datos de Cost Management**

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.

7.19 Anexo - Despliegue_Azur.drawio.pdf -

Arquitectura de referencia del Distrito-

7.20 Glosario de términos técnicos

Término	Descripción técnica	Explicación sencilla
Principios y modelos de adopción en la nube		
Cloud-First	Estrategia que privilegia la selección de servicios en la nube frente a infraestructuras locales para nuevas cargas de trabajo.	*«Primero la nube» significa que, antes de comprar servidores propios, la entidad evalúa si un servicio en línea satisface la necesidad de forma más ágil y económica.*
Cloud-Native	Conjunto de prácticas que aprovechan arquitecturas de microservicios, contenedores, despliegues automáticos y observabilidad continua.	*Se diseña el software pensando desde el inicio en escalar, recuperarse y actualizarse con mínimas interrupciones.*
Infrastructure as Code (IaC)	Gestión de la infraestructura (redes, máquinas, servicios) mediante archivos de configuración versionados (p. ej., Terraform, Bicep).	*En lugar de "hacer clic" en un portal, todo se define en código: así se despliega o restaura un entorno completo con un comando.*
IaaS / PaaS / SaaS	Modelos de servicio donde el proveedor administra, respectivamente, infraestructura básica, plataformas de desarrollo o aplicaciones completas.	*IaaS es "alquilar un servidor", PaaS es "alquilar un entorno listo para programar" y SaaS es "usar la aplicación ya hecha" (como correo en línea).*
Zero Trust	Marco de seguridad que asume que ninguna identidad o dispositivo es fiable por defecto; exige verificación continua y privilegios mínimos.	*Aunque esté "dentro" de la red, cada quien debe probar quién es y solo obtiene el acceso estrictamente necesario.*
Identidad y gestión de acceso		
Microsoft Entra ID (antes Azure AD)	Servicio de identidad y directorio que centraliza autenticación, autorización y políticas de acceso condicional para recursos de Azure y SaaS.	*Es la "agenda de usuarios" en la nube: controla quién entra, con qué contraseña y desde qué dispositivo.*
Multi-Factor Authentication (MFA)	Requiere al menos dos factores distintos (contraseña + código o biometría) para autenticar a un usuario.	*Además del password, llega un código al celular; si alguien roba la clave, sigue sin poder entrar.*
Privileged Identity Management (PIM)	Módulo de Entra ID que concede permisos elevados solo por tiempo limitado y con aprobación explícita.	*Los "superpoderes" de administrador se otorgan temporalmente y se registran en auditoría.*

Término	Descripción técnica	Explicación sencilla
Azure Key Vault / Customer Managed Keys (BYOK/CMK)	Bóveda de claves y secretos protegida por hardware; permite que la organización controle la clave raíz de cifrado.	*Es la caja fuerte digital donde se guardan contraseñas y certificados; la entidad puede traer y gestionar sus propias llaves.*
Seguridad de red		
Azure Firewall Premium	Firewall de red administrado con inspección TLS, filtrado web y prevención de intrusiones (IDPS).	*Actúa como "aduana" inteligente: inspecciona el tráfico cifrado, bloquea webs maliciosas y detiene ataques.*
Azure DDoS Protection	Servicio que mitiga ataques de denegación de servicio distribuidos mediante análisis adaptativo y respuesta automática.	*Detecta cuando miles de equipos intentan saturar el sistema y desvía esa avalancha antes de que afecte la página.*
Network Security Group (NSG)	Filtros de paquetes por puerto, protocolo y dirección IP que se aplican a subredes o tarjetas de red.	*Lista de reglas que define "este servidor solo recibe correo por el puerto 25 y responde por el 80", nada más.*
Azure Bastion	Puente seguro en el portal Azure para conexiones RDP/SSH sin exponer IP públicas.	*En vez de abrir la puerta del servidor a internet, se entra por una consola web con túnel protegido.*
Just-In-Time VM Access (JIT)	Habilita acceso a máquinas virtuales solo durante una ventana temporal aprobada.	*Como prestar la llave por unas horas y luego se vuelve a cerrar; reduce el tiempo de exposición.*
Azure Private Link	Conecta servicios PaaS a través de IP privadas dentro de la VNet del cliente.	*El tráfico hacia bases de datos o almacenamiento nunca "sale a internet", circula internamente.*
Entrega de aplicaciones y APIs		
Application Gateway v2 (WAF)	Balanceador de capa 7 con enrutamiento por URL y firewall de aplicaciones (WAF) incorporado.	*Reparte el tráfico web entre servidores y filtra ataques típicos (inyección SQL, XSS).*
Azure Front Door	Servicio global de CDN y enrutamiento inteligente con caché y aceleración HTTPS.	*Copia los archivos estáticos cerca del usuario para que la página cargue más rápido y protege con WAF.*
API Management	Plataforma para exponer y securizar APIs con versionamiento, cuotas y autenticación OAuth 2.0.	*Es la "puerta de enlace" que controla quién y cómo consume los servicios de datos de la entidad.*
Microservicios y contenedores		

Término	Descripción técnica	Explicación sencilla
Azure Kubernetes Service (AKS)	Servicio administrado de Kubernetes que orquesta contenedores con escalado automático y actualizaciones sin interrupción.	*Permite ejecutar muchas piezas de aplicación en contenedores; si aumenta la demanda, crea más copias automáticamente.*
Azure Red Hat OpenShift (ARO)	Plataforma OpenShift gestionada conjuntamente por Microsoft y Red Hat para cargas empresariales críticas.	*Variante de Kubernetes con herramientas adicionales listas para uso corporativo.*
Azure Container Registry (ACR)	Registro privado de imágenes Docker con geo-replicación y escaneo de vulnerabilidades.	*El "almacén" donde se guardan las versiones de los contenedores antes de enviarlas a producción.*
Canary Deployment	Estrategia que entrega una nueva versión a un pequeño porcentaje de usuarios y amplía si no hay fallos.	*Se prueba la actualización "en vivo" con pocos usuarios; si va bien, se extiende al resto, si no, se revierte rápido.*
Bases de datos y almacenamiento		
Azure Database for PostgreSQL Flexible Server	PostgreSQL administrado con configuraciones flexibles y alta disponibilidad zonal.	*Base de datos que el proveedor mantiene; la entidad ajusta memoria y CPU sin preocuparse por parches.*
Azure SQL Managed Instance (MI)	SQL Server PaaS compatible casi al 100 % con implementaciones locales, con backups y parches automáticos.	*Migrar bases existentes sin reescribir el código; Microsoft se encarga del mantenimiento.*
Azure Cosmos DB	Base NoSQL distribuida globalmente con latencia de milisegundos y acuerdos de nivel de servicio (SLA) del 99,999 %.	*Para apps que necesitan responder rápido en cualquier parte del mundo, con varios modelos de datos (documentos, grafos, etc.).*
Azure Data Lake Storage Gen2	Almacenamiento escalable para datos estructurados y no estructurados con jerarquía de directorios nativa.	*"Gran depósito" donde se guardan archivos o grandes volúmenes de datos sin límites rígidos de tamaño.*
Backup GRS	Copia de seguridad geo-redundante que replica datos a otra región Azure.	*Si ocurre un desastre en la zona principal, existe una copia lista en otro lugar.*
Analítica e inteligencia artificial		
Azure Synapse Analytics	Plataforma unificada para data warehouse, big data y analítica en tiempo real.	*Combina consultas SQL y análisis masivo de datos en un único espacio de trabajo.*

Término	Descripción técnica	Explicación sencilla
Azure Databricks	Entorno colaborativo basado en Apache Spark para procesamiento distribuido y notebooks.	*Pizarra interactiva donde equipos de datos limpian, procesan y modelan información a gran escala.*
Azure Machine Learning (Azure ML)	Servicio para entrenar, registrar y desplegar modelos de IA con MLOps integrado.	*Laboratorio en la nube que automatiza las etapas de un proyecto de inteligencia artificial.*
Azure Data Factory (ADF)	Orquestador de flujos ETL/ELT con más de 90 conectores para fuentes on-premise y cloud.	*Cinta transportadora que mueve y transforma datos desde distintos orígenes hacia el lago o la base de análisis.*
Azure Purview (Microsoft Purview)	Catálogo de datos con linaje, clasificación y políticas de gobierno centralizadas.	*Mapa que dice dónde vive cada dato, quién lo usa y qué normas aplica.*
Power BI	Herramienta de visualización e informes interactivos conectada a múltiples orígenes de datos.	*Crea tableros con gráficas dinámicas que se actualizan solos para apoyar decisiones.*
Monitoreo, observabilidad y respuesta		
Azure Monitor	Plataforma central para métricas, logs y alertas de recursos Azure.	*"Centro de control" donde se ve si un servicio está lento o caído.*
Log Analytics	Motor de consultas Kusto que analiza grandes volúmenes de registros en tiempo casi real.	*Permite buscar en millones de líneas de registro "qué pasó" a las 3 a. m.*
Application Insights	APM (Application Performance Monitoring) que telemetría el rendimiento de aplicaciones .NET, Java, Node, etc.	*Termómetro de la app: mide tiempos de respuesta y dónde falla el código.*
Microsoft Sentinel (SIEM/SOAR)	Plataforma de información y respuesta ante incidentes de seguridad basada en IA y reglas KQL.	*Analista virtual que detecta comportamientos sospechosos y puede lanzar acciones automáticas.*
DevSecOps y automatización		
Azure DevOps	Conjunto de servicios para repositorios Git, pipelines CI/CD, gestión de artefactos y tableros ágil.	*Herramienta todo-en-uno para que desarrollo, pruebas y operaciones trabajen coordinados.*

Término	Descripción técnica	Explicación sencilla
GitHub Enterprise	Plataforma de repositorios y flujos CI/CD alojada en la nube o on-premise con controles empresariales.	*"Hub" interno donde se guarda el código y se ejecutan pruebas automáticas antes de mezclar cambios.*
Terraform / Bicep	Lenguajes declarativos de IaC; Terraform es multi-cloud, Bicep es nativo de Azure.	*Archivos de texto que describen la infraestructura; al aplicarlos, se crean o actualizan los recursos.*
Quality Gate	Conjunto de métricas (cobertura, vulnerabilidades) que un pipeline debe aprobar antes de pasar a la siguiente fase.	*"Barreras" de calidad que evitan liberar código con errores graves.*
SAST / SCA	Análisis de código estático y de dependencias para detectar vulnerabilidades antes de la ejecución.	*Escáner que revisa el código fuente y las librerías externas en busca de fallos de seguridad conocidos.*
Gestión de costos y FinOps		
Azure Cost Management	Portal y APIs para analizar, presupuestar y optimizar el gasto en Azure.	*Tablero que muestra en qué y cuánto se está gastando, con alertas al superar el presupuesto.*
Azure Budgets	Regla configurable que envía notificaciones cuando el consumo alcanza un umbral (p. ej., 80 %).	*"Semáforo" que avisa antes de que la factura se dispare.*
Azure Advisor	Servicio de recomendaciones basado en prácticas de rendimiento, seguridad y costos.	*Consultor automático que sugiere apagar recursos ociosos o cambiar a instancias más baratas.*
FinOps	Disciplina que combina prácticas financieras con operaciones cloud para maximizar valor y responsabilidad del gasto.	*Mantener la "métrica" del dinero en la nube tan controlada como el rendimiento técnico.*
Normas y marcos de referencia		
CIS Controls for Azure	Guías del Center for Internet Security adaptadas a la arquitectura y servicios de Microsoft Azure.	*Checklist paso a paso para configurar la nube con ajustes seguros por defecto.*
OWASP Top 10	Ranking de las 10 vulnerabilidades web más críticas publicado por la comunidad OWASP.	*Los "diez pecados" más frecuentes en las aplicaciones web que los firewalls y desarrolladores deben vigilar.*

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.

8. Glosario

Anonimización de microdatos: es el proceso que impide la identificación de las unidades de estudio que son fuente para los registros individuales del conjunto de microdatos.

Archivo digital: es un archivo que una organización opera, que puede formar parte de una organización más amplia, de personas y sistemas, que ha aceptado la responsabilidad de conservar información y mantenerla disponible para una comunidad designada. (NTC-ISO 14721:2018)[32]

Autenticación: Proceso de probar una aseveración a fin de establecer un nivel de confianza en la veracidad de dicha aseveración.

Autenticidad: Característica técnica para preservar la seguridad de la información que busca asegurar la validez en el tiempo, forma y distribución. Así mismo, garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

[32] https://tienda.icontec.org/gp-sistemas-de-datos-espaciales-y-transferencia-de-informacion-sistema-dehttps://tienda.icontec.org/gp-sistemas-de-datos-espaciales-y-transferencia-de-informacion-sistema-de-informacion-de-archivo-abierto-oais-modelo-de-referencia-ntc-iso14721-2018.htmlinformacion-de-archivo-abierto-oais-modelo-de-referencia-ntc-iso14721-2018.html

Autenticidad del origen: En una comunicación electrónica el suscriptor puede acreditar Válidamente su identidad y su condición ante otra persona demostrando la posesión de la clave privada asociada con la respectiva clave pública contenida en el certificado.

Base de datos relacional: Una base de datos es una colección organizada de datos estructurados, típicamente almacenada en un sistema de información, con fácil acceso, para recuperación, inserción, modificación y eliminación.

Campo: Un campo es la unidad básica de una base de datos. Un campo puede ser, por ejemplo, el nombre de una persona. Los nombres de los campos no pueden empezar con espacios en blanco y caracteres especiales. No pueden llevar puntos, ni signos de exclamación o corchetes.

Clave principal: La clave principal en una tabla de una base de datos, es un campo o conjunto de campos que se seleccionan para identificar de forma unívoca cada registro de la tabla. Por ejemplo, en una tabla de alumnos podría ser un valor numérico autoincremental.

Correo electrónico certificado: Es el servicio de correo electrónico seguro y certificado que permite administrar las comunicaciones de manera ágil, segura y verificable, conservando un registro del envío, entrega y contenido transmitido con fecha y hora, cumpliendo normativa colombiana, que confiere a los correos electrónicos total credibilidad y permanencia en el tiempo, ya que deja a su disposición el registro de la comunicación y de todos los eventos involucrados en ella para cualquier consulta, conservando siempre su autenticidad e integridad.

De esta forma las comunicaciones adquieren la credibilidad del correo tradicional y las ventajas del correo electrónico, porque el sistema actual de comunicaciones exige la velocidad de respuesta que el correo tradicional no puede darnos, pero con la garantía que el mensaje sea confiable, seguro y permanezca disponible en el tiempo con confiabilidad y seguridad.

ataSet: Un DataSet o conjunto de datos, corresponde a los contenidos de una única tabla de una base de datos o una única matriz de datos estadística, donde cada columna de la tabla representa una variable en particular y cada fila representa un miembro determinado del conjunto de datos.

Desarrollo a la medida: Toda herramienta informática desarrollada que satisface los requerimientos específicos de las necesidades de gestión de la información de una empresa, o grupo o persona en particular. El sistema se adapta a la empresa.

Documento electrónico: información generada, enviada, recibida, almacenada y comunicada por medios electrónicos, ópticos o similares. (Guía para la gestión de documentos y expedientes electrónicos, 2018).

Documento electrónico de archivo: registro de información generada, recibida, almacenada y comunicada por medios electrónicos, que permanece en estos medios durante su ciclo vital. Es producida por una persona o entidad en razón de sus actividades o funciones y que debe ser tratada conforme a los principios y procesos archivísticos. (Acuerdo 027 de 2006).

Firma Digital: Mecanismo de seguridad incluido dentro de un registro digital que posibilita la identificación del creador del objeto digital y que también puede emplearse para detectar y rastrear cualquier cambio que se haya realizado al objeto digital.

El certificado digital puede ser utilizado para los siguientes propósitos:

Autenticación de identidad. La firma digital puede utilizarse para identificar a una persona física o jurídica como quien dice ser en el ámbito de su actividad.

Certificado Digital. Los Certificados digitales ofrecen los medios de respaldo al garantizar la autenticidad del origen, la integridad de los datos firmados y el no repudio.

Hardware: Se refiere a las partes físicas, tangibles, de un sistema informático, sus componentes eléctricos, electrónicos, electromecánicos y mecánicos. Los cables, así como los gabinetes o cajas, los periféricos de todo tipo, y cualquier otro elemento físico involucrado, componen el hardware o soporte físico.

Información: Conjunto de datos ya procesados y analizados para su comprensión y que puedan ser utilizados como base sobre un asunto, materia o fenómeno determinado.

Implementación: Instalación, puesta en funcionamiento, ejecución, soporte y mantenimiento de un sistema de información en infraestructura propia local (On premise) o en infraestructura de Nube.

Integridad: Se refiere a la garantía de que una información no ha sido alterada, borrada, reordenada, copiada, etc., bien durante el proceso de transmisión o en su propio equipo de origen.

Lineamiento: Es una directriz o disposición obligatoria debe ser implementada por los grupos de valor o interés. Los lineamientos pueden ser a través de estándares, guías, recomendaciones o buenas prácticas.

Metadatos: información estructurada o semiestructurada que posibilita la creación, la gestión y el uso de los registros a lo largo del tiempo.

Microdatos: son los datos sobre las características de las unidades de una población, (individuos, hogares, establecimientos, entre otros), que constituyen una unidad de información en una base de datos y que son recogidos por medio de una operación estadística.

Migración: Acto de mover registros de un sistema a otro, al tiempo que se mantiene la autenticidad, integridad, confiabilidad y usabilidad de los registros. La migración incluye un conjunto de tareas organizadas diseñadas para transferir de forma periódica material digital de una configuración de hardware o software a otra, o de una generación de tecnología a otra.

Modelo de datos: El modelado de datos es una manera de estructurar y organizar los datos, para que puedan ser utilizados y almacenados de forma eficiente.

Modelo relacional: Un modelo relacional consiste en representar datos por medio de tablas relacionadas cuyas filas se llaman tuplas y las columnas variables, conformando así una base de datos.

Objeto digital: es la agregación de valores discretos, diferenciados o discontinuos de una o más cadenas de bits con datos acerca de un objeto documental y los metadatos acerca de las propiedades del mismo. Adicionalmente, cuando sea necesario, la descripción de los métodos para realizar operaciones sobre el objeto (pueden ser textos, bases de datos, imágenes fijas o en movimiento, grabaciones sonoras, material gráfico, programas informáticos o páginas web), sin perjuicio de los formatos que puedan surgir en el futuro.

Obsolescencia tecnológica: desplazamiento de una solución tecnológica establecida en un mercado como resultado de mejoras o desarrollos importantes en la tecnología. (GTC-ISO-TR 18492:2013)[33]

[33] https://tienda.icontec.org/gp-preservacion-a-largo-plazo-de-la-informacion-basada-en-documentoshttps://tienda.icontec.org/gp-preservacion-a-largo-plazo-de-la-informacion-basada-en-documentos-electronicos-gtc-iso-tr18492-2013.htmlelectronicos-gtc-iso-tr18492-2013.html

Procedimiento: declaración escrita que especifica las acciones que se requieren para completar un servicio, o para lograr un estado o condición específica. Los procedimientos especifican como se han de cumplir los diversos aspectos de los planes relevantes de implementación de la preservación. (NTC-ISO16363:2016)[34]

Registro: Un registro es el conjunto de información referida a una misma unidad.

Servicios SAAS: Software como servicio. Es una solución de software integral que se adquiere de un proveedor de servicios en la nube mediante un modelo de pago por uso. Se alquila el uso de una aplicación para la organización y los usuarios se conectan a ella a través de Internet, normalmente con un explorador web. Toda la infraestructura subyacente, el middleware, el software y los datos de las aplicaciones se encuentran en el centro de datos del proveedor. El proveedor de servicios administra el hardware y el software y, con el contrato de servicio adecuado, garantizará también la disponibilidad y la seguridad de la aplicación y de sus datos

Sistema: es un conjunto de elementos relacionados entre sí mediante una cadena de actividades que buscan alcanzar un objetivo planteado. Reciben entradas del

[34] https://www.icontec.org/rules/sistemas-de-transferencia-de-informacion-y-datos-espaciales-auditoriahttps://www.icontec.org/rules/sistemas-de-transferencia-de-informacion-y-datos-espaciales-auditoria-y-certificacion-de-repositorios-digitales-de-confianza/y-certificacion-de-repositorios-digitales-de-confianza

medio en forma de datos, energía, información, y proveen salidas al entorno en carácter de información, materia, etc.

Sistema de información: es un conjunto de componentes relacionados entre sí que recogen, almacenan, procesan y muestran información para apoyar la coordinación, control y toma de decisiones en una organización.

Sistema Integrado de Conservación: es el conjunto de planes, programas, estrategias, procesos y procedimientos de conservación documental y preservación digital, bajo el concepto de archivo total, acorde con la política de gestión documental y demás sistemas organizacionales; tendiente a asegurar el adecuado mantenimiento de cualquier tipo de información, independiente del medio o tecnología con la cual se haya elaborado, conservando atributos tales como unidad, integridad autenticidad, inalterabilidad, originalidad, fiabilidad y accesibilidad, desde el momento de su producción y/o recepción, durante su gestión, hasta su disposición final, es decir, en cualquier etapa de su ciclo vital.

Software: conjunto de los programas de cómputo, procedimientos, reglas, documentación y datos asociados, que forman parte de las operaciones de un sistema de computación. (Tomado del estándar 729 del IEEE5)

Software comercial: Es aquel que se puede adquirir ya desarrollado con unas funcionalidades predeterminadas por su fabricante. A diferencia del desarrollo a la medida, si bien se pueden parametrizar o personalizar algunos aspectos, en términos generales la empresa se adapta al sistema.

Software de Aplicación: Es un programa informático generalmente instalado en el sistema para llevar a cabo un objetivo determinado y concreto.

Software gratis (FreeWare): El término software gratis (en inglés freeware, abreviatura de free software, a veces confundido erróneamente con "software libre", por la ambigüedad del término en inglés) define un tipo de software que se distribuye sin costo, disponible para su uso, pero que mantiene restricciones de derechos de autor, por lo que no se puede modificar o vender o utilizar libremente como ocurre con el software libre.

Software libre (Open Source): Según la Free Software Foundation[35], el software libre se refiere a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el Software; de modo más preciso, se refiere a cuatro libertades de los usuarios del software: la libertad de usar el programa, con cualquier propósito; de estudiar el funcionamiento del programa, y adaptarlo a las necesidades; de distribuir copias, con lo cual se puede ayudar a otros y de mejorar el programa y hacer públicas las mejoras, de modo que toda la comunidad se beneficie (para la segunda y última libertad mencionadas, el acceso al código fuente es un requisito previo). Es necesario puntualizar que el Software Libre establece muchas

[35] https://www.fsf.org/es

libertades, pero no es gratuito. Conservando sus libertades puede ser distribuido de manera comercial, garantizando sus derechos de modificación y re distribución.

Tabla: Unidad donde crearemos el conjunto de datos de nuestra base de datos. Estos datos estarán ordenados en columnas verticales. En ella se definen los campos y sus características.

Tupla: También se denomina de este modo a un registro o fila de una tabla.

Valor nulo: Representa un valor para un atributo que es actualmente desconocido o no es aplicable para ese registro.

WORM: Write Once Ready Many; escribir una vez, leer muchas; prevención de alteración de datos y retención del contenido original, se refiere a los dispositivos grabables en los cuales, una vez escrita la información, ésta no puede modificarse ni sobreescribirse, se puede almacenar hasta su capacidad total, pero si se requiere eliminar la información debe destruirse el dispositivo como tal.

Access point: Un Access point es un dispositivo de red que permite que los dispositivos con capacidad inalámbrica se conecten a una red cableada. Es más

simple y fácil instalar WAP para conectar todas las computadoras o los dispositivos de la red que usar cables.[36]

ANS: Un acuerdo de nivel de servicio (ANS), o en inglés Service Level Agreement (SLA), es un documento que establece los acuerdos sobre las normas de un servicio o producto. En el mundo TIC, este tipo de documento se encuentra en forma de un contrato formal entre el partner de implementación y la empresa que adquiere el software. Un ANS se encarga de que ambas partes sepan qué esperar, y también, es un medio judicial para hacer que estos pactos se cumplan.[37]

Simetría de Red: Las conexiones simétricas permiten la carga y descarga de información simultáneamente sin experimentar fallas en la disponibilidad de banda ancha o la velocidad del internet[38]

Censo Mapping: Estudio documental que permite contabilizar posibles putos de conexión de una red con atributos, a través de un estudio de campo y con la ayuda de herramientas de georreferenciación

Confiabilidad: La confiabilidad de una red es una medida que refleja la capacidad de la misma de continuar operativa frente a posibles fallos de algunos de sus

---

36 Tomado de https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/what-is-access-point.html
37 Tomado de https://www.ticportal.es/glosario-tic/acuerdo-nivel-servicio-ans
38 Tomado de https://www.fibraopticahoy.com/conexiones-simetricas-vs-asimetricas/

componentes, y se define como la probabilidad de comunicación exitosa entre cierto conjunto de nodos de la red[39]

Direccionamiento IP: (v4) Es una dirección lógica de 4 bytes o 32 bits cada uno de ellos separados por un punto, con la que se identifica unívocamente a un equipo o host en una red.[40]

Disponibilidad: La disponibilidad de la red se refiere al estado operacional de una red de ordenadores y su capacidad para establecer conexiones, procesar el tráfico y responder a las solicitudes de los usuarios de forma rápida.[41]

Georreferenciación: La georreferenciación o rectificación es un proceso que permite determinar la posición de un elemento en un sistema de coordenadas

---

[39] Tomado de https://repositorio.uniandes.edu.co/bitstream/handle/1992/21502/u251065.pdf?sequence=1#:~:text=La%20confiabilidad%20de%20una%20red,funcionamiento%20de%20los%20componentes%20y

[40] Tomado de https://www.profesionalreview.com/2019/01/12/direccionamiento-ip/#:~:text=Direcci%C3%B3n%20IP,-En%20primer%20lugar&text=Es%20una%20direcci%C3%B3n%20l%C3%B3gica%20de,o%20host%20en%20una%20red.&text=Estamos%20ante%20una%20cadena%20de,uno%20puede%20representar%20128%20bits.

[41] Tomado de https://www.google.com/search?q=disponibildad+de+red&rlz=1C1ALOY_esCO969CO969&oq=disponibildad+de+red&aqs=chrome.. 69i57j0i13l7j0i22i30l2.4613j1j4&sourceid=chrome&ie=UTF-8

espacial diferente al que se encuentra. Existen por tanto dos sistemas de coordenadas: el sistema origen y el sistema destino.[42]

GPON XPON XGPON: Definen las redes de fibra óptica Pasiva (PON por sus siglas en Ingles). La GPON asume redes con capacidad de 1Gbps, la XPON define todas las tecnologías PON, XGPON Define todas las redes con capacidades superiores a 1 Gbps.

ICMP: Protocolo de control de mensajes de internet de la capa de red del protocolo OSI.

Ip v6: Es un protocolo de direccionamiento de Hots dentro de una red, es una actualización del protocolo IP v4, debido al agotamiento de direcciones ipv4.

ITU G. 984. X: Estándar de la unión Internacional de comunicaciones (ITU por sus siglas en ingles Internacional Telecomunications Union) que define las características de las Redes basadas en fibra óptica Pasiva PON (por sus siglas en inglés Pasive optical Network).

[42] Tomado de https://www.ign.es/web/resources/docs/IGNCnig/CTC-Ibercarto-V-Georreferenciacion.pdf#:~:text=La%20georreferenciaci%C3%B3n%20o%20rectificaci%C3%B3n%20es,origen%20y%20el%20sistema%20destino.

KPI: Indicadores de claves de rendimiento, el cual es una medida de desempeño que está directamente relacionado con un objetivo preestablecido

Modelo OSI: El modelo OSI describe una estructura con siete capas para las actividades de red, diseñado por la ISO Organización internacional de estandarización

MPLS: Es conmutación de etiquetas multiprotocolo o MPLS (Multiprotocolo Label Switching en inglés) es un mecanismo para transportar datos estándar diseñado para las redes basadas en circuitos y en paquetes

NETFLOW: NetFlow es un protocolo de red desarrollado por Cisco para recoger el tráfico de red IP a medida que entra o sale de una interfaz. El dispositivo habilitado para NetFlow (router/switch) registra un nuevo flujo si un paquete con identificaciones únicas en los valores de 7 claves pasa a través de su interfaz.[43]

[43] Tomado de https://www.whatsupgold.com/es/monitoreo-del-trafico-dehttps://www.whatsupgold.com/es/monitoreo-del-trafico-de-red/netflow -:~:text=NetFlow%20es%20un%20protocolo%20de,o%20sale%20de%20una%20interfaz.&text=El%20dispositivo%20habilitado%20para%20NetFlow,a%20trav%C3%A9s%20de%20su%20interfazred/netflow#:~:text=NetFlow%20es%20un%20protocolo%20de,o%20sale%20de%20una%20interfaz.&text=El%20dispositivo%20habilitado%20para%20NetFlow,a%20trav%C3%A9s%20de%20su%20interfaz.

Red oscura: Hace referencia a la red de fibra óptica disponible para implementar una red de telecomunicaciones, la cual no tiene asociado tecnología que ilumine dicha red

SD-WAN: Una red de área amplia definida por software es una red de área amplia que utiliza tecnología de red definida por software, como la comunicación a través de Internet mediante túneles superpuestos que se cifran cuando están destinados a ubicaciones internas de la organización.[44]

Seguridad: La seguridad de red es cualquier actividad diseñada para proteger el acceso, el uso y la integridad de la red y los datos corporativos. Incluye tecnologías de hardware y software, está orientada a diversas amenazas que evita que ingresen o se propaguen por la red.[45]

SNMP: Simple Network Management Protocol (SNMP) es un protocolo de capa de aplicación basado en IP que intercambia información entre una solución de administración de red y cualquier dispositivo habilitado para SNMP.[46]

---

[44] Tomado de https://en.wikipedia.org/wiki/SD-WAN
[45] Tomado de https://www.cisco.com/c/es_mx/products/security/what-is-network-security.html
[46] Tomado de https://www.whatsupgold.com/es/snmp#:~:text=Simple%20Network%20Management%20Protocol%20(SNMP,cualquier%20dispositivo%20habilitado %20para%20SNMP. [30] Tomado de https://www.google.com/search?q=switch+ethernet&rlz=1C1ALOY_esCO969CO969&oq=switch+ethernet&aqs=chrome..69i57j0i512l9.6225j0j4&sourc eid=chrome&ie=UTF-8

Switch Ethernet: Un switch o conmutador es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet (o técnicamente IEEE 802.3).[30]

WIFI: Tecnología que permite conectar diferentes equipos informáticos a través de una red inalámbrica de banda ancha.