



## MODELO DE GESTIÓN DE GOBIERNO TI (MGGTI)

Alcaldía municipal de Chía

### DESCRIPCIÓN BREVE MGGTI 2025-2028

El modelo de gestión y gobierno de TI de la alcaldía municipal de Chía, se concibe como el marco estratégico, operativo y organizacional que orienta la planeación, la toma de decisiones, la gestión del riesgo, la inversión tecnológica y la articulación entre las dependencias, garantizando que las tecnologías de la información apoyen efectivamente los objetivos institucionales y las metas del plan de desarrollo municipal.

Elaborado por: Ing. Eliany Rocío Montejo Carrascal

Revisado/aprobado por: Ing. Gustavo Carvajal Millán

## Contenido

<b>1</b>	<b>Introducción .....</b>	<b>20</b>
<b>2</b>	<b>Alcance del documento.....</b>	<b>24</b>
2.1	DESGLOSE DEL ALCANCE POR DOMINIOS .....	24
2.1.1	Dominio de estrategia TI .....	24
2.1.2	Dominio de gobierno TI .....	24
2.1.3	Dominio de gestión de la información .....	24
2.1.4	Dominio de gestión de sistemas de información .....	25
2.1.5	Dominio de gestión de servicios de TI .....	25
2.1.6	Dominio de uso y apropiación de TI .....	25
<b>3</b>	<b>Objetivo general.....</b>	<b>27</b>
3.1	OBJETIVOS ESPECÍFICOS:.....	27
<b>4</b>	<b>Estrategia TI .....</b>	<b>29</b>
4.1	ENTENDIMIENTO ESTRATÉGICO .....	29
4.2	DOCUMENTACIÓN DE LA ESTRATEGIA DE TI EN EL PETIC .....	31
4.2.1	Dominio: Estrategia de TI.....	31
4.2.2	Dominio: Gobierno de TI .....	31
4.2.3	Dominio: Gestión de la información.....	32
4.2.4	Dominio: Sistemas de información .....	32
4.2.5	Dominio: Infraestructura y Tecnología .....	33
4.2.6	Dominio: Uso y apropiación de TI.....	33
4.3	POLÍTICAS DE TI.....	33
4.3.1	Lineamientos de gobierno, gestión y planeación de TI .....	34
4.3.2	Lineamientos de seguridad de la información .....	35
4.4	GESTIÓN DE LOS PROYECTOS CON COMPONENTES DE TI.....	35
4.5	GESTIÓN DEL PRESUPUESTO DE TI .....	36
4.6	CATÁLOGO DE SERVICIOS DE TI .....	37
4.7	EVALUACIÓN DE LA GESTIÓN DE LA ESTRATEGIA DE TI .....	39
4.7.1	Lineamientos generales de evaluación de la estrategia TI.....	39
4.7.2	Lineamientos para la evaluación del cumplimiento estratégico .....	40
4.7.3	Lineamientos para la evaluación de la arquitectura TI .....	40
4.7.4	Lineamientos para la evaluación de la actualización de la estrategia TI.....	41
4.8	TABLERO DE INDICADORES DE TI .....	41
4.8.1	Lineamientos generales para la implementación del tablero de indicadores	41
4.8.2	Lineamientos tablero de indicadores catálogo de servicios TI.....	42

4.9	INVESTIGACIÓN E INNOVACIÓN EN TIC .....	43
4.9.1	Lineamientos estratégicos para la innovación TIC .....	43
4.9.2	Lineamientos culturales y de gestión del cambio.....	44
4.9.3	Lineamientos para la investigación tecnológica .....	44
4.10	DISEÑO IMPULSADO CON EL USUARIO .....	45
4.10.1	Lineamientos estratégicos del diseño impulsado con el usuario.....	45
4.10.2	Lineamientos metodológicos del diseño impulsado con el usuario.....	45
4.10.3	Lineamientos del diseño impulsado con el usuario, en los sistemas de información.....	46
4.11	INSTRUMENTOS DE PLANEACIÓN INSTITUCIONAL CON COMPONENTES DE TIC.....	47
4.11.1	Lineamientos generales para la planeación institucional con componentes de TIC	47
4.11.2	Lineamientos para la articulación del PDM con el PETIC y el MAE .....	48
4.11.3	Lineamientos para la planeación técnica de proyectos TIC .....	48
4.11.4	Lineamientos para la articulación con las capacidades institucionales .....	49
<b>5</b>	<b>Gobierno TI.....</b>	<b>50</b>
5.1	ESQUEMA DE GOBIERNO DE TI.....	50
5.1.1	Propósito del esquema de gobierno de TI.....	51
5.1.2	Principios del esquema de gobierno de TI .....	51
5.1.3	Niveles del gobierno de TI .....	51
5.1.4	Instancias del esquema de gobierno de TI.....	52
5.1.5	Roles y responsabilidades claves.....	53
5.1.6	Mecanismos de articulación del esquema.....	53
5.1.7	Evaluación y mejora del esquema de gobierno de TI.....	53
5.2	GESTIÓN DE LAS NO CONFORMIDADES.....	54
5.2.1	Objetivo .....	54
5.2.2	Alcance de la gestión de no conformidades en TI .....	54
5.2.3	Definición de no conformidad en el MGGTI .....	54
5.2.4	Principios para la gestión de no conformidades.....	55
5.2.5	Fuentes de identificación de no conformidades .....	55
5.2.6	Proceso de gestión de las no conformidades .....	55
5.2.7	Roles y responsabilidades .....	56
5.2.8	Articulación con el PETIC y el dominio de gobierno TI .....	57
5.2.9	Indicadores de gestión de no conformidades .....	57
5.3	MACROPROCESO DE GESTIÓN DE TI.....	57
5.3.1	Objetivo del macroproceso de gestión de TI.....	58
5.3.2	Estructura del macroproceso de gestión de TI .....	58

5.3.3	Articulación del macroproceso de gestión de TI con el mapa de procesos institucional.....	60
5.4	GESTIÓN DE CAMBIOS.....	60
5.4.1	Objetivo de la gestión de cambios en el MGGTI.....	60
5.4.2	Alcance de la gestión de cambios.....	61
5.4.3	Lineamientos de adherencia a la gestión de cambios.....	61
5.5	CAPACIDADES Y RECURSOS DE TI.....	64
5.5.1	Objetivo de las capacidades y recursos de TI.....	64
5.5.2	Enfoque de capacidades de TI.....	64
5.5.3	Estructura de capacidades institucionales.....	65
5.5.4	Capacidades de TI por dominio.....	65
5.5.5	Niveles de madurez y metas de desarrollo.....	67
5.5.6	Requerimientos de la gestión de TI.....	67
5.5.7	Enfoque de desarrollo progresivo de capacidades.....	67
5.6	CAPACIDADES Y OPTIMIZACIÓN DE RECURSOS DE TI.....	68
5.6.1	Objetivo de las capacidades y la optimización de recursos de TI.....	68
5.6.2	Enfoque institucional.....	68
5.6.3	Capacidades institucionales de TI.....	69
5.6.4	Optimización de los recursos de TI.....	69
5.6.5	Articulación entre capacidades y optimización de recursos.....	70
5.6.6	Seguimiento y mejora continua.....	70
5.7	EVALUACIÓN DEL DESEMPEÑO DE LA GESTIÓN DE TIC.....	71
5.7.1	Objetivo de la evaluación del desempeño de la gestión de TIC.....	71
5.7.2	Alcance de la evaluación.....	71
5.7.3	Enfoque de la evaluación del desempeño.....	71
5.7.4	Componentes de la evaluación del desempeño de TIC.....	72
5.7.5	Instrumentos para la evaluación del desempeño.....	73
5.7.6	Periodicidad de la evaluación.....	73
5.7.7	Uso de los resultados de la evaluación.....	73
5.8	MEJORAMIENTO DE LOS PROCESOS.....	74
5.8.1	Objetivo del mejoramiento de los procesos.....	74
5.8.2	Principios del mejoramiento de los procesos.....	74
5.8.3	Enfoque de mejoramiento de procesos desde la arquitectura empresarial.....	74
5.8.4	Lineamientos para la identificación de procesos a mejorar.....	75
5.8.5	Lineamientos para la articulación de procesos, servicios TIC y tecnología.....	75
5.8.6	Lineamientos para el mejoramiento de procesos con apoyo de TIC.....	75

5.8.7	Lineamientos para la implementación y seguimiento .....	77
5.9	GESTIÓN DE PROVEEDORES DE TIC .....	78
5.9.1	Objetivo de la gestión de proveedores de TI .....	78
5.9.2	Alcance.....	78
5.9.3	Principios de la gestión de proveedores de TIC .....	78
5.9.4	Lineamientos para la planeación de la contratación de TI.....	79
5.9.5	Lineamientos para la selección de proveedores de TI .....	79
5.9.6	Lineamientos para la gestión y supervisión contractual.....	79
5.9.7	Lineamientos para la gestión de riesgos y seguridad.....	79
5.9.8	Lineamientos para la evaluación del desempeño de los proveedores .....	80
5.9.9	Seguimiento y mejora continua .....	80
<b>6</b>	<b>Gestión de información.....</b>	<b>81</b>
6.1	GOBIERNO DE LA INFORMACIÓN.....	81
6.1.1	Objetivo del gobierno de la información.....	82
6.1.2	Alcance.....	82
6.1.3	Principios del gobierno de la información.....	82
6.1.4	Estructura de gobierno de la información .....	82
6.1.5	Lineamientos para la gestión del ciclo de vida de la información.....	83
6.1.6	Lineamientos de calidad de la información .....	83
6.1.7	Lineamientos de seguridad y acceso a la información.....	84
6.1.8	Lineamientos de interoperabilidad y uso estratégico.....	84
6.1.9	Seguimiento y mejora continua .....	84
6.2	GESTIÓN DE LA CALIDAD DE LOS DATOS.....	84
6.2.1	Objetivo de la gestión de la calidad de los datos .....	84
6.2.2	Alcance.....	85
6.2.3	Principios de calidad de los datos.....	85
6.2.4	Dimensiones de la calidad de los datos.....	85
6.2.5	Lineamientos para la gestión de la calidad de los datos.....	85
6.2.6	Seguimiento y control .....	86
6.3	GESTIÓN DE DOCUMENTOS ELECTRÓNICOS.....	87
6.3.1	Objetivo de la gestión de documentos electrónicos.....	87
6.3.2	Alcance.....	87
6.3.3	Principios de la gestión de documentos electrónicos .....	87
6.3.4	Lineamientos para la gestión del ciclo de vida del documento electrónico..	88
6.3.5	Lineamientos para el uso de tecnologías de gestión documental .....	89
6.3.6	Lineamientos de metadatos documentales.....	89

6.3.7	Lineamientos de seguridad de los documentos electrónicos .....	89
6.3.8	Seguimiento y mejora continua .....	89
6.3.9	Flujo del proceso de gestión documental .....	91
6.4	MARCO DE REFERENCIA GEOESPACIAL .....	93
6.4.1	Objetivo del marco de referencia geoespacial.....	93
6.4.2	Alcance.....	93
6.4.3	Principios del marco de referencia geoespacial .....	94
6.4.4	Lineamientos para la arquitectura de información geoespacial.....	94
6.4.5	Lineamientos de estandarización e interoperabilidad.....	94
6.4.6	Lineamientos de calidad de la información geoespacial .....	94
6.4.7	Lineamientos de roles y responsabilidades .....	95
6.4.8	Lineamientos de seguridad y acceso .....	95
6.4.9	Lineamientos para el uso estratégico de la información geoespacial.....	95
6.4.10	Seguimiento y mejora continua .....	95
6.5	PUBLICACIÓN DE LOS SERVICIOS DE INTERCAMBIO DE INFORMACIÓN .....	96
6.5.1	Objetivo de la publicación de servicios de intercambio de información.....	96
6.5.2	Alcance.....	96
6.5.3	Principios para la publicación de servicios de intercambio de información..	96
6.5.4	Lineamientos para la identificación de servicios de intercambio .....	97
6.5.5	Lineamientos para el diseño de los servicios de intercambio .....	97
6.5.6	Lineamientos para la publicación de los servicios .....	97
6.5.7	Lineamientos de seguridad y control.....	98
6.5.8	Lineamientos de operación y monitoreo .....	98
6.5.9	Lineamientos para la interoperabilidad externa.....	98
6.5.10	Seguimiento y mejora continua .....	98
6.6	ACUERDOS DE INTERCAMBIO DE INFORMACIÓN.....	98
6.6.1	Objetivo de los acuerdos de intercambio de información .....	99
6.6.2	Alcance.....	99
6.6.3	Principios de los acuerdos de intercambio de información.....	99
6.6.4	Lineamientos para la identificación de acuerdos de intercambio .....	99
6.6.5	Lineamientos para la definición de los acuerdos.....	100
6.6.6	Lineamientos de seguridad y protección de la información.....	100
6.6.7	Lineamientos para la formalización y aprobación .....	100
6.6.8	Lineamientos para la operación y seguimiento de los acuerdos .....	101
6.6.9	Seguimiento y mejora continua .....	101
6.7	USO DEL CÓDIGO POSTAL COLOMBIANO .....	101

6.7.1	Objetivo del uso del código postal colombiano.....	101
6.7.2	Alcance.....	101
6.7.3	Principios para el uso del código postal colombiano .....	102
6.7.4	Lineamientos para la gestión del código postal colombiano como dato maestro	102
6.7.5	Lineamientos para el uso del código postal en sistemas de información...	102
6.7.6	Lineamientos de calidad de datos asociados al código postal.....	102
6.7.7	Lineamientos para interoperabilidad e intercambio de información .....	103
6.7.8	Lineamientos de roles y responsabilidades .....	103
6.7.9	Lineamientos de seguridad y protección .....	103
6.7.10	Seguimiento y mejora continua .....	103
6.8	EXPLOTACIÓN DE DATOS.....	104
6.8.1	Objetivo de la explotación de datos.....	104
6.8.2	Alcance.....	104
6.8.3	Principios para la explotación de datos.....	104
6.8.4	Lineamientos para la arquitectura de explotación de datos .....	105
6.8.5	Lineamientos para el análisis y aprovechamiento de la información .....	105
6.8.6	Lineamientos para servicios de información analítica .....	105
6.8.7	Lineamientos para la interoperabilidad y explotación de datos externos ...	106
6.8.8	Lineamientos para roles y responsabilidades .....	106
6.8.9	Lineamientos de seguridad y ética en la explotación de datos.....	106
6.8.10	Desarrollo de capacidades para la explotación de datos.....	106
6.8.11	Seguimiento y mejora continua .....	107
<b>7</b>	<b>Gestión de sistemas de información .....</b>	<b>108</b>
7.1	METODOLOGÍA PARA EL DESARROLLO DE SISTEMAS DE INFORMACIÓN .....	108
7.1.1	Objetivo de la metodología .....	109
7.1.2	Alcance.....	109
7.1.3	Principios orientadores de la metodología .....	109
7.1.4	Enfoque metodológico .....	109
7.1.5	Fases de la metodología para el desarrollo de sistemas de información...	110
7.1.6	Lineamientos de roles y responsabilidades .....	111
7.1.7	Lineamientos de seguridad y cumplimiento .....	111
7.1.8	Seguimiento y control .....	111
7.2	CATÁLOGO DE SISTEMAS DE INFORMACIÓN .....	111
7.2.1	Objetivo del catálogo de sistemas de información.....	112
7.2.2	Alcance.....	112

7.2.3	Principios del catálogo de sistemas de información .....	112
7.2.4	Lineamientos para la estructuración del catálogo .....	112
7.2.5	Lineamientos para la relación con el catálogo de servicios TIC .....	113
7.2.6	Lineamientos para la administración y actualización del catálogo .....	113
7.2.7	Lineamientos para el uso del catálogo de sistemas de información .....	113
7.2.8	Lineamientos de gobierno y control.....	114
7.2.9	Articulación con el modelo de arquitectura empresarial.....	114
7.2.10	Seguimiento y mejora continua .....	114
7.3	GUÍA DE ESTILO Y USABILIDAD.....	114
7.3.1	Objetivo de la guía de estilo y usabilidad .....	115
7.3.2	Alcance.....	115
7.3.3	Principios orientadores de la guía.....	115
7.3.4	Lineamientos de diseño visual .....	115
7.3.5	Lineamientos de usabilidad .....	115
7.3.6	Lineamientos de accesibilidad.....	116
7.3.7	Lineamientos de experiencia de usuario (UX).....	116
7.3.8	Lineamientos para desarrollo y evolución .....	116
7.3.9	Roles y responsabilidades .....	116
7.3.10	Seguimiento y mejora continua .....	117
7.4	AMBIENTES INDEPENDIENTES EN EL CICLO DE VIDA DE LOS SISTEMAS DE INFORMACIÓN .....	117
7.4.1	Objetivo de los ambientes independientes.....	117
7.4.2	Alcance.....	117
7.4.3	Principios para la gestión de ambientes .....	117
7.4.4	Tipos de ambientes institucionales.....	118
7.4.5	Lineamientos para el uso de datos en los ambientes.....	119
7.4.6	Lineamientos de seguridad por ambiente.....	119
7.4.7	Lineamientos para despliegue y cambios.....	119
7.4.8	Roles y responsabilidades .....	119
7.4.9	Seguimiento y control .....	120
7.5	ANÁLISIS DE REQUERIMIENTOS DE LOS SISTEMAS DE INFORMACIÓN.....	120
7.5.1	Objetivo del análisis de requerimientos .....	121
7.5.2	Alcance.....	121
7.5.3	Principios del análisis de requerimientos.....	121
7.5.4	Lineamientos para la identificación de la necesidad.....	121
7.5.5	Lineamientos para el levantamiento de requerimientos.....	122
7.5.6	Lineamientos para la documentación de requerimientos.....	122

7.5.7	Lineamientos para la priorización de requerimientos .....	123
7.5.8	Lineamientos para la gestión de cambios en requerimientos .....	123
7.5.9	Lineamientos de roles y responsabilidades .....	123
7.5.10	Articulación con el ciclo de vida del sistema .....	123
7.5.11	Seguimiento y control .....	124
7.6	INTEGRACIÓN CONTINUA DURANTE EL CICLO DE VIDA DE LOS SISTEMAS DE INFORMACIÓN .....	124
7.6.1	Objetivo de la integración continua.....	125
7.6.2	Alcance.....	125
7.6.3	Principios de la integración continua.....	125
7.6.4	Lineamientos para la gestión del código y versiones .....	125
7.6.5	Lineamientos para la automatización de integraciones .....	126
7.6.6	Lineamientos para pruebas dentro de la integración continua.....	126
7.6.7	Lineamientos para la gestión de ambientes.....	126
7.6.8	Lineamientos de seguridad en la integración continua .....	126
7.6.9	Lineamientos de roles y responsabilidades .....	126
7.6.10	Articulación con el ciclo de vida del sistema .....	127
7.6.11	Seguimiento y control .....	127
7.7	ENTREGA CONTINUA DURANTE EL CICLO DE VIDA DE LOS SISTEMAS DE INFORMACIÓN .....	127
7.7.1	Objetivo de la entrega continua.....	127
7.7.2	Alcance.....	128
7.7.3	Principios de la entrega continua.....	128
7.7.4	Lineamientos para la preparación de entregas .....	128
7.7.5	Lineamientos para la validación previa a la entrega.....	128
7.7.6	Lineamientos para el despliegue en ambientes .....	129
7.7.7	Lineamientos de seguridad en la entrega continua .....	129
7.7.8	Lineamientos para la gestión de fallas y reversión .....	129
7.7.9	Lineamientos de roles y responsabilidades .....	129
7.7.10	Seguimiento y control .....	130
7.8	DESPLIEGUE CONTINUO DURANTE EL CICLO DE VIDA DE LOS SISTEMAS DE INFORMACIÓN .....	130
7.8.1	Objetivo del despliegue continuo .....	130
7.8.2	Alcance.....	130
7.8.3	Principios del despliegue continuo.....	131
7.8.4	Lineamientos para la preparación del despliegue.....	131
7.8.5	Lineamientos para la automatización del despliegue .....	131
7.8.6	Lineamientos para despliegue por ambientes .....	131
7.8.7	Lineamientos de seguridad en el despliegue continuo.....	132

7.8.8	Lineamientos para manejo de fallas y reversión .....	132
7.8.9	Lineamientos de roles y responsabilidades .....	132
7.8.10	Seguimiento y control .....	132
7.9	PLAN DE PRUEBAS DURANTE EL CICLO DE VIDA DE LOS SISTEMAS DE INFORMACIÓN .....	133
7.9.1	Objetivo del plan de pruebas .....	133
7.9.2	Alcance.....	133
7.9.3	Principios del plan de pruebas .....	133
7.9.4	Lineamientos para la planeación de pruebas .....	134
7.9.5	Tipos de pruebas a considerar .....	134
7.9.6	Lineamientos para la ejecución de pruebas.....	135
7.9.7	Lineamientos para la documentación de resultados.....	135
7.9.8	Lineamientos para aprobación y liberación.....	135
7.9.9	Lineamientos de roles y responsabilidades .....	135
7.9.10	Seguimiento y mejora continua .....	136
7.10	MANUAL DEL USUARIO, TÉCNICO Y DE OPERACIÓN DE LOS SISTEMAS DE INFORMACIÓN .....	136
7.10.1	Objetivo de los manuales .....	136
7.10.2	Alcance.....	136
7.10.3	Principios para la documentación de sistemas de información .....	136
7.10.4	Lineamientos generales para todos los manuales.....	137
7.10.5	Lineamientos para el manual del usuario .....	137
7.10.6	Lineamientos para el manual técnico.....	139
7.10.7	Lineamientos para el manual de operación .....	141
7.10.8	Lineamientos de validación y aprobación.....	142
7.10.9	Lineamientos de roles y responsabilidades .....	142
7.10.10	Seguimiento y mejora continua .....	143
7.11	ESTRATEGIA DE MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN .....	143
7.11.1	Objetivo de la estrategia de mantenimiento .....	143
7.11.2	Alcance.....	143
7.11.3	Principios de la estrategia de mantenimiento .....	144
7.11.4	Tipos de mantenimiento .....	144
7.11.5	Lineamientos para la planificación del mantenimiento .....	145
7.11.6	Lineamientos de priorización y criticidad .....	145
7.11.7	Lineamientos de seguridad y control.....	146
7.11.8	Lineamientos de documentación y trazabilidad.....	146
7.11.9	Lineamientos de roles y responsabilidades .....	147
7.11.10	Seguimiento y mejora continua .....	147

7.12	SERVICIOS DE MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN CON TERCERAS PARTES .....	148
7.12.1	Objetivo de los servicios de mantenimiento con terceros .....	148
7.12.2	Alcance .....	148
7.12.3	Principios para la gestión de servicios con terceros .....	148
7.12.4	Lineamientos para la definición del alcance contractual .....	148
7.12.5	Lineamientos de seguridad y confidencialidad .....	149
7.12.6	Lineamientos para la gestión de accesos y ambientes .....	149
7.12.7	Lineamientos para la ejecución del mantenimiento .....	149
7.12.8	Lineamientos para la documentación y transferencia de conocimiento .....	149
7.12.9	Lineamientos de seguimiento y control del servicio .....	150
7.12.10	Lineamientos de evaluación y cierre contractual .....	150
7.13	PLAN DE CALIDAD DE LOS SISTEMAS DE INFORMACIÓN .....	150
7.13.1	Objetivo del plan de calidad .....	150
7.13.2	Alcance .....	151
7.13.3	Principios de calidad .....	151
7.13.4	Dimensiones de la calidad de los sistemas de información .....	151
7.13.5	Lineamientos para la planificación de la calidad .....	151
7.13.6	Lineamientos para el aseguramiento de la calidad .....	152
7.13.7	Lineamientos para el control y verificación de la calidad .....	152
7.13.8	Lineamientos de indicadores de calidad .....	152
7.13.9	Lineamientos de roles y responsabilidades .....	153
7.13.10	Seguimiento y mejora continua .....	154
7.14	REQUERIMIENTOS NO FUNCIONALES Y ATRIBUTOS CALIDAD DE LOS SISTEMAS DE INFORMACIÓN .....	154
7.14.1	Objetivo .....	154
7.14.2	Alcance .....	154
7.14.3	Principios para la definición de requerimientos no funcionales y atributos de calidad .....	155
7.14.4	Lineamientos para la identificación de requerimientos no funcionales .....	155
7.14.5	Atributos de calidad institucionales .....	155
7.14.6	Lineamientos para la documentación de requerimientos no funcionales .....	156
7.14.7	Lineamientos para la validación y aprobación .....	156
7.14.8	Lineamientos para el seguimiento y control .....	157
7.14.9	Roles y responsabilidades .....	157
7.15	ACCESIBILIDAD .....	157
7.15.1	Objetivo .....	157
7.15.2	Alcance .....	158

7.15.3	Principios de accesibilidad .....	158
7.15.4	Lineamientos generales de accesibilidad .....	158
7.15.5	Lineamientos de accesibilidad funcional y visual .....	158
7.15.6	Lineamientos de accesibilidad cognitiva y de contenido .....	158
7.15.7	Lineamientos de accesibilidad tecnológica .....	159
7.15.8	Lineamientos para la validación y pruebas de accesibilidad .....	159
7.15.9	Lineamientos para desarrollos y proveedores .....	159
7.15.10	Lineamientos de roles y responsabilidades .....	159
7.15.11	Seguimiento y mejora continua .....	159
7.16	ARQUITECTURA DE SOFTWARE .....	160
7.16.1	Objetivo .....	160
7.16.2	Alcance .....	160
7.16.3	Principios de la arquitectura de software .....	160
7.16.4	Lineamientos para la definición de la arquitectura de software .....	161
7.16.5	Lineamientos de estilos y patrones arquitectónicos .....	161
7.16.6	Lineamientos para la documentación de la arquitectura .....	161
7.16.7	Lineamientos de integración e interoperabilidad .....	162
7.16.8	Lineamientos de seguridad en la arquitectura .....	162
7.16.9	Lineamientos de escalabilidad y rendimiento .....	162
7.16.10	Lineamientos para el control de cambios arquitectónicos .....	162
7.16.11	Lineamientos de roles y responsabilidades .....	162
7.16.12	Seguimiento y mejora continua .....	163
7.16.13	Representación conceptual arquitectura por capas .....	163
7.16.14	Representación arquitectura por componentes .....	164
7.16.15	Arquitectura de integración e interoperabilidad .....	164
<b>8</b>	<b>Gestión de servicios TI .....</b>	<b>165</b>
8.1	LINEAMIENTOS GENERALES PARA LA GESTIÓN DE LOS SERVICIOS DE TI .....	165
8.1.1	Objetivo de la gestión de servicios de TI .....	166
8.1.2	Alcance .....	166
8.1.3	Principios de la gestión de servicios de TI .....	166
8.1.4	Definición lineamientos generales .....	167
8.1.5	Lineamientos para el ciclo de vida de los servicios de TI .....	167
8.2	CATÁLOGO DE SERVICIOS DE TECNOLOGÍA .....	169
8.2.1	Objetivo del catálogo de servicios de tecnología .....	169
8.2.2	Alcance .....	169
8.2.3	Principios del catálogo de servicios de tecnología .....	170

8.2.4	Lineamientos para la estructuración del catálogo .....	170
8.2.5	Clasificación de los servicios de tecnología .....	170
8.2.6	Lineamientos para la definición de niveles de servicio.....	171
8.2.7	Lineamientos para la gestión y actualización del catálogo .....	171
8.2.8	Lineamientos para la comunicación y uso del catálogo .....	171
8.2.9	Lineamientos de roles y responsabilidades .....	171
8.2.10	Seguimiento y mejora continua .....	172
8.3	ACCESO A SERVICIOS EN LA NUBE.....	172
8.3.1	Objetivo .....	172
8.3.2	Alcance.....	172
8.3.3	Principios para el acceso a servicios en la nube.....	173
8.3.4	Lineamientos para la habilitación del acceso.....	173
8.3.5	Lineamientos de gestión de identidades y accesos.....	173
8.3.6	Lineamientos de seguridad de la información .....	174
8.3.7	Lineamientos para el acceso remoto y conectividad .....	174
8.3.8	Lineamientos para el uso de servicios en la nube por terceros.....	175
8.3.9	Lineamientos de monitoreo y control.....	176
8.3.10	Lineamientos de continuidad y disponibilidad.....	176
8.3.11	Roles y responsabilidades .....	176
8.4	CONTINUIDAD Y DISPONIBILIDAD DE LOS SERVICIOS DE TI .....	176
8.4.1	Objetivo .....	177
8.4.2	Alcance.....	177
8.4.3	Principios de continuidad y disponibilidad .....	177
8.4.4	Lineamientos para la identificación de servicios críticos.....	177
8.4.5	Lineamientos para la disponibilidad de los servicios de TI.....	178
8.4.6	Lineamientos para la continuidad de los servicios de TI.....	178
8.4.7	Lineamientos para la gestión de incidentes y fallas.....	179
8.4.8	Lineamientos para la gestión de proveedores y terceros .....	180
8.4.9	Lineamientos de monitoreo y control.....	180
8.4.10	Lineamientos de roles y responsabilidades .....	180
8.4.11	Seguimiento y mejora continua .....	181
8.5	ALTA DISPONIBILIDAD DE LOS SERVICIOS DE TI.....	181
8.5.1	Objetivo .....	181
8.5.2	Alcance.....	181
8.5.3	Principios de alta disponibilidad .....	182
8.5.4	Lineamientos para la identificación de servicios con alta disponibilidad ....	182

8.5.5	Lineamientos para el diseño de arquitecturas de alta disponibilidad .....	183
8.5.6	Lineamientos para la alta disponibilidad en servicios en la nube .....	184
8.5.7	Lineamientos para la operación y monitoreo de la alta disponibilidad.....	184
8.5.8	Lineamientos para pruebas de alta disponibilidad .....	184
8.5.9	Lineamientos para la gestión de proveedores .....	184
8.5.10	Lineamientos de roles y responsabilidades .....	185
8.5.11	Seguimiento y mejora continua .....	185
8.6	CAPACIDAD DE LOS SERVICIOS TECNOLÓGICOS.....	185
8.6.1	Objetivo .....	185
8.6.2	Alcance.....	186
8.6.3	Principios de la gestión de capacidad .....	186
8.6.4	Lineamientos para la planificación de la capacidad.....	186
8.6.5	Lineamientos para la gestión de la demanda .....	186
8.6.6	Lineamientos para el monitoreo de la capacidad.....	187
8.6.7	Lineamientos para el control y ajuste de la capacidad.....	187
8.6.8	Lineamientos para la capacidad en servicios en la nube.....	187
8.6.9	Lineamientos para la gestión de capacidad con proveedores .....	187
8.6.10	Lineamientos de roles y responsabilidades .....	188
8.6.11	Seguimiento y mejora continua .....	188
8.7	ACUERDOS DE NIVEL DE SERVICIOS.....	188
8.7.1	Objetivo .....	188
8.7.2	Alcance.....	188
8.7.3	Principios de los acuerdos de niveles de Servicio .....	189
8.7.4	Lineamientos para la definición de los acuerdos de niveles de servicio ....	189
8.7.5	Lineamientos para la caracterización y priorización .....	189
8.7.6	Lineamientos para los componentes mínimos de los acuerdos de niveles de servicio	190
8.7.7	Lineamientos para la gestión de acuerdos de niveles de servicio con proveedores.....	190
8.7.8	Lineamientos para el seguimiento y control de los acuerdos de niveles de servicio	190
8.7.9	Lineamientos para la revisión y mejora de los acuerdos de niveles de servicio	190
8.7.10	Lineamientos de roles y responsabilidades .....	191
8.8	SOPORTE A LOS SERVICIOS DE TI.....	191
8.8.1	Objetivo .....	191
8.8.2	Alcance.....	191

8.8.3	Principios del soporte a los servicios de TI .....	192
8.8.4	Lineamientos generales del soporte.....	192
8.8.5	Lineamientos para la mesa de servicios (MDS) .....	192
8.8.6	Lineamientos para los niveles de soporte .....	192
8.8.7	Lineamientos para la gestión de incidentes y requerimientos.....	193
8.8.8	Lineamientos para el soporte en seguridad de la información.....	194
8.8.9	Lineamientos para la comunicación y seguimiento.....	194
8.8.10	Lineamientos para la calidad del soporte .....	195
8.8.11	Lineamientos de roles y responsabilidades .....	195
8.9	PLANES DE MANTENIMIENTO.....	195
8.9.1	Objetivo .....	195
8.9.2	Alcance.....	196
8.9.3	Principios de los planes de mantenimiento .....	196
8.9.4	Lineamientos para la definición de los planes de mantenimiento .....	196
8.9.5	Tipos de mantenimiento de los servicios de TI.....	196
8.9.6	Lineamientos para la planificación y programación .....	197
8.9.7	Lineamientos para la ejecución del mantenimiento .....	197
8.9.8	Lineamientos para el mantenimiento de servicios en la nube.....	197
8.9.9	Lineamientos para el control y seguimiento .....	197
8.9.10	Lineamientos para la articulación con la capacidad y disponibilidad .....	197
8.9.11	Lineamientos de roles y responsabilidades .....	198
8.9.12	Plantilla plan de mantenimiento de servicios de tecnologías de la información (TI).....	198
8.10	CONTROL DE CONSUMO DE LOS RECURSOS COMPARTIDOS POR SERVICIOS TECNOLÓGICOS .....	201
8.10.1	Objetivo .....	202
8.10.2	Alcance.....	202
8.10.3	Principios para el control del consumo .....	202
8.10.4	Lineamientos para la identificación de recursos compartidos.....	202
8.10.5	Lineamientos para la medición del consumo .....	203
8.10.6	Lineamientos para la asignación y límites de consumo .....	203
8.10.7	Lineamientos para el control del consumo en servicios en la nube .....	203
8.10.8	Lineamientos para el análisis y optimización del consumo .....	203
8.10.9	Lineamientos para la gestión de riesgos asociados al consumo.....	204
8.10.10	Lineamientos de roles y responsabilidades .....	204
8.10.11	Seguimiento y mejora continua .....	204
8.11	GESTIÓN PREVENTIVA DE LOS SERVICIOS TECNOLÓGICOS .....	204

8.11.1	Objetivo .....	205
8.11.2	Alcance.....	205
8.11.3	Principios de la gestión preventiva .....	205
8.11.4	Lineamientos generales de gestión preventiva .....	205
8.11.5	Lineamientos de prevención asociados a la seguridad de la información .	206
8.11.6	Lineamientos preventivos en la operación de los servicios TI .....	206
8.11.7	Lineamientos preventivos en mantenimiento y capacidad .....	206
8.11.8	Lineamientos preventivos en el uso de recursos tecnológicos .....	206
8.11.9	Lineamientos de prevención mediante capacitación y concientización.....	207
8.11.10	Lineamientos para la gestión preventiva con proveedores.....	207
8.11.11	Lineamientos de seguimiento y control.....	207
8.12	RESPALDO Y RECUPERACIÓN DE LOS SERVICIOS TECNOLÓGICOS.....	207
8.12.1	Objetivo .....	208
8.12.2	Alcance.....	208
8.12.3	Principios del respaldo y la recuperación .....	208
8.12.4	Lineamientos para la definición de respaldos.....	208
8.12.5	Lineamientos para la gestión de respaldos.....	209
8.12.6	Lineamientos para respaldos en servicios en la nube.....	209
8.12.7	Lineamientos para la recuperación de los servicios tecnológicos .....	209
8.12.8	Lineamientos de recuperación ante incidentes de seguridad .....	211
8.12.9	Lineamientos para pruebas de respaldo y recuperación .....	211
8.12.10	Lineamientos para la documentación y trazabilidad .....	211
8.12.11	Lineamientos de roles y responsabilidades .....	211
8.13	ANÁLISIS DE RIESGOS .....	212
8.13.1	Objetivo .....	212
8.13.2	Alcance.....	212
8.13.3	Principios del análisis de riesgos .....	212
8.13.4	Lineamientos para la identificación de riesgos .....	213
8.13.5	Lineamientos para el análisis y evaluación de riesgos.....	213
8.13.6	Lineamientos para el tratamiento de riesgos .....	213
8.13.7	Lineamientos para la articulación con la gestión de incidentes .....	214
8.13.8	Lineamientos para el monitoreo y seguimiento .....	214
8.13.9	Lineamientos para roles y responsabilidades .....	214
8.13.10	Documentación y trazabilidad .....	214
8.14	SEGURIDAD INFORMÁTICA .....	215
8.14.1	Objetivo .....	215

8.14.2	Alcance.....	215
8.14.3	Enfoque de gestión .....	215
8.14.4	Lineamientos estratégicos .....	215
8.15	DISPOSICIÓN DE RESIDUOS TECNOLÓGICOS.....	218
8.15.1	Objetivo .....	218
8.15.2	Alcance.....	218
8.15.3	Principios para la disposición de residuos tecnológicos .....	218
8.15.4	Lineamientos generales de gestión de residuos tecnológicos .....	219
8.15.5	Clasificación de residuos tecnológicos .....	219
8.15.6	Lineamientos para la protección de la información.....	219
8.15.7	Lineamientos para la disposición ambientalmente responsable.....	219
8.15.8	Lineamientos para la trazabilidad y control .....	220
8.15.9	Lineamientos de roles y responsabilidades .....	221
8.15.10	Seguimiento y mejora continua .....	221
8.15.11	Reglas institucionales obligatorias.....	221
8.16	GESTIÓN DE PROBLEMAS DE TI .....	222
8.16.1	Objetivo .....	222
8.16.2	Alcance.....	222
8.16.3	Principios de la gestión de problemas.....	222
8.16.4	Definición institucional de problema .....	222
8.16.5	Lineamientos para la identificación de problemas .....	223
8.16.6	Lineamientos para el análisis de problemas .....	223
8.16.7	Lineamientos para soluciones temporales y definitivas .....	224
8.16.8	Lineamientos para la articulación con la seguridad de la información.....	224
8.16.9	Lineamientos para el seguimiento y cierre .....	225
8.16.10	Lineamientos de roles y responsabilidades .....	225
8.16.11	Articulación con la gestión de servicios de TI .....	225
8.16.12	Indicadores de la gestión de problemas .....	225
8.16.13	Reglas institucionales obligatorias.....	226
8.17	GESTIÓN DE CAMBIOS DE TI .....	226
8.17.1	Objetivo .....	226
8.17.2	Alcance.....	226
8.17.3	Principios de la gestión de cambios .....	227
8.17.4	Tipos de cambios de TI .....	227
8.17.5	Lineamientos para el registro y clasificación.....	227
8.17.6	Lineamientos para el análisis y aprobación .....	227

8.17.7	Lineamientos para la planeación del cambio.....	228
8.17.8	Lineamientos para la implementación.....	228
8.17.9	Lineamientos para pruebas y validación.....	228
8.17.10	Lineamientos para el cierre y documentación .....	228
8.17.11	Articulación con la seguridad de la información .....	229
8.17.12	Roles y responsabilidades .....	229
8.17.13	Seguimiento y control .....	229
8.18	IMPLEMENTACIÓN DEL PROTOCOLO DE INTERNET VERSIÓN 6 (IPv6) .....	231
8.18.1	Objetivo .....	231
8.18.2	Alcance.....	231
8.18.3	Estado de implementación.....	231
8.18.4	Lineamientos de gobierno para IPv6.....	232
8.18.5	Seguridad de la información .....	232
8.18.6	Interoperabilidad y servicios .....	232
8.18.7	Relación con proveedores .....	233
8.18.8	Seguimiento y mejora continua .....	233
8.18.9	Reglas institucionales obligatorias.....	234
<b>9</b>	<b>Uso y apropiación de TI.....</b>	<b>236</b>
9.1	ESTRATEGIA DE USO Y APROPIACIÓN DE TI .....	236
9.1.1	Alcance.....	236
9.1.2	Principios orientadores .....	237
9.1.3	Lineamientos estratégicos .....	237
9.1.4	Reglas institucionales .....	238
9.1.5	Tipos de acciones de apropiación .....	240
9.2	ESQUEMA DE INCENTIVOS.....	240
9.2.1	Objetivo .....	240
9.2.2	Alcance.....	240
9.2.3	Principios orientadores .....	240
9.2.4	Tipología de incentivos .....	241
9.2.5	Criterios para la asignación de incentivos .....	241
9.2.6	Lineamientos de implementación .....	242
9.2.7	Seguimiento y evaluación .....	242
9.2.8	Reglas institucionales obligatorias.....	243
9.3	PLAN DE FORMACIÓN.....	243
9.3.1	Objetivo .....	243
9.3.2	Alcance.....	243

9.3.3	Principios orientadores .....	243
9.3.4	Lineamientos del Plan de Formación .....	244
9.3.5	Modalidades de formación .....	244
9.3.6	Articulación con la gestión del cambio .....	245
9.3.7	Roles y responsabilidades .....	245
9.3.8	Registro y evidencias .....	245
9.3.9	Evaluación y mejora continua .....	245
9.3.10	Plantilla del plan anual de formación en uso y apropiación de TIC .....	245
9.4	EVALUACIÓN DEL NIVEL DE ADOPCIÓN DE TI .....	246
9.4.1	Objetivo .....	246
9.4.2	Alcance .....	246
9.4.3	Principios orientadores .....	247
9.4.4	Dimensiones de evaluación .....	247
9.4.5	Niveles de adopción de TI .....	248
9.4.6	Fuentes de información para la evaluación .....	248
9.4.7	Periodicidad de la evaluación .....	248
9.4.8	Roles y responsabilidades .....	248
9.4.9	Uso de los resultados .....	249
9.5	PLAN DE CAPACITACIÓN Y ENTRENAMIENTO PARA LOS SISTEMAS DE INFORMACIÓN .....	249
9.5.1	Objetivo .....	249
9.5.2	Alcance .....	249
9.5.3	Principios orientadores .....	249
9.5.4	Lineamientos para la elaboración del plan .....	250
9.5.5	Periodicidad del plan .....	251
<b>10</b>	<b>Glosario .....</b>	<b>252</b>
<b>11</b>	<b>Referencias bibliográficas .....</b>	<b>253</b>

## Listado de tablas

- Tabla No. 1. ANS generales servicios TIC
- Tabla No. 2 Matriz de relación: Gestión de cambios, gobierno TI, MAE y proyectos TI
- Tabla No. 3. Matriz de mejoramiento de procesos
- Tabla No. 4 Matriz de gestión de documentos electrónicos
- Tabla No. 5 Ejemplo matriz de requerimiento vs proceso vs sistema.
- Tabla No. 6 Clasificación de requerimientos
- Tabla No. 7 Matriz de trazabilidad
- Tabla No. 8 Matriz de seguimiento y control
- Tabla No. 9 Matriz de mantenimiento de los sistemas de información
- Tabla No. 10 Clasificación de criticidad (referencia)
- Tabla No. 11 Ejemplo matriz de priorización del mantenimiento
- Tabla No. 12 Ejemplo matriz de control y trazabilidad del mantenimiento
- Tabla No. 13 Matriz de responsabilidades (RACI – Mantenimiento)
- Tabla No. 14 Matriz de criterios e indicadores de calidad
- Tabla No. 15 Clasificación de niveles de acceso
- Tabla No. 16 Matriz de riesgos asociados al acceso CLOUD
- Tabla No. 17 Matriz de control de acceso a servicios en la nube
- Tabla No. 18 Matriz de continuidad y disponibilidad de servicios de TI
- Tabla No. 19 Clasificación de criticidad
- Tabla No. 20 Matriz de alta disponibilidad de los servicios de TI
- Tabla No. 21 Tipos de arquitectura de alta disponibilidad
- Tabla No. 22 Matriz incidente / requerimiento
- Tabla No. 23 Tipos de respaldo
- Tabla No. 24 Matriz de respaldo y recuperación de los servicios tecnológicos
- Tabla No. 25 Matriz de disposición de residuos tecnológicos
- Tabla No. 26 Ejemplo de matriz de gestión de problemas
- Tabla No. 27 Matriz de gestión de cambios TI
- Tabla No. 28 Criterios de clasificación del riesgo
- Tabla No. 29 Matriz servicio IPV6
- Tabla No. 30 Criterios del tipo de dependencia IPV6
- Tabla No. 31 Matriz de uso y apropiación
- Tabla No. 32 Matriz asignación de incentivos

## 1 Introducción

El modelo de gestión de gobierno de tecnologías de la información, de la alcaldía municipal de Chía, se establece como el marco rector que orienta el uso estratégico, eficiente y seguro de las tecnologías en la administración pública. Este modelo articula los principios de la arquitectura empresarial, los lineamientos de la política de gobierno digital y el plan estratégico de tecnologías de la información y las comunicaciones (PETIC), con el fin de asegurar que las iniciativas tecnológicas aporten de manera directa al cumplimiento del plan de desarrollo municipal y al fortalecimiento de la gestión institucional.

La construcción del modelo parte del análisis integral de la situación actual de las TIC, las capacidades institucionales, los sistemas de información existentes y las necesidades expresadas por las dependencias, insumos obtenidos a través del levantamiento de la arquitectura empresarial y sintetizados en el documento del modelo de arquitectura empresarial (MAE). Este diagnóstico permitió identificar brechas, riesgos, oportunidades y prioridades estratégicas que se reflejan en la hoja de ruta de arquitectura empresarial, orientando la evolución tecnológica hacia una arquitectura integrada, interoperable y centrada en el ciudadano.

En este contexto, el modelo de gestión de gobierno TI, propone una estructura clara de gobernanza, roles y procesos para dirigir la gestión de TI, promover una adecuada toma de decisiones, garantizar la protección y calidad de la información, impulsar la transformación digital de los servicios municipales y asegurar la sostenibilidad tecnológica. Así mismo, establece los lineamientos para la gestión del riesgo tecnológico, la seguridad digital, la operación de los servicios de TI y la alineación continua entre las iniciativas tecnológicas y los objetivos estratégicos de la entidad, orientada a la mejora continua, garantizando que los servicios prestados a través de la Oficina TIC, actúen como un habilitador clave del desarrollo institucional y del bienestar de la comunidad.

## MODELO DE GESTIÓN Y GOBIERNO TI (MGGTI)

El modelo de gestión y gobierno de tecnologías de la información de la alcaldía municipal de Chía, constituye el marco integral que orienta la planeación, formulación, ejecución y control de las decisiones relacionadas con el uso estratégico de las tecnologías en la entidad, fundamentado en los principios de la arquitectura empresarial, en la política de gobierno digital y en los lineamientos del plan estratégico de tecnologías de la información y las comunicaciones (PETIC), articulando la gestión tecnológica con los objetivos institucionales y las metas del plan de desarrollo municipal (PDM), convirtiéndose en un habilitador transversal que potencia el desempeño institucional, mejora la prestación de los servicios ciudadanos, alineado a las políticas de seguridad de la información, optimizando la operación interna y estableciendo los lineamientos, guiando los procesos y proporcionando estructuras necesarias para:

- Dirigir la TI con criterios estratégicos.
- Gestionar el riesgo tecnológico y la seguridad digital.
- Impulsar la transformación digital y la interoperabilidad.
- Garantizar la calidad, trazabilidad y disponibilidad de los datos institucionales.
- Integrar las iniciativas tecnológicas bajo una visión arquitectónica común.
- Asegurar la sostenibilidad y continuidad de los servicios de TI.

El modelo de gestión y gobierno TI, integra insumos del modelo de arquitectura empresarial (MAE), el cual proporciona el contexto estructural de los dominios: información, aplicaciones, infraestructura, seguridad y procesos, consolida el diagnóstico del estado actual de estos dominios, evidenciando la necesidad de fortalecer la integración entre sistemas, consolidar repositorios de datos, modernizar plataformas y estandarizar la gestión de TI. Prioriza iniciativas críticas en la hoja de ruta, como la consolidación del sistema estadístico municipal, la modernización de la ventanilla única virtual, el fortalecimiento de plataformas sectoriales y la creación del repositorio AE.

Mediante el modelo de gestión y gobierno TI, se establece una estructura organizacional y decisional basada en roles claramente definidos:

- Comité de gestión y desempeño: instancia máxima para la toma de decisiones estratégicas, priorización de proyectos y aprobación de políticas.
- Oficina TIC: responsable de la dirección técnica, gestión de infraestructura, mantenimiento y evolución de sistemas, interoperabilidad, seguridad digital y ejecución del PETIC.
- Líderes de arquitectura empresarial: Garantes de alineación de estrategias y políticas, con la arquitectura empresarial.
- Equipo de infraestructura tecnológica: responsables de implementar las políticas, controles, monitoreo, respuesta a incidentes y gestión de vulnerabilidades.
- Enlaces de arquitectura empresarial: responsables de definir requerimientos funcionales, roles de propietario del dato y cumplimiento normativo.

El modelo presenta los lineamientos que organizan la gestión tecnológica en procesos que abarcan todo el ciclo de vida de la TI, alineados con el PETIC, de la alcaldía municipal de Chía:

### **Planeación y gobierno TI**

- Gestión del portafolio de proyectos TI.
- Definición y seguimiento de políticas, estándares y lineamientos.
- Alineación de TI con el modelo operativo institucional y MIPG.

### **Gestión de información y datos**

- Gobernanza del dato, definiciones de calidad, flujos y metadatos.
- Consolidación de repositorios y plataformas estadísticas.
- Servicios de intercambio y analítica institucional.

### **Gestión de sistemas de información**

- Arquitectura de referencia y mapa de aplicaciones.
- Integración mediante APIs, servicios y componentes comunes.
- Ciclo de vida del software: desarrollo, pruebas, despliegue y mantenimiento.

### **Gestión de infraestructura TI**

- Capacidad, disponibilidad, continuidad del servicio.
- Redes, servidores, nube, virtualización y seguridad perimetral.
- Administración de entornos y monitoreo.

### **Seguridad digital y gestión del riesgo**

- Controles y políticas basadas en ISO 27001, gobierno digital y MIPG.
- Gestión de incidentes, vulnerabilidades y continuidad operacional.
- Identificación, análisis y tratamiento del riesgo TIC.

### **Uso y apropiación de TI**

- Capacitación para servidores públicos.
- Cultura de datos, ciberseguridad y transformación digital.

### **Habilitadores tecnológicos**

- Plataformas de integración (APIs, servicios SOA).
- Repositorios de datos y observatorios sectoriales.

- Infraestructura escalable para sistemas de misión crítica.
- Mecanismos de interoperabilidad con el estado colombiano (Carpeta ciudadana digital, X-Road).
- Herramientas de monitoreo, trazabilidad y seguridad digital.
- Portales y servicios digitales orientados al ciudadano.

#### **Convergencia estratégica: MAE vs Hoja de Ruta vs PETIC**

- Modelo de arquitectura empresarial (MAE): describe el estado actual y el modelo objetivo de la TI.
- Hoja de ruta AE: define iniciativas estratégicas priorizadas que deben ejecutarse para cerrar brechas.
- PETIC: establece la visión, las capacidades, el portafolio de proyectos y los lineamientos operativos para la TI municipal.

USO INSTITUCIONAL - ALCALDÍA DE CHÍA

## 2 Alcance del documento

El modelo de gestión y gobierno de tecnologías de la información (MGGTI), define el marco institucional para la planificación, dirección, control y evaluación del uso estratégico de las TIC en la alcaldía municipal de Chía, mediante la definición de directrices para la estructuración de políticas, procesos, roles, capacidades, y mecanismos de toma de decisiones, que aseguran que la inversión, operación, desarrollo y uso de las tecnologías estén alineadas con:

- El plan de desarrollo municipal.
- El plan estratégico de tecnologías de la información y las comunicaciones (PETIC).
- El modelo de arquitectura empresarial (MAE).
- La política de gobierno digital, la política de seguridad de la información y el marco normativo MinTIC.
- Las necesidades misionales, estratégicas y de servicio a la ciudadanía.

### 2.1 Desglose del alcance por dominios

#### 2.1.1 Dominio de estrategia TI

- Definir principios y lineamientos estratégicos para la toma de decisiones en TI.
- Asegurar la alineación del PETIC con la arquitectura empresarial, el PDM y los lineamientos de gobierno digital.
- Integrar necesidades transversales identificadas en el MAE: interoperabilidad, analítica de datos, sistematización de procesos, digitalización de trámites.
- Establecer criterios institucionales para evaluar inversiones, riesgos y beneficios de las iniciativas TI.

#### 2.1.2 Dominio de gobierno TI

- Definir la estructura de gobierno: Comité de gestión y desempeño, comité técnico AE conformado por los enlaces, Oficina TIC y líderes por dominio.
- Establecer roles y modelo RACI para la toma de decisiones en TI, arquitectura empresarial, seguridad e información.
- Definir políticas institucionales: Gobierno digital, seguridad digital, seguridad de la información.
- Implementar mecanismos de seguimiento, control y evaluación del desempeño TI.
- Consolidar el repositorio institucional de arquitectura y productos de gobierno TI.

#### 2.1.3 Dominio de gestión de la información

- Definir el modelo de información institucional (fuentes, flujos, metadatos, roles y responsabilidades).

- Integrar lineamientos de gestión de datos basados en DAMA (Data management association) y DCAM (Data management capability assesmen model).
- Establecer estándares para la captura, almacenamiento, interoperabilidad e intercambio seguro de datos.
- Definir roles: administradores de datos, custodios, propietarios y analistas.
- Establecer lineamientos para integrar información con plataformas internas y externas.

#### 2.1.4 Dominio de gestión de sistemas de información

- Estandarizar lineamientos de caracterización de los sistemas existentes.
- Definir la arquitectura de aplicaciones en alineación con el modelo de AE de la alcaldía de Chía.
- Identificar redundancias, brechas tecnológicas y oportunidades de convergencia.
- Definir lineamientos para adquisiciones, desarrollos, mantenimiento, pruebas e interoperabilidad.
- Establecer lineamientos de actualización del catálogo de servicios y funcionalidades por sistema.

#### 2.1.5 Dominio de gestión de servicios de TI

- Definir directrices para la actualización del catálogo de servicios TI institucional (infraestructura, aplicaciones, soporte, redes, seguridad).
- Establecer niveles de servicio (ANS/SLAs) y métricas de operación.
- Definir lineamientos para procesos basados en mejores prácticas (ITIL/Mintic):
  - Gestión de incidentes
  - Gestión de problemas
  - Gestión de cambios
  - Gestión de capacidad
  - Gestión de continuidad
- Definir los mecanismos a implementar de monitoreo, evaluación y mejora continua.
- Establecer directrices para lograr integrar la gestión de infraestructura tecnológica (red, servidores, nube, almacenamiento, respaldo).
- Articular los servicios TI al MAE.

#### 2.1.6 Dominio de uso y apropiación de TI

- Diseñar la estrategia institucional de uso y apropiación, alineada al MAE, de la alcaldía municipal de Chía.
- Definir programas de formación y capacitación transversales en:
  - Herramientas tecnológicas
  - Gobierno digital
  - Seguridad digital

- Analítica de datos
- Uso de la ventanilla única virtual
- Diseñar campañas de sensibilización para fomentar la cultura digital.
- Establecer indicadores de apropiación y adopción tecnológica.
- Acompañar la gestión del cambio para iniciativas de digitalización.
- Crear mecanismos de retroalimentación con usuarios internos y ciudadanía.

USO INSTITUCIONAL - ALCALDÍA DE CHÍA

### 3 Objetivo general

Establecer el marco integral de gobernanza, planificación, operación y control de las tecnologías de la información en la alcaldía municipal de Chía, que permita alinear la estrategia institucional con la arquitectura empresarial, fortalecer la toma de decisiones basada en datos, garantizar la seguridad y disponibilidad de la información, optimizar los servicios digitales y asegurar que las iniciativas tecnológicas generen valor público, mejoren la gestión interna y contribuyan al cumplimiento del plan de desarrollo municipal y del plan estratégico de tecnologías de la información y las comunicaciones.

#### 3.1 Objetivos específicos:

- Definir una estructura de gobierno TI que incluya roles, procesos, responsabilidades y mecanismos de decisión articulados con la arquitectura empresarial.
- Alinear la ejecución tecnológica con el PETIC, el PDM y los lineamientos de gobierno digital.
- Implementar un modelo de gestión y gobierno del dato que asegure calidad, integridad, trazabilidad, interoperabilidad y seguridad.
- Establecer directrices para garantizar la disponibilidad y uso de la información para la toma de decisiones.
- Establecer lineamientos, estándares y responsabilidades para la administración de datos en todas las dependencias.
- Caracterizar, integrar y armonizar los sistemas existentes, según las necesidades misionales y la arquitectura objetivo definida en el MAE.
- Promover la modernización de plataformas, la eliminación de redundancias y la adopción de modelos interoperables basados en servicios (APIs, SOA).
- Establecer lineamientos para garantizar el ciclo de vida adecuado de las soluciones tecnológicas: desarrollo, mantenimiento, pruebas, despliegue y seguimiento.
- Establecer directrices para actualizar y gestionar un catálogo de servicios TI con niveles de servicio (ANS) claros y medibles.
- Alinear el MGGTI, el MAE y las políticas de seguridad de la información, cuya implementación permita mejorar la disponibilidad, continuidad, rendimiento y seguridad de la infraestructura tecnológica.
- Impulsar la implementación de procesos de operación TI basados en buenas prácticas (ITIL, MinTIC): incidentes, problemas, cambios, disponibilidad, continuidad y capacidad.
- Desarrollar políticas, controles y mecanismos de protección alineados con la política de seguridad digital, ISO 27001 y lineamientos del MinTIC.
- Gestionar riesgos tecnológicos y operativos mediante estrategias de prevención, detección y respuesta a incidentes.
- Desarrollar estrategias de capacitación y fortalecimiento de competencias digitales para servidores públicos.
- Impulsar la adopción efectiva de sistemas, plataformas y servicios digitales en las dependencias y la ciudadanía.

- Fomentar la cultura de seguridad digital, uso responsable de la información, analítica y transformación digital.
- Establecer mecanismos de seguimiento, medición de madurez y mejora continua del modelo.
- Consolidar el repositorio institucional de la arquitectura y productos TI para asegurar trazabilidad y gestión del conocimiento.
- Integrar el gobierno TI con MIPG, los procesos institucionales y el ciclo de planeación municipal.

USO INSTITUCIONAL - ALCALDÍA DE CHÍA

## 4 Estrategia TI

La estrategia establecida, consiste en lograr un enfoque integral, sostenible y alineado a la misión institucional, al modelo de arquitectura empresarial, al plan estratégico de tecnologías de la información y las comunicaciones, al plan de desarrollo municipal y se fundamenta en los dominios de la arquitectura empresarial, desarrollando las capacidades institucionales y generando valor al ciudadano, contribuyendo con ello, al cumplimiento de los objetivos establecidos en el presente modelo de gestión y gobierno TI.

A continuación, se presenta la ilustración de las etapas que se desarrollan en el dominio de estrategia TI, definido por MinTIC:

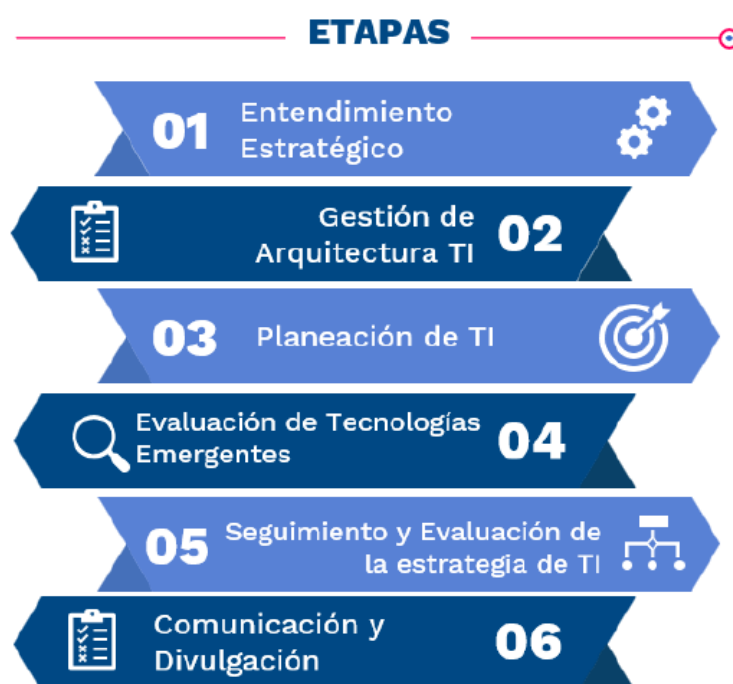


Ilustración No. 1. Etapas de la estrategia TI  
Fuente: Guía Dominio MGGTI.G.ES - Estrategia de TI, MinTIC 2023

### 4.1 Entendimiento estratégico

El plan estratégico de tecnologías de la información y las comunicaciones (PETIC), de la alcaldía municipal de Chía, define que las tecnologías deben operar como un elemento transversal que soporte las funciones administrativas, facilite la modernización institucional y fortalezca la interacción con la ciudadanía. En este marco, el modelo de gestión y gobierno de tecnologías de la información (MGGTI) reconoce la TI no como un componente meramente operativo, sino como un activo estratégico que impulsa:

- La toma de decisiones basadas en datos.
- La interoperabilidad entre dependencias y con entidades externas.
- La digitalización de procesos y trámites.

- La eficiencia en la gestión institucional.
- La transparencia y la rendición de cuentas.
- El cumplimiento de metas del plan de desarrollo municipal.

El modelo de arquitectura empresarial (MAE 2025), de la alcaldía municipal de Chía, proporciona la estructura conceptual y técnica, para entender la organización desde los dominios de procesos, información, aplicaciones y tecnología. Bajo este enfoque, el MGGTI se construye como el mecanismo que gobierna, regula y coordina la evolución de estos dominios, garantizando:

- Una arquitectura integrada y coherente.
- La alineación de los sistemas con los procesos misionales.
- La gestión del dato como activo estratégico.
- La seguridad digital como pilar transversal.
- La estandarización de prácticas y lineamientos tecnológicos.

Tanto el PETIC como el MAE, de la alcaldía municipal de Chía, identifican brechas en digitalización, integración de sistemas, calidad de datos y madurez en gestión tecnológica.

El modelo de gestión y gobierno TI (MGGTI), asume estas brechas como punto de partida para impulsar procesos de transformación digital que permitan:

- Modernizar la ventanilla única virtual y demás plataformas institucionales.
- Asegurar servicios más simples, oportunos y orientados al ciudadano.
- Implementar infraestructura confiable y resiliente.
- Integrar datos y sistemas mediante APIs, servicios y estándares de interoperabilidad.
- Promover el gobierno del dato y la analítica institucional.

El modelo de arquitectura empresarial y en el presente modelo de gestión y gobierno TI (MGGTI), incorporan el entendimiento de que la seguridad no es un requisito técnico aislado, sino un componente esencial de la estrategia institucional, por lo tanto, la entidad reconoce la necesidad de:

- Proteger la información institucional y los datos personales.
- Asegurar la continuidad del negocio y la resiliencia operativa.
- Gestionar riesgos tecnológicos y cibernéticos de manera proactiva.
- Implementar controles basados en estándares (ISO 27001, políticas MinTIC).

El PETIC evidencia que la entidad requiere mayor formalización de roles, procesos y mecanismos de coordinación en torno a la tecnología. El MGGTI se fundamenta en la convicción de que para avanzar hacia niveles superiores de madurez es indispensable:

- Formalizar roles como custodios, propietarios del dato, arquitectos, responsables de seguridad y gestores TI.
- Establecer procesos uniformes para la operación tecnológica.
- Implementar repositorios institucionales de arquitectura, información y activos TI.

- Fortalecer la gestión del cambio y la apropiación tecnológica.

## 4.2 Documentación de la estrategia de TI en el PETIC

En el plan estratégico de tecnologías de la información y las comunicaciones, se dejó documentada la estrategia, metas y proyectos, que se ejecutarán en el período comprendido del 2024-2028, abarcando todas las áreas operativas y administrativas de la alcaldía municipal de Chía, alineados a los objetivos misionales estratégicos y de apoyo de la entidad.

En el PETIC, se detallan desde la situación actual de la Oficina TIC, llegando a la situación deseada, dejando establecido en base a la hoja de ruta, el catálogo de iniciativas a implementar, de acuerdo al presupuesto asignado.

En el sitio web de la alcaldía municipal de Chía, módulo de transparencia, se encuentra publicado el PETIC, para su consulta: <https://chia-cundinamarca.gov.co/web/2023/12/7-5-plan-estrategico-de-sistemas/>

La documentación estratégica de TI, consolida los dominios de gestión de TI, cada uno con sus actividades principales, alineados al modelo de arquitectura empresarial (MAE), los cuales se describen a continuación:

### 4.2.1 Dominio: Estrategia de TI

Este dominio define los elementos estratégicos que orientan toda la gestión tecnológica de la alcaldía municipal de Chía e incluye el entendimiento institucional, planeación estratégica, arquitectura, innovación y evaluación. Las principales actividades para su desarrollo son:

- Comprender la estrategia institucional, la gestión misional y el portafolio de trámites y servicios.
- Articular la arquitectura de TI con la arquitectura empresarial, liderar su implementación, mantenimiento y evolución.
- Estructurar planes, programas, proyectos, definir hoja de ruta, recursos y plan de adquisiciones.
- Investigar e incorporar iniciativas, teniendo en cuenta innovaciones tecnológicas, orientadas a generación de valor público.
- Establecer lineamientos para monitorear indicadores, desempeño y resultados de TI para la mejora continua.
- Promover la cultura digital y apropiación de la estrategia institucional.

### 4.2.2 Dominio: Gobierno de TI

El gobierno de TI debe consolidar una Oficina TIC estructurada, capaz de asegurar sostenibilidad técnica, financiera y organizacional para la ejecución de la estrategia, es por ello que para lograrlo se deben ejecutar las siguientes actividades:

- Diseñar y mantener la estructura organizacional de TI para apoyar procesos, servicios y arquitectura institucional.
- Definir políticas de TI, incluyendo gobierno digital, seguridad digital y seguridad de la información.
- Establecer acuerdos de niveles de servicio (SLAs/OLAs) con áreas internas para mejorar procesos y asegurar disponibilidad.
- Consolidar instancias de decisión: Comité de gestión y desempeño y comité de seguridad de la información, con sus responsabilidades formales en la implementación del PETIC.
- Gestionar los riesgos y la continuidad operativa, incluidos ciberseguridad, alta disponibilidad y planes de respuesta a incidentes

#### 4.2.3 Dominio: Gestión de la información

Debemos tener en cuenta que la información debe provenir de los sistemas institucionales, habilitando toma de decisiones y procesos, por lo tanto, las principales actividades a realizar son las siguientes:

- Alinear necesidades de información con la estrategia institucional y los procesos.
- Configurar flujos permanentes de información para potenciar análisis y soporte a decisiones y servicios ciudadanos.
- Implementar políticas de calidad de datos (confiabilidad, oportunidad, consistencia, relevancia).
- Habilitar herramientas de analítica y uso de información existentes y disponibles para las dependencias y la ciudadanía.
- Desarrollar soluciones y servicios digitales basados en analítica, transformación digital e innovación tecnológica, alineados al gobierno digital y su marco normativo.

#### 4.2.4 Dominio: Sistemas de información

El desarrollo de este dominio se debe orientar a garantizar sistemas de información que satisfagan necesidades de procesos, servicios y alineación sectorial. Teniendo esto en cuenta, las principales actividades a ejecutar son las siguientes:

- Desarrollar soluciones digitales e interoperables, incluyendo módulos para atención ciudadana, automatización y ventanilla única
- Diseñar y mantener sistemas basados en arquitectura empresarial, cumpliendo principios de interoperabilidad y seguridad.
- Aplicar prácticas de desarrollo seguro, control de versiones, pruebas de penetración y gestión de vulnerabilidades.

- Automatizar procesos priorizados alineados al plan de desarrollo municipal.

#### 4.2.5 Dominio: Infraestructura y Tecnología

Este dominio es un habilitador de servicios, seguridad y continuidad, por lo tanto, se debe tener en cuenta:

- Gestionar infraestructura tecnológica: Datacenter, servidores, redes, UPS, conectividad y equipos institucionales.
- Garantizar seguridad perimetral y de red, incluyendo firewalls, IDS/IPS, segmentación y configuraciones seguras.
- Gestionar disponibilidad, redundancia y recuperación ante desastres (DRP) para sistemas críticos.
- Operar plataformas y herramientas claves: Antivirus centralizado, VPN, backup seguro, X-Road y servicios SOA.
- Administrar licencias, costos tecnológicos y servicios en la nube conforme al presupuesto establecido.

#### 4.2.6 Dominio: Uso y apropiación de TI

El modelo de arquitectura empresarial (MAE), de la alcaldía de Chía, establece que la apropiación reforzará una cultura orientada a planificación, interoperabilidad y toma de decisiones basada en evidencia. Los lineamientos establecidos dentro de este dominio abarcan las siguientes actividades:

- Capacitar en competencias digitales y herramientas institucionales.
- Implementar estrategia de sensibilización, fortalecimiento de capacidades y comunicación, conforme a los componentes del modelo de arquitectura empresarial.
- Aplicar casos de uso reales, especialmente interoperabilidad, ventanilla única y modelo de datos municipal.
- Ejecutar ejercicios de apropiación mediante divulgación, capacitación y acompañamiento a dependencias.

### 4.3 Políticas de TI

El conjunto de políticas institucionales relacionadas con la gestión, seguridad y uso de las tecnologías de la información, constituyen un pilar esencial del modelo de gestión de gobierno TI de la alcaldía municipal de Chía. Estas políticas establecen criterios unificados de operación tecnológica y definen las responsabilidades de todos los actores involucrados en el ciclo de vida de la información, los sistemas y los servicios digitales.

Las políticas de TI se estructuran alrededor de tres marcos normativos centrales:

- Política de gobierno digital, que orienta la transformación digital, la prestación de servicios ciudadanos digitales, la interoperabilidad y la innovación pública.
- Política de seguridad digital, que regula la gestión del riesgo cibernético, la respuesta a incidentes y la protección de la infraestructura crítica digital.
- Política de seguridad de la información, que establece los lineamientos para la protección de los activos de información en todo su ciclo de vida, conforme al MSPI y a la norma ISO/IEC 27001:2022.

Teniendo en cuenta estas tres políticas, a continuación, se consolidan los lineamientos para el modelo de gestión de gobierno TI:

#### 4.3.1 Lineamientos de gobierno, gestión y planeación de TI

- Establecer una estructura de gobernanza clara, soportada por la Oficina TIC, comités institucionales y roles definidos en la operación tecnológica.
- Asegurar que toda decisión relacionada con sistemas, datos, infraestructura y servicios digitales esté alineada con el plan de desarrollo municipal, el PETIC, la arquitectura empresarial y los marcos MinTIC.
- Garantizar una articulación permanente con el MIPG, el modelo de seguridad y privacidad de la información (MSPI) y el marco de referencia de arquitectura empresarial.
- Elaborar, mantener y actualizar el PETIC y la arquitectura TI como instrumentos que guíen la inversión, proyectos y priorización tecnológica.
- Integrar elementos habilitadores del gobierno digital: arquitectura TI, seguridad digital, servicios ciudadanos digitales y cultura digital.
- Incorporar lineamientos de innovación pública digital orientados a servicios digitales inteligentes, decisiones basadas en datos y gobierno abierto.
- Garantizar que toda iniciativa tecnológica cuente con análisis de costo/beneficio, riesgos, valor público y alcance.
- Priorizar soluciones tecnológicas interoperables, seguras, escalables y alineadas con estándares nacionales.
- Operar bajo buenas prácticas ITIL para mesa de ayuda, soporte técnico, atención de incidentes, gestión de cambios y disponibilidad.
- Gestionar redes, servidores, bases de datos, VPN, dispositivos y aplicativos con estándares certificados.
- Controlar todo acceso lógico y físico a centros de datos y entornos digitales.
- Adoptar estándares de interoperabilidad definidos por MinTIC.
- Integrar trámites y servicios digitales con plataformas como carpeta ciudadana Digital.
- Desarrollar programas permanentes de capacitación en gobierno digital, seguridad digital y seguridad de la información.
- Fortalecer la cultura organizacional basada en prácticas éticas y seguras en el uso de TIC.
- Promover alfabetización digital a través del punto vive digital y otros programas sociales.

- Garantizar inclusión digital, especialmente para poblaciones vulnerables.

#### 4.3.2 Lineamientos de seguridad de la información

- Realizar diagnósticos periódicos de vulnerabilidades, riesgos de ciberseguridad y exposición digital.
- Mantener actualizada la matriz de riesgos informáticos, incorporando controles correctivos, preventivos y de contingencia alineados con la guía del DAFP V7, el MSPI y la ISO/IEC 27005 y 27002:2022
- Implementar controles avanzados para protección del entorno digital: Segmentación de red, identificación y acceso, cifrado, registros de auditoría, monitoreo y restricción física de zonas críticas.
- Implementar controles de acceso, gestión de usuarios, privilegios y uso de software institucional.
- Asegurar la disponibilidad y resiliencia de los servicios mediante planes de continuidad, redundancia, respaldo y recuperación ante desastres.
- Mantener actualizado el procedimiento de gestión de incidentes, para que los usuarios sepan qué deben hacer ante un incidente o riesgo de seguridad y tomar las acciones para restaurar el sistema y documentar las lecciones aprendidas, ayudándonos a mejorar continuamente frente a experiencias pasadas dentro de la entidad.
- Coordinar acciones con entes nacionales como ColCERT y otros equipos CSIRT institucionales.
- Mantener las plataformas tecnológicas actualizadas y alineadas con estándares nacionales de ciberseguridad y lineamientos del MinTIC.
- Evaluar tecnologías emergentes y ajustar periódicamente los controles.
- Establecer estándares para la transferencia segura de información, gestión de redes, uso de dispositivos móviles y administración de sistemas.
- Implementar criptografía y mecanismos seguros de acceso remoto.
- Asegurar que todos los proyectos de software cumplan con requisitos de seguridad desde su concepción (desarrollo seguro).
- Mantener entornos separados de desarrollo, pruebas y producción.

#### 4.4 Gestión de los proyectos con componentes de TI

Los proyectos se deben generar producto del trabajo conjunto, entre las diferentes dependencias de la alcaldía municipal de Chía, en articulación con el modelo de arquitectura empresarial, siendo gestionados por cada una de las dependencias en las que se identificó la necesidad dando origen al proyecto, siendo priorizado de acuerdo al impacto a la ciudadanía, viabilidad técnica, la capacidad de recurso humano asignado y modernización institucional.

Todos los proyectos con componentes TI, deben demostrar la alineación con el PETIC, el MAE, las políticas de gobierno digital, seguridad digital y los objetivos estratégicos del plan de desarrollo municipal.

Los proyectos deben gestionarse de acuerdo a las fases, los hitos y los entregables establecidos en el MGPTI: Inicio, planeación, ejecución, control, cierre y transferencia a la operación.

Las metodologías a utilizar se encuentran definidas en el MGPTI, de la siguiente manera:

- Para desarrollo y automatización: ScrumBan.
- Para proyectos de datos: CRISP-DM.
- Para interoperabilidad: Estándares del MinTIC y la política de servicios ciudadanos digitales.

Se debe elaborar una ficha técnica por cada proyecto con un alcance claro, que incluya el propósito y la justificación, la necesidad a la cual se dará solución, beneficiarios internos y/o externos e identificación de los riesgos con su respectivo plan de tratamiento.

De acuerdo a la ficha técnica, se deben identificar los interesados que se verán afectados positiva o negativamente con el proyecto, realizar la reunión de inicio y asignación del líder del proyecto.

Siguiendo los lineamientos establecidos dentro del MGPTI, en la fase de planeación se debe realizar el análisis DOFA, la definición de los requerimientos funcionales, tecnológicos y criterios de calidad, definir el plan de trabajo y establecer el plan de comunicaciones y de gestión de cambios, teniendo en cuenta los costos estimados por cada una de las fases.

Alineados a la metodología de gestión de proyectos MGA y PMP, se debe realizar seguimiento, monitoreo y control durante todo el ciclo de vida de los proyectos, formalizando ante el comité de cambios toda modificación que llegue a surgir en tiempos, costos o calidad.

Una vez desarrollados los entregables del proyecto se entra a la fase de cierre la cual debe quedar formalizada mediante un acta, en la cual conste el recibo a satisfacción de cada uno de los entregables establecidos en la fase de planeación, la transferencia de conocimientos formal a la operación y las lecciones aprendidas.

Todo proyecto que implique desarrollo de sistemas de información debe cumplir con los estándares de interoperabilidad, desarrollo de software seguro y sostenibilidad tecnológica.

#### **4.5 Gestión del presupuesto de TI**

Es obligatorio la alineación con las metas establecidas en el plan de desarrollo municipal, el modelo de arquitectura empresarial y el plan estratégico de tecnologías de la información y las comunicaciones.

Para la implementación de estrategias de TIC, se debe proyectar las necesidades presupuestales conforme a la metas e iniciativas identificadas en el MAE y alineadas al PDM, de manera que se cuente con recursos financieros y asignación de estos a través del certificado de disponibilidad presupuestal.

El presupuesto de la Oficina TIC, debe estimarse teniendo en cuenta la infraestructura requerida (servidores, redes, wifi, cableado estructurado, equipos activos), sistemas de información y desarrollos, seguridad digital y alta disponibilidad, innovación y analítica de datos, servicios ciudadanos digitales, soporte y mantenimiento, gestión del cambio, licenciamiento, servicios en la nube y tercerizados.

La ejecución de los proyectos debe realizarse de acuerdo al plan anual mensualizado de caja (PAC) y el plan operativo anual de inversiones (POAI), los contratos y las adquisiciones aprobadas de TIC, las cuales deben realizarse bajo las normas aplicables en SECOP II, ley 80, ley 1150 y manuales internos de contratación.

Se deben consolidar informes de seguimiento en los cuales se incluya la ejecución presupuestal por proyecto y meta del PDM, estado de los hitos y entregables, alertas, gestiones de cambios realizadas (si aplica), reprogramaciones y limitaciones presupuestales (si aplica).

Teniendo en cuenta en el modelo de arquitectura empresarial, fue definida la hoja de ruta, se debe garantizar el cumplimiento de esta y para ello se requiere garantizar recursos para conectividad priorizando la solución de redundancia geográfica, seguridad perimetral servicios en alta disponibilidad, la recuperación ante desastres, financiar la interoperabilidad, API, UX/UI y las pruebas de despliegue, inversiones en IA, machine learning, IoT, infraestructura de datos, visores de tableros y sistemas estadísticos, garantizando la sostenibilidad, seguridad y gobernanza de datos.

Toda inversión que lleve componentes de tecnologías de la información y las comunicaciones, debe producir impacto positivo, mejorando el servicio al ciudadano, logrando inclusión digital, transparencia en los trámites, seguridad digital, evitando la dependencia de proveedores únicos y duplicidad de sistemas, favoreciendo la integración y reutilización de componentes de los sistemas de información, de manera que logremos el cumplimiento de los lineamientos establecidos en el modelo de arquitectura empresarial, las normas ISO 27001:2022 / 27002:2022 y demás normatividad nacional como la ley de transparencia, el decreto 1008 de 2018 y lineamientos establecidos por MinTIC.

#### **4.6 Catálogo de servicios de TI**

El catálogo de servicios de TI constituye un instrumento estratégico y operativo que permite describir, organizar y comunicar los servicios tecnológicos que la Oficina TIC presta a usuarios internos y externos, garantizando claridad, estandarización, control y medición del valor entregado.

Su actualización se debe realizar de manera periódica fortaleciendo la gobernanza, soportando los procesos institucionales y permitiendo establecer acuerdos de niveles de servicio (ANS) objetivos y verificables.

El catálogo debe reflejar los servicios de TI necesarios para habilitar la operación institucional en coherencia con:

- PETIC 2024–2028
- El modelo de arquitectura empresarial

- Políticas de TI

La actualización de los servicios debe realizarse aplicando las mejores prácticas de ITIL, mediante el árbol de categorías, clasificación en problemas, incidentes y requerimientos, con su respectivo ANS (Acuerdos de niveles de servicios) y asignando responsables.

Cada vez que se realice la actualización del catálogo de servicios, este debe verse reflejado en la configuración del árbol de categorías vs los ANS, en la herramienta de gestión de mesa de ayuda (GLPI), en la cual queda registrado el seguimiento y cumplimiento de los tiempos de atención, solución y cierre de cada uno de los casos. Este proceso nos permite documentar y registrar lecciones aprendidas, implementando de esta manera al mismo tiempo la gestión del conocimiento.

La implementación del catálogo de servicios, mediante las herramientas de gestión de mesa de ayuda, nos proporciona información mediante dashboard que nos permite tomar decisiones, y tener una mayor visualización de las necesidades de la entidad en materia de tecnologías de la información y las comunicaciones.

Cada servicio del catálogo debe estar estructurado de manera uniforme y bajo estándares de gestión de servicios. Por ello, cada ficha de servicio debe incluir:

#### **Datos generales del servicio**

- Código único (TIC-XXX).
- Versión.
- Fecha de creación/actualización.
- Categoría de servicio.

#### **Detalles técnicos**

- Equipos, plataformas o software involucrados.
- Infraestructura asociada.
- Requerimientos previos.

#### **Responsabilidades**

- Responsable del servicio.
- Áreas involucradas.
- Alcance de soporte que presta la Oficina TIC.

#### **ANS – Acuerdos de niveles de servicio**

- Disponibilidad del servicio.
- Tiempos de respuesta y solución.
- Cierre.

#### **Canales de acceso al servicio**

- Mesa de ayuda (GLPI).
- Teléfono (601 8844 444 ext. 2301).
- Correo institucional (mesadeservicio\_tic@chia.gov.co).
- Intranet o extranet.

En el catálogo de servicios los ANS se deben definir como mínimo para estas tres categorías, las cuales deben integrarse al tablero de control de la herramienta de gestión de mesa de servicios GLPI:

#### **Plazos / Tiempos**

- Tiempo de respuesta.
- Tiempo de solución.
- Tiempo de asignación de caso.

#### **Calidad**

- Satisfacción del usuario.
- Calidad percibida del servicio.
- Cumplimiento de objetivos del proceso.

#### **Disponibilidad**

- Porcentaje de disponibilidad real vs. objetivo (99%).
- Impacto de interrupciones.

El catálogo de servicios debe ser publicado en la intranet de la alcaldía municipal de Chía, de manera que todas las dependencias lo conozcan y apropien, teniendo en cuenta que es dinámico y con la implementación de nuevos proyectos de tecnología de la información y comunicaciones, pueden surgir nuevos servicios.

### **4.7 Evaluación de la gestión de la estrategia de TI**

La evaluación de la gestión de la estrategia de tecnologías de la información, es el proceso mediante el cual la alcaldía municipal de Chía mide, monitorea y determina el grado de cumplimiento, impacto, pertinencia y eficacia de la implementación de la estrategia definida en el PETIC, así como su articulación con el modelo de arquitectura empresarial (MAE) y las políticas de gobierno digital, seguridad digital y seguridad de la información, asegurando de esta manera el ciclo de mejora continua, permitiendo ajustar prioridades, optimizar recursos, fortalecer la toma de decisiones y garantizar que las tecnologías de la información, continúen siendo un habilitador estratégico del desarrollo municipal.

#### **4.7.1 Lineamientos generales de evaluación de la estrategia TI**

La evaluación deberá guiar ajustes periódicos a la estrategia, permitiendo evolucionar el PETIC según brechas, necesidades institucionales y cambios normativos.

La evaluación debe verificar el cumplimiento de los objetivos estratégicos definidos en el dominio estrategia TI:

- Entendimiento estratégico.

- Arquitectura TI.
- Planeación TI.
- Evaluación de tecnologías emergentes.
- Actualización de la estrategia.

La medición de la percepción ciudadana se realiza a través de encuesta de satisfacción, y los datos obtenidos refleja el impacto positivo o negativo realmente causado, las lecciones aprendidas y los puntos a mejorar.

Todos los resultados deberán documentarse en informes, actas y repositorios institucionales, asegurando trazabilidad del proceso.

#### 4.7.2 Lineamientos para la evaluación del cumplimiento estratégico

Para cada proyecto se evaluará:

- Avance y cumplimiento del alcance.
- Contribución al objetivo estratégicos del PETIC.
- Alineación al modelo de arquitectura empresarial.

Se deberá medir el aporte real de la TI al cumplimiento de las metas del PDM, especialmente en:

- Servicios ciudadanos digitales.
- Eficiencia operativa.
- Transparencia.
- Seguridad digital.
- Transformación institucional.

El proceso debe verificar la implementación de lineamientos derivados de:

- Política de gobierno digital.
- Política de seguridad digital.
- Política de seguridad de la información.

#### 4.7.3 Lineamientos para la evaluación de la arquitectura TI

Se deberá evaluar anualmente la alineación de la estrategia TI con los modelos de:

- Procesos.
- Datos.
- Aplicaciones.
- Tecnología.

Verificar el cumplimiento de hitos, actividades, ejercicios piloto y prioridades definidas en la hoja de ruta de AE.

Evaluar si la estrategia evita sistemas duplicados, procesos manuales innecesarios o plataformas aisladas.

Determinar el nivel de interoperabilidad, estandarización y calidad alcanzado.

#### 4.7.4 Lineamientos para la evaluación de la actualización de la estrategia TI

El PETIC deberá actualizarse mínimo cada dos años para:

- Ajustarse a cambios normativos.
- Incorporar nuevas prioridades institucionales.
- Integrar necesidades detectadas en AE y comités TIC.

La evaluación debe analizar si la estrategia sigue siendo financieramente viable.

Cada iniciativa deberá examinar:

- Nivel de avance.
- Obstáculos o riesgos.
- Necesidad de replanteamiento, continuidad o cierre.

La ciudadanía, las dependencias y los equipos técnicos deberán participar con insumos sobre el desempeño de la estrategia TI.

### 4.8 Tablero de indicadores de TI

El tablero de indicadores de TI es una herramienta estratégica para medir el desempeño, la operación, la madurez y la contribución de la tecnología en la entidad. Su función es proporcionar información confiable, oportuna y alineada al PETIC, al modelo de arquitectura empresarial y a las políticas de TI, permitiendo la toma de decisiones basada en evidencia.

#### 4.8.1 Lineamientos generales para la implementación del tablero de indicadores

Los indicadores se deben organizar por dimensiones:

- Infraestructura tecnológica y seguridad.
- Servicios de TI y soporte técnico.
- Sistemas de información y desarrollo de software.
- Gestión de proyectos TI.
- Uso, apropiación y capacitación (MAE 2025).
- Datos, analítica e innovación.

Cada indicador debe tener una ficha técnica que incluya: definición, fórmula, frecuencia, fuente y responsable.

Se debe realizar una revisión anual del tablero de indicadores y actualizarse en caso de que se requiera, con el objetivo de que permitan evidenciar el cumplimiento de la hoja de ruta establecida en el modelo de arquitectura empresarial, la hoja de ruta vs iniciativas del plan estratégico de tecnologías de la información y las comunicaciones y la apropiación de las políticas de gobierno digital, seguridad digital y seguridad de la información.

#### 4.8.2 Lineamientos tablero de indicadores catálogo de servicios TI

El tablero de indicadores se encuentra definido dentro de los acuerdos de niveles de servicio, y se relacionan con los servicios prestados. Estos indicadores deben ser actualizados al menos una vez al año, según necesidad o cambios generados en los procesos TIC.

A continuación, se presenta un resumen de los ANS establecidos para los incidentes y requerimientos, relacionados en el catálogo de servicios TIC.

Tabla No. 1. ANS generales servicios TIC

Servicio	Clasificación	ANS (horas hábiles)
Soporte técnico	Incidentes	Atención: 1 hora Solución: 4 horas Cierre: 30 min
	Requerimientos	Atención: 4 horas Solución: 8 horas Cierre: 1 hora
Cableado estructurado	Incidentes	Atención: 1 hora Solución: 2 horas Cierre: 30 min
	Requerimientos	Atención: 4 horas Solución: 8 horas Cierre: 1 hora
Equipos activos de red	Incidentes	Atención: 1 hora Solución: 2 horas Cierre: 30 min
	Requerimientos	Atención: 4 horas Solución: 8 horas Cierre: 1 hora
Documentación estratégica gobierno digital	Requerimientos	Atención: 4 horas Solución: 18 horas Cierre: 1 hora
Desarrollo aplicaciones	Incidentes	Atención: 1 hora Solución: 2 horas Cierre: 30 min
	Requerimientos	Atención: 4 horas Solución: 8 horas Cierre: 1 hora

Estos indicadores deben estar configurados en la herramienta de gestión de mesa de ayuda GLPI, de manera que permitan generar reportes que evidencien:

- Medición de la eficiencia del soporte (tiempo de atención, solución, satisfacción).
- Registro mantenimientos programados vs. ejecutados.
- Medición de la disponibilidad de servicios TI y cumplimiento de ANS.
- Integración de indicadores por categorías del catálogo de servicios TI.
- Medición de disponibilidad, continuidad y resiliencia del datacenter.

- La realización de seguimiento a:
  - Copias de seguridad
  - Mantenimientos correctivos y preventivos
  - Estado de activos tecnológicos
- Registro de número de desarrollos completados vs. solicitados.
- Medición de la disponibilidad y estabilidad de aplicaciones institucionales.

#### 4.9 Investigación e innovación en TIC

La investigación e innovación en tecnologías de la información y las comunicaciones, es una capacidad estratégica que permite a la alcaldía municipal de Chía incorporar tecnologías emergentes, optimizar procesos institucionales, fortalecer la toma de decisiones y generar valor público, por lo tanto, su implementación debe considerar la realidad cultural de la entidad, actualmente caracterizada por la resistencia al cambio y, lo que nos lleva a que debemos implementar procesos progresivos, acompañados, medibles y orientados a la apropiación digital.

##### 4.9.1 Lineamientos estratégicos para la innovación TIC

La innovación tecnológica, debe priorizar proyectos y tecnologías que fortalezcan:

- Servicios ciudadanos digitales.
- Interoperabilidad.
- Automatización.
- Analítica y sistema estadístico municipal.
- Infraestructura inteligente.
- Transformación digital institucional.

Los esfuerzos deben enfocarse en resolver problemas reales del municipio y de la administración:

- Reducción de tiempos de trámites.
- Atención ciudadana más efectiva.
- Simplificación de procesos internos.
- Reducción de costos operativos.
- Transparencia y trazabilidad.

Las nuevas tecnologías deberán evaluarse en términos de:

- Seguridad digital.
- Privacidad.
- Cumplimiento normativo.
- Sostenibilidad presupuestal.
- Gobernanza del dato.

- Riesgos operativos.
- Ciclo de vida de soluciones.

#### 4.9.2 Lineamientos culturales y de gestión del cambio

Considerando la resistencia al cambio, en el modelo de gestión de gobierno TI (MGGTI), se definen los siguientes lineamientos obligatorios:

- Implementar tecnologías emergentes en ciclos iterativos y controlados, evitando cambios disruptivos sin preparación institucional.
- Antes de escalar soluciones, ejecutar pilotos con grupos reducidos.
- Evaluar impacto, riesgos y aceptación del usuario.
- Documentar lecciones aprendidas.
- Cada iniciativa debe incluir:
  - Sensibilización.
  - Capacitación.
  - Acompañamiento.
  - Material pedagógico.
- Involucrar áreas misionales en el diseño de soluciones.
- Aplicar metodologías de co-creación y diseño centrado en el usuario.
- Asegurar que la innovación responda a necesidades reales.
- Realizar campañas de comunicación interna.
- Reconocer buenas prácticas de uso de tecnología.
- Incentivar la adopción de herramientas institucionales.

#### 4.9.3 Lineamientos para la investigación tecnológica

La Oficina TIC debe monitorear tendencias sobre:

- Inteligencia artificial y automatización.
- Analítica de datos y Big Data.
- IoT y sensores urbanos.
- Ciberseguridad avanzada.
- Servicios en la nube.
- Arquitecturas modernas (APIs, microservicios).
- Plataformas de participación ciudadana.

Se debe consolidar documentación sobre tecnologías emergentes, registrar evaluaciones técnicas, pilotos y recomendaciones e integrar hallazgos al repositorio AE.

Cada tecnología debe analizarse teniendo en cuenta lo siguiente:

- Valor público.
- Riesgo.
- Contribución al PETIC y AE.
- Sostenibilidad técnica y presupuestal.

- Impacto en talento humano.
- Capacidades existentes.

#### 4.10 Diseño impulsado con el usuario

El diseño impulsado con el usuario, garantiza que las soluciones tecnológicas, los servicios digitales, los sistemas de información y los procesos automatizados se construyan con base en necesidades reales, capacidades culturales de la organización, comportamiento de los usuarios, expectativas de calidad, la experiencia ciudadana y del funcionario.

##### 4.10.1 Lineamientos estratégicos del diseño impulsado con el usuario

Toda iniciativa tecnológica debe partir del entendimiento de:

- Perfiles de usuario (funcionario, ciudadano, dependencia misional).
- Necesidades reales y problemas concretos.
- Capacidades digitales actuales.
- Flujos de experiencia antes, durante y después del servicio.

Las decisiones de diseño deben orientarse a:

- Mejorar la experiencia del ciudadano.
- Reducir tiempos de atención.
- Facilitar el trabajo del funcionario.
- Incrementar eficiencia, trazabilidad y transparencia.

El diseño impulsado con el usuario debe apoyar:

- Los objetivos establecidos en el PETIC.
- La hoja de ruta priorizada en el modelo de arquitectura empresarial.

##### 4.10.2 Lineamientos metodológicos del diseño impulsado con el usuario

Mediante el presente modelo de gestión y gobierno TI, se establece que toda iniciativa debe seguir cinco fases mínimas de diseño centrado en el usuario:

Comprender

- Realizar entrevistas, encuestas o talleres con funcionarios y/o ciudadanos.
- Mapear barreras de adopción y fricciones culturales.
- Identificar limitaciones tecnológicas, habilidades digitales y procesos actuales.

Definir el problema

- Formular claramente el problema institucional desde la perspectiva del usuario, no desde la tecnología.
- Priorizar necesidades con criterios del PETIC (impacto, valor público, urgencia, viabilidad).
- Definir grupos de usuarios: básicos, intermedios, avanzados.

#### Idear

- Realizar talleres de co-creación con las dependencias de la alcaldía de Chía.
- Proponer alternativas viables considerando la resistencia al cambio.
- Incorporar funcionalidades mínimas necesarias.

#### Prototipar

- Crear prototipos de baja y media fidelidad para validar conceptos.
- Incluir diagramas de flujos y formularios.

#### Probar y medir

- Ejecutar pruebas con usuarios reales, preferiblemente aquellos con baja alfabetización digital.
- Documentar mejoras, ajustes, resistencia percibida y barreras culturales.
- Ajustar antes de la implementación definitiva.

#### 4.10.3 Lineamientos del diseño impulsado con el usuario, en los sistemas de información

Los sistemas deben cumplir criterios de diseño universal para:

- Claridad.
- Coherencia visual.
- Contraste.
- Accesibilidad para personas con discapacidad.
- Legibilidad en dispositivos móviles.

El modelo de arquitectura empresarial, define que los sistemas deben:

- Integrarse según los modelos de proceso y datos.
- Evitar duplicidad de tareas para el usuario.
- Reducir carga operativa.

Antes de entregar un sistema a producción se deben realizar:

- Pruebas de accesibilidad.
- Pruebas con funcionarios poco familiarizados con TI.

Se deben elaborar manuales y materiales pedagógicos centrado en el usuario

- Guías paso a paso.
- Videos cortos pedagógicos.
- Infografías.

#### 4.11 Instrumentos de planeación institucional con componentes de TIC

Como entidad pública debemos adoptar la metodología de MGA, del DNP, la cual ha sido actualizada y se está alineando a la metodología PMP, incluyendo en su última versión procesos ágiles, permitiendo la flexibilidad de acuerdo al proyecto a implementar.

Los proyectos son formulados en MGA Web y viabilizados, para posteriormente realizar el seguimiento a través del PIIP, plataforma del DNP. Este seguimiento se realiza en base al cumplimiento de la triada (tiempo, costo, calidad), establecidos durante la fase de formulación y planeación de los programas y proyectos, según lo estipulado en MGA Web.

Teniendo en cuenta que los proyectos son únicos, la información registrada en MGA Web va desde el inicio hasta el cierre del proyecto, esta plataforma no permite cambios. Sin embargo, en la realización del seguimiento en la PIIP, se registran las variaciones que puedan llegar a presentarse dentro del proyecto y las acciones realizadas para la alineación dentro de los parámetros establecidos sin afectar el alcance.

Otro instrumento utilizado en el seguimiento de los proyectos es la herramienta interna de la alcaldía llamada Sitesigo en la cual se registran los avances de acuerdo a los recursos adquiridos por presupuesto de inversión, la cual se sincroniza con Seygob, herramienta mediante la cual se lleva la gestión financiera de los programas y proyectos que hacen parte del plan de desarrollo municipal.

Los instrumentos de planeación institucional que incorporan componentes de Tecnologías de la Información constituyen la columna vertebral que articula las decisiones estratégicas con la ejecución operativa.

Con la contextualización anterior podemos apreciar como todos estos instrumentos garantizan, en la alcaldía de Chía, cohesión, trazabilidad, priorización, sostenibilidad y alineación entre:

- El plan de desarrollo municipal (PDM).
- El plan estratégico de tecnologías de la información y las comunicaciones.
- El modelo de arquitectura empresarial.
- El modelo de gestión y gobierno TI.
- Las políticas de gobierno digital, seguridad digital y seguridad de la información

##### 4.11.1 Lineamientos generales para la planeación institucional con componentes de TIC

Cada iniciativa, proyecto o inversión en TI deberá demostrar coherencia explícita con:

- El plan de desarrollo municipal.
- El plan estratégico de tecnologías de la información y las comunicaciones (PETIC 2024–2028).
- La hoja de ruta del modelo de arquitectura empresarial.
- Los lineamientos del modelo de gestión y gobierno TI.
- Las políticas institucionales de TIC.

Siguiendo los lineamientos establecidos en el modelo de arquitectura empresarial y teniendo en cuenta los instrumentos de planeación institucional, los componentes TIC deben implementarse de forma progresiva e incremental, como parte de la estrategia institucional, lo cual implica que:

- Se deben incorporar mejoras graduales.
- Las dependencias deben ser acompañadas según su nivel de madurez.
- Planeación fundamentada en el diagnóstico institucional

La planificación de la implementación de los componentes TIC, debe partir del:

- Levantamiento de información de procesos.
- Inventario de sistemas de información.
- Infraestructura existente.
- Brechas identificadas modelo de arquitectura empresarial.
- Requerimientos sectoriales.
- Coherencia con las capacidades institucionales.

Se debe garantizar la alineación con las capacidades institucionales definidas en el modelo de arquitectura empresarial, que integra capacidades estratégicas, operativas y tecnológicas.

#### 4.11.2 Lineamientos para la articulación del PDM con el PETIC y el MAE

El PDM define el “qué”; el PETI define el “cómo tecnológico”, por ello todo proyecto TI debe evidenciar la habilitación de metas del PDM como:

- Gobernabilidad y confianza
- Modernización institucional
- Servicios al ciudadano

El PETIC debe reflejar la hoja de ruta del modelo de arquitectura empresarial, de manera que la planeación de TIC asegure:

- Evitar duplicidades.
- Reducir silos organizacionales.
- Aumentar la interoperabilidad.
- Integrar sistemas y datos.

#### 4.11.3 Lineamientos para la planeación técnica de proyectos TIC

Se debe apropiarse el ciclo de vida de la gestión de proyectos TIC, cumpliendo las siguientes fases:

- Inicio.
- Planeación.
- Ejecución.

- Seguimiento y control.
- Cierre.
- Transferencia a la operación.

Todo proyecto debe tener un responsable designado, quien debe coordinar la estructuración técnica, cronogramas, entregables, requisitos y procedimientos.

La planeación debe incluir los siguientes componentes obligatorios:

- WBS / EDT.
- Cronogramas.
- Hitos.
- Presupuesto.
- Condiciones técnicas.
- Requerimientos funcionales y no funcionales.
- Análisis de brechas identificadas.

#### 4.11.4 Lineamientos para la articulación con las capacidades institucionales

Se deben fortalecer capacidades estratégicas en:

- Planeación articulada.
- Toma de decisiones basada en datos.
- Gobierno digital y abierto.
- Gestión del cambio.

Se deben fortalecer capacidades operativas en:

- Procesos optimizados.
- Gestión por servicios y trámites.
- Enlaces TIC.

Se deben fortalecer capacidades tecnológicas en:

- Infraestructura moderna.
- Sistemas de información articulados.
- Seguridad digital.
- Interoperabilidad y datos.

## 5 Gobierno TI

El gobierno de tecnologías de la información, constituye un componente estratégico y transversal del modelo de gestión y gobierno TI de la alcaldía municipal de Chía, orientado a asegurar que las decisiones, inversiones, procesos y servicios tecnológicos se encuentren alineados con los objetivos institucionales, el plan de desarrollo municipal, el plan estratégico de tecnologías de la información y las comunicaciones y el modelo de arquitectura empresarial.

En el contexto de la administración pública municipal, el gobierno TI no se limita a la gestión operativa de la tecnología, sino que establece el marco de dirección, control y toma de decisiones que permite que las TI generen valor público, fortalezcan la transparencia, mitiguen riesgos, optimicen recursos y habiliten la transformación digital de la entidad de manera ordenada y sostenible.

Para la alcaldía de Chía, el gobierno TI se concibe como el mecanismo mediante el cual se articulan la estrategia institucional, los procesos misionales, la gestión de la información, los sistemas de información, la infraestructura tecnológica, la seguridad digital y la gestión del cambio, garantizando coherencia entre la planeación, la ejecución y la evaluación de las iniciativas tecnológicas.

Mediante el gobierno TI, se establecen los principios, estructuras, instancias de decisión, roles, responsabilidades y lineamientos que permiten formalizar la gobernanza de TI en la entidad, en concordancia con los lineamientos del modelo de gobierno y gestión de TI (MGGTI) del MinTIC, el modelo integrado de planeación y gestión (MIPG) y la normativa nacional vigente en materia de gobierno digital, seguridad digital y seguridad de la información.

El gobierno TI en la alcaldía municipal de Chía reconoce además las particularidades del contexto institucional, caracterizado por una cultura organizacional con resistencia al cambio, por lo cual se priorizan esquemas de gobernanza claros, participativos y progresivos, que faciliten la apropiación de las decisiones tecnológicas por parte de la alta dirección, las dependencias misionales y la Oficina TIC, fortaleciendo la corresponsabilidad institucional en el uso de las tecnologías.

A través del esquema de gobierno TI, se establecen instancias formales para la toma de decisiones estratégicas, técnicas y de seguridad de la información; se definen mecanismos de priorización y seguimiento de iniciativas TIC; se promueve la alineación entre proyectos, servicios y arquitectura empresarial; y se garantiza la gestión adecuada de riesgos, proveedores y recursos tecnológicos, asegurando la sostenibilidad y continuidad de los servicios digitales de la entidad.

### 5.1 Esquema de gobierno de TI

El esquema de gobierno de TI de la alcaldía municipal de Chía, define la estructura organizacional, las instancias de decisión, los roles y los mecanismos de articulación necesarios para dirigir, controlar y supervisar la gestión de las tecnologías de la información, asegurando su alineación con la estrategia institucional, el plan de desarrollo

municipal, el plan estratégico de tecnologías de la información y las comunicaciones y el modelo de arquitectura empresarial (MAE).

Este esquema establece un marco claro de responsabilidad compartida, en el cual la alta dirección, las dependencias misionales y la Oficina TIC participan de manera coordinada en la toma de decisiones relacionadas con la planeación, priorización, ejecución, seguimiento y evaluación de las iniciativas tecnológicas, garantizando que las TICs generen valor público, mitigue riesgos y contribuya a la transformación digital del municipio.

#### 5.1.1 Propósito del esquema de gobierno de TI

- Asegurar que las decisiones en materia de TIC estén alineadas con los objetivos estratégicos institucionales.
- Establecer instancias formales para la toma de decisiones estratégicas, tácticas y operativas en TI.
- Garantizar la adecuada gestión de riesgos tecnológicos, de seguridad digital y de información.
- Promover la transparencia, la trazabilidad y el control sobre las inversiones y servicios de TI.
- Facilitar la articulación entre la estrategia, la arquitectura empresarial, los proyectos, los servicios y el presupuesto de TI.

#### 5.1.2 Principios del esquema de gobierno de TI

- Alineación estratégica: la TI debe soportar directamente el cumplimiento del PDM y el PETIC.
- Valor público: las decisiones tecnológicas deben generar beneficios tangibles para la ciudadanía y la administración.
- Responsabilidad y corresponsabilidad: la gestión de TI es un compromiso institucional, no exclusivo de la Oficina TIC.
- Transparencia y control: todas las decisiones deben ser documentadas y trazables.
- Gestión del riesgo: la seguridad digital y la continuidad de los servicios son prioritarias.
- Mejora continua: el esquema debe evaluarse y ajustarse periódicamente.

#### 5.1.3 Niveles del gobierno de TI

El esquema de gobierno de TI se estructura en tres niveles complementarios:

##### 5.1.3.1 Nivel estratégico

Responsable de definir lineamientos, políticas y decisiones de alto nivel relacionadas con la TI.

- Define prioridades estratégicas de TI.
- Aprueba el PETIC, la hoja de ruta AE y las políticas TI.
- Supervisa el cumplimiento de objetivos estratégicos y el uso eficiente de los recursos.

#### 5.1.3.2 Nivel táctico

Encargado de traducir la estrategia en planes, proyectos y lineamientos técnicos.

- Prioriza y valida el portafolio de proyectos TI.
- Garantiza la alineación de los proyectos con la AE y el MGGTI.
- Realiza seguimiento a indicadores, presupuesto y riesgos.

#### 5.1.3.3 Nivel operativo

Responsable de la ejecución, operación y soporte de la tecnología.

- Implementa proyectos y servicios de TI.
- Administra infraestructura, sistemas y datos.
- Presta soporte a usuarios y asegura continuidad operativa.

#### 5.1.4 Instancias del esquema de gobierno de TI

El esquema de gobierno de TI se soporta en las siguientes instancias:

##### 5.1.4.1 Comité institucional de gestión y desempeño

- Instancia estratégica que aprueba lineamientos generales de TI.
- Articula la gestión de TI con el MIPG y la planeación institucional.

##### 5.1.4.2 Equipo de gobierno digital / gobierno TI

- Realiza diagnóstico, analiza y elabora las políticas TIC.
- Analiza situación actual y formula el PETIC y el portafolio de proyectos TIC.
- En conjunto con el jefe de la Oficina TIC prioriza la hoja de ruta de proyectos TIC y formula lineamientos de transformación digital.

##### 5.1.4.3 Comité técnico de arquitectura empresarial

- Garantiza la alineación entre procesos, datos, aplicaciones y tecnología.
- Valida iniciativas TIC desde la perspectiva de la AE.
- Identifica brechas y define hojas de ruta técnicas.

##### 5.1.4.4 Comité de seguridad de la información

- Define lineamientos de seguridad y gestión del riesgo digital.
- Supervisa el cumplimiento de las políticas de seguridad.
- Atiende y gestiona incidentes de seguridad.

## 5.1.5 Roles y responsabilidades claves

### 5.1.5.1 Alta dirección

- Orienta la estrategia institucional de TIC.
- Aprueba decisiones estratégicas y presupuestales.

### 5.1.5.2 Oficina TIC

- Lidera la gestión integral de TIC.
- Actúa como secretaría técnica de los comités TIC.
- Formula el PETIC, gestiona proyectos, servicios y arquitectura TI.
- Administra el catálogo de servicios, indicadores y presupuesto TI.

### 5.1.5.3 Dependencias misionales

- Identifican necesidades tecnológicas.
- Participan en la definición y validación de proyectos y servicios TI.
- Son corresponsables de la adopción y uso de las soluciones.

### 5.1.5.4 Control interno

- Verifica el cumplimiento normativo y procedimental.
- Apoya la evaluación del gobierno TI.

## 5.1.6 Mecanismos de articulación del esquema

El esquema de gobierno TI se articula mediante:

- El PETIC como instrumento rector de la estrategia TI.
- El MAE como marco técnico de alineación y evolución tecnológica.
- El MGPTI para la gestión de proyectos con componentes de TI.
- El catálogo de servicios TI para la operación y prestación de servicios.
- El tablero de indicadores TI para el seguimiento y evaluación.
- Las políticas de TI para el control normativo y de seguridad.

## 5.1.7 Evaluación y mejora del esquema de gobierno de TI

El esquema de gobierno TI será evaluado de manera anual con el fin de:

- Medir su efectividad y nivel de madurez.
- Identificar oportunidades de mejora.

- Ajustar roles, instancias y procesos según cambios organizacionales, tecnológicos o normativos.

## 5.2 Gestión de las no conformidades

La gestión de las no conformidades en el marco del gobierno de TI de la alcaldía municipal de Chía tiene como propósito identificar, analizar, tratar y cerrar de manera oportuna aquellas desviaciones, incumplimientos o fallas que afecten el cumplimiento de los objetivos estratégicos de TI, los lineamientos del PETIC, las políticas institucionales, la normatividad vigente y los estándares definidos en el MGGTI.

### 5.2.1 Objetivo

Constituir la gestión de las no conformidades, como un mecanismo de control y mejora continua, orientado no solo a la corrección de fallas, sino a la prevención de su recurrencia, fortaleciendo la gobernanza, la transparencia, la calidad de los servicios de TI y la generación de valor público.

### 5.2.2 Alcance de la gestión de no conformidades en TI

La gestión de no conformidades aplica a:

- Procesos del gobierno TI.
- Proyectos con componentes de TIC.
- Servicios de TIC incluidos en el catálogo de servicios.
- Sistemas de información y su operación.
- Gestión de la información y los datos.
- Seguridad digital y seguridad de la información.
- Cumplimiento del PETIC, MAE, políticas TI y lineamientos normativos.

### 5.2.3 Definición de no conformidad en el MGGTI

Se considera no conformidad toda situación en la cual:

- No se cumple un requisito normativo, estratégico, técnico o procedimental.
- Existe desviación frente a lo establecido en el PETIC, el dominio de gobierno TI, las políticas TI o el MGGTI.
- Se presentan fallas recurrentes en servicios o sistemas de TIC.
- No se cumplen metas o compromisos aprobados.
- Se identifican riesgos no gestionados o materializados.
- Se incumplen acuerdos de nivel de servicio (ANS/SLA).

#### 5.2.4 Principios para la gestión de no conformidades

- **Transparencia:** todas las no conformidades deben ser registradas y documentadas en GLPI.
- **Responsabilidad:** cada no conformidad debe contar con un responsable definido.
- **Oportunidad:** las acciones deben ejecutarse dentro de plazos establecidos.
- **Enfoque preventivo:** se prioriza la eliminación de causas raíz.
- **Mejora continua:** las lecciones aprendidas fortalecen el MGGTI.
- **Corresponsabilidad institucional:** no es exclusiva de la Oficina TIC.

#### 5.2.5 Fuentes de identificación de no conformidades

Las no conformidades pueden identificarse a partir de:

- Auditorías internas y externas.
- Reportes de comités al equipo de gobierno TI.
- Incidentes de seguridad digital o de información.
- Fallas en proyectos o servicios TI.
- Quejas, reclamos o solicitudes de usuarios.
- Respuestas a encuestas de satisfacción.
- Evaluaciones de control interno.

#### 5.2.6 Proceso de gestión de las no conformidades

La alcaldía de Chía establece el siguiente ciclo para la gestión de no conformidades en TIC:

##### 5.2.6.1 *Identificación y registro*

- Toda no conformidad debe registrarse formalmente.
- El registro debe incluir: descripción, origen, impacto, proceso afectado y evidencia.
- El registro se consolida a través de la herramienta de gestión de la mesa de ayuda GLPI.

##### 5.2.6.2 *Clasificación y priorización*

Las no conformidades se clasifican según:

- Nivel de impacto (alto, medio, bajo).
- Riesgo institucional y tecnológico.
- Afectación a servicios ciudadanos y/o institucionales.

- Incumplimiento normativo o estratégico.

#### 5.2.6.3 *Análisis de causa raíz*

- Se debe identificar la causa real del incumplimiento.
- Se evalúan causas organizacionales, técnicas, procedimentales o culturales.
- Este análisis es obligatorio antes de definir acciones.

#### 5.2.6.4 *Definición del plan de acción*

El plan de acción debe incluir:

- Acciones correctivas.
- Acciones preventivas.
- Responsable(s).
- Cronograma.
- Recursos necesarios.
- Indicadores de seguimiento.

#### 5.2.6.5 *Implementación de acciones*

- Las acciones deben ejecutarse conforme a lo aprobado.
- Se debe documentar la evidencia de ejecución.

#### 5.2.6.6 *Seguimiento y verificación*

- El avance se revisa en instancias de gobierno TI y/o responsable de dar solución a la no conformidad.
- Se valida la efectividad de las acciones implementadas.

#### 5.2.6.7 *Cierre de la no conformidad*

- Solo se cierra cuando se verifica la solución y no recurrencia.
- El cierre debe quedar documentado y aprobado.

#### 5.2.7 Roles y responsabilidades

- Oficina TIC:
  - Lidera el proceso de gestión de no conformidades TI.
  - Consolida registros, planes de acción y seguimiento.
- Dependencias responsables:
  - Implementan las acciones definidas.
  - Participan en el análisis de causa raíz.
- Equipo de gobierno TI:
  - Revisa no conformidades críticas.

- Toma decisiones estratégicas y correctivas.
- Control Interno:
  - Verifica el cumplimiento del proceso.
  - Evalúa la efectividad de las acciones.

#### 5.2.8 Articulación con el PETIC y el dominio de gobierno TI

La gestión de no conformidades es un insumo clave para:

- Ajustes al PETIC.
- Actualización del MAE y hojas de ruta.
- Revisión de políticas y lineamientos TI.
- Fortalecimiento del esquema de gobierno TI.
- Mejora del desempeño de servicios y proyectos.

#### 5.2.9 Indicadores de gestión de no conformidades

Se deben medir, como mínimo:

- Número de no conformidades identificadas.
- Tiempo promedio de cierre.
- Porcentaje de no conformidades recurrentes.
- Cumplimiento de planes de acción.

### 5.3 Macroproceso de gestión de TI

El macroproceso de gestión de tecnologías de la información de la alcaldía municipal de Chía constituye el conjunto articulado de procesos estratégicos, tácticos y operativos mediante los cuales la entidad planifica, gobierna, ejecuta, controla y mejora el uso de las tecnologías de la información como habilitadoras del cumplimiento de su misión institucional y de la generación de valor público.

Este macroproceso se integra al mapa de procesos institucional, específicamente dentro de los procesos estratégicos, y actúa de manera transversal sobre los procesos misionales, de apoyo y de evaluación, garantizando que las soluciones tecnológicas respondan de forma coherente a las necesidades de la administración y de la ciudadanía.

Desde el enfoque del gobierno TI, el macroproceso de gestión de TI permite establecer un marco estructurado de dirección, control y mejora continua, alineado con el plan estratégico de tecnologías de la información y las comunicaciones (PETIC), el modelo de arquitectura empresarial (MAE), las políticas institucionales de TI y los lineamientos del dominio de gobierno TI, asegurando la trazabilidad entre la planeación estratégica, la ejecución operativa y la evaluación del desempeño tecnológico.

### 5.3.1 Objetivo del macroproceso de gestión de TI

Establecer lineamientos para la planificación, dirección, implementación, operación, control y mejora continua de las tecnologías de la información, en la alcaldía municipal de Chía, garantizando su alineación con la estrategia institucional, la optimización de recursos, la gestión adecuada de riesgos, la calidad de los servicios tecnológicos y el fortalecimiento de la transformación digital del municipio.

### 5.3.2 Estructura del macroproceso de gestión de TI

El macroproceso de gestión de TI se estructura en subprocesos integrados, alineados con el dominio de gobierno TI y con los instrumentos institucionales de planeación, control y evaluación.

#### 5.3.2.1 Planeación y dirección estratégica de TI

Este subproceso orienta el direccionamiento estratégico de la TI y articula las decisiones tecnológicas con la planeación institucional.

Incluye:

- Formulación, actualización y seguimiento del PETIC.
- Articulación de la TI con el plan de desarrollo municipal.
- Alineación con el modelo de arquitectura empresarial.
- Priorización de iniciativas y proyectos TI.
- Definición de políticas, lineamientos y estándares tecnológicos.

#### 5.3.2.2 Control de TI

Este subproceso establece los mecanismos de gobernanza, control y toma de decisiones sobre la gestión de TI.

Incluye:

- Operación del esquema de gobierno TI.
- Funcionamiento de comités y roles de decisión.
- Gestión de riesgos tecnológicos y de seguridad digital.
- Gestión de no conformidades.
- Seguimiento al cumplimiento normativo y de políticas TI.

#### 5.3.2.3 Gestión de proyectos con componentes de TI

Este subproceso garantiza que las iniciativas tecnológicas se formulen, ejecuten y controlen bajo metodologías estandarizadas.

Incluye:

- Aplicación del MGPTI.
- Planeación, ejecución, seguimiento y cierre de proyectos TI.
- Alineación de proyectos con la AE y el PETI.
- Gestión del cambio y apropiación tecnológica.
- Transferencia de proyectos a la operación.

#### 5.3.2.4 *Gestión de servicios de TI*

Este subproceso asegura la prestación eficiente y controlada de los servicios tecnológicos institucionales.

Incluye:

- Administración del catálogo de servicios TI.
- Definición y seguimiento de acuerdos de niveles de servicio (ANS).
- Operación de la mesa de ayuda.
- Gestión de incidentes, problemas y requerimientos.
- Mejora continua de la calidad del servicio.

#### 5.3.2.5 *Gestión de infraestructura, sistemas y seguridad*

Este subproceso garantiza la disponibilidad, continuidad y protección de los activos tecnológicos y de información.

Incluye:

- Administración de infraestructura tecnológica.
- Gestión de sistemas de información.
- Seguridad digital y seguridad de la información.
- Respaldo, continuidad y recuperación ante desastres.
- Gestión de activos tecnológicos.

#### 5.3.2.6 *Gestión de la información*

Este subproceso permite administrar la información como un activo estratégico institucional.

Incluye:

- Calidad, integridad y disponibilidad de la información.
- Interoperabilidad de sistemas.
- Analítica y soporte a la toma de decisiones.
- Articulación con el sistema estadístico municipal.

#### 5.3.2.7 *Seguimiento, evaluación y mejora continua de la gestión de TI*

Este subproceso cierra el ciclo del macroproceso, asegurando la mejora permanente.

Incluye:

- Evaluación del cumplimiento del PETIC y la AE.
- Identificación de brechas y planes de mejora.
- Retroalimentación a la planeación estratégica.

### 5.3.3 Articulación del macroproceso de gestión de TI con el mapa de procesos institucional

El macroproceso de gestión de TI:

- Se ubica como proceso estratégico dentro del mapa institucional.
- Soporta transversalmente los procesos misionales, de apoyo y de evaluación.
- Facilita la sistematización, interoperabilidad y modernización de los procesos institucionales.
- Permite identificar oportunidades de transformación digital por proceso.

## 5.4 Gestión de cambios

La gestión de cambios en el marco del modelo de gestión y gobierno TI de la alcaldía municipal de Chía es el proceso mediante el cual se garantiza que toda modificación tecnológica u organizacional relacionada con las TI sea identificada, evaluada, aprobada, implementada, documentada y controlada de manera formal, con el fin de minimizar riesgos, asegurar la continuidad de los servicios y preservar la integridad de la información institucional.

Este proceso aplica a los cambios que impacten infraestructura tecnológica, sistemas de información, aplicaciones, servicios TI, configuraciones, seguridad, datos y componentes asociados, y se fundamenta en las buenas prácticas de COBIT e ITIL, en coherencia con el plan estratégico de tecnologías de la información (PETIC), el modelo de arquitectura empresarial (MAE), la política de gobierno digital y las políticas de seguridad de la información y seguridad digital.

La gestión de cambios es un mecanismo clave de control del gobierno TI, permitiendo a la entidad avanzar en procesos de modernización, innovación y transformación digital de forma progresiva, controlada y trazable, particularmente relevante en un contexto institucional con resistencia al cambio, donde la planificación y la comunicación son factores críticos de éxito.

### 5.4.1 Objetivo de la gestión de cambios en el MGGTI

Garantizar que todos los cambios tecnológicos y de procesos TIC sean gestionados de forma estructurada, transparente y segura, reduciendo el impacto operativo, previniendo incidentes, asegurando la continuidad de los servicios institucionales y fortaleciendo la mejora continua de la gestión de TI.

#### 5.4.2 Alcance de la gestión de cambios

La gestión de cambios aplica a:

- Infraestructura tecnológica (servidores, redes, almacenamiento, seguridad).
- Sistemas de información y aplicaciones (desarrollos propios o de terceros).
- Servicios TI incluidos en el catálogo de servicios.
- Cambios en configuraciones, parches, versiones y licenciamiento.
- Cambios asociados a proveedores tecnológicos.
- Ajustes derivados de cambios normativos o de políticas internas.

No se incluyen actividades operativas rutinarias sin impacto significativo, salvo que alteren la configuración, seguridad o funcionalidad de los servicios

#### 5.4.3 Lineamientos de adherencia a la gestión de cambios

##### 5.4.3.1 Adherencia obligatoria a la metodología de gestión del cambio TIC

- Todo cambio debe gestionarse conforme a la metodología de gestión del cambio TIC adoptada por la alcaldía municipal de Chía.
- No se permitirá la implementación de cambios sin su registro, evaluación y aprobación previa, salvo los cambios de emergencia debidamente documentados.

##### 5.4.3.2 Uso obligatorio del formato de control de cambios TIC

- Para todo cambio se debe diligenciar el formato de control de cambios de desarrollos tecnológicos, validado por el área de calidad y disponible en Kawak.
- En el formato se debe diligenciar como mínimo:
  - Descripción del cambio.
  - Justificación.
  - Riesgos asociados.
  - Plan de tratamiento del riesgo.
  - Plan de implementación.
  - Plan de pruebas.
  - Plan de reversión (roll-back).
  - Aprobaciones correspondientes.
  - Lecciones aprendidas.

##### 5.4.3.3 Registro y trazabilidad de los cambios

- Toda solicitud de cambio (RFC) debe registrarse en la mesa de servicios GLPI.
- Cada cambio debe contar con un número de caso, responsable asignado y seguimiento documentado.
- Los cambios deben reflejarse en los activos de configuración (CMDB) cuando aplique.

#### 5.4.3.4 Clasificación de los cambios

Los cambios deben clasificarse según su impacto y riesgo en:

- Cambios normales: requieren análisis, planeación y aprobación formal.
- Cambios estándar: de bajo riesgo y alta recurrencia, previamente autorizados.
- Cambios de emergencia: orientados a restablecer servicios críticos o mitigar vulnerabilidades graves.

Cada tipo de cambio debe cumplir los ANS definidos y las actividades establecidas en la metodología.

#### 5.4.3.5 Aprobación y control del cambio

Ningún cambio podrá ejecutarse sin la aprobación correspondiente del:

- Jefe de la Oficina TIC
- Comité de cambios (CAB), cuando aplique
- Responsables funcionales del servicio afectado
- Las aprobaciones deben quedar documentadas en el formato y en GLPI.

#### 5.4.3.6 Gestión de riesgos y seguridad

- Todo cambio debe incluir análisis de riesgos operativos y de seguridad de la información.
- Los cambios que afecten datos, accesos o infraestructura crítica, deben contar con la validación del rol encargado de la seguridad de la información.
- Se deben definir controles preventivos, pruebas y planes de reversión.

#### 5.4.3.7 Implementación, pruebas y reversión

- Los cambios deben ejecutarse conforme al plan aprobado.
- Se deben realizar pruebas de funcionamiento y validación.
- Debe existir un plan de roll-back documentado para mitigar fallas durante la implementación.

#### 5.4.3.8 Documentación, cierre y lecciones aprendidas

- Todo cambio debe cerrarse formalmente una vez verificada su correcta implementación.
- Las lecciones aprendidas deben registrarse en GLPI y en el formato de control de cambios.
- La información recolectada alimentará los procesos de mejora continua del MGGTI.

#### 5.4.3.9 Articulación con el gobierno TI y el MAE

La gestión de cambios se articula con:

- El esquema de gobierno TI, como mecanismo de control y decisión.
- El MAE, garantizando que los cambios contribuyan al cierre de brechas arquitectónicas.

- El PETIC, como insumo para ajustes estratégicos y priorización futura.

Tabla No. 2 Matriz de relación: Gestión de cambios, gobierno TI, MAE y proyectos TI

Elemento de gestión del cambio	Relación con gobierno TI	Relación con MAE	Relación con proyectos TI (MGPTI)	Responsable Principal	Evidencia / Instrumento
Identificación del cambio	Permite control y trazabilidad de decisiones TI	Identifica dominios impactados (procesos, datos, aplicaciones, tecnología)	Se registra como ajuste al proyecto	Oficina TIC / Dependencia solicitante	Solicitud de cambio (RFC) – GLPI
Clasificación del cambio (normal, estándar, emergencia)	Apoya la toma de decisiones según impacto y riesgo	Define nivel de afectación arquitectónica	Determina ajustes al cronograma del proyecto	Oficina TIC	Metodología de gestión del cambio
Análisis de impacto y riesgo TIC	Fortalece la gestión del riesgo	Evalúa impacto en arquitectura actual y objetivo	Analiza riesgos del proyecto y continuidad	Oficina TIC / Seguridad de la información	Formato control de cambios
Aprobación del cambio	Se ejecuta en instancias del comité de gestión de cambios (CAB)	Valida coherencia con la hoja de ruta AE	Autoriza la actualización sin afectar el alcance del proyecto	Comité de gestión del cambio / Jefe TIC	Formato control de cambios aprobado
Planeación del cambio	Garantiza control y orden institucional	Define alineación con arquitectura objetivo	Define cronograma y entregables	Líder de proyecto TIC	Plan de implementación del cambio
Implementación del cambio	Asegura ejecución conforme a decisiones de gobierno	Materializa ajustes arquitectónicos	Ejecuta actividades del proyecto	Oficina TIC / Proveedor	Registro de implementación
Pruebas y validación	Controla calidad y continuidad del servicio	Verifica consistencia entre dominios AE	Valida entregables del proyecto	Oficina TIC / Usuarios clave	Evidencias de pruebas
Plan de reversión (roll-back)	Mitiga riesgos y garantiza continuidad	Protege arquitectura y servicios críticos	Reduce impacto ante fallas del proyecto	Oficina TIC	Plan de reversión documentado
Comunicación del	Facilita la	Apoya	Gestiona	Oficina TIC /	Comunicaciones

Elemento de gestión del cambio	Relación con gobierno TI	Relación con MAE	Relación con proyectos TI (MGPTI)	Responsable Principal	Evidencia / Instrumento
cambio	adopción y gestión del cambio organizacional	apropiación de la AE	expectativas de interesados	Líder del proyecto	internas
Cierre del cambio	Formaliza control y cumplimiento	Actualiza documentación arquitectónica	Cierra actividades del proyecto	Oficina TIC	Cierre en GLPI / Formato diligenciado
Lecciones aprendidas	Alimenta la mejora continua del gobierno TI	Ajusta lineamientos y arquitectura futura	Mejora ejecución de proyectos futuros	Oficina TIC	Registro de lecciones aprendidas

## 5.5 Capacidades y recursos de TI

Las capacidades y recursos de TI constituyen el conjunto de habilidades organizacionales, conocimientos, procesos, tecnologías y recursos humanos, técnicos y financieros que permiten a la alcaldía municipal de Chía, planificar, gobernar, operar y mejorar el uso de las tecnologías de la información como habilitadoras estratégicas del cumplimiento de sus objetivos institucionales.

En el marco del modelo de gestión y gobierno TI, las capacidades de TI se conciben como un activo institucional estratégico, cuyo fortalecimiento progresivo es fundamental para garantizar la alineación entre la estrategia, los procesos, la información, los sistemas de información y la infraestructura tecnológica, de acuerdo con los lineamientos del plan estratégico de tecnologías de la información y las comunicaciones (PETIC) y el modelo de arquitectura empresarial (MAE).

### 5.5.1 Objetivo de las capacidades y recursos de TI

Establecer lineamientos que permitan identificar las capacidades actuales y proyectadas de TI en la alcaldía municipal de Chía, fortalecer aquellas existentes y desarrollar nuevas capacidades, garantizando su alineación con los objetivos estratégicos institucionales, a través de la arquitectura empresarial, como instrumento articulador entre procesos, talento humano, tecnología e inversión pública.

### 5.5.2 Enfoque de capacidades de TI

El enfoque de capacidades adoptado por la alcaldía municipal de Chía se fundamenta en los siguientes principios:

- Alineación estratégica: las capacidades de TI deben soportar directamente el plan de desarrollo municipal, el plan estratégico de tecnologías de la información y las comunicaciones y el modelo de arquitectura empresarial.
- Enfoque progresivo: el desarrollo de capacidades se realizará por fases, considerando la madurez institucional y la resistencia al cambio.
- Articulación institucional: las capacidades no son exclusivas de la Oficina TIC; requieren corresponsabilidad de todas las dependencias.
- Valor público: el fortalecimiento de capacidades debe traducirse en mejores servicios, mayor eficiencia y transparencia.
- Sostenibilidad: el desarrollo de capacidades debe ser viable técnica, financiera y operativamente.

### 5.5.3 Estructura de capacidades institucionales

De acuerdo con el modelo de arquitectura empresarial, las capacidades institucionales se estructuran en tres niveles complementarios:

#### 5.5.3.1 Capacidades estratégicas

Orientadas a la dirección y toma de decisiones institucionales

- Planificación institucional articulada.
- Toma de decisiones basada en datos.
- Gestión del cambio y apropiación de TI.

#### 5.5.3.2 Capacidades operativas

Enfocadas en la ejecución eficiente de procesos y servicios:

- Gestión por procesos.
- Gestión de servicios y trámites.
- Talento humano y liderazgo.
- Articulación entre dependencias.

#### 5.5.3.3 Capacidades tecnológicas y de información

Relacionadas con la provisión y sostenibilidad de soluciones tecnológicas:

- Infraestructura tecnológica sostenible.
- Gestión integrada de la información.
- Sistemas de información estratégicos.
- Ciberseguridad y continuidad del negocio.

### 5.5.4 Capacidades de TI por dominio

La gestión de TI en la alcaldía municipal de Chía, contempla capacidades específicas por dominio, las cuales deben fortalecerse o desarrollarse según el diagnóstico institucional:

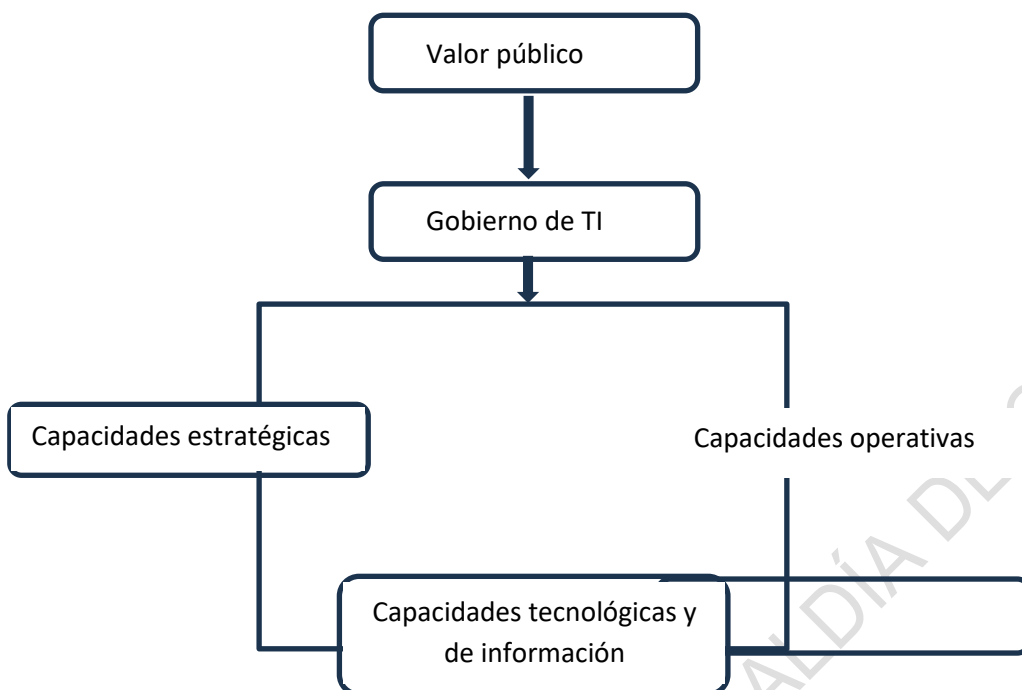


Ilustración No. 2. Estructura capacidades por dominios (Elaboración propia)

#### 5.5.4.1 Estrategia:

- Gestionar la arquitectura empresarial.
- Gestionar proyectos de TI.
- Definir políticas de TI.

#### 5.5.4.2 Gobierno:

- Gestionar procesos de TI.
- Realizar capacitaciones.

#### 5.5.4.3 Información:

- Administrar modelos de datos.
- Gestionar flujos de información.

#### 5.5.4.4 Sistemas de Información:

- Definir la arquitectura de sistemas.
- Administrar sistemas de información.
- Interoperar plataformas.

#### 5.5.4.5 Infraestructura:

- Gestionar disponibilidad.
- Soporte a usuarios.
- Gestión de cambios.

- Administración de infraestructura tecnológica.

#### 5.5.4.6 *Uso y Apropiación:*

- Apropiar el uso de las TI en la gestión institucional.

#### 5.5.4.7 *Seguridad:*

- Gestionar la seguridad de la información.

### 5.5.5 Niveles de madurez y metas de desarrollo

El diagnóstico de capacidades evidencia niveles actuales entre 1 y 2, con una meta institucional de alcanzar nivel 4 al año 2027, especialmente en capacidades críticas como:

- Toma de decisiones basada en datos.
- Gestión integrada de la información.
- Sistemas de información estratégicos.
- Seguridad tecnológica y desarrollo de software seguro.

### 5.5.6 Requerimientos de la gestión de TI

- Recursos humanos
  - Equipos técnicos especializados.
  - Enlaces TIC en dependencias misionales.
  - Capacitación continua en gobierno TI, AE, datos, seguridad y transformación digital.
- Recursos tecnológicos
  - Infraestructura de hardware y software.
  - Plataformas de información y analítica.
  - Herramientas de gestión de servicios, proyectos y cambios.
  - Soluciones de seguridad y continuidad.
- Recursos financieros
  - Presupuesto asignado a TI.
  - Inversión en proyectos estratégicos.
  - Sostenibilidad financiera de servicios y plataformas.

### 5.5.7 Enfoque de desarrollo progresivo de capacidades

El fortalecimiento de capacidades se realizará por fases:

- Levantamiento y versión inicial (2024–2025): talento humano y procesos.
- Fase piloto (2025–2026): servicios digitales, analítica e interoperabilidad.
- Fase de expansión (2027): automatización y gobierno del dato.

- Sostenibilidad (2027-2028): evaluación de impacto y mejora continua.

## 5.6 Capacidades y optimización de recursos de TI

Las capacidades y la optimización de los recursos de tecnologías de la información, constituyen un pilar fundamental del modelo de gestión de gobierno TI de la alcaldía municipal de Chía, en la medida en que permiten asegurar que la estrategia tecnológica se ejecute de manera eficiente, sostenible y alineada con los objetivos institucionales, garantizando la generación de valor público y el uso responsable de los recursos del estado, e integra dos componentes importantes:

- Las capacidades institucionales de TI, entendidas como el conjunto de habilidades organizacionales, conocimientos, procesos y competencias necesarias para gestionar la tecnología.
- La optimización de los recursos de TI, orientada a maximizar el aprovechamiento de los recursos humanos, tecnológicos y financieros disponibles, evitando duplicidades, ineficiencias y riesgos.

En el contexto de la alcaldía municipal de Chía, caracterizado por restricciones presupuestales, diversidad de necesidades misionales y resistencia organizacional al cambio, la consolidación progresiva de capacidades y la optimización de recursos se convierten en elementos estratégicos para garantizar la sostenibilidad del gobierno TI y la transformación digital institucional.

### 5.6.1 Objetivo de las capacidades y la optimización de recursos de TI

Fortalecer y desarrollar de manera progresiva las capacidades institucionales de TI de la alcaldía municipal de Chía, optimizando el uso de los recursos humanos, tecnológicos y financieros, con el fin de asegurar una gestión eficiente, alineada con el PETIC y el modelo de arquitectura empresarial (MAE) de la alcaldía municipal de Chía.

### 5.6.2 Enfoque institucional

La gestión de capacidades y la optimización de recursos de TI se fundamenta en los siguientes enfoques:

- Alineación estratégica: las capacidades y recursos deben soportar directamente el plan de desarrollo municipal, el plan estratégico de tecnologías de la información y las comunicaciones (PETIC) y la hoja de ruta del modelo de arquitectura empresarial (MAE).
- Eficiencia y racionalización: priorizar el uso compartido, la estandarización y la reutilización de recursos tecnológicos.
- Progresividad: fortalecer capacidades por fases, considerando la madurez institucional y la gestión del cambio.

- Corresponsabilidad: la optimización de recursos es una responsabilidad compartida entre la Oficina TIC y las dependencias usuarias.
- Sostenibilidad: asegurar la viabilidad técnica, operativa y financiera de las soluciones TI en el tiempo.

### 5.6.3 Capacidades institucionales de TI

Las capacidades de TI de la alcaldía municipal de Chía, se estructuran en coherencia con el modelo de arquitectura empresarial, y se agrupan en los siguientes niveles:

#### 5.6.3.1 Capacidades estratégicas

Permiten direccionar y gobernar el uso de la TI:

- Gobierno de TI.
- Planeación estratégica de TI.
- Arquitectura empresarial.
- Gestión del cambio organizacional.
- Toma de decisiones basada en datos.

#### 5.6.3.2 Capacidades operativas

Permiten ejecutar y controlar la gestión de TI:

- Gestión de proyectos de TI.
- Gestión de servicios de TI.
- Gestión de cambios.
- Gestión de proveedores tecnológicos.
- Uso y apropiación de TI.
- Diseño impulsado con el usuario.
- Gestión de no conformidades.

#### 5.6.3.3 Capacidades tecnológicas y de información

Soportan la operación y la transformación digital:

- Infraestructura tecnológica.
- Sistemas de información.
- Gestión de la información y los datos.
- Seguridad digital y de la información.
- Innovación y transformación digital.

### 5.6.4 Optimización de los recursos de TI

La optimización de recursos de TI se orienta a maximizar el valor de los recursos disponibles y se desarrolla sobre tres dimensiones principales:

#### 5.6.4.1 Optimización de los recursos humanos

Lineamientos clave:

- Fortalecer las competencias del personal TIC y de los enlaces TIC de las dependencias.
- Evitar la duplicidad de funciones mediante roles claros y responsabilidades definidas.
- Promover la capacitación continua en gobierno TI, AE, seguridad, datos y transformación digital.
- Fomentar la transferencia de conocimiento entre equipos y proveedores.

#### 5.6.4.2 Optimización de los recursos tecnológicos

Lineamientos clave:

- Estandarizar plataformas, herramientas y tecnologías.
- Reutilizar infraestructuras y servicios tecnológicos existentes.
- Consolidar inventarios y activos tecnológicos.
- Priorizar soluciones interoperables y escalables.
- Evitar sistemas duplicados o aislados.

#### 5.6.4.3 Optimización de los recursos financieros

Lineamientos clave:

- Priorizar inversiones TI alineadas con el PETIC y el MAE.
- Sustentar decisiones de inversión con análisis de costo/beneficio.
- Garantizar sostenibilidad financiera de los servicios TI.
- Optimizar la contratación tecnológica y el uso del presupuesto TI.

#### 5.6.5 Articulación entre capacidades y optimización de recursos

La optimización de recursos solo es posible cuando existen capacidades institucionales adecuadas. Por ello:

- El fortalecimiento de capacidades habilita una mejor planeación y uso de recursos.
- La arquitectura empresarial permite identificar redundancias y oportunidades de optimización.
- El gobierno TI prioriza y controla el uso de los recursos.
- El seguimiento mediante indicadores asegura la mejora continua.

#### 5.6.6 Seguimiento y mejora continua

El fortalecimiento de capacidades y la optimización de recursos de TI deben evaluarse de manera periódica a través de:

- Indicadores de eficiencia en el uso de recursos tecnológicos.
- Encuestas de capacitaciones TIC.
- Resultados del tablero de indicadores de TI.

## 5.7 Evaluación del desempeño de la gestión de TIC

La evaluación del desempeño de la gestión de tecnologías de la información y las comunicaciones (TIC), realizada a través del FURAG, es un componente esencial, orientado a medir de manera sistemática, objetiva y periódica el grado de cumplimiento, efectividad, eficiencia y madurez de la gestión tecnológica institucional, permitiendo verificar que las TICs, estén cumpliendo su rol como habilitador estratégico del plan de desarrollo municipal, asegurando la alineación con el plan estratégico de tecnologías de la información y las comunicaciones (PETIC), el modelo de arquitectura empresarial (MAE) y las políticas institucionales de gobierno digital, seguridad digital y seguridad de la información. Asimismo, constituye un mecanismo clave de control, transparencia y mejora continua, que soporta la toma de decisiones de la alta dirección.

### 5.7.1 Objetivo de la evaluación del desempeño de la gestión de TIC

Proponer un método adicional al FURAG, para evaluar de forma integral el desempeño de la gestión de TI en la alcaldía municipal de Chía, a través de indicadores, mecanismos de monitoreo y evaluaciones de madurez, con el fin de identificar logros, brechas, riesgos y oportunidades de mejora que permitan fortalecer el gobierno TI y asegurar la generación de valor público.

### 5.7.2 Alcance de la evaluación

La evaluación del desempeño de la gestión de TIC aplica a:

- La ejecución y cumplimiento del PETIC.
- La gestión de proyectos con componentes de TIC.
- La prestación de servicios TIC y el cumplimiento de ANS.
- La infraestructura tecnológica, su disponibilidad y continuidad.
- La gestión de la información, los datos y la interoperabilidad.
- La seguridad digital y la seguridad de la información.
- El desarrollo de capacidades y la optimización de recursos TIC.

### 5.7.3 Enfoque de la evaluación del desempeño

La evaluación del desempeño de la gestión de TIC se fundamenta en los siguientes enfoques:

- Orientada a resultados: evalúa el impacto de la TIC en los procesos y servicios institucionales.
- Progresiva: reconoce la madurez actual de la entidad y promueve la mejora continua.
- Articulada: se integra con los sistemas de planeación, control interno y MIPG.

#### 5.7.4 Componentes de la evaluación del desempeño de TIC

##### 5.7.4.1 Evaluación estratégica

Permite medir el grado de alineación entre la gestión de TIC y la estrategia institucional.

Incluye:

- Cumplimiento de objetivos y líneas estratégicas del PETIC.
- Aporte de las TICs a las metas del plan de desarrollo municipal.
- Avance de la hoja de ruta del MAE.

##### 5.7.4.2 Evaluación operativa

Mide la eficiencia y efectividad de la operación tecnológica.

Incluye:

- Desempeño de los servicios TI (disponibilidad, tiempos de atención, satisfacción).
- Cumplimiento de acuerdos de nivel de servicio (ANS).
- Gestión de incidentes, problemas y cambios.
- Ejecución de proyectos TIC frente a alcance, tiempo y costo.

##### 5.7.4.3 Evaluación técnica y de infraestructura

Se orienta a garantizar la continuidad, disponibilidad y seguridad de los activos tecnológicos.

Incluye:

- Monitoreo de infraestructura y servicios.
- Dashboards de disponibilidad y rendimiento.
- Registro y análisis de logs y trazabilidad transaccional.
- Evaluación de estrategias de alta disponibilidad, respaldo y recuperación ante desastres.

##### 5.7.4.4 Evaluación de capacidades y recursos de TIC

Permite medir:

- Nivel de madurez de las capacidades institucionales de TIC.
- Eficiencia en el uso de recursos humanos, tecnológicos y financieros.
- Resultados del plan de capacitaciones TIC.

- Grado de adopción y apropiación de las soluciones tecnológicas.

#### 5.7.4.5 Evaluación de seguridad digital y de la información

Incluye:

- Cumplimiento de políticas y controles de seguridad.
- Gestión de incidentes de seguridad.
- Resultados de auditorías y pruebas de seguridad.
- Nivel de riesgo tecnológico residual.

#### 5.7.5 Instrumentos para la evaluación del desempeño

La alcaldía municipal de Chía utilizará los siguientes instrumentos para la evaluación de la gestión de TIC:

- Matriz de madurez institucional en arquitectura empresarial (MinTIC).
- Reportes de monitoreo de infraestructura y servicios.
- Informes de auditoría interna y externa.
- Evaluaciones de satisfacción de usuarios y ciudadanos.
- Planes de mejora derivados de evaluaciones previas

#### 5.7.6 Periodicidad de la evaluación

La evaluación del desempeño de la gestión de TIC se realizará con la siguiente periodicidad:

- Mensual: evaluación operativa, cumplimiento de ANS establecidos.
- Cuatrimestral: evaluación de proyectos, servicios y capacidades.
- Anual: evaluación integral de la gestión de TI, mediante la matriz de madurez institucional de la AE y definición de planes de mejora.

#### 5.7.7 Uso de los resultados de la evaluación

Los resultados de la evaluación del desempeño de la gestión de TIC serán utilizados para:

- Tomar decisiones estratégicas y correctivas en los comités de la Oficina TIC.
- Ajustar el PETIC, el MAE y la hoja de ruta de transformación digital.
- Priorizar inversiones y proyectos TI.
- Fortalecer capacidades y optimizar recursos.
- Gestionar riesgos tecnológicos y operativos.

## 5.8 Mejoramiento de los procesos

El mejoramiento de los procesos en el marco del modelo de gestión de gobierno TI de la alcaldía municipal de Chía es el conjunto de lineamientos, prácticas y mecanismos orientados a optimizar, modernizar y transformar los procesos institucionales mediante el uso estratégico de las tecnologías de la información, garantizando mayor eficiencia, calidad del servicio, transparencia y generación de valor público.

### 5.8.1 Objetivo del mejoramiento de los procesos

Establecer lineamientos que permitan mejorar de manera continua los procesos de la Oficina TIC, de la alcaldía municipal de Chía, mediante su alineación con los servicios y las soluciones tecnológicas, asegurando coherencia entre qué hace, cómo lo hace, con qué tecnología y para quién lo hace, de acuerdo con los principios del gobierno TI y la arquitectura empresarial.

### 5.8.2 Principios del mejoramiento de los procesos

- Enfoque en el ciudadano y el usuario interno: los procesos deben diseñarse y mejorarse desde la experiencia del usuario.
- Alineación estratégica: los procesos deben contribuir al cumplimiento de los objetivos institucionales.
- Simplificación y eficiencia: eliminar actividades innecesarias, reprocesos y duplicidades.
- Uso racional de la tecnología: priorizar soluciones tecnológicas que generen valor real.
- Interoperabilidad: favorecer la integración entre sistemas y dependencias.
- Mejora continua: los procesos deben evaluarse y ajustarse periódicamente.
- Gestión del cambio: reconocer la resistencia organizacional y acompañar la adopción de mejoras.

### 5.8.3 Enfoque de mejoramiento de procesos desde la arquitectura empresarial

La arquitectura empresarial es el instrumento que permite alinear los procesos institucionales con los servicios TIC y la tecnología disponible.

En este sentido:

- Los procesos se analizan desde su estado actual (AS-IS).
- Se define un estado objetivo (TO-BE) apoyado en servicios digitales.
- Se identifican brechas, redundancias y oportunidades de automatización.
- Se priorizan mejoras según impacto institucional y valor público.

#### 5.8.4 Lineamientos para la identificación de procesos a mejorar

##### 5.8.4.1 *Priorización basada en impacto*

Se priorizarán procesos que:

- Tengan alto impacto en la ciudadanía.
- Sean críticos para la operación institucional.
- Presenten altos tiempos de respuesta o reprocesos.
- Estén asociados a trámites, servicios o contratos.

##### 5.8.4.2 *Análisis de procesos misionales, estratégicos y de apoyo*

El mejoramiento no se limita a procesos TIC; aplica a todos los procesos institucionales que puedan ser habilitados o fortalecidos con tecnología.

##### 5.8.4.3 *Uso de insumos de evaluación*

Se deben considerar:

- Resultados de auditorías.
- Quejas y reclamos de ciudadanos.
- Evaluaciones del desempeño de la gestión de TIC.

#### 5.8.5 Lineamientos para la articulación de procesos, servicios TIC y tecnología

- Cada proceso debe tener servicios TIC asociados.
- Todo proceso priorizado debe identificar claramente:
  - El servicio TIC que lo soporta.
  - La tecnología utilizada.
  - Las necesidades tecnológicas no cubiertas.
  - Evitar soluciones aisladas
- No se deben implementar herramientas tecnológicas que no estén integradas al ecosistema institucional.
- Interoperabilidad como criterio obligatorio: Las mejoras deben propender por la integración entre sistemas (PQRS, trámites, pagos, gestión documental).

#### 5.8.6 Lineamientos para el mejoramiento de procesos con apoyo de TIC

- Automatización progresiva:
  - Digitalización.
  - Automatización.
  - Interoperabilidad.
  - Analítica.

- Diseño impulsado con el usuario: Los procesos mejorados deben diseñarse considerando la experiencia del ciudadano y del funcionario.
- Gestión de cambios obligatoria: Toda mejora tecnológica de un proceso debe pasar por el proceso formal de gestión de cambios.
- Gestión de proyectos TIC: Las mejoras de alto impacto deben gestionarse como proyectos TIC bajo el MGPTI.

Tabla No. 3. Matriz de mejoramiento de procesos

Proceso Institucional	Tipo de Proceso	Servicio TIC Asociado	Tecnología / Solución	Tipo de Mejora	Mejora Esperada	Indicador de Seguimiento	Responsable
Gestión de PQRS	Misional	Sistema de PQRS	Aplicación web integrada	Automatización / Integración	Reducción de tiempos de respuesta y trazabilidad completa del caso	% PQRS atendidas en tiempo	Dependencia misional / TIC
Trámites al ciudadano	Misional	Ventanilla única virtual	Plataforma de trámites	Digitalización	Disminución de atención presencial y mayor accesibilidad	% trámites digitales	TIC / Atención al ciudadano
Gestión documental	Apoyo	Sistema de gestión documental	Plataforma documental	Integración / Estandarización	Eliminación de reprocesos y pérdida de información	% documentos digitalizados	Servicios administrativos / Gestión documental
Gestión financiera	Apoyo	Sistema financiero	Seygob	Integración	Mayor control presupuestal y trazabilidad	% ejecución presupuestal	Hacienda
Gestión de talento humano	Apoyo	Sistema de RRHH	Plataforma de RRHH	Digitalización	Agilidad en procesos de nómina y talento humano	Tiempo promedio de trámite	Talento Humano
Planeación institucional	Estratégico	Herramienta de planeación	Sitesigo	Analítica / Integración	Mejor seguimiento a planes	% metas cumplidas	Planeación

Proceso Institucional	Tipo de Proceso	Servicio TIC Asociado	Tecnología / Solución	Tipo de Mejora	Mejora Esperada	Indicador de Seguimiento	Responsable
					y metas		
Gestión de servicios TIC	Apoyo	Mesa de servicios	GLPI	Automatización	Mejor atención y control de incidentes	Tiempo promedio de atención	Oficina TIC
Seguridad de la información	Estratégico	Servicio de seguridad TI	Herramientas de seguridad	Control / Prevención	Reducción de incidentes de seguridad	# incidentes reportados	Seguridad de la Información / Oficina TIC
Gestión de infraestructura TI	Apoyo	Servicio de infraestructura	Plataformas de monitoreo	Optimización	Mayor disponibilidad y continuidad del servicio	% disponibilidad	Oficina TIC
Atención al ciudadano	Misional	Canales digitales	Web, apps, chat	Mejora de experiencia	Mayor satisfacción del ciudadano	Índice de satisfacción	Dependencias
Control interno	Estratégico	Sistema de seguimiento	Plataforma de control	Integración	Mejor control y seguimiento institucional	% planes de mejora cerrados	Control Interno

### 5.8.7 Lineamientos para la implementación y seguimiento

#### 5.8.7.1 Documentación del proceso mejorado:

- Diagramas actualizados.
- Procedimientos revisados.
- Manuales y guías de uso.
- 

#### 5.8.7.2 Capacitación y apropiación:

- Capacitación a funcionarios.
- Acompañamiento inicial.
- Material pedagógico.

#### 5.8.7.3 Seguimiento mediante indicadores:

- Reducción de tiempos.
- Mejora en calidad del servicio.

- Nivel de adopción del proceso.
- Satisfacción del usuario.

#### 5.8.7.4 *Evaluación periódica del proceso:*

- Los procesos mejorados deben revisarse al menos una vez al año.

## 5.9 Gestión de proveedores de TIC

La gestión de proveedores de tecnologías de la información y las comunicaciones, en la alcaldía municipal de Chía es un proceso clave del modelo de gestión de gobierno TI, orientado a garantizar que los bienes y servicios tecnológicos adquiridos o contratados con terceros aporten valor institucional, se encuentren alineados con la estrategia, cumplan con los niveles de servicio esperados y se administren de manera transparente, eficiente y controlada.

### 5.9.1 Objetivo de la gestión de proveedores de TI

Establecer lineamientos institucionales para planear, seleccionar, administrar, supervisar y evaluar a los proveedores de TIC, asegurando que su gestión contribuya al cumplimiento de los objetivos estratégicos de la alcaldía municipal de Chía, fortalezca el gobierno TI y garantice la calidad, continuidad y seguridad de los servicios tecnológicos.

### 5.9.2 Alcance

La gestión de proveedores de TIC aplica a:

- Proveedores de bienes y servicios tecnológicos.
- Contratos de desarrollo, soporte, mantenimiento, licenciamiento y consultoría TI.
- Proveedores de infraestructura, plataformas, software y servicios en la nube.
- Contratistas que participen en proyectos con componentes de TIC.

### 5.9.3 Principios de la gestión de proveedores de TIC

- Alineación estratégica: los proveedores deben contribuir al cumplimiento del modelo de arquitectura empresarial (MAE), el plan estratégico de tecnologías de la información y las comunicaciones (PETIC) y del plan de desarrollo municipal.
- Transparencia y legalidad: la contratación debe cumplir la normatividad vigente y los principios de la función pública.
- Valor público: la contratación TI debe generar beneficios claros para la entidad y la ciudadanía.

- Gestión del riesgo: se deben identificar y mitigar riesgos técnicos, operativos, financieros y de seguridad.
- Responsabilidad compartida: los proveedores deben asumir compromisos claros frente a resultados y niveles de servicio.
- Sostenibilidad: las soluciones contratadas deben ser viables en el tiempo y evitar dependencias tecnológicas innecesarias.

#### 5.9.4 Lineamientos para la planeación de la contratación de TI

- La contratación de proveedores de TI debe derivarse de la planeación estratégica, en coherencia con el PETIC y el MAE.
- No se deben adelantar procesos contractuales sin justificación técnica y alineación estratégica.
- Se debe priorizar la reutilización de servicios y plataformas existentes antes de contratar nuevas soluciones.
- La Oficina TIC debe participar obligatoriamente en la definición de requerimientos técnicos.

#### 5.9.5 Lineamientos para la selección de proveedores de TI

Los criterios de selección deben incluir, además del precio:

- Capacidad técnica y experiencia comprobada.
- Cumplimiento de estándares y buenas prácticas.
- Capacidad de soporte y transferencia de conocimiento.
- Cumplimiento de requisitos de seguridad de la información.
- Se debe evitar la dependencia de proveedores únicos cuando sea posible.
- Las soluciones propuestas deben ser interoperables y alineadas con la arquitectura institucional.

#### 5.9.6 Lineamientos para la gestión y supervisión contractual

- Todo contrato de TIC debe contar con un supervisor técnico, preferiblemente de la Oficina TIC.
- Se deben definir y monitorear acuerdos de niveles de servicio (ANS).
- Los entregables deben validarse técnica y funcionalmente antes de su aceptación.
- La supervisión debe documentarse y generar evidencias de cumplimiento.

#### 5.9.7 Lineamientos para la gestión de riesgos y seguridad

Los proveedores deben cumplir las políticas institucionales de:

- Seguridad de la información.
- Seguridad digital.
- Gobierno digital.

Se deben incluir cláusulas contractuales relacionadas con:

- Protección de datos.
- Confidencialidad.
- Continuidad del servicio.
- Gestión de incidentes de seguridad.

#### 5.9.8 Lineamientos para la evaluación del desempeño de los proveedores

Los proveedores de TI deben evaluarse periódicamente con base en:

- Cumplimiento de ANS.
- Calidad de los entregables.
- Cumplimiento de cronogramas.
- Nivel de soporte y atención.
- Gestión de incidentes y cambios.

Los resultados de la evaluación deben:

- Utilizarse como insumo para decisiones futuras de contratación.
- Alimentar planes de mejora o acciones correctivas cuando aplique.

#### 5.9.9 Seguimiento y mejora continua

La Oficina TIC deberá:

- Mantener un registro actualizado de proveedores TIC.
- Realizar seguimiento periódico al desempeño contractual.
- Identificar oportunidades de mejora en la gestión de proveedores.
- Proponer ajustes a los lineamientos según resultados y cambios estratégicos.

## 6 Gestión de información

La gestión de la información constituye un componente estratégico del modelo de gestión de gobierno TI de la alcaldía municipal de Chía, en la medida en que reconoce a la información como un activo institucional fundamental para la toma de decisiones, la formulación de políticas públicas, la prestación eficiente de servicios y el fortalecimiento de la transparencia y la confianza ciudadana.

En el contexto de la transformación digital y en concordancia con los lineamientos de la política de gobierno digital, la gestión de la información busca asegurar que los datos generados, capturados, procesados y utilizados por la entidad sean confiables, oportunos, accesibles, seguros e interoperables, permitiendo su aprovechamiento tanto para la gestión interna como para la atención al ciudadano y el cumplimiento de obligaciones con entes de control.

El diagnóstico institucional evidenció que la información en la alcaldía municipal de Chía se encuentra actualmente dispersa en múltiples fuentes, plataformas y formatos, con bajos niveles de estandarización, integración y gobierno del dato, lo que limita su uso estratégico y afecta la eficiencia operativa. Esta situación hace necesario establecer un marco claro de gestión que permita evolucionar desde un uso operativo de la información hacia un modelo de gestión basada en datos, alineado con el plan estratégico de tecnologías de la información y las comunicaciones (PETIC) y el modelo de arquitectura empresarial (MAE).

Mediante la gestión de la información, se definen los lineamientos para organizar, integrar, gobernar y optimizar el ciclo de vida de la información institucional, desde su generación y registro hasta su análisis, intercambio y uso para la toma de decisiones. Asimismo, se promueve la adopción de una arquitectura de información institucional, soportada en procesos de integración, analítica y visualización de datos, que facilite la interoperabilidad interna y externa, incluyendo la articulación con la carpeta ciudadana, de manera que se consolide la información como un habilitador clave del gobierno TI, permitiendo decisiones más informadas, procesos más eficientes, servicios más oportunos y una mayor generación de valor público para la ciudadanía.

### 6.1 Gobierno de la información

El gobierno de la información es el conjunto de principios, roles, estructuras, reglas y mecanismos mediante los cuales la alcaldía municipal de Chía dirige, controla y asegura el uso adecuado de la información institucional, reconociéndola como un activo estratégico esencial para la toma de decisiones, la prestación de servicios, el cumplimiento normativo y la generación de valor público.

En el marco del modelo de gestión y gobierno TI, el gobierno de la información permite pasar de una gestión fragmentada y operativa de los datos a un modelo integrado, controlado y orientado a resultados, alineado con el modelo de arquitectura empresarial (MAE), el plan estratégico de tecnologías de la información y las comunicaciones (PETIC) y las políticas institucionales de gobierno digital, seguridad de la información y seguridad digital.

### 6.1.1 Objetivo del gobierno de la información

Establecer lineamientos institucionales para dirigir, coordinar y controlar la gestión de la información en la alcaldía municipal de Chía, garantizando su calidad, integridad, disponibilidad, seguridad, interoperabilidad y uso estratégico, en coherencia con los objetivos institucionales y el gobierno TI.

### 6.1.2 Alcance

El gobierno de la información aplica a:

- Toda la información producida, recibida, administrada o utilizada por la alcaldía municipal de Chía.
- Datos estructurados y no estructurados.
- Información contenida en sistemas de información, bases de datos, documentos, repositorios y plataformas tecnológicas.
- Información compartida con otras entidades del estado y con la ciudadanía.

### 6.1.3 Principios del gobierno de la información

- Información como activo institucional: la información tiene valor y debe gestionarse como tal.
- Calidad de la información: los datos deben ser completos, confiables, consistentes y oportunos.
- Disponibilidad y accesibilidad: la información debe estar disponible para quienes la requieren, según su rol.
- Seguridad y confidencialidad: la información debe protegerse conforme a su nivel de sensibilidad.
- Interoperabilidad: la información debe poder integrarse y compartirse entre sistemas y entidades.
- Transparencia y trazabilidad: el uso de la información debe ser auditable y verificable.
- Responsabilidad y corresponsabilidad: cada actor es responsable del uso adecuado de la información.

### 6.1.4 Estructura de gobierno de la información

Para garantizar el gobierno de la información, la alcaldía municipal de Chía establece la siguiente estructura:

#### 6.1.4.1 Instancias de gobierno

- Equipo de gobierno TI / Equipo de innovación y desarrollo / Jefe Oficina TIC:

- Define lineamientos estratégicos de gestión de la información.
- Prioriza iniciativas relacionadas con datos e información.
- Oficina TIC:
  - Lidera la implementación del gobierno de la información.
  - Define estándares, modelos y lineamientos técnicos.
- Dependencias misionales y de apoyo:
  - Son responsables de la generación, uso y calidad de la información bajo su competencia.

#### 6.1.4.2 Roles claves

- Responsable de la Información:
  - Define el uso, reglas y niveles de acceso a la información.
- Administrador de la Información:
  - Garantiza calidad, consistencia y actualización de los datos.
- Usuarios de la Información:
  - Utilizan la información conforme a los lineamientos definidos.

#### 6.1.5 Lineamientos para la gestión del ciclo de vida de la información

El gobierno de la información debe garantizar el control del ciclo de vida completo de la información:

- Creación y captura:
  - La información debe generarse bajo estándares definidos.
- Clasificación y catalogación:
  - La información debe clasificarse según su tipo, uso y nivel de sensibilidad.
- Almacenamiento:
  - Debe realizarse en repositorios institucionales autorizados.
- Uso y aprovechamiento:
  - La información debe utilizarse para la gestión, análisis y toma de decisiones.
- Intercambio e interoperabilidad:
  - Se debe facilitar el intercambio controlado de información.
- Conservación y disposición:
  - Debe cumplir con las normas archivísticas y de gestión documental.

#### 6.1.6 Lineamientos de calidad de la información

- Se deben definir reglas de calidad para los datos críticos.
- Se deben identificar y gestionar fuentes oficiales de información.
- Las inconsistencias y duplicidades deben corregirse oportunamente.
- Los indicadores de calidad de datos deben ser monitoreados.

#### 6.1.7 Lineamientos de seguridad y acceso a la información

- La información debe protegerse conforme a las políticas de seguridad vigentes.
- Los accesos deben definirse por roles y funciones.
- Se debe garantizar la trazabilidad del acceso y uso de la información.
- Los incidentes relacionados con información deben gestionarse formalmente.

#### 6.1.8 Lineamientos de interoperabilidad y uso estratégico

- Se debe promover la integración entre sistemas de información.
- Se deben evitar silos de información.
- La información debe aprovecharse para analítica, indicadores y planeación.

#### 6.1.9 Seguimiento y mejora continua

La Oficina TIC debe:

- Evaluar periódicamente el nivel de madurez del gobierno de la información.
- Proponer planes de mejora derivados de evaluaciones y auditorías.
- Ajustar lineamientos conforme a cambios normativos y estratégicos.

### 6.2 Gestión de la calidad de los datos

La gestión de la calidad de los datos es un componente esencial del dominio de gestión de la información y del modelo de gestión de gobierno TI de la alcaldía municipal de Chía, orientado a garantizar que los datos institucionales sean confiables, completos, consistentes, oportunos y útiles para la operación institucional, la toma de decisiones, la formulación de políticas públicas y la prestación de servicios a la ciudadanía.

El diagnóstico institucional evidenció la existencia de datos dispersos, duplicados, con inconsistencias y bajos niveles de estandarización, lo cual limita su aprovechamiento estratégico. En este contexto, la gestión de la calidad de los datos se convierte en un habilitador clave para avanzar hacia un modelo de gestión pública basada en datos, en coherencia con el modelo de arquitectura empresarial (MAE) y el plan estratégico de tecnologías de la información y las comunicaciones.

#### 6.2.1 Objetivo de la gestión de la calidad de los datos

Establecer lineamientos institucionales para asegurar, medir, controlar y mejorar de manera continua la calidad de los datos de la alcaldía municipal de Chía, garantizando que

estos soporten adecuadamente los procesos, los servicios TIC, la toma de decisiones y el cumplimiento normativo.

### 6.2.2 Alcance

La gestión de la calidad de los datos aplica a:

- Datos maestros, de referencia y transaccionales.
- Información contenida en sistemas de información, bases de datos, repositorios documentales y plataformas digitales.
- Datos producidos, capturados, intercambiados o explotados por las dependencias de la alcaldía.
- Datos compartidos con otras entidades del estado y con la ciudadanía.

### 6.2.3 Principios de calidad de los datos

- Responsabilidad: cada conjunto de datos debe tener un responsable claramente definido.
- Datos como activo: los datos deben gestionarse como activos institucionales.
- Calidad por diseño: la calidad debe incorporarse desde la generación del dato, no solo corregirse posteriormente.
- Trazabilidad: los datos deben poder rastrearse desde su origen hasta su uso.
- Mejora continua: la calidad de los datos debe evaluarse y mejorarse de forma permanente.

### 6.2.4 Dimensiones de la calidad de los datos

La alcaldía municipal de Chía gestionará la calidad de los datos considerando, como mínimo, las siguientes dimensiones:

- Exactitud: los datos representan correctamente la realidad.
- Completitud: los datos requeridos están presentes.
- Consistencia: no existen contradicciones entre fuentes o sistemas.
- Oportunidad: los datos están disponibles cuando se requieren.
- Validez: los datos cumplen reglas y formatos definidos.
- Unicidad: no existen duplicidades innecesarias.

### 6.2.5 Lineamientos para la gestión de la calidad de los datos

#### 6.2.5.1 Identificación de datos críticos

- Se deben identificar y priorizar los elementos de datos críticos para la operación y la toma de decisiones.

- La priorización debe basarse en impacto institucional, riesgo y valor público.

#### 6.2.5.2 *Definición de reglas de calidad*

- Cada dato crítico debe contar con reglas claras de calidad (formato, rango, obligatoriedad, consistencia).
- Las reglas deben documentarse y mantenerse actualizadas.
- Las reglas de calidad deben integrarse a los procesos y sistemas de información.

#### 6.2.5.3 *Asignación de roles y responsabilidades*

- Cada dominio de datos debe contar con:
  - Dueño del dato.
  - Administrador o custodio del dato.
- Los responsables deben velar por la calidad, uso adecuado y corrección de los datos bajo su competencia.

#### 6.2.5.4 *Monitoreo y medición de la calidad*

- Se deben definir indicadores de calidad de datos asociados a las dimensiones establecidas.
- Los resultados deben consolidarse en tableros de control institucionales.
- El monitoreo debe realizarse de manera periódica.

#### 6.2.5.5 *Gestión de incidentes de calidad de datos*

- Se deben establecer mecanismos para:
  - Identificar inconsistencias y errores.
  - Registrar incidentes de calidad de datos.
  - Asignar responsables y acciones correctivas.
- Los incidentes recurrentes deben analizarse para corregir causas raíz.

#### 6.2.5.6 *Mejora continua de la calidad de los datos*

- Los resultados del monitoreo deben alimentar planes de mejora.
- Las mejoras pueden incluir:
  - Ajustes a procesos.
  - Cambios en sistemas de información.
  - Capacitación a los usuarios.
- La mejora de la calidad de los datos debe gestionarse como un proceso continuo y no como una actividad puntual.

#### 6.2.6 Seguimiento y control

La Oficina TIC, en conjunto con las dependencias responsables de los datos, deberá:

- Evaluar periódicamente el nivel de madurez de la calidad de los datos.
- Analizar resultados.
- Ajustar lineamientos conforme a resultados, riesgos y cambios normativos.

### 6.3 Gestión de documentos electrónicos

La gestión de documentos electrónicos constituye un componente esencial del dominio de gestión de la información dentro del modelo de gestión y gobierno TI de la alcaldía municipal de Chía, al permitir la administración integral de los documentos y expedientes producidos, recibidos y gestionados en medios digitales a lo largo de su ciclo de vida.

En un entorno institucional orientado a la transformación digital, la correcta gestión de los documentos electrónicos es fundamental para preservar la memoria institucional, garantizar la transparencia administrativa, asegurar la trazabilidad de las actuaciones públicas y facilitar la toma de decisiones basada en información confiable. De acuerdo con los lineamientos del MGGTI, la gestión documental electrónica debe entenderse como un proceso transversal, articulado con los procesos misionales, estratégicos y de apoyo, y no únicamente como una función tecnológica o archivística.

#### 6.3.1 Objetivo de la gestión de documentos electrónicos

Establecer lineamientos institucionales para planear, implementar, operar y mejorar la gestión de documentos y expedientes electrónicos en la alcaldía municipal de Chía, garantizando su autenticidad, integridad, disponibilidad, confidencialidad, conservación y disposición final, en coherencia con el gobierno TI y el gobierno de la Información.

#### 6.3.2 Alcance

La gestión de documentos electrónicos aplica a:

- Documentos generados o recibidos en formato digital.
- Expedientes electrónicos asociados a trámites, procesos y actuaciones administrativas.
- Documentos electrónicos producidos por sistemas de información, plataformas, formularios, correos electrónicos y herramientas colaborativas.
- Documentos digitalizados provenientes de soportes físicos.
- Involucra a todas las dependencias de la alcaldía, con liderazgo de la secretaría general y articulación con las áreas de dirección de servicios administrativos (grupo de gestión documental), jurídica, control interno y la Oficina TIC.

#### 6.3.3 Principios de la gestión de documentos electrónicos

- Documento como activo de información: Los documentos electrónicos hacen parte del patrimonio informacional de la entidad.
- Gestión durante todo el ciclo de vida: Desde la creación hasta la disposición final.
- Autenticidad e integridad: Los documentos deben conservar su valor probatorio.
- Accesibilidad controlada: El acceso debe garantizarse según roles y niveles de autorización.
- Interoperabilidad: Los documentos deben poder integrarse con otros sistemas y entidades.
- Cumplimiento normativo: Alineación con la normativa archivística y de gestión pública.

#### 6.3.4 Lineamientos para la gestión del ciclo de vida del documento electrónico

La alcaldía municipal de Chía deberá gestionar los documentos electrónicos considerando las siguientes etapas:

##### 6.3.4.1 *Creación y captura*

- Los documentos electrónicos deben generarse en formatos estándar y definidos en la entidad.
- La captura de documentos debe realizarse a través de sistemas autorizados.
- Todo documento debe asociarse a un proceso o trámite institucional.

##### 6.3.4.2 *Clasificación y organización*

- Los documentos deben clasificarse conforme a las tablas de retención documental (TRD).
- Se debe garantizar la correcta identificación de expedientes electrónicos.
- La clasificación debe facilitar la búsqueda, recuperación y control.

##### 6.3.4.3 *Almacenamiento y preservación*

- Los documentos electrónicos deben almacenarse en repositorios institucionales seguros.
- Se deben implementar mecanismos de respaldo y recuperación.
- La preservación digital debe garantizar la legibilidad y disponibilidad en el tiempo.

##### 6.3.4.4 *Uso, consulta y acceso*

- El acceso a los documentos debe definirse por perfiles y roles.
- Se debe garantizar la trazabilidad del acceso y uso de los documentos.
- Los documentos deben estar disponibles para apoyar la gestión institucional y la atención al ciudadano.

#### 6.3.4.5 Disposición final

- La eliminación, transferencia o conservación permanente debe realizarse conforme a la normativa archivística.
- Las decisiones de disposición final deben documentarse y ser auditables.

#### 6.3.5 Lineamientos para el uso de tecnologías de gestión documental

- La entidad debe evaluar e implementar herramientas tecnológicas que soporten la gestión integral de documentos electrónicos.
- Las soluciones tecnológicas deben permitir:
  - Gestión de expedientes electrónicos.
  - Automatización de flujos documentales.
  - Gestión de metadatos documentales.
  - Integración con otros sistemas institucionales.
- La selección de herramientas debe estar alineada con el modelo de arquitectura empresarial y el plan estratégico de tecnologías de la información y las comunicaciones (PETIC).

#### 6.3.6 Lineamientos de metadatos documentales

- Todo documento electrónico debe contar con metadatos mínimos que permitan su identificación, gestión y preservación.
- Los metadatos deben ser consistentes con el modelo institucional de información.
- Se debe evitar la duplicidad de metadatos entre sistemas.

#### 6.3.7 Lineamientos de seguridad de los documentos electrónicos

- Los documentos electrónicos deben protegerse conforme a su nivel de clasificación y sensibilidad.
- Se deben aplicar controles de acceso, confidencialidad y trazabilidad.
- Los incidentes relacionados con documentos electrónicos deben gestionarse formalmente.

#### 6.3.8 Seguimiento y mejora continua

La dirección de servicios administrativos a través de su grupo de gestión documental en articulación con la Oficina TIC y en coordinación con las áreas responsables, deberá:

- Evaluar periódicamente el nivel de madurez de la gestión de documentos electrónicos.
- Identificar brechas y oportunidades de mejora.

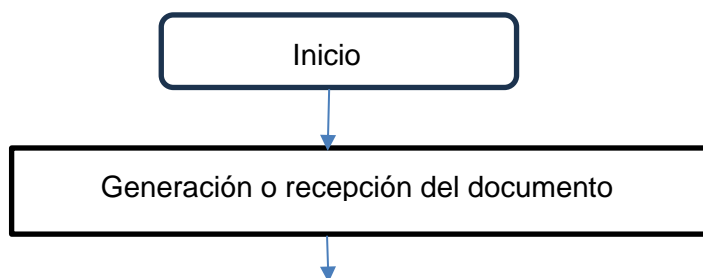
- Proponer acciones de fortalecimiento y optimización.
- Ajustar lineamientos conforme a cambios normativos y estratégicos.

Tabla No. 4 Matriz de gestión de documentos electrónicos

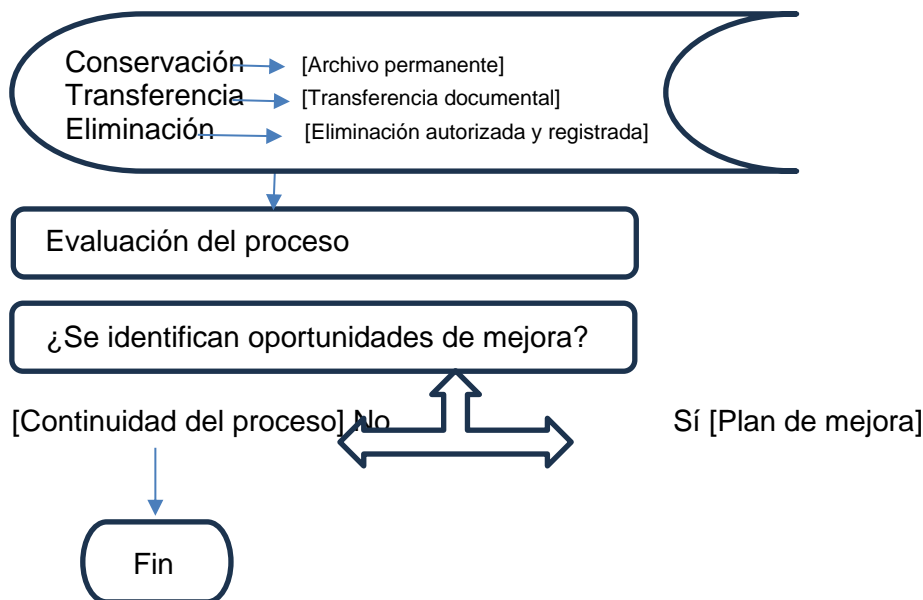
Etapa del ciclo de vida	Actividad	Lineamiento institucional	Herramienta / Soporte TIC	Rol responsable	Producto / Evidencia	Indicador de seguimiento
Creación / Captura	Generación de documento electrónico	Los documentos deben generarse en formatos estándar y sistemas autorizados	Sistemas de información, SGDEA	Dependencia generadora	Documento electrónico registrado	% documentos generados en sistema
Creación / Captura	Digitalización de documentos físicos	La digitalización debe garantizar integridad y legibilidad	Escáner + SGDEA	Gestión documental	Documento digitalizado validado	% documentos digitalizados
Clasificación	Clasificación documental	Clasificación conforme a TRD	SGDEA	Gestión documental	Documento clasificado	% documentos correctamente clasificados
Clasificación	Asociación a expediente electrónico	Todo documento debe asociarse a un expediente	SGDEA	Dependencia / gestión Documental	Expediente electrónico actualizado	% documentos asociados a expediente
Organización	Organización documental	La organización debe facilitar búsqueda y recuperación	SGDEA	Gestión documental	Estructura documental definida	Tiempo promedio de búsqueda
Almacenamiento	Almacenamiento seguro	Los documentos deben almacenarse en repositorios institucionales	Repositorios documentales	Gestión documental / Oficina TIC	Repositorio seguro	% documentos en repositorios oficiales
Preservación	Preservación digital	Garantizar disponibilidad y legibilidad a largo plazo	Copias de seguridad	TIC / Gestión documental	Plan de preservación	% documentos preservados

Etapa del ciclo de vida	Actividad	Lineamiento institucional	Herramienta / Soporte TIC	Rol responsable	Producto / Evidencia	Indicador de seguimiento
Acceso y Uso	Control de accesos	El acceso debe definirse por roles y perfiles	SGDEA / IAM	TIC / Seguridad de la información	Matriz de accesos	% accesos autorizados
Acceso y Uso	Consulta y trazabilidad	El uso del documento debe ser trazable	Logs del sistema	TIC	Registro de accesos	% documentos con trazabilidad
Interoperabilidad	Intercambio documental	Facilitar interoperabilidad entre sistemas	Integraciones / APIs	TIC	Documentos interoperables	# integraciones activas
Seguridad	Protección de la información	Aplicar controles según nivel de sensibilidad	Herramientas de seguridad	Seguridad de la información	Controles aplicados	# incidentes documentales
Disposición Final	Transferencia documental	Cumplir normas archivísticas	SGDEA	Gestión documental	Actas de transferencia	% transferencias realizadas
Disposición Final	Eliminación autorizada	La eliminación debe ser controlada y auditada	SGDEA	Gestión documental	Acta de eliminación	% eliminaciones autorizadas
Seguimiento	Evaluación del proceso	Evaluar desempeño de la gestión documental electrónica	Tablero de indicadores	Gestión documental	Informe de evaluación	Nivel de madurez documental
Mejora Continua	Acciones de mejora	Implementar acciones correctivas y preventivas	Planes de mejora	TIC / Dependencias	Plan de mejora	% acciones ejecutadas

### 6.3.9 Flujo del proceso de gestión documental







#### 6.4 Marco de referencia geoespacial

El marco de referencia geoespacial constituye un componente estratégico del dominio de gestión de la información dentro del modelo de gestión de gobierno TI de la alcaldía municipal de Chía, orientado a organizar, estandarizar, integrar y gobernar la información geográfica y geoespacial producida, administrada y utilizada por la entidad.

La información geoespacial es un activo clave para la planeación territorial, la gestión urbana y rural, la formulación de políticas públicas, la prestación de servicios al ciudadano y la toma de decisiones informadas. Sin embargo, el diagnóstico institucional evidenció que este tipo de información se encuentra dispersa, con diferentes formatos, escalas, referencias y niveles de calidad, lo que limita su aprovechamiento estratégico y genera riesgos de inconsistencias y duplicidades.

En este contexto, el marco de referencia geoespacial establece los lineamientos que permiten consolidar una visión institucional unificada del territorio, asegurando que la información geográfica sea confiable, interoperable, segura y alineada con el modelo de arquitectura empresarial (MAE) y el plan estratégico de tecnologías de la información y las comunicaciones (PETIC).

##### 6.4.1 Objetivo del marco de referencia geoespacial

Establecer lineamientos institucionales para la gestión integral de la información geoespacial de la alcaldía municipal de Chía, de manera que se garantice su estandarización, calidad, interoperabilidad, seguridad y uso estratégico, como soporte para la planeación, la gestión territorial y la toma de decisiones institucionales.

##### 6.4.2 Alcance

El marco de referencia geoespacial aplica a:

- Información cartográfica y geográfica.
- Datos espaciales y alfanuméricos asociados al territorio.
- Capas geoespaciales utilizadas por dependencias misionales y de apoyo.
- Sistemas de información geográfica (SIG) y plataformas de visualización.
- Información geoespacial intercambiada con otras entidades del estado.

#### 6.4.3 Principios del marco de referencia geoespacial

La gestión de la información geoespacial se rige por los siguientes principios:

- Unicidad del territorio: Debe existir una visión institucional única del territorio.
- Estandarización: Uso de estándares comunes para datos y servicios geoespaciales.
- Interoperabilidad: Capacidad de integrar información geoespacial entre sistemas y entidades.
- Calidad y confiabilidad: La información debe ser precisa, actualizada y verificable.
- Seguridad y acceso controlado: protección según nivel de sensibilidad.
- Uso estratégico: La información geoespacial debe apoyar decisiones y políticas públicas.

#### 6.4.4 Lineamientos para la arquitectura de información geoespacial

- La información geoespacial debe integrarse al modelo de arquitectura de información institucional.
- Se deben definir bases institucionales (límites administrativos, vías, predios).
- Se debe evitar la duplicidad de repositorios geoespaciales.
- Las fuentes oficiales de información geoespacial deben estar claramente identificadas.

#### 6.4.5 Lineamientos de estandarización e interoperabilidad

- Se deben adoptar estándares geoespaciales reconocidos (formatos, proyecciones, servicios).
- Los sistemas SIG deben interoperar con otros sistemas de información institucionales.
- Se deben habilitar servicios de intercambio geoespacial (visualización y consulta).
- La información geoespacial debe poder integrarse con plataformas nacionales cuando aplique.

#### 6.4.6 Lineamientos de calidad de la información geoespacial

- Se debe documentar la procedencia, fecha y escala de la información.
- Las actualizaciones deben realizarse de manera controlada y trazable.
- Las inconsistencias geoespaciales deben registrarse y corregirse oportunamente.

#### 6.4.7 Lineamientos de roles y responsabilidades

En la implementación del marco de referencia geoespacial se establecen, como mínimo, los siguientes roles:

- Responsable de la información geoespacial: define el uso y reglas de la información geoespacial.
- Administrador de información geoespacial: gestiona la actualización, calidad y disponibilidad.
- Usuarios de información geoespacial: utilizan la información conforme a los lineamientos definidos.
- Oficina TIC: apoya en la definición de estándares, plataformas y lineamientos técnicos.

#### 6.4.8 Lineamientos de seguridad y acceso

- La información geoespacial debe clasificarse según su nivel de sensibilidad.
- Los accesos deben definirse por perfiles y roles.
- El uso de la información debe ser trazable y auditable.
- Los incidentes relacionados con información geoespacial deben gestionarse formalmente.

#### 6.4.9 Lineamientos para el uso estratégico de la información geoespacial

- La información geoespacial debe apoyar procesos de:
  - Planeación territorial
  - Ordenamiento urbano y rural
  - Gestión del riesgo
  - Infraestructura y servicios públicos
- Se deben promover tableros y visualizaciones geoespaciales para la toma de decisiones.
- La información geoespacial debe integrarse con datos estadísticos y administrativos.

#### 6.4.10 Seguimiento y mejora continua

La Oficina TIC, en coordinación con las dependencias responsables, deberá:

- Identificar brechas y oportunidades de mejora.
- Proponer acciones de fortalecimiento y optimización.
- Ajustar lineamientos conforme a cambios estratégicos y normativos.

## 6.5 Publicación de los servicios de intercambio de información

La publicación de los servicios de intercambio de información es un componente estratégico del dominio de gestión de la información dentro del modelo de gestión de gobierno TI de la alcaldía municipal de Chía, orientado a habilitar el intercambio seguro, estandarizado y controlado de información entre los sistemas de información institucionales, las dependencias internas y otras entidades del estado.

Este lineamiento responde a la necesidad de superar la fragmentación de la información, eliminar silos de datos y garantizar que la información institucional pueda ser reutilizada, compartida y aprovechada para la mejora de procesos, la prestación de servicios al ciudadano y la toma de decisiones, en coherencia con el plan estratégico de tecnologías de la información y las comunicaciones (PETIC), el modelo de arquitectura empresarial (MAE) y los principios de interoperabilidad del estado colombiano.

### 6.5.1 Objetivo de la publicación de servicios de intercambio de información

Establecer lineamientos institucionales para diseñar, publicar, administrar y consumir servicios de intercambio de información, de manera que se garantice su interoperabilidad, seguridad, trazabilidad y alineación con el gobierno TI.

### 6.5.2 Alcance

La publicación de servicios de intercambio de información aplica a:

- Servicios de consulta, intercambio y actualización de información entre sistemas institucionales.
- Servicios de interoperabilidad con entidades externas del estado.
- Interfaces, servicios web, APIs y mecanismos de integración definidos por la entidad.
- Información estructurada y no estructurada compartida a través de servicios tecnológicos.

### 6.5.3 Principios para la publicación de servicios de intercambio de información

La publicación de servicios de intercambio de información se rige por los siguientes principios:

- Interoperabilidad: los servicios deben facilitar la integración entre sistemas.
- Reutilización: la información debe compartirse mediante servicios reutilizables.
- Estandarización: los servicios deben cumplir estándares definidos institucionalmente.
- Seguridad y privacidad: la información intercambiada debe protegerse según su clasificación.
- Trazabilidad: el uso de los servicios debe ser monitoreable y auditable.
- Orientación a servicios: la información se publica como servicios, no como accesos directos a bases de datos.

#### 6.5.4 Lineamientos para la identificación de servicios de intercambio

- Se deben identificar los conjuntos de información susceptibles de ser compartidos.
- Los servicios deben priorizarse según:
  - Impacto institucional.
  - Valor público.
  - Frecuencia de uso.
  - Riesgo asociado.
- Los servicios deben alinearse con procesos misionales, estratégicos y de apoyo.

#### 6.5.5 Lineamientos para el diseño de los servicios de intercambio

- Los servicios deben diseñarse bajo un enfoque orientado a servicios.
- Se deben definir claramente:
  - Propósito del servicio.
  - Datos expuestos.
  - Reglas de negocio.
  - Frecuencia de actualización.
- Los servicios deben desacoplar los sistemas consumidores de los productores.

#### 6.5.6 Lineamientos para la publicación de los servicios

- Todo servicio de intercambio debe:
  - Ser documentado.
  - Contar con un responsable funcional y técnico.
- La publicación debe incluir:
  - Descripción del servicio.
  - Datos intercambiados.
  - Condiciones de uso.
  - Restricciones de acceso.

#### 6.5.7 Lineamientos de seguridad y control

- Los servicios deben implementar mecanismos de:
  - Autenticación.
  - Autorización.
  - Control de accesos por roles.
- La información intercambiada debe cumplir con las políticas de:
  - Seguridad de la información.
  - Seguridad digital.
  - Protección de datos personales.
- Se debe garantizar la trazabilidad del consumo de los servicios.

#### 6.5.8 Lineamientos de operación y monitoreo

- Los servicios publicados deben:
  - Contar con niveles de servicio definidos
  - Ser monitoreados en disponibilidad y desempeño
  - Gestionarse a través de la mesa de servicios TIC
- Los incidentes asociados a los servicios deben gestionarse formalmente.

#### 6.5.9 Lineamientos para la interoperabilidad externa

- Los servicios de intercambio con entidades externas deben:
  - Cumplir los lineamientos nacionales de interoperabilidad.
  - Estar formalizados mediante acuerdos o convenios.
  - Garantizar el uso adecuado de la información compartida.
- Se debe evitar la duplicidad de intercambio de información.

#### 6.5.10 Seguimiento y mejora continua

La Oficina TIC deberá:

- Mantener actualizado el catálogo de servicios de intercambio de información.
- Evaluar periódicamente el uso, desempeño y valor de los servicios publicados.
- Identificar oportunidades de mejora y nuevos servicios a publicar.
- Ajustar los lineamientos conforme a cambios tecnológicos, normativos y estratégicos.

### 6.6 Acuerdos de intercambio de información

Los acuerdos de intercambio de información constituyen un instrumento fundamental del dominio de gestión de la información dentro del modelo de gestión y gobierno TI de la

alcaldía municipal de Chía, orientado a regular, formalizar y controlar el intercambio de información entre dependencias internas, con otras entidades del estado y, cuando aplique, con terceros autorizados; permitiendo garantizar que el intercambio de información se realice de manera segura, estandarizada, trazable y conforme a la normatividad vigente; evitando usos indebidos, duplicidades, reprocesos y riesgos asociados a la confidencialidad, integridad y disponibilidad de la información. Asimismo, aseguran que la interoperabilidad tecnológica esté respaldada por compromisos claros de tipo jurídico, organizacional y operativo.

#### 6.6.1 Objetivo de los acuerdos de intercambio de información

Establecer lineamientos institucionales para definir, suscribir, administrar y evaluar acuerdos de intercambio de información, garantizando que el uso y la transferencia de información se realicen de forma controlada, segura y alineada con los objetivos estratégicos y con la política de seguridad de la información de la alcaldía municipal de Chía.

#### 6.6.2 Alcance

Los acuerdos de intercambio de información aplican a:

- Intercambio de información entre dependencias internas de la alcaldía.
- Intercambio de información con entidades del orden nacional, departamental o municipal.
- Intercambio de información soportado en servicios de interoperabilidad, APIs o plataformas tecnológicas.
- Información estructurada y no estructurada, independientemente del medio de intercambio.

#### 6.6.3 Principios de los acuerdos de intercambio de información

Los acuerdos de intercambio de información se rigen por los siguientes principios:

- Legalidad: el intercambio debe cumplir la normatividad vigente.
- Finalidad: la información debe usarse exclusivamente para los fines definidos en el acuerdo.
- Seguridad: la información debe protegerse conforme a su nivel de clasificación.
- Minimización: solo se debe intercambiar la información estrictamente necesaria.
- Trazabilidad: el intercambio debe ser auditable y verificable.
- Responsabilidad compartida: las partes son corresponsables del uso adecuado de la información.

#### 6.6.4 Lineamientos para la identificación de acuerdos de intercambio

- Todo intercambio recurrente o sistemático de información debe formalizarse mediante un acuerdo.
- Se deben priorizar acuerdos que:
  - Reduzcan reprocesos y duplicidades.
  - Mejoren la prestación de servicios al ciudadano.
  - Apoyen procesos misionales, estratégicos o de control.
- No se permitirá el intercambio informal o no documentado de información institucional.

#### 6.6.5 Lineamientos para la definición de los acuerdos

Todo acuerdo de intercambio de información debe definir, como mínimo:

- Partes involucradas.
- Objetivo y alcance del intercambio.
- Tipo de información a intercambiar.
- Finalidad y usos autorizados.
- Periodicidad y mecanismos de intercambio.
- Responsables funcionales y técnicos.
- Niveles de seguridad y confidencialidad.
- Mecanismos de control, auditoría y seguimiento.
- Vigencia y condiciones de terminación.

#### 6.6.6 Lineamientos de seguridad y protección de la información

- Los acuerdos deben alinearse con las políticas institucionales de:
  - Seguridad de la información.
  - Seguridad digital.
  - Protección de datos personales.
- Se deben definir responsabilidades claras frente a incidentes de seguridad.
- El acceso a la información intercambiada debe controlarse por roles y perfiles.
- La información sensible debe contar con medidas adicionales de protección.

#### 6.6.7 Lineamientos para la formalización y aprobación

- Los acuerdos deben ser revisados y avalados por:
  - Oficina TIC (aspectos técnicos).
  - Área jurídica (aspectos legales).
  - Seguridad de la información (aspectos de seguridad).
- La aprobación final debe realizarse conforme a los procedimientos institucionales.
- Todo acuerdo aprobado debe registrarse en un repositorio institucional.

#### 6.6.8 Lineamientos para la operación y seguimiento de los acuerdos

- Se debe realizar seguimiento periódico al cumplimiento de los acuerdos.
- Se deben monitorear:
  - Uso de la información intercambiada.
  - Cumplimiento de condiciones de seguridad.
- Los incumplimientos deben gestionarse mediante acciones correctivas.

#### 6.6.9 Seguimiento y mejora continua

La Oficina TIC, en coordinación con las dependencias responsables, deberá:

- Mantener un inventario actualizado de acuerdos de intercambio de información.
- Proponer ajustes o terminación de acuerdos cuando sea necesario.
- Incorporar lecciones aprendidas para fortalecer futuros acuerdos.

### 6.7 Uso del código postal colombiano

El código postal colombiano es un elemento clave de estandarización territorial que permite identificar de manera precisa y unívoca las zonas geográficas del país, facilitando la localización, el intercambio de información, la interoperabilidad entre sistemas y la calidad de los datos asociados a direcciones y ubicaciones.

En el marco del modelo de gestión y gobierno TI de la alcaldía municipal de Chía, el uso adecuado del código postal colombiano se reconoce como un habilitador de la gestión de la información y del gobierno de datos, al contribuir a la normalización de la información geográfica, la mejora de la calidad de los datos de dirección, la integración entre sistemas y la interoperabilidad con otras entidades del estado, en concordancia con los lineamientos de MinTIC.

#### 6.7.1 Objetivo del uso del código postal colombiano

Establecer lineamientos institucionales para el uso, gestión y aprovechamiento del código postal colombiano en los sistemas de información, procesos y servicios de la alcaldía municipal de Chía, garantizando la estandarización, calidad, interoperabilidad y uso estratégico de la información territorial.

#### 6.7.2 Alcance

Los presentes lineamientos aplican a:

- Sistemas de información institucionales que gestionen direcciones, ubicaciones o información territorial.
- Bases de datos que almacenen información de ciudadanos, predios, establecimientos, trámites o servicios.
- Procesos misionales, estratégicos y de apoyo que utilicen información de localización.
- Intercambio de información con entidades externas y plataformas del estado.

### 6.7.3 Principios para el uso del código postal colombiano

El uso del código postal colombiano se rige por los siguientes principios:

- Estandarización: el código postal debe utilizarse como identificador oficial de zona geográfica.
- Unicidad: cada registro debe asociarse a un único código postal válido.
- Interoperabilidad: el código postal facilita la integración entre sistemas.
- Calidad del dato: su uso mejora la consistencia y confiabilidad de la información de dirección.
- Reutilización: el código postal debe reutilizarse como dato maestro transversal.
- Actualización: se debe garantizar el uso de versiones oficiales y vigentes.

### 6.7.4 Lineamientos para la gestión del código postal colombiano como dato maestro

- El código postal colombiano debe ser tratado como dato maestro institucional.
- Se debe identificar una fuente oficial y única para la consulta y validación del código postal.
- Los sistemas de información deben obtener el código postal desde fuentes confiables y actualizadas.
- No se deben crear códigos postales propios o no oficiales.

### 6.7.5 Lineamientos para el uso del código postal en sistemas de información

- Todo sistema que gestione direcciones debe:
  - Incluir el campo de código postal colombiano.
  - Validar el código contra la fuente oficial.
  - Evitar el ingreso manual sin validación.
- El código postal debe almacenarse en formato estándar definido oficialmente.
- Los cambios en el código postal deben gestionarse mediante control de cambios tecnológicos.

### 6.7.6 Lineamientos de calidad de datos asociados al código postal

- Se deben definir reglas de calidad para el dato código postal, tales como:
  - Longitud y formato válidos.
  - Correspondencia con municipio y zona.
- Se deben implementar controles para evitar duplicidades e inconsistencias.
- Los indicadores de calidad del dato deben ser monitoreados periódicamente.

#### 6.7.7 Lineamientos para interoperabilidad e intercambio de información

- El código postal colombiano debe utilizarse como campo común en:
  - Servicios de intercambio de información.
  - APIs y servicios de interoperabilidad.
- Debe facilitar la integración con plataformas del estado y con otras entidades.
- En los acuerdos de intercambio de información debe especificarse el uso del código postal como estándar territorial.

#### 6.7.8 Lineamientos de roles y responsabilidades

- Oficina TIC:
  - Define los estándares técnicos y de integración.
  - Garantiza la correcta implementación en sistemas de información.
- Responsables de la información:
  - Aseguran el uso adecuado del código postal en los datos bajo su competencia.
- Administradores del dato:
  - Verifican la calidad, consistencia y actualización del código postal.
- Usuarios de la información:
  - Utilizan el código postal conforme a los lineamientos establecidos.

#### 6.7.9 Lineamientos de seguridad y protección

- El uso del código postal colombiano debe cumplir las políticas de:
  - Seguridad de la información.
  - Seguridad digital.
  - Protección de datos personales.
- El acceso y modificación del dato debe estar controlado por roles.
- Se debe garantizar la trazabilidad de cambios asociados al código postal.

#### 6.7.10 Seguimiento y mejora continua

La alcaldía municipal de Chía deberá:

- Evaluar periódicamente el uso del código postal en los sistemas institucionales.
- Identificar brechas de implementación o calidad del dato.

- Definir planes de mejora para fortalecer su uso y aprovechamiento.
- Ajustar los lineamientos conforme a cambios normativos o técnicos.

## 6.8 Explotación de datos

La explotación de datos es un componente estratégico del dominio de gestión de la información dentro del modelo de gestión y gobierno TI de la alcaldía municipal de Chía, orientado a transformar los datos institucionales en información útil, conocimiento accionable y valor público, mediante procesos de análisis, visualización, interoperabilidad y apoyo a la toma de decisiones.

En el marco de la política de gobierno digital y de los lineamientos de MinTIC, la explotación de datos, permite evolucionar desde un uso operativo de la información hacia un modelo de gestión pública basada en datos, que soporte la planeación, el seguimiento de políticas públicas, la mejora de los servicios al ciudadano y el fortalecimiento de la transparencia institucional. Este enfoque se apoya en la integración de sistemas, el intercambio de información y el desarrollo de capacidades analíticas.

### 6.8.1 Objetivo de la explotación de datos

Establecer lineamientos institucionales para analizar, integrar, visualizar y aprovechar los datos generados y administrados por la alcaldía municipal de Chía, garantizando su calidad, seguridad e interoperabilidad, con el fin de apoyar la toma de decisiones, la planeación territorial, la formulación de políticas públicas y la generación de valor público.

### 6.8.2 Alcance

La explotación de datos aplica a:

- Datos estructurados y no estructurados generados por sistemas de información institucionales.
- Información proveniente de procesos misionales, estratégicos y de apoyo.
- Datos intercambiados con otras entidades del estado mediante servicios de interoperabilidad.
- Información territorial y geoespacial.
- Datos utilizados para análisis, indicadores, tableros de control y modelos analíticos.

### 6.8.3 Principios para la explotación de datos

La explotación de datos se rige por los siguientes principios:

- Datos como activo estratégico: los datos deben aprovecharse para generar valor público.

- Calidad y confiabilidad: solo deben explotarse datos validados y de calidad.
- Interoperabilidad: la explotación debe apoyarse en la integración de fuentes diversas.
- Seguridad y privacidad: el análisis debe respetar la clasificación y sensibilidad de la información.
- Reutilización: los datos deben analizarse y reutilizarse para múltiples propósitos.
- Toma de decisiones basada en datos: el análisis debe apoyar decisiones institucionales.

#### 6.8.4 Lineamientos para la arquitectura de explotación de datos

- La explotación de datos debe alinearse con la arquitectura de Información institucional.
- Se debe promover la centralización lógica de datos para análisis y consulta.
- La arquitectura debe soportar:
  - Integración de fuentes internas y externas.
  - Análisis descriptivo, diagnóstico y exploratorio.
  - Visualización y publicación de información analítica.
- Se debe documentar técnicamente la infraestructura de datos para consulta institucional.

#### 6.8.5 Lineamientos para el análisis y aprovechamiento de la información

- Se deben desarrollar procesos de:
  - Análisis descriptivo (qué ocurrió).
  - Análisis diagnóstico (por qué ocurrió).
  - Análisis exploratorio (tendencias y patrones).
- El análisis debe vincular fuentes diversas, incluyendo datos administrativos, territoriales y, cuando aplique, datos provenientes de IoT y sensores.
- Los resultados del análisis deben traducirse en:
  - Indicadores.
  - Informes ejecutivos.
  - Tableros de control.
  - Visualizaciones comprensibles para tomadores de decisión.

#### 6.8.6 Lineamientos para servicios de información analítica

- La entidad debe ofrecer servicios de información analítica, tales como:
  - Publicación de estadísticas institucionales.
  - Visualización de información territorial.
  - Consulta de indicadores estratégicos.
- Estos servicios deben alinearse con los lineamientos de servicios ciudadanos digitales y gobierno digital.

- La publicación de información analítica debe garantizar claridad, oportunidad y reutilización.

#### 6.8.7 Lineamientos para la interoperabilidad y explotación de datos externos

- La explotación de datos debe apoyarse en servicios de intercambio de información internos y externos.
- Se debe priorizar la integración con:
  - Plataformas institucionales internas.
  - Carpeta ciudadana digital.
  - Otras entidades del estado.
- La interoperabilidad debe realizarse mediante servicios estandarizados y seguros, conforme a los lineamientos de MinTIC.

#### 6.8.8 Lineamientos para roles y responsabilidades

- Oficina TIC:
  - Define la arquitectura, herramientas y lineamientos técnicos.
- Responsables de la información / datos:
  - Autorizan el uso y explotación de los datos bajo su competencia.
- Administradores del dato:
  - Garantizan calidad, consistencia y documentación de los datos.
- Usuarios Analíticos:
  - Utilizan la información para análisis, planeación y toma de decisiones.

#### 6.8.9 Lineamientos de seguridad y ética en la explotación de datos

- La explotación de datos debe cumplir las políticas de:
  - Seguridad de la información.
  - Seguridad digital.
  - Protección de datos personales.
- Se deben aplicar criterios de anonimización cuando aplique.
- El uso de los datos debe ser trazable, auditable y ético.

#### 6.8.10 Desarrollo de capacidades para la explotación de datos

La alcaldía municipal de Chía debe:

- Fortalecer las competencias del personal técnico y usuarios finales en:
  - Análisis de datos.
  - Interpretación de información.

- Uso de herramientas analíticas.
- Promover iniciativas de innovación, analítica y transformación digital.
- Impulsar la gestión del conocimiento y la cultura de datos en la entidad.

#### 6.8.11 Seguimiento y mejora continua

La Oficina TIC en coordinación con las dependencias responsables, deberá:

- Evaluar periódicamente el nivel de madurez en explotación de datos.
- Medir el uso y valor de los productos analíticos generados.
- Identificar nuevas oportunidades de explotación de datos.
- Ajustar los lineamientos conforme a resultados y cambios estratégicos.

USO INSTITUCIONAL - ALCALDÍA DE CHÍA

## 7 Gestión de sistemas de información

La gestión de sistemas de información constituye un pilar fundamental del modelo de gestión y gobierno TI de la alcaldía municipal de Chía, en la medida en que articula los sistemas tecnológicos que soportan los procesos estratégicos, misionales y de apoyo de la entidad, garantizando la generación, administración y uso eficiente de la información institucional.

En el contexto de la transformación digital y el fortalecimiento del gobierno digital, los sistemas de información deben habilitar las transacciones de los procesos que producen la información, asegurar su calidad, facilitar la interoperabilidad interna y externa, y proveer insumos confiables para la toma de decisiones a nivel directivo, táctico y operativo. Estos sistemas representan un activo estratégico que contribuye directamente a la mejora de los servicios al ciudadano, la eficiencia administrativa, la transparencia y el cumplimiento de los objetivos del plan de desarrollo municipal.

Este dominio establece los lineamientos para la gestión integral de los sistemas de información a lo largo de su ciclo de vida, desde la identificación de necesidades, la definición de requerimientos y el diseño arquitectónico, hasta el desarrollo o adquisición, implantación, operación, mantenimiento, evolución y eventual retiro, alineado con el modelo de arquitectura empresarial, la estrategia de TI y el esquema de gobierno de TI definido para la entidad.

La gestión de sistemas de información en la alcaldía de Chía promueve una visión integrada del portafolio de aplicaciones institucionales, a través de la administración del catálogo de sistemas de información, la definición de arquitecturas de referencia y de solución, y el análisis permanente del valor que estos sistemas generan frente a los procesos que soportan. Así mismo, impulsa la adopción de buenas prácticas de desarrollo de software, aseguramiento de la calidad, seguridad de la información, accesibilidad, interoperabilidad y sostenibilidad técnica y financiera.

De esta manera, se orienta a la entidad en la consolidación de un ecosistema de sistemas de información coherente, interoperable y evolutivo, que responda de forma efectiva a las necesidades institucionales y ciudadanas, y que se integre armónicamente con los demás dominios del modelo de gestión y gobierno TI, especialmente con la estrategia de TI, el gobierno TI, la gestión de la información y la gestión de los servicios de TI.

### 7.1 Metodología para el desarrollo de sistemas de información

La metodología para el desarrollo de sistemas de información se establece como el marco institucional que orienta la planeación, análisis, diseño, construcción, implementación, mantenimiento y evolución de los sistemas de información de la alcaldía municipal de Chía, garantizando que estos respondan a necesidades reales de los procesos, se alineen con la estrategia institucional y aporten valor público.

Este lineamiento reconoce que los sistemas de información son habilitadores clave de la gestión pública y, por tanto, su desarrollo debe realizarse de manera estructurada, controlada y gobernada, integrando aspectos técnicos, funcionales, organizacionales y

normativos, en coherencia con el dominio de gestión de sistemas de información y el esquema de gobierno TI.

#### 7.1.1 Objetivo de la metodología

Establecer lineamientos institucionales para el desarrollo de sistemas de información que aseguren calidad, interoperabilidad, seguridad, sostenibilidad y alineación estratégica, durante todo el ciclo de vida de las soluciones tecnológicas de la alcaldía municipal de Chía.

#### 7.1.2 Alcance

La metodología aplica a:

- Desarrollo de nuevos sistemas de información.
- Evolución, mejora o modernización de sistemas existentes.
- Soluciones desarrolladas internamente o por terceros.
- Proyectos de TI con componentes de desarrollo de software.
- Integraciones y servicios de interoperabilidad asociados a sistemas de información.

#### 7.1.3 Principios orientadores de la metodología

- Alineación estratégica: Todo desarrollo debe responder al plan estratégico de tecnologías de la información y las comunicaciones (PETIC), al modelo de arquitectura empresarial (MAE), al plan de desarrollo municipal y a los objetivos institucionales.
- Enfoque en procesos y usuarios: Los sistemas deben soportar procesos y mejorar la experiencia del usuario.
- Arquitectura por diseño: Las soluciones deben alinearse con el modelo de arquitectura empresarial.
- Calidad y sostenibilidad: Los sistemas deben ser mantenibles, escalables y documentados.
- Seguridad desde el diseño: La seguridad debe incorporarse desde las primeras etapas.
- Interoperabilidad: Los sistemas deben facilitar el intercambio de información.
- Gobernanza y control: El desarrollo debe someterse a instancias de decisión y seguimiento.

#### 7.1.4 Enfoque metodológico

La alcaldía municipal de Chía adoptará una metodología de desarrollo flexible y adaptable, que podrá combinar enfoques tradicionales y ágiles, según el tipo, complejidad y criticidad del sistema de información, garantizando siempre el cumplimiento de los lineamientos institucionales.

La selección del enfoque metodológico deberá ser aprobada por la Oficina TIC, teniendo en cuenta el impacto institucional, los riesgos y la capacidad organizacional.

#### 7.1.5 Fases de la metodología para el desarrollo de sistemas de información

##### 7.1.5.1 *Identificación de la necesidad*

- La necesidad del sistema debe originarse en un proceso institucional.
- Debe existir una justificación funcional y estratégica.
- La iniciativa debe estar alineada con el portafolio de proyectos de TI.

##### 7.1.5.2 *Análisis y definición de requerimientos*

- Se deben levantar requerimientos funcionales, no funcionales y técnicos.
- Los requerimientos deben validarse con los usuarios y responsables del proceso.
- Se deben identificar dependencias, integraciones y riesgos asociados.

##### 7.1.5.3 *Diseño de la solución*

- El diseño debe alinearse con el modelo de arquitectura empresarial y de TI.
- Se deben definir arquitecturas de solución, modelos de datos, flujos y componentes.
- El diseño debe considerar interoperabilidad, seguridad y escalabilidad.

##### 7.1.5.4 *Construcción / Desarrollo*

- El desarrollo debe seguir estándares de codificación y buenas prácticas.
- Se debe garantizar versionamiento, control de cambios y documentación técnica.
- Las pruebas deben realizarse de manera progresiva y controlada.

##### 7.1.5.5 *Pruebas y aseguramiento de la calidad*

- Se deben ejecutar pruebas funcionales, técnicas y de seguridad.
- Los resultados deben documentarse y aprobarse antes de la implementación.
- Los defectos deben corregirse conforme a procedimientos definidos.

##### 7.1.5.6 *Implementación y puesta en producción*

- La implementación debe realizarse mediante el proceso formal de gestión de cambios.
- Se debe garantizar capacitación a los usuarios.
- Se deben definir planes de contingencia y reversión.

##### 7.1.5.7 *Operación y mantenimiento*

- El sistema debe incorporarse al catálogo de sistemas de información.

- Se deben definir responsables de soporte y mantenimiento.
- Los incidentes deben gestionarse conforme a la gestión de servicios de TI.

#### 7.1.5.8 Evaluación y mejora continua

- Se debe evaluar periódicamente el desempeño del sistema.
- Se deben identificar oportunidades de mejora funcional y tecnológica.
- Las mejoras deben gestionarse como nuevas iteraciones o proyectos.

#### 7.1.6 Lineamientos de roles y responsabilidades

- Oficina TIC: Define estándares, valida arquitectura y supervisa el desarrollo.
- Dueño del sistema: Representa la necesidad del proceso y valida resultados.
- Usuarios clave: Participan en el levantamiento y validación de requerimientos.
- Equipo de desarrollo / proveedor: Ejecuta el desarrollo conforme a la metodología.

#### 7.1.7 Lineamientos de seguridad y cumplimiento

- Todo desarrollo debe cumplir las políticas de:
  - Seguridad de la información.
  - Seguridad digital.
  - Protección de datos personales.
- La seguridad debe incorporarse desde la fase de análisis y diseño.
- Los accesos y privilegios deben definirse por roles.

#### 7.1.8 Seguimiento y control

La Oficina TIC deberá:

- Verificar el cumplimiento de la metodología en los desarrollos.
- Realizar revisiones periódicas de avance y calidad.
- Documentar lecciones aprendidas.
- Ajustar la metodología conforme a la evolución institucional.

## 7.2 Catálogo de sistemas de información

El catálogo de sistemas de información es un instrumento fundamental del dominio de gestión de sistemas de información dentro del modelo de gestión y gobierno TI de la alcaldía municipal de Chía, que permite identificar, organizar, administrar y gobernar el conjunto de aplicaciones y sistemas tecnológicos que soportan los procesos institucionales y la prestación de servicios al ciudadano.

Este catálogo constituye la fuente oficial de información sobre los sistemas de información de la entidad, facilitando la toma de decisiones, la planeación tecnológica, la interoperabilidad, la gestión de riesgos, la optimización de recursos y la alineación entre procesos, información, tecnología y servicios TIC.

#### 7.2.1 Objetivo del catálogo de sistemas de información

Establecer lineamientos institucionales para la definición, administración y actualización del catálogo de sistemas de información de la alcaldía municipal de Chía, garantizando su alineación con el modelo de arquitectura empresarial, y la estrategia de TI.

#### 7.2.2 Alcance

El catálogo de sistemas de información aplica a:

- Sistemas de información misionales, estratégicos y de apoyo.
- Aplicaciones desarrolladas internamente o adquiridas a terceros.
- Sistemas en operación, en desarrollo, en transición o en proceso de retiro.
- Sistemas que soportan servicios TIC internos o servicios digitales al ciudadano.
- Incluye tanto soluciones centralizadas como descentralizadas que utilicen infraestructura institucional.

#### 7.2.3 Principios del catálogo de sistemas de información

- Unicidad: Debe existir un único catálogo institucional oficial.
- Integralidad: El catálogo debe cubrir todos los sistemas de información.
- Actualización permanente: La información debe mantenerse vigente.
- Transparencia: La información del catálogo debe ser accesible para la gestión institucional.
- Alineación arquitectónica: Los sistemas deben estar alineados con el modelo de arquitectura empresarial.
- Orientación a servicios: Los sistemas se relacionan con los servicios TIC que soportan.

#### 7.2.4 Lineamientos para la estructuración del catálogo

El catálogo de sistemas de información debe estructurarse, como mínimo, con la siguiente información por cada sistema:

- Nombre del sistema de información.
- Tipo de sistema (misional, estratégico, apoyo, evaluación y mejora).
- Proceso(s) que soporta.
- Servicio(s) TIC asociados.
- Dependencia dueña del sistema.

- Estado del sistema (en operación, en desarrollo, en transición, retirado).
- Tipo de desarrollo (interno, externo, adquirido sin/con modificaciones).
- Proveedor o desarrollador (si aplica).
- Información básica de arquitectura e integraciones.
- Acuerdos de niveles de servicio.

#### 7.2.5 Lineamientos para la relación con el catálogo de servicios TIC

- Todo sistema de información debe estar asociado a uno o varios servicios TIC del catálogo de servicios de la Oficina TIC.
- No se deben operar sistemas que no estén registrados en el catálogo.
- La creación, modificación o retiro de un sistema debe reflejarse en ambos catálogos.
- El catálogo debe permitir identificar claramente qué sistemas soportan cada servicio TIC.

#### 7.2.6 Lineamientos para la administración y actualización del catálogo

- La dirección de sistemas de información y estadística, junto con la Oficina TIC, son responsables de:
  - Administrar el catálogo de sistemas de información.
  - Garantizar su actualización.
- Las dependencias dueñas de los sistemas deben:
  - Reportar cambios, evoluciones o incidencias relevantes.
- El catálogo debe actualizarse:
  - Ante la incorporación de nuevos sistemas.
  - Ante cambios significativos.
  - Ante el retiro o reemplazo de sistemas.

#### 7.2.7 Lineamientos para el uso del catálogo de sistemas de información

El catálogo debe utilizarse como insumo para:

- Planeación y priorización de proyectos de TI.
- Evaluación de redundancias y obsolescencia tecnológica.
- Análisis de impacto de cambios tecnológicos.
- Gestión de riesgos y continuidad del servicio.
- Evaluación del desempeño de la gestión de sistemas de información.
- Auditorías y ejercicios de control interno y externo.

### 7.2.8 Lineamientos de gobierno y control

- El catálogo de sistemas de información debe ser validado anualmente.
- Los sistemas que no cumplan los lineamientos institucionales deben ser objeto de planes de mejora o racionalización.
- El catálogo debe articularse con:
  - El modelo de arquitectura empresarial.
  - Gestión de proyectos TIC.
  - Gestión de cambios.
  - Gestión de servicios TIC.

### 7.2.9 Articulación con el modelo de arquitectura empresarial

El catálogo de sistemas de información es un componente esencial de la arquitectura de aplicaciones, y debe:

- Reflejar el estado actual (AS-IS) y objetivo (TO-BE) del portafolio de aplicaciones.
- Apoyar la definición de hojas de ruta tecnológicas.
- Facilitar la evolución controlada del ecosistema de sistemas de información.

### 7.2.10 Seguimiento y mejora continua

La dirección de sistemas de información y estadística, junto con la oficina TIC deberán:

- Evaluar periódicamente la cobertura y calidad del catálogo.
- Identificar oportunidades de consolidación o modernización de sistemas.
- Proponer acciones de mejora alineadas con el PETIC y el MAE.
- Ajustar los lineamientos conforme a cambios estratégicos o tecnológicos.

## 7.3 Guía de estilo y usabilidad

La guía de estilo y usabilidad es un instrumento fundamental dentro del dominio de gestión de sistemas de información del modelo de gestión y gobierno TI de la alcaldía municipal de Chía, cuyo propósito es establecer criterios comunes para el diseño, desarrollo y evolución de las interfaces de usuario de los sistemas de información y servicios digitales institucionales.

Esta guía busca garantizar que las soluciones tecnológicas de la alcaldía ofrezcan una experiencia de usuario coherente, intuitiva, accesible y centrada en las necesidades del ciudadano y del usuario interno, contribuyendo a la eficiencia operativa, la apropiación de las tecnologías y la confianza en los servicios digitales de la entidad.

### 7.3.1 Objetivo de la guía de estilo y usabilidad

Establecer lineamientos institucionales de diseño visual, interacción y usabilidad que orienten la construcción y evolución de los sistemas de información y servicios digitales de la alcaldía municipal de Chía, garantizando consistencia, accesibilidad, facilidad de uso y alineación con la identidad institucional.

### 7.3.2 Alcance

La guía de estilo y usabilidad aplica a:

- Sistemas de información institucionales (misionales, estratégicos y de apoyo).
- Servicios digitales orientados al ciudadano.
- Portales web, aplicaciones internas y externas, y plataformas digitales.
- Soluciones desarrolladas internamente o por terceros.
- Proyectos de TI que incluyan componentes de interfaz de usuario.

### 7.3.3 Principios orientadores de la guía

- Enfoque centrado en el usuario: El diseño debe responder a las necesidades reales de los usuarios.
- Simplicidad y claridad: Las interfaces deben ser intuitivas y fáciles de entender.
- Consistencia: Los elementos visuales y de interacción deben ser uniformes.
- Accesibilidad: Los sistemas deben ser utilizables por todas las personas.
- Eficiencia: El diseño debe facilitar la realización de tareas con el menor esfuerzo visible.
- Confianza y transparencia: El diseño debe transmitir seguridad y claridad en la información.

### 7.3.4 Lineamientos de diseño visual

- Se debe respetar la identidad visual institucional (colores, tipografías, logotipos).
- El diseño debe ser limpio, ordenado y jerarquizado visualmente.
- Se deben utilizar iconos y elementos gráficos comprensibles y consistentes.
- Los textos deben ser claros, legibles y en lenguaje sencillo.
- Se debe evitar la sobrecarga visual y el uso innecesario de elementos gráficos.

### 7.3.5 Lineamientos de usabilidad

- Las interfaces deben ser intuitivas y reducir la curva de aprendizaje.

- Las acciones principales deben ser fácilmente identificables.
- Los formularios deben:
  - Solicitar solo la información necesaria.
  - Proveer ayudas y mensajes claros.
  - Validar errores de manera comprensible.
- La navegación debe ser clara, predecible y consistente.
- El sistema debe ofrecer retroalimentación visible ante las acciones del usuario.

#### 7.3.6 Lineamientos de accesibilidad

- Los sistemas deben cumplir con criterios de accesibilidad reconocidos.
- Se debe garantizar:
  - Contraste adecuado de colores.
  - Navegación mediante teclado.
  - Textos alternativos para elementos visuales.
- La accesibilidad debe considerarse desde la fase de diseño y no como un ajuste posterior

#### 7.3.7 Lineamientos de experiencia de usuario (UX)

- Se deben analizar los perfiles de usuarios internos y ciudadanos.
- El diseño debe considerar el contexto de uso y las limitaciones tecnológicas.
- Se deben realizar pruebas de usabilidad cuando aplique.
- La retroalimentación de los usuarios debe incorporarse en la mejora continua.

#### 7.3.8 Lineamientos para desarrollo y evolución

- Todo desarrollo o mejora de sistemas debe:
  - Cumplir la guía de estilo y usabilidad.
  - Ser validado por la Oficina TIC antes de su implementación.
- Los proveedores externos deben adoptar los lineamientos definidos.
- La guía debe actualizarse conforme a nuevas necesidades o estándares.

#### 7.3.9 Roles y responsabilidades

- Oficina TIC:
  - Define y mantiene la guía de estilo y usabilidad.
  - Valida el cumplimiento en los sistemas de información.
- Equipos de desarrollo / proveedores:
  - Aplican los lineamientos en el diseño y desarrollo.
- Usuarios clave:
  - Participan en validaciones y pruebas de usabilidad.

### 7.3.10 Seguimiento y mejora continua

La Oficina TIC deberá:

- Identificar oportunidades de mejora en la experiencia de usuario.
- Ajustar la guía conforme a cambios tecnológicos y organizacionales.
- Promover la apropiación de los lineamientos en la entidad.

## 7.4 Ambientes independientes en el ciclo de vida de los sistemas de información

Los ambientes independientes son un componente crítico de la gestión de sistemas de información, ya que permiten controlar riesgos, asegurar la calidad, proteger la información y garantizar la estabilidad operativa durante el ciclo de vida de las soluciones tecnológicas. La separación de ambientes evita impactos negativos en la operación institucional y fortalece la gobernanza sobre los cambios tecnológicos.

En el marco del modelo de gestión y gobierno TI, la alcaldía municipal de Chía adopta la separación de ambientes como un principio obligatorio para el desarrollo, pruebas, despliegue y operación de sistemas de información, alineado con el esquema de gobierno TI y la gestión de cambios.

### 7.4.1 Objetivo de los ambientes independientes

Establecer lineamientos institucionales para la definición, uso, administración y control de ambientes independientes en el ciclo de vida de los sistemas de información, garantizando calidad, seguridad, trazabilidad y continuidad del servicio.

### 7.4.2 Alcance

Estos lineamientos aplican a:

- Sistemas de información nuevos y existentes.
- Desarrollos internos y tercerizados.
- Proyectos TIC que incluyan construcción, evolución o integración de software.
- Infraestructura local, en la nube o híbrida.

### 7.4.3 Principios para la gestión de ambientes

- Separación obligatoria: Cada ambiente cumple un propósito específico.

- No contaminación: Los cambios no deben propagarse sin autorización.
- Seguridad por diseño: Cada ambiente tiene controles acordes a su nivel de riesgo.
- Trazabilidad: Todo despliegue debe ser identificable y auditable.
- Control y gobernanza: Los cambios siguen el proceso formal de gestión de cambios.
- Estabilidad operativa: El ambiente productivo debe protegerse prioritariamente.

#### 7.4.4 Tipos de ambientes institucionales

La alcaldía municipal de Chía define, como mínimo, los siguientes ambientes:

##### 7.4.4.1 Ambiente de desarrollo

Propósito: Construcción y configuración inicial de funcionalidades.

Lineamientos:

- Uso exclusivo para desarrollo.
- Datos ficticios o anonimizados.
- Acceso restringido a equipos técnicos.
- Cambios frecuentes y controlados por versionamiento.

##### 7.4.4.2 Ambiente de pruebas (TEST / QA)

Propósito: Validación funcional, técnica y de seguridad.

Lineamientos:

- Replica controlada del entorno productivo.
- Ejecución de pruebas funcionales, de integración y seguridad.
- Datos de prueba anonimizados.
- Aprobación obligatoria para avanzar a siguientes ambientes.

##### 7.4.4.3 Ambiente de preproducción

Propósito: Validación final antes del paso a producción.

Lineamientos:

- Configuración idéntica o muy cercana a producción.
- Pruebas de aceptación por usuarios clave.
- Autorización formal de paso a producción.
- Sin desarrollos directos.

##### 7.4.4.4 Ambiente de producción

Propósito: Operación oficial del sistema.

Lineamientos:

- Uso exclusivo para operación institucional.
- Acceso altamente restringido.
- Prohibidos cambios directos sin gestión de cambios.
- Monitoreo, respaldo y contingencia obligatorios.

#### 7.4.4.5 *Ambientes adicionales (cuando aplique)*

- Capacitación: formación de usuarios.
- Contingencia / DRP: continuidad del servicio.

#### 7.4.5 Lineamientos para el uso de datos en los ambientes

- Está prohibido usar datos reales en ambientes distintos a producción, salvo autorización expresa.
- Los datos de prueba deben:
  - Ser anonimizados o ficticios.
  - Representar escenarios reales.
- La copia de datos desde producción debe registrarse y controlarse.

#### 7.4.6 Lineamientos de seguridad por ambiente

- Cada ambiente debe contar con:
  - Controles de acceso diferenciados.
  - Políticas de respaldo acordes al riesgo.
  - Registro de eventos y accesos.
- El ambiente productivo debe cumplir los niveles más altos de seguridad.

#### 7.4.7 Lineamientos para despliegue y cambios

- Todo paso entre ambientes debe:
  - Estar documentado.
  - Contar con evidencia de pruebas.
  - Ser aprobado según la gestión de cambios.
- No se permiten accesos directos ni modificaciones manuales en producción.

#### 7.4.8 Roles y responsabilidades

- Oficina TIC:
  - Define y controla la arquitectura de ambientes.
  - Autoriza despliegues a producción.
- Equipo de desarrollo / proveedor:

- Usa correctamente cada ambiente.
- Documenta cambios y versiones.
- Usuarios claves:
  - Validan funcionalidades en pruebas y preproducción.

#### 7.4.9 Seguimiento y control

La Oficina TIC deberá:

- Verificar el cumplimiento de la separación de ambientes.
- Gestionar incumplimientos mediante acciones correctivas.
- Ajustar los lineamientos según evolución tecnológica.

### 7.5 Análisis de requerimientos de los sistemas de información

El análisis de requerimientos de los sistemas de información es una etapa crítica dentro del ciclo de vida de los sistemas de información de la alcaldía municipal de Chía, ya que permite identificar, comprender y documentar de manera estructurada las necesidades funcionales, técnicas y de información de los procesos institucionales que serán soportados por soluciones tecnológicas.

Un análisis de requerimientos adecuado reduce riesgos de reprocesos, sobrecostos y soluciones que no generan valor, y garantiza que los sistemas de información estén alineados con los objetivos estratégicos, el plan estratégico de tecnologías de la información y las comunicaciones (PETIC), el modelo de arquitectura empresarial y el esquema de gobierno TI de la entidad.

Tabla No. 5 Ejemplo matriz de requerimiento vs proceso vs sistema

ID Re q	Nombre del Requerimiento	Tipo de Requerimiento	Proceso o Institucional	Sistema de Información	Usuario / Rol	Prioridad	Fuente del Requerimiento	Dependencias / Integraciones	Criterios de Aceptación	Estado	Aprobación
R-001	Registro de solicitudes ciudadanas	Funcional	Atención al ciudadano	Sistema PQRS	Funcionario atención	Alta	Necesidad del proceso	Integración con carpeta ciudadana	Registro exitoso y notificación automática	Validado	Aprobado
R-002	Autenticación por roles	No funcional / Seguridad	Gestión administrativa	Sistema PQRS	Usuario interno	Alta	Política de seguridad	Atención al ciudadano	Acceso según perfil definido	Pendiente	Pendiente

ID	Nombre del Requerimiento	Tipo de Requerimiento	Proceso Institucional	Sistema de Información	Usuario / Rol	Prioridad	Fuente del Requerimiento	Dependencias / Integraciones	Criterios de Aceptación	Estado	Aprobación
		d					d	o	o		

### 7.5.1 Objetivo del análisis de requerimientos

Establecer lineamientos institucionales para realizar el análisis de requerimientos de los sistemas de información, asegurando que las necesidades de los procesos y usuarios se identifiquen, documenten, validen y prioricen de manera clara, coherente y alineada con la estrategia institucional.

### 7.5.2 Alcance

El análisis de requerimientos aplica a:

- Desarrollo de nuevos sistemas de información.
- Evolución, mejora o modernización de sistemas existentes.
- Proyectos TI con componentes de software o integración.
- Soluciones desarrolladas internamente o por proveedores externos.

### 7.5.3 Principios del análisis de requerimientos

- Enfoque en procesos: Los requerimientos deben derivarse de procesos institucionales.
- Alineación estratégica: Los requerimientos deben contribuir a objetivos institucionales.
- Participación de usuarios: Los usuarios claves deben participar activamente.
- Claridad y trazabilidad: Los requerimientos deben ser claros y rastreables.
- Viabilidad: Los requerimientos deben ser técnica y financieramente posibles.
- Control y gobernanza: Los cambios en requerimientos deben gestionarse formalmente.

### 7.5.4 Lineamientos para la identificación de la necesidad

- Toda iniciativa debe originarse en una necesidad del proceso institucional.
- La necesidad debe documentarse indicando:
  - Problema u oportunidad identificada.
  - Proceso afectado.

- Beneficio esperado.
- La Oficina TIC debe validar la alineación con el plan estratégico de tecnologías de la información y las comunicaciones (PETIC) y el modelo de arquitectura empresarial.

#### 7.5.5 Lineamientos para el levantamiento de requerimientos

El levantamiento de requerimientos debe realizarse mediante técnicas estructuradas, tales como:

- Reuniones con usuarios y responsables del proceso.
- Talleres de trabajo colaborativos.
- Análisis de procesos actuales (AS-IS).
- Revisión de normativa, procedimientos y sistemas existentes.
- Observación directa del proceso cuando aplique.

Los requerimientos deben clasificarse como:

- Requerimientos funcionales.
- Requerimientos no funcionales.
- Requerimientos de información y datos.
- Requerimientos de interoperabilidad e integración.

Tabla No. 6 Clasificación de requerimientos

Tipo	Descripción
Funcional	Funcionalidad del sistema
No funcional	Seguridad, rendimiento, disponibilidad, usabilidad
Información	Datos, reportes, calidad, explotación
Interoperabilidad	Integraciones, APIs, intercambio de información

#### 7.5.6 Lineamientos para la documentación de requerimientos

- Los requerimientos deben documentarse de forma clara, precisa y verificable.
- Cada requerimiento debe contar con:
  - Identificador único.
  - Descripción clara.
  - Proceso y usuario asociado.
  - Prioridad.
  - Criterios de aceptación.
- La documentación debe almacenarse en repositorios institucionales autorizados.

#### 7.5.6.1.1 Lineamientos para la validación y aprobación de requerimientos

- Los requerimientos deben validarse con:
  - Usuarios claves del proceso.
  - Dueño del sistema o proceso.
  - Oficina TIC (viabilidad técnica y alineación arquitectónica).
- La aprobación formal es obligatoria antes de iniciar diseño o desarrollo.
- Los requerimientos aprobados constituyen la línea base del sistema.

#### 7.5.7 Lineamientos para la priorización de requerimientos

- Los requerimientos deben priorizarse según:
  - Impacto institucional.
  - Valor para el ciudadano o usuario interno.
  - Riesgo operativo o normativo.
  - Esfuerzo de implementación.
- La priorización debe ser avalada por el jefe de la Oficina TIC y/o el comité de gestión y desempeño, cuando aplique.

#### 7.5.8 Lineamientos para la gestión de cambios en requerimientos

- Todo cambio posterior a la aprobación debe:
  - Justificarse formalmente.
  - Evaluar impacto en alcance, tiempo y costo.
  - Tramitarse a través del proceso de gestión de cambios.
- No se permiten cambios informales o no documentados.

#### 7.5.9 Lineamientos de roles y responsabilidades

- Oficina TIC:
  - Orienta el análisis y valida la viabilidad técnica y arquitectónica.
- Dueño del proceso / sistema:
  - Define necesidades funcionales y valida requerimientos.
- Usuarios claves:
  - Aportan conocimiento operativo y validan necesidades reales.
- Equipo de análisis / proveedor:
  - Documenta los requerimientos conforme a los lineamientos.

#### 7.5.10 Articulación con el ciclo de vida del sistema

El análisis de requerimientos se articula con:

- Metodología de desarrollo de sistemas de información.
- El modelo de arquitectura empresarial (AS-IS / TO-BE).
- Gestión de proyectos TI.
- Gestión de cambios.
- Gestión de servicios TI.

#### 7.5.11 Seguimiento y control

La Oficina TIC deberá:

- Verificar la calidad y completitud de los requerimientos.
- Asegurar la trazabilidad durante el ciclo de vida del sistema.
- Documentar lecciones aprendidas.
- Ajustar los lineamientos según evolución institucional.

Tabla No. 7 Matriz de trazabilidad

ID Req	Objetivo Estratégico	PETI	Dominio TI	Arquitectura Empresarial	Proyecto TI
R-001	Mejora servicio al ciudadano	Línea 2	Gestión SI	Aplicaciones	Proyecto PQRS
R-002	Seguridad de la información	Línea 4	Gobierno TI	Seguridad	Proyecto PQRS

Tabla No. 8 Matriz de seguimiento y control

ID Req	Validado por Usuario	Validado Oficina TIC	Viabilidad Técnica	Viabilidad Presupuestal	Autorizado para Diseño
R-001	Sí	Sí	Alta	Sí	Sí
R-002	Sí	Pendiente	Media	Pendiente	No

## 7.6 Integración continua durante el ciclo de vida de los sistemas de información

La integración continua, es una práctica clave para garantizar la calidad, estabilidad y evolución controlada de los sistemas de información de la alcaldía municipal de Chía. Consiste en integrar de manera frecuente y automatizada los cambios realizados sobre el código, configuraciones y componentes del sistema, permitiendo detectar errores de forma temprana, reducir riesgos operativos y asegurar coherencia durante todo el ciclo de vida del software.

En el marco del modelo de gestión y gobierno TI (MGGTI), la integración continua se adopta como un lineamiento institucional obligatorio para los desarrollos nuevos y las evoluciones de sistemas existentes, articulándose con la metodología de desarrollo de sistemas de información, la gestión de cambios y el esquema de gobierno TI.

#### 7.6.1 Objetivo de la integración continua

Establecer lineamientos institucionales para implementar prácticas de integración continua durante el ciclo de vida de los sistemas de información, garantizando calidad, trazabilidad, seguridad y control en los desarrollos tecnológicos de la alcaldía municipal de Chía.

#### 7.6.2 Alcance

La integración continua aplica a:

- Sistemas de información desarrollados internamente.
- Sistemas desarrollados o mantenidos por proveedores externos.
- Proyectos TI que incluyan desarrollo, mantenimiento o integración de software.
- Componentes de software, integraciones, APIs y configuraciones técnicas.

#### 7.6.3 Principios de la integración continua

La integración continua se rige por los siguientes principios:

- Automatización: las integraciones deben ejecutarse de forma automática.
- Frecuencia: los cambios deben integrarse de manera periódica y controlada.
- Calidad temprana: los errores deben detectarse lo antes posible.
- Trazabilidad: cada integración debe ser identificable y auditable.
- Seguridad integrada: los controles de seguridad deben incorporarse en el proceso.

#### 7.6.4 Lineamientos para la gestión del código y versiones

- Todo desarrollo debe contar con un repositorio de código fuente institucional o autorizado.
- Se debe implementar control de versiones para:
  - Código fuente.
  - Scripts de base de datos.
  - Configuraciones.
- Cada cambio debe estar asociado a:
  - Un requerimiento aprobado.
  - Un responsable identificado.
- No se permiten integraciones directas en ambientes productivos.

#### 7.6.5 Lineamientos para la automatización de integraciones

- Se deben definir procesos automatizados para:
  - Compilación del código.
  - Validación de dependencias.
  - Ejecución de pruebas básicas.
- Las integraciones deben ejecutarse en ambientes distintos a producción.
- Los resultados de cada integración deben quedar registrados.

#### 7.6.6 Lineamientos para pruebas dentro de la integración continua

- La integración continua debe incluir pruebas automáticas mínimas, tales como:
  - Pruebas unitarias.
  - Validaciones funcionales básicas.
  - Verificaciones de seguridad cuando aplique.
- Las fallas detectadas deben corregirse antes de avanzar a otros ambientes.
- No se deben integrar cambios que no superen las pruebas definidas.

#### 7.6.7 Lineamientos para la gestión de ambientes

- La integración continua debe ejecutarse en ambientes definidos (desarrollo, pruebas).
- El paso a ambientes superiores debe:
  - Contar con evidencia de integración exitosa.
  - Ser aprobado conforme a la gestión de cambios.
- Los ambientes productivos no deben usarse para pruebas de integración.

#### 7.6.8 Lineamientos de seguridad en la integración continua

- Se deben proteger los repositorios y herramientas de integración mediante:
  - Control de accesos por roles.
  - Autenticación fuerte.
  - La información sensible no debe almacenarse en el código.
- Los registros de integración deben conservarse para auditoría.

#### 7.6.9 Lineamientos de roles y responsabilidades

- Oficina TIC:
  - Define estándares y herramientas de integración continua.

- Supervisa el cumplimiento de los lineamientos.
- Equipos de desarrollo / proveedores:
  - Implementan y utilizan la integración continua conforme a lo definido.
  - Documentan y corrigen fallas detectadas.
- Dueños de sistemas:
  - Aseguran que los cambios estén alineados con las necesidades del proceso.

#### 7.6.10 Articulación con el ciclo de vida del sistema

La integración continua se articula con:

- Metodología de desarrollo de sistemas de información.
- Análisis de requerimientos.
- Gestión de cambios.
- Gestión de servicios TI.

#### 7.6.11 Seguimiento y control

La Oficina TIC deberá:

- Verificar la adopción de prácticas de integración continua.
- Monitorear resultados de integraciones y fallas recurrentes.
- Gestionar incumplimientos mediante acciones correctivas.
- Ajustar los lineamientos conforme a la madurez institucional.

### 7.7 Entrega continua durante el ciclo de vida de los sistemas de información

La entrega continua, es una práctica que permite que los sistemas de información de la alcaldía municipal de Chía se encuentren en todo momento en condiciones controladas para ser liberados a producción, garantizando estabilidad, calidad y seguridad en cada entrega tecnológica.

Dentro del modelo de gestión y gobierno TI (MGGTI), la entrega continua se adopta como un lineamiento institucional que complementa la integración continua y fortalece la gobernanza del ciclo de vida del software, asegurando que los cambios tecnológicos se desplieguen de forma planificada, autorizada y alineada con la gestión de cambios y la gestión de servicios TI.

#### 7.7.1 Objetivo de la entrega continua

Establecer lineamientos institucionales para la preparación, validación y liberación controlada de cambios en los sistemas de información, garantizando que las entregas a los ambientes productivos se realicen de manera segura, trazable y alineada con los objetivos institucionales.

#### 7.7.2 Alcance

La entrega continua aplica a:

- Sistemas de información nuevos y existentes.
- Desarrollos internos y tercerizados.
- Proyectos TI que incluyan despliegues de software.
- Cambios funcionales, técnicos y de configuración que impacten sistemas de información.

#### 7.7.3 Principios de la entrega continua

La entrega continua se rige por los siguientes principios:

- Preparación permanente: los sistemas deben estar listos para ser liberados en cualquier momento.
- Control institucional: ninguna entrega se realiza sin autorización.
- Calidad verificada: solo se liberan cambios previamente probados.
- Seguridad y estabilidad: la protección del ambiente productivo es prioritaria.
- Trazabilidad: toda entrega debe ser registrada y auditable.
- Continuidad del servicio: las entregas deben minimizar impactos al usuario.

#### 7.7.4 Lineamientos para la preparación de entregas

- Toda entrega debe derivarse de:
  - Requerimientos aprobados
  - Cambios autorizados
- Los componentes a entregar deben:
  - Haber pasado por integración continua
  - Contar con evidencia de pruebas exitosas
- Se debe documentar claramente:
  - Alcance del cambio
  - Riesgos asociados
  - Plan de despliegue y reversión

#### 7.7.5 Lineamientos para la validación previa a la entrega

Antes de una entrega, se debe validar:

- Cumplimiento de requerimientos funcionales.
- Resultados satisfactorios de pruebas técnicas y de seguridad.
- Compatibilidad con otros sistemas e integraciones.
- Disponibilidad de respaldos y mecanismos de contingencia.

La validación debe contar con el aval de la Oficina TIC y, cuando aplique, de los usuarios claves.

#### 7.7.6 Lineamientos para el despliegue en ambientes

- Las entregas deben realizarse de forma progresiva:
  - Desarrollo – Pruebas - Preproducción - Producción
- El paso a producción debe:
  - Estar autorizado mediante la gestión de cambios
  - Ejecutarse en ventanas definidas
- No se permiten entregas directas ni informales en producción.

#### 7.7.7 Lineamientos de seguridad en la entrega continua

- El acceso a los ambientes de entrega debe estar restringido por roles.
- Las credenciales y configuraciones sensibles deben gestionarse de forma segura.
- Se debe garantizar la trazabilidad de:
  - Quién realiza la entrega.
  - Cuando se realiza.
  - Qué componentes se liberan.

#### 7.7.8 Lineamientos para la gestión de fallas y reversión

- Toda entrega debe contar con:
  - Plan de reversión documentado.
  - Procedimiento de atención de incidentes.
- Ante fallas críticas, se debe:
  - Activar el plan de reversión.
  - Informar a las instancias correspondientes.
  - Registrar el incidente para análisis posterior.

#### 7.7.9 Lineamientos de roles y responsabilidades

- Oficina TIC:
  - Autoriza y supervisa las entregas a producción.

- Define estándares y ventanas de despliegue.
- Equipo de desarrollo / proveedor:
  - Prepara y ejecuta las entregas conforme a los lineamientos.
  - Documenta evidencias y resultados.
- Usuarios claves / Dueños del sistema:
  - Validan funcionalmente los cambios antes de producción.

#### 7.7.10 Seguimiento y control

La Oficina TIC deberá:

- Verificar el cumplimiento del proceso de entrega continua.
- Monitorear impactos posteriores a las entregas.
- Evaluar la efectividad de los planes de reversión.
- Ajustar los lineamientos según la madurez institucional.

### 7.8 Despliegue continuo durante el ciclo de vida de los sistemas de información

El despliegue continuo, es una práctica que permite que los cambios aprobados en los sistemas de información se desplieguen de forma automatizada, controlada y repetible en los ambientes definidos, reduciendo tiempos de liberación, errores manuales y riesgos operativos.

En el marco del modelo de gestión y gobierno TI (MGGTI), el despliegue continuo se adopta como un lineamiento institucional para fortalecer la madurez tecnológica, garantizar coherencia entre ambientes y asegurar que las entregas tecnológicas se realicen con altos estándares de calidad, seguridad y trazabilidad, sin comprometer la estabilidad de los servicios institucionales.

#### 7.8.1 Objetivo del despliegue continuo

Establecer lineamientos institucionales para ejecutar despliegues automatizados y controlados de los sistemas de información durante su ciclo de vida, garantizando consistencia, seguridad, trazabilidad y continuidad del servicio en la alcaldía municipal de Chía.

#### 7.8.2 Alcance

El despliegue continuo aplica a:

- Sistemas de información nuevos y existentes.
- Desarrollos internos y tercerizados.

- Cambios funcionales, técnicos y de configuración.
- Infraestructura local, en la nube o híbrida.
- Integraciones, APIs y servicios tecnológicos asociados.

### 7.8.3 Principios del despliegue continuo

- Automatización controlada: Los despliegues deben ejecutarse mediante mecanismos automatizados.
- Consistencia entre ambientes: Los despliegues deben reproducirse de forma uniforme.
- Seguridad y estabilidad: La protección del ambiente productivo es prioritaria.
- Trazabilidad total: Todo despliegue debe ser auditable.
- Gobernanza: El despliegue continuo debe alinearse con la gestión de cambios y el gobierno TI.
- Continuidad del servicio: Los despliegues deben minimizar interrupciones.

### 7.8.4 Lineamientos para la preparación del despliegue

- Todo despliegue debe originarse en:
  - Requerimientos aprobados.
  - Cambios autorizados.
- Los componentes a desplegar deben:
  - Haber pasado por integración continua y entrega continua.
  - Contar con pruebas satisfactorias.
- Se debe documentar:
  - Componentes a desplegar.
  - Impacto esperado.
  - Riesgos y dependencias.
  - Plan de reversión.

### 7.8.5 Lineamientos para la automatización del despliegue

- Los despliegues deben realizarse mediante scripts o herramientas automatizadas.
- Se debe evitar la ejecución manual directa en producción.
- Los scripts de despliegue deben:
  - Versionarse.
  - Documentarse.
  - Probarse previamente en ambientes inferiores.
- El mismo mecanismo de despliegue debe utilizarse en todos los ambientes.

### 7.8.6 Lineamientos para despliegue por ambientes

- El despliegue debe seguir la secuencia institucional de ambientes:
  - Desarrollo - Pruebas - Preproducción – Producción.
- El paso a producción debe:
  - Contar con autorización formal.
  - Ejecutarse en ventanas de despliegue definidas.
- No se permiten despliegues directos que omitan ambientes intermedios.

#### 7.8.7 Lineamientos de seguridad en el despliegue continuo

- El acceso a las herramientas de despliegue debe:
  - Estar controlado por roles.
  - Usar mecanismos de autenticación segura.
- Las credenciales y configuraciones sensibles deben:
  - Gestionarse de forma segura.
  - No almacenarse en texto plano.

#### 7.8.8 Lineamientos para manejo de fallas y reversión

- Todo despliegue debe contar con:
  - Plan de reversión documentado.
  - Procedimiento de recuperación.
- Ante fallas críticas, se debe:
  - Activar el plan de reversión.
  - Notificar a la Oficina TIC.
  - Registrar el incidente y analizar la causa raíz.

#### 7.8.9 Lineamientos de roles y responsabilidades

- Oficina TIC:
  - Define estándares y autoriza despliegues en producción.
  - Supervisa la correcta ejecución del despliegue continuo.
- Equipo de desarrollo / proveedor:
  - Implementa y ejecuta los despliegues conforme a los lineamientos.
  - Garantiza evidencias y documentación.
- Dueños del sistema / usuarios clave:
  - Validan funcionalmente los cambios desplegados.

#### 7.8.10 Seguimiento y control

La Oficina TIC deberá:

- Verificar el cumplimiento de los lineamientos de despliegue continuo.
- Monitorear impactos posteriores a los despliegues.
- Evaluar incidentes asociados a despliegues.
- Ajustar los lineamientos según la evolución tecnológica y organizacional.

## 7.9 Plan de pruebas durante el ciclo de vida de los sistemas de información

El plan de pruebas es un componente esencial de la gestión de sistemas de información, cuyo propósito es verificar, validar y asegurar que los sistemas de información cumplan los requerimientos funcionales, técnicos, de seguridad y de calidad definidos, antes y después de su puesta en producción.

En el marco del modelo de gestión y gobierno TI (MGGTI), el plan de pruebas permite reducir riesgos operativos, prevenir fallas en los servicios institucionales y garantizar que los cambios tecnológicos generen el valor esperado para los procesos y los ciudadanos.

### 7.9.1 Objetivo del plan de pruebas

Establecer lineamientos institucionales para planear, ejecutar, documentar y aprobar las pruebas de los sistemas de información durante todo su ciclo de vida, garantizando calidad, seguridad, trazabilidad y estabilidad operativa en la alcaldía municipal de Chía.

### 7.9.2 Alcance

El plan de pruebas aplica a:

- Sistemas de información nuevos y existentes.
- Evoluciones, mejoras o modernizaciones de sistemas.
- Proyectos TI con desarrollo de software o integraciones.
- Desarrollos internos y tercerizados.

### 7.9.3 Principios del plan de pruebas

- Prevención de errores: Detectar fallas antes de producción.
- Cobertura integral: Probar funcionalidades, seguridad y desempeño.
- Trazabilidad: Cada prueba debe asociarse a requerimientos aprobados.
- Independencia: Las pruebas deben realizarse en ambientes separados.
- Evidencia: Los resultados deben documentarse.
- Gobernanza: Las pruebas deben aprobarse formalmente.

#### 7.9.4 Lineamientos para la planeación de pruebas

Todo sistema de información debe contar con un plan de pruebas que incluya, como mínimo:

- Alcance y objetivos de las pruebas.
- Tipos de pruebas a ejecutar.
- Ambientes de prueba definidos.
- Roles y responsabilidades.
- Criterios de entrada y salida.
- Cronograma de ejecución.
- Gestión de riesgos y contingencias.

El plan de pruebas debe elaborarse desde las fases tempranas del desarrollo.

#### 7.9.5 Tipos de pruebas a considerar

Pruebas funcionales:

- Verifican que el sistema cumpla los requerimientos funcionales.
- Se basan en los casos de uso y criterios de aceptación.

Pruebas no funcionales:

- Pruebas de rendimiento y carga.
- Pruebas de disponibilidad y continuidad.
- Pruebas de usabilidad y accesibilidad.

Pruebas de seguridad

- Validan controles de acceso, autenticación y autorización.
- Identifican vulnerabilidades y riesgos de seguridad.

Pruebas de integración

- Verifican la correcta interacción entre sistemas, APIs y servicios.
- Aseguran la interoperabilidad definida.

Pruebas de aceptación de usuario

- Validan que el sistema satisface las necesidades del proceso.
- Son realizadas por usuarios claves y dueños del sistema.

#### 7.9.6 Lineamientos para la ejecución de pruebas

- Las pruebas deben ejecutarse en ambientes distintos a producción.
- Los datos de prueba deben ser ficticios o anonimizados.
- Toda falla debe:
  - Registrarse.
  - Analizarse.
  - Corregirse antes de avanzar.
- No se permite avanzar a producción sin pruebas satisfactorias.

#### 7.9.7 Lineamientos para la documentación de resultados

- Cada ejecución de pruebas debe generar evidencias documentadas.
- Los resultados deben indicar:
  - Pruebas ejecutadas.
  - Pruebas exitosas y fallidas.
  - Observaciones y riesgos.
- La documentación debe almacenarse en repositorios institucionales.

#### 7.9.8 Lineamientos para aprobación y liberación

- La aprobación de las pruebas es obligatoria antes de:
  - Entrega continua.
  - Despliegue a producción.
- Debe existir acta o registro de aprobación por:
  - Oficina TIC.
  - Dueño del sistema / usuarios clave.

#### 7.9.9 Lineamientos de roles y responsabilidades

- Oficina TIC:
  - Define estándares y valida el plan de pruebas.
  - Autoriza el paso a producción.
- Equipo de desarrollo / proveedor:
  - Diseña y ejecuta las pruebas técnicas.
  - Corrige defectos identificados.
- Usuarios clave / Dueños del sistema:
  - Ejecutan pruebas de aceptación.
  - Validan el cumplimiento funcional.

#### 7.9.10 Seguimiento y mejora continua

La Oficina TIC deberá:

- Verificar la ejecución adecuada de los planes de prueba.
- Analizar defectos recurrentes.
- Incorporar lecciones aprendidas.
- Ajustar lineamientos conforme a la madurez institucional.

#### 7.10 Manual del usuario, técnico y de operación de los sistemas de información

La documentación adecuada de los sistemas de información es un elemento esencial para garantizar su uso correcto, operación continua, mantenimiento sostenible y apropiación institucional. Los manuales del usuario, técnico y de operación permiten asegurar la transferencia de conocimiento, reducir la dependencia de personas o proveedores específicos y fortalecer la continuidad del servicio tecnológico.

En el marco del modelo de gestión y gobierno TI (MGGTI), la alcaldía municipal de Chía establece la elaboración y actualización de estos manuales como un requisito obligatorio durante el ciclo de vida de los sistemas de información, articulado con la metodología de desarrollo, la gestión de servicios TI y la gestión de cambios.

##### 7.10.1 Objetivo de los manuales

Establecer lineamientos institucionales para la construcción, mantenimiento y uso de los manuales del usuario, técnico y de operación de los sistemas de información, garantizando claridad, estandarización, trazabilidad y sostenibilidad de las soluciones tecnológicas de la alcaldía municipal de Chía.

##### 7.10.2 Alcance

Estos lineamientos aplican a:

- Sistemas de información nuevos y existentes.
- Desarrollos internos y tercerizados.
- Sistemas misionales, estratégicos y de apoyo.
- Soluciones tecnológicas en operación, transición o modernización.

##### 7.10.3 Principios para la documentación de sistemas de información

- Claridad: La información debe ser comprensible para su público objetivo.

- Estandarización: Los manuales deben seguir una estructura institucional común.
- Actualización permanente: La documentación debe mantenerse vigente.
- Transferencia de conocimiento: Los manuales reducen dependencia de terceros.
- Trazabilidad: Los manuales deben reflejar la versión real del sistema.
- Accesibilidad: La documentación debe ser fácilmente consultable.

#### 7.10.4 Lineamientos generales para todos los manuales

- Todo sistema de información debe contar, como mínimo, con:
  - Manual del usuario.
  - Manual técnico.
  - Manual de operación.
- Los manuales deben elaborarse como parte del proyecto o desarrollo, no de forma posterior.
- Deben actualizarse ante:
  - Cambios funcionales relevantes.
  - Cambios técnicos o de arquitectura.
  - Cambios operativos.
- La documentación debe almacenarse en repositorios institucionales autorizados.

#### 7.10.5 Lineamientos para el manual del usuario

Propósito: Orientar a los usuarios finales en el uso correcto y eficiente del sistema.

Lineamientos de contenido mínimo:

- Objetivo y alcance del sistema.
- Perfil de usuarios.
- Requisitos básicos de acceso.
- Descripción de funcionalidades.
- Procedimientos paso a paso.
- Mensajes comunes del sistema y su significado.
- Buenas prácticas de uso.

Lineamientos de forma:

- Lenguaje claro y no técnico.
- Uso de capturas de pantalla y ejemplos.
- Estructura lógica y secuencial.

##### 7.10.5.1 Plantilla manual de usuario

**Portada:**

- Nombre del sistema de información.
- Manual del usuario.
- Dependencia responsable.
- Versión.
- Fecha.
- Logo institucional.

**Introducción:** Descripción general del sistema y propósito del manual.

**Objetivo del manual:** Explicar el objetivo del documento y a quién está dirigido.

**Alcance:** Indicar qué funcionalidades y procesos cubre el manual.

**Perfil de usuarios:**

- Tipo de usuario.
- Rol.
- Nivel de acceso.

**Requisitos para el uso del sistema:**

- Navegadores compatibles.
- Credenciales de acceso.
- Requisitos técnicos mínimos.

**Acceso al sistema:**

- URL o medio de acceso.
- Procedimiento de inicio de sesión.
- Recuperación de contraseña.

**Descripción funcional del sistema:** Descripción general de los módulos.

**Procedimientos paso a paso, para cada funcionalidad:**

- Nombre del proceso.
- Descripción.
- Pasos numerados.
- Capturas de pantalla (si aplica).

**Mensajes del sistema:**

- Mensajes informativos.
- Advertencias.
- Errores comunes y solución.

**Buenas prácticas de uso:** Recomendaciones para un uso adecuado del sistema.

**Soporte y contacto:**

- Mesa de ayuda.
- Correo / teléfono.

- Horarios de atención.

#### Control de versiones:

Versión	Fecha	Descripción del cambio	Elaboró	Aprobó
#	dd-mm-aaaa	xxxx	OPS o Líder área de desarrollo	Jefe Oficina TIC

#### Glosario (opcional).

##### 7.10.6 Lineamientos para el manual técnico

Propósito: Documentar la arquitectura, configuración y componentes técnicos del sistema.

Lineamientos de contenido mínimo:

- Descripción general del sistema.
- Arquitectura de la solución.
- Componentes de software y hardware.
- Modelos de datos relevantes.
- Integraciones y dependencias.
- Reglas de seguridad y control de accesos.
- Procedimientos de instalación y configuración.

Lineamientos de forma:

- Lenguaje técnico y preciso.
- Diagramas arquitectónicos.
- Versionamiento explícito del documento.

##### 7.10.6.1 Plantilla manual técnico

#### Portada:

- Nombre del sistema de información.
- Manual técnico.
- Dependencia responsable.
- Versión.
- Fecha.
- Logo institucional.

**Introducción:** Descripción técnica general del sistema.

**Objetivo del manual técnico:** Definir el propósito del documento y público objetivo.

**Alcance técnico:** Componentes y capas documentadas.

**Arquitectura del sistema:**

- Diagrama de arquitectura.
- Descripción de capas.
- Tecnologías utilizadas.

**Componentes del sistema:**

- Frontend.
- Backend.
- Base de datos.
- Servicios externos.

**Modelo de datos:**

- Descripción general.
- Diagramas.

**Integraciones e interoperabilidad:**

- Sistemas integrados.
- APIs / servicios.
- Protocolos y formatos.

**Seguridad del sistema:**

- Autenticación.
- Autorización.
- Gestión de roles.
- Controles de seguridad.

**Instalación y configuración:**

- Requisitos de infraestructura.
- Procedimiento de instalación.
- Variables de configuración.

**Gestión de versiones y despliegues:**

- Control de versiones.
- Flujo integración y/o despliegue.
- Ambientes definidos.

**Mantenimiento y evolución:**

- Procedimientos de actualización.
- Buenas prácticas.

**Dependencias y riesgos técnicos.**

### 7.10.7 Lineamientos para el manual de operación

Propósito: Orientar la operación diaria del sistema y asegurar su continuidad.

Lineamientos de contenido mínimo:

- Procedimientos de inicio y cierre del sistema.
- Monitoreo y verificación del servicio.
- Gestión de incidentes comunes.
- Procedimientos de respaldo y restauración.
- Manejo de fallas y contingencias.
- Contactos y escalamiento.

Lineamientos de forma:

- Instrucciones claras y accionables.
- Flujos operativos cuando aplique.
- Referencia a herramientas y roles responsables.

#### 7.10.7.1 Plantilla manual de operación

**Portada:**

- Nombre del sistema de información.
- Manual de operación.
- Dependencia responsable.
- Versión.
- Fecha.
- Logo institucional.

**Introducción:** Descripción del propósito operativo del sistema.

**Objetivo del manual de operación:** Orientar la operación diaria y asegurar continuidad.

**Alcance operativo:** Procesos operativos cubiertos.

**Roles y responsabilidades:**

- Operador.
- Administrador.
- Soporte.

**Procedimientos de operación diaria:**

- Inicio del sistema.
- Verificación de servicios.
- Cierre controlado.

**Monitoreo y control:**

- Indicadores.
- Herramientas de monitoreo.
- Alertas.

#### **Gestión de incidentes:**

- Incidentes comunes.
- Procedimiento de atención.
- Escalamiento.

#### **Respaldo y recuperación**

- Frecuencia de backups.
- Procedimiento de restauración.

#### **Gestión de cambios operativos:**

- Tipos de cambios.
- Autorizaciones.
- Registro.

#### **Continuidad del servicio:**

- Procedimientos de contingencia.
- Plan de reversión.

#### **Contactos y escalamiento**

- Mesa de ayuda.
- Oficina TIC.
- Proveedores (si aplica).

#### **Anexos (opcional).**

##### 7.10.8 Lineamientos de validación y aprobación

- Los manuales deben ser:
  - Revisados por la Oficina TIC.
  - Validados por los dueños del sistema.
- La aprobación es obligatoria antes de:
  - Puesta en producción.
  - Cierre del proyecto.
- La versión aprobada debe quedar registrada.

##### 7.10.9 Lineamientos de roles y responsabilidades

- Oficina TIC:
  - Define estándares de documentación.
  - Verifica la calidad y completitud de los manuales.

- Equipo de desarrollo / proveedor:
  - Elabora y actualiza los manuales.
  - Dueños del sistema / usuarios clave.
  - Validan la utilidad y claridad del Manual del Usuario.

#### 7.10.10 Seguimiento y mejora continua

La Oficina TIC deberá:

- Verificar periódicamente la vigencia de los manuales.
- Exigir su actualización ante cambios significativos.
- Incorporar lecciones aprendidas.
- Ajustar los lineamientos conforme a la madurez institucional.
- Fortalecer la sostenibilidad del ecosistema tecnológico.

### 7.11 Estrategia de mantenimiento de los sistemas de información

Los sistemas de información de la alcaldía municipal de Chía constituyen activos tecnológicos críticos que soportan los procesos misionales, estratégicos y de apoyo de la entidad. Su adecuado mantenimiento es fundamental para garantizar la continuidad del servicio, la seguridad de la información, la calidad de los datos y la satisfacción de los usuarios, así como para proteger la inversión institucional en tecnología.

En el marco del modelo de gestión y gobierno TI (MGGTI), la estrategia de mantenimiento de los sistemas de información, establece un enfoque integral y sistemático para asegurar que los sistemas se mantengan operativos, actualizados, seguros y alineados con las necesidades institucionales, durante todo su ciclo de vida.

#### 7.11.1 Objetivo de la estrategia de mantenimiento

Definir lineamientos institucionales para planear, ejecutar, controlar y mejorar las actividades de mantenimiento de los sistemas de información, garantizando su disponibilidad, desempeño, seguridad y sostenibilidad en la alcaldía municipal de Chía.

#### 7.11.2 Alcance

La estrategia de mantenimiento aplica a:

- Sistemas de información misionales, estratégicos y de apoyo.
- Soluciones desarrolladas internamente o adquiridas a terceros.
- Sistemas en operación, transición o proceso de modernización.

- Infraestructura tecnológica asociada directamente a los sistemas de información.

### 7.11.3 Principios de la estrategia de mantenimiento

- Continuidad del servicio: El mantenimiento debe minimizar interrupciones.
- Prevención: Priorizar acciones que eviten fallas.
- Seguridad por defecto: Proteger los sistemas frente a amenazas.
- Trazabilidad: Documentar todas las actividades de mantenimiento.
- Priorización basada en criticidad: Enfocar esfuerzos en sistemas críticos.

### 7.11.4 Tipos de mantenimiento

**Mantenimiento correctivo:** Acciones realizadas para corregir fallas o errores identificados en el sistema.

Lineamientos:

- Debe registrarse como incidente o solicitud.
- Priorizarse según impacto y urgencia.
- Documentarse la causa raíz y la solución aplicada.

**Mantenimiento preventivo:** Acciones planificadas para evitar fallas futuras.

Lineamientos:

- Actualizaciones periódicas.
- Revisión de configuraciones.
- Limpieza de datos y optimización.
- Ejecución en ventanas de mantenimiento.

**Mantenimiento evolutivo:** Mejoras o ampliaciones funcionales del sistema.

Lineamientos:

- Debe derivarse de requerimientos aprobados.
- Gestionarse como proyecto o cambio formal.
- Pasar por pruebas y aprobación antes de producción.

**Mantenimiento adaptativo:** Ajustes requeridos por cambios normativos, tecnológicos o del entorno.

Lineamientos:

- Debe analizarse impacto legal y técnico.
- Priorizarse cuando afecte cumplimiento normativo.

#### 7.11.5 Lineamientos para la planificación del mantenimiento

- Cada sistema debe contar con un plan de mantenimiento.
- El plan debe incluir:
  - Tipo de mantenimiento.
  - Frecuencia.
  - Responsables.
  - Ventanas de ejecución.
- El plan debe alinearse con la criticidad del sistema.

Tabla No. 9 Matriz de mantenimiento de los sistemas de información

Sistema de Información	Proceso que Soporta	Criticidad	Tipo de Mantenimiento	Descripción de la Actividad	Frecuencia	Ventana de Mantenimiento	Responsable	Soporte / Proveedor
Sistema PQRS	Atención al ciudadano	Alta	Preventivo	Actualización de componentes y revisión de logs	Trimestral	Nocturna	Atención al ciudadano / Oficina TIC	Proveedor
Sistema Predial	Gestión tributaria	Alta	Correctivo	Corrección de error en cálculo	Bajo demanda	Programada	Sec. Hacienda / Proveedor	Proveedor
Sistema documental	Gestión documental	Media	Evolutivo	Mejora en búsqueda de documentos	Semestral	Programada	Servicios administrativos / Oficina TIC	Proveedor
Sistema talento humano	Gestión del talento	Media	Adaptativo	Ajuste por cambio normativo	Según norma	Programada	Dirección función pública / Oficina TIC	Proveedor

#### 7.11.6 Lineamientos de priorización y criticidad

- Los sistemas deben clasificarse según:
  - Impacto en procesos misionales.
  - Afectación al ciudadano.
  - Riesgos de seguridad.

- Los sistemas críticos deben tener:
  - Mayor frecuencia de mantenimiento.
  - Planes de contingencia definidos.

Tabla No. 10 Clasificación de criticidad (referencia)

Nivel	Descripción
Alta	Impacta procesos misionales o atención al ciudadano
Media	Impacta procesos internos estratégicos
Baja	Impacto limitado o administrativo

Tabla No. 11 Ejemplo matriz de priorización del mantenimiento

Sistema	Criticidad	Impacto al Ciudadano	Riesgo de Seguridad	Prioridad de Mantenimiento
PQRS	Alta	Alto	Medio	Alta
Predial	Alta	Alto	Alto	Alta
Documental	Media	Medio	Bajo	Media
Talento Humano	Media	Bajo	Medio	Media

#### 7.11.7 Lineamientos de seguridad y control

- Toda actividad de mantenimiento debe:
  - Cumplir las políticas de seguridad de la información.
  - Gestionarse mediante la gestión de cambios.
- Los accesos para mantenimiento deben:
  - Ser temporales.
  - Estar registrados y controlados.

#### 7.11.8 Lineamientos de documentación y trazabilidad

- Toda actividad de mantenimiento debe documentarse, indicando:
  - Fecha.
  - Tipo de mantenimiento.
  - Componentes afectados.
  - Responsable.
  - Resultado.
- La documentación debe almacenarse en repositorios institucionales.

Tabla No. 12 Ejemplo matriz de control y trazabilidad del mantenimiento

Sistema	Fecha	Tipo de Mantenimiento	Actividad Realizada	Incidente Asociado	Resultado	Aprobado por	Evidencia
PQRS	15/03/2026	Preventivo	Actualización librerías	N/A	Exitoso	Oficina TIC	Acta / Registro
Predial	22/04/2026	Correctivo	Corrección bug cálculo	INC-045	Exitoso	Oficina TIC	Ticket cerrado

#### 7.11.9 Lineamientos de roles y responsabilidades

- Oficina TIC:
  - Define la estrategia y estándares de mantenimiento.
  - Supervisa la ejecución y cumplimiento.
- Equipo técnico / proveedor:
  - Ejecuta las actividades de mantenimiento.
  - Reporta resultados y riesgos.
- Dueño del sistema:
  - Prioriza necesidades de mantenimiento.
  - Valida impactos funcionales.

Tabla No. 13 Matriz de responsabilidades (RACI – Mantenimiento)

Actividad	Oficina TIC	Proveedor	Dueño del Sistema
Planificar mantenimiento	R	C	A
Ejecutar mantenimiento	C	R	I
Validar resultado	A	C	R
Autorizar paso a producción	A	I	C
Documentar mantenimiento	R	R	I

R: Responsable, A: Aprueba, C: Consulta, I: Informa

#### 7.11.10 Seguimiento y mejora continua

La Oficina TIC deberá:

- Monitorear indicadores de mantenimiento (incidentes, disponibilidad).
- Analizar fallas recurrentes.
- Actualizar planes de mantenimiento.
- Incorporar lecciones aprendidas.

## 7.12 Servicios de mantenimiento de sistemas de información con terceras partes

La contratación de servicios de mantenimiento de sistemas de información con terceras partes es una práctica necesaria para asegurar la continuidad, sostenibilidad y evolución de las soluciones tecnológicas de la alcaldía municipal de Chía, especialmente cuando se requiere conocimiento especializado, soporte del fabricante o capacidad técnica adicional.

En el marco del modelo de gestión y gobierno TI (MGGTI), estos servicios deben gestionarse bajo criterios estrictos de gobernanza, control, seguridad, trazabilidad y alineación estratégica, garantizando que el mantenimiento tercerizado proteja los activos de información, la continuidad del servicio y el interés público.

### 7.12.1 Objetivo de los servicios de mantenimiento con terceros

Establecer lineamientos institucionales para la contratación, gestión, control y evaluación de los servicios de mantenimiento de sistemas de información prestados por terceras partes, asegurando calidad, seguridad, continuidad operativa y transferencia de conocimiento.

### 7.12.2 Alcance

Estos lineamientos aplican a:

- Contratos de mantenimiento correctivo, preventivo, evolutivo o adaptativo.
- Sistemas de información misionales, estratégicos y de apoyo.
- Proveedores de software, fábricas de desarrollo, fabricantes o integradores.
- Servicios prestados en modalidad presencial, remota o mixta.

### 7.12.3 Principios para la gestión de servicios con terceros

- Gobernanza institucional: La Oficina TIC mantiene el control técnico.
- Transparencia contractual: Los alcances y obligaciones deben ser claros.
- Seguridad y confidencialidad: Protección de la información institucional.
- Continuidad del servicio: Evitar dependencias críticas del proveedor.
- Transferencia de conocimiento: Asegurar apropiación institucional.
- Evaluación permanente: Medir desempeño y cumplimiento.

### 7.12.4 Lineamientos para la definición del alcance contractual

Los contratos de mantenimiento deben definir claramente:

- Tipo de mantenimiento incluido.

- Sistemas de información cubiertos.
- Componentes técnicos y funcionales.
- Acuerdos de niveles de servicio (SLA).
- Horarios y tiempos de atención.
- Mecanismos de escalamiento.
- Entregables y reportes.

No se permitirán contratos con alcances ambiguos o no medibles.

#### 7.12.5 Lineamientos de seguridad y confidencialidad

- Todo proveedor debe:
  - Firmar acuerdos de confidencialidad.
  - Cumplir las políticas de seguridad de la información y seguridad digital.
- Los accesos otorgados deben:
  - Ser mínimos y temporales.
  - Estar registrados y auditados.
- Está prohibido el uso no autorizado de datos institucionales.

#### 7.12.6 Lineamientos para la gestión de accesos y ambientes

- Los proveedores deben trabajar en ambientes definidos y controlados.
- El acceso a producción solo se permite:
  - Con autorización expresa.
  - Bajo supervisión de la Oficina TIC.
- Todo cambio debe gestionarse mediante la gestión de cambios.

#### 7.12.7 Lineamientos para la ejecución del mantenimiento

- Las actividades de mantenimiento deben:
  - Estar programadas y documentadas.
  - Ajustarse a ventanas de mantenimiento.
- Los mantenimientos correctivos críticos deben:
  - Atenderse con prioridad definida en el SLA.
  - No se permiten modificaciones informales o no documentadas.

#### 7.12.8 Lineamientos para la documentación y transferencia de conocimiento

- El proveedor debe entregar:
  - Reportes de mantenimiento.
  - Actualizaciones de manuales técnicos y operativos.

- Se debe asegurar la transferencia de conocimiento al personal institucional.
- La documentación entregada es propiedad de la alcaldía municipal de Chía.

#### 7.12.9 Lineamientos de seguimiento y control del servicio

- La Oficina TIC debe:
  - Monitorear el cumplimiento del SLA.
  - Evaluar la calidad del servicio prestado.
  - Registrar incidentes y desviaciones.
- Los incumplimientos deben generar:
  - Acciones correctivas.
  - Penalidades contractuales cuando aplique.

#### 7.12.10 Lineamientos de evaluación y cierre contractual

- Al cierre del contrato se debe:
  - Evaluar el desempeño del proveedor.
  - Verificar la entrega completa de documentación.
  - Revocar accesos otorgados.
- Los resultados deben alimentar decisiones futuras de contratación.

### 7.13 Plan de calidad de los sistemas de información

La calidad de los sistemas de información es un factor determinante para la eficiencia institucional, la continuidad de los servicios, la seguridad de la información y la confianza de los ciudadanos. Un sistema que no cumple criterios de calidad genera reprocesos, riesgos operativos, fallas de seguridad y bajo nivel de adopción por parte de los usuarios.

En este contexto, la alcaldía municipal de Chía establece el plan de calidad de los sistemas de información como un instrumento del modelo de gestión y gobierno TI, que define los lineamientos, criterios, actividades y responsabilidades, para asegurar que los sistemas de información, cumplan estándares mínimos de calidad durante todo su ciclo de vida.

#### 7.13.1 Objetivo del plan de calidad

Establecer lineamientos institucionales para planificar, asegurar, evaluar y mejorar la calidad de los sistemas de información, de la alcaldía municipal de Chía, garantizando su alineación estratégica, confiabilidad, seguridad, usabilidad y sostenibilidad.

### 7.13.2 Alcance

El plan de calidad aplica a:

- Sistemas de información misionales, estratégicos y de apoyo.
- Sistemas nuevos, en evolución o en mantenimiento.
- Desarrollos internos y tercerizados.
- Componentes de software, integraciones y servicios tecnológicos asociados.

### 7.13.3 Principios de calidad

- Calidad por diseño: La calidad debe incorporarse desde las etapas iniciales.
- Enfoque en el usuario: Los sistemas deben responder a necesidades reales.
- Prevención de errores: Priorizar controles tempranos.
- Trazabilidad: Todo requisito debe verificarse.
- Mejora continua: La calidad se evalúa y ajusta permanentemente.

### 7.13.4 Dimensiones de la calidad de los sistemas de información

La calidad de los sistemas de información debe evaluarse, como mínimo, en las siguientes dimensiones:

- Funcionalidad: Cumplimiento de requerimientos.
- Confiabilidad: Estabilidad y correcto funcionamiento.
- Disponibilidad: Acceso oportuno al sistema.
- Seguridad: Protección de la información y los accesos.
- Usabilidad: Facilidad de uso y experiencia del usuario.
- Rendimiento: Tiempos de respuesta adecuados.
- Mantenibilidad: Facilidad para corregir y evolucionar el sistema.
- Interoperabilidad: Capacidad de integrarse con otros sistemas.

### 7.13.5 Lineamientos para la planificación de la calidad

- Todo sistema de información debe contar con un plan de calidad específico o estar cubierto por este plan institucional.
- El plan de calidad debe definir:
  - Criterios de calidad aplicables.
  - Actividades de aseguramiento.
  - Indicadores de calidad.
  - Roles y responsabilidades.
- La planificación de la calidad debe realizarse desde la fase de análisis de requerimientos.

### 7.13.6 Lineamientos para el aseguramiento de la calidad

- La calidad debe asegurarse mediante:
  - Revisión de requerimientos.
  - Pruebas funcionales y no funcionales.
  - Validaciones de seguridad.
  - Cumplimiento de la guía de estilo y usabilidad.
- No se permite el paso a producción sin evidencias de calidad satisfactorias.

### 7.13.7 Lineamientos para el control y verificación de la calidad

- Se deben realizar controles periódicos de calidad en:
  - Desarrollo.
  - Pruebas.
  - Producción.
- Las no conformidades deben:
  - Registrarse.
  - Analizarse.
  - Corregirse mediante planes de mejora.
- Los resultados deben documentarse.

### 7.13.8 Lineamientos de indicadores de calidad

El plan de calidad debe incluir indicadores, tales como:

- Porcentaje de requerimientos cumplidos.
- Número de defectos en producción.
- Disponibilidad del sistema.
- Tiempo promedio de atención de incidentes.
- Nivel de satisfacción de usuarios.

Tabla No. 14 Matriz de criterios e indicadores de calidad

Dimensión de Calidad	Criterio de Calidad	Indicador	Fórmula / Medición	Frecuencia	Meta	Responsable	Fuente de Información
Funcionalidad	Cumplimiento de requerimientos	% de requerimientos cumplidos	$(\text{Req. cumplidos} / \text{Req. totales}) \times 100$	Trimestral	$\geq 95\%$	Oficina TIC / Proveedor	Actas de pruebas
Funcionalidad	Incidencias funcionales	Nº defectos funcionales en	Conteo	Mensual	$\leq 3$	Oficina TIC / Proveedor	Mesa de ayuda

Dimensión de Calidad	Criterio de Calidad	Indicador	Fórmula / Medición	Frecuencia	Meta	Responsable	Fuente de Información
		producción					
Confiabilidad	Estabilidad del sistema	N° caídas no programadas	Conteo	Mensual	$\leq 1$	Oficina TIC / Proveedor	Monitoreo
Disponibilidad	Disponibilidad del servicio	% de disponibilidad	$(\text{Horas disponibles} / \text{Horas totales}) \times 100$	Mensual	$\geq 99\%$	Oficina TIC / Proveedor	Herramientas monitoreo
Seguridad	Incidentes de seguridad	N° incidentes de seguridad	Conteo	Mensual	0	Oficina TIC / Proveedor	Reportes de seguridad
Seguridad	Cumplimiento de controles	% controles de seguridad cumplidos	$(\text{Controles cumplidos} / \text{Totales}) \times 100$	Semestral	100%	Oficina TIC / Proveedor	Auditorías
Usabilidad	Satisfacción del usuario	Nivel de satisfacción	Encuesta (escala 1-5)	Semestral	$\geq 4$	Oficina TIC	Encuestas
Usabilidad	Errores de uso	N° errores por mal uso	Conteo	Trimestral	Tendencia a la baja	Oficina TIC	Mesa de ayuda
Rendimiento	Tiempo de respuesta	Tiempo promedio de respuesta	Segundos	Mensual	$\leq 3$ seg	Oficina TIC	Pruebas técnicas
Mantenibilidad	Tiempo de corrección	Tiempo promedio de solución	Horas / días	Mensual	$\leq$ SLA	Oficina TIC / Proveedor	Tickets
Interoperabilidad	Integraciones operativas	% integraciones funcionando	$(\text{Integraciones OK} / \text{Totales}) \times 100$	Trimestral	100%	Oficina TIC / Proveedor	Reportes técnicos
Continuidad	Recuperación del servicio	Tiempo de recuperación (RTO)	Horas	Anual / Incidente	$\leq$ definido	Oficina TIC / Proveedor	Pruebas DRP

### 7.13.9 Lineamientos de roles y responsabilidades

- Oficina TIC:

Carrera 7 N° 12-100  
PBX: (601) 884 4444 Ext. 2300-2301  
oficinatic@chia.gov.co  
www.chia-cundinamarca.gov.co

- Define estándares y supervisa el cumplimiento del plan de calidad.
- Equipos de desarrollo / proveedores:
  - Aplican controles y generan evidencias de calidad.
- Dueños del sistema / usuarios clave:
  - Validan la calidad funcional y la usabilidad.

#### 7.13.10 Seguimiento y mejora continua

La Oficina TIC deberá:

- Evaluar periódicamente la calidad de los sistemas.
- Analizar tendencias y causas raíz de defectos.
- Proponer acciones de mejora.
- Actualizar el plan de calidad conforme a la madurez institucional.

### 7.14 Requerimientos no funcionales y atributos calidad de los sistemas de Información

Los requerimientos no funcionales y los atributos de calidad definen cómo debe comportarse un sistema de información y bajo qué condiciones debe operar, complementando los requerimientos funcionales que describen qué hace el sistema. Estos requerimientos son determinantes para asegurar la calidad, seguridad, desempeño, disponibilidad y sostenibilidad de los sistemas de información institucionales.

En el marco del modelo de gestión y gobierno TI (MGGTI), la definición adecuada de los requerimientos no funcionales y atributos de calidad permite reducir riesgos tecnológicos, garantizar continuidad del servicio, proteger la información y asegurar que los sistemas de información de la alcaldía municipal de Chía, cumplan estándares mínimos de calidad durante todo su ciclo de vida.

#### 7.14.1 Objetivo

Establecer lineamientos institucionales para identificar, definir, documentar, validar y controlar los requerimientos no funcionales y los atributos de calidad de los sistemas de información, garantizando coherencia, trazabilidad y alineación con el gobierno TI y el modelo de arquitectura empresarial.

#### 7.14.2 Alcance

Estos lineamientos aplican a:

- Sistemas de información nuevos y existentes.

- Proyectos de desarrollo, mantenimiento o modernización.
- Desarrollos internos y tercerizados.
- Integraciones, servicios digitales y plataformas tecnológicas.

#### 7.14.3 Principios para la definición de requerimientos no funcionales y atributos de calidad

- Calidad desde el diseño: Los requerimientos no funcionales deben definirse desde el análisis de requerimientos.
- Alineación al riesgo: Los requerimientos no funcionales deben responder a la criticidad del sistema.
- Trazabilidad: Los requerimientos no funcionales deben asociarse a procesos, riesgos y objetivos institucionales.
- Mejora continua: Los requerimientos no funcionales pueden ajustarse según madurez y contexto.

#### 7.14.4 Lineamientos para la identificación de requerimientos no funcionales

- Los requerimientos no funcionales deben identificarse a partir de:
  - Análisis de procesos institucionales.
  - Riesgos operativos y de seguridad.
  - Políticas institucionales (Seguridad de la información, gobierno digital, seguridad digital).
  - Normatividad aplicable.
- Todo sistema debe contar con requerimientos no funcionales mínimos obligatorios definidos por la Oficina TIC.

#### 7.14.5 Atributos de calidad institucionales

**Disponibilidad:** Capacidad del sistema para estar accesible cuando se requiere.

- Ejemplo de requerimiento no funcional:
  - El sistema debe tener una disponibilidad mínima del 99% mensual.

**Rendimiento:** Capacidad del sistema para responder en tiempos adecuados.

- Ejemplo de requerimiento no funcional:
  - El tiempo de respuesta no debe superar los 3 segundos en condiciones normales.

**Seguridad:** Protección de la información y control de accesos.

- Ejemplo de requerimiento no funcional:
  - El sistema debe implementar autenticación y control de accesos por roles.

**Usabilidad:** Facilidad de uso y experiencia del usuario.

- Ejemplo de requerimiento no funcional:

- El sistema debe cumplir la guía de estilo y usabilidad institucional.

Confiabilidad: Capacidad del sistema para operar sin fallas.

- Ejemplo de requerimiento no funcional:
  - El sistema no debe presentar más de una caída no programada al mes.

Mantenibilidad: Facilidad para corregir, actualizar o evolucionar el sistema.

- Ejemplo de requerimiento no funcional:
  - El sistema debe permitir actualizaciones sin afectar la operación productiva.

Escalabilidad: Capacidad del sistema para crecer ante mayor demanda.

- Ejemplo de requerimiento no funcional:
  - El sistema debe soportar un incremento del 30% de usuarios sin degradación.

Interoperabilidad: Capacidad de integrarse con otros sistemas.

- Ejemplo de requerimiento no funcional:
  - El sistema debe exponer servicios de integración conforme a estándares definidos.

Continuidad: Capacidad de recuperación ante fallas.

- Ejemplo de requerimiento no funcional:
  - El sistema debe recuperarse en un tiempo máximo definido (RTO).

#### 7.14.6 Lineamientos para la documentación de requerimientos no funcionales

- Todo requerimiento no funcional debe documentarse indicando:
  - Identificador único.
  - Atributo de calidad asociado.
  - Descripción clara.
  - Métrica y valor objetivo.
  - Método de verificación.
- Los requerimientos no funcionales deben incluirse en la matriz de requerimientos institucional.

#### 7.14.7 Lineamientos para la validación y aprobación

- Los requerimientos no funcionales deben ser:
  - Validados por la Oficina TIC.
  - Aprobados por el dueño del sistema.
- La aprobación de los requerimientos no funcionales es obligatoria antes del diseño y desarrollo.

- Los requerimientos no funcionales aprobados constituyen una línea base de calidad.

#### 7.14.8 Lineamientos para el seguimiento y control

- El cumplimiento de los requerimientos no funcionales debe verificarse mediante:
  - Pruebas técnicas.
  - Indicadores de calidad.
  - Monitoreo en producción.
- El incumplimiento de los requerimientos no funcionales debe generar:
  - Acciones correctivas.
  - Planes de mejora.
  - Gestión de cambios cuando aplique.

#### 7.14.9 Roles y responsabilidades

- Oficina TIC:
  - Define requerimientos no funcionales mínimos institucionales.
  - Supervisa su cumplimiento.
- Dueños del sistema:
  - Priorizan requerimientos no funcionales según impacto del proceso.
- Equipos de desarrollo / proveedores:
  - Implementan los requerimientos no funcionales definidos.

### 7.15 Accesibilidad

La accesibilidad en los sistemas de información es un principio fundamental del gobierno digital y un requisito clave para garantizar el acceso equitativo a los servicios digitales, la inclusión social y el ejercicio pleno de los derechos de los ciudadanos, independientemente de sus condiciones físicas, sensoriales, cognitivas, tecnológicas o contextuales.

En el marco del modelo de gestión y gobierno TI, la alcaldía municipal de Chía adopta la accesibilidad como un criterio obligatorio de calidad en el diseño, desarrollo, adquisición, operación y evolución de sus sistemas de información, asegurando que estos puedan ser utilizados por la mayor cantidad de personas posible, sin barreras indebidas.

#### 7.15.1 Objetivo

Establecer lineamientos institucionales para garantizar la accesibilidad de los sistemas de información de la alcaldía municipal de Chía, promoviendo soluciones digitales inclusivas, usables y alineadas con los estándares de calidad, durante todo su ciclo de vida.

### 7.15.2 Alcance

Estos lineamientos aplican a:

- Sistemas de información misionales, estratégicos y de apoyo.
- Portales web, aplicaciones internas y externas.
- Sistemas nuevos, en mantenimiento o modernización.
- Desarrollos internos y soluciones provistas por terceros.

### 7.15.3 Principios de accesibilidad

- Inclusión: Los sistemas deben poder ser utilizados por todas las personas.
- Diseño universal: Considerar la diversidad desde el diseño inicial.
- Equidad: Ofrecer igualdad de acceso a la información y los servicios.
- Usabilidad: Facilitar la interacción y comprensión.
- Calidad: La accesibilidad es parte integral de la calidad del sistema.
- Gobernanza: La accesibilidad debe gestionarse y evaluarse.

### 7.15.4 Lineamientos generales de accesibilidad

- La accesibilidad debe considerarse desde la fase de análisis de requerimientos.
- Todo sistema de información debe incorporar criterios mínimos de accesibilidad.
- La accesibilidad aplica tanto a interfaces gráficas como a contenidos digitales.
- No se permitirá la puesta en producción de sistemas que ignoren criterios básicos de accesibilidad, salvo justificación técnica debidamente documentada.

### 7.15.5 Lineamientos de accesibilidad funcional y visual

Los sistemas de información deben:

- Permitir navegación mediante teclado.
- Ofrecer contraste adecuado entre texto y fondo.
- Usar tamaños de fuente legibles y escalables.
- Evitar depender exclusivamente del color para transmitir información.
- Incorporar textos alternativos en imágenes y elementos gráficos.

### 7.15.6 Lineamientos de accesibilidad cognitiva y de contenido

- Utilizar lenguaje claro, sencillo y coherente.

- Evitar textos excesivamente técnicos para usuarios finales.
- Estructurar la información de forma lógica y predecible.
- Proveer mensajes de error comprensibles y orientados a la solución.

#### 7.15.7 Lineamientos de accesibilidad tecnológica

- Garantizar compatibilidad con lectores de pantalla y tecnologías de asistencia.
- Evitar dependencias tecnológicas que limiten el acceso.
- Asegurar funcionamiento en navegadores y dispositivos comunes.
- Considerar condiciones de conectividad variable.

#### 7.15.8 Lineamientos para la validación y pruebas de accesibilidad

- La accesibilidad debe validarse mediante:
  - Pruebas funcionales.
  - Revisión de cumplimiento de criterios de accesibilidad.
  - Pruebas con usuarios cuando sea posible.
- Los resultados deben documentarse como parte del plan de pruebas y del plan de calidad.

#### 7.15.9 Lineamientos para desarrollos y proveedores

- Los contratos de desarrollo o adquisición de software deben:
  - Incluir requisitos explícitos de accesibilidad.
  - Exigir cumplimiento de estándares definidos por la entidad.
- El incumplimiento de requisitos de accesibilidad debe considerarse no conformidad.

#### 7.15.10 Lineamientos de roles y responsabilidades

- Oficina TIC:
  - Define criterios mínimos de accesibilidad.
  - Verifica su cumplimiento antes de producción.
- Dueños del sistema / áreas usuarias:
  - Validan la accesibilidad desde la perspectiva del usuario.
- Equipos de desarrollo / proveedores:
  - Implementan los criterios de accesibilidad definidos.

#### 7.15.11 Seguimiento y mejora continua

La Oficina TIC deberá:

- Evaluar periódicamente el nivel de accesibilidad de los sistemas.
- Incorporar observaciones y retroalimentación de usuarios.
- Actualizar criterios conforme a avances tecnológicos y normativos.
- Promover la sensibilización institucional sobre accesibilidad digital.

## 7.16 Arquitectura de software

La arquitectura de software define la estructura fundamental de los sistemas de información, sus componentes, relaciones, principios de diseño y decisiones técnicas que condicionan su evolución, calidad y sostenibilidad. Una arquitectura mal definida incrementa los riesgos operativos, la dependencia tecnológica, los costos de mantenimiento y las dificultades de integración.

En el marco del modelo de gestión y gobierno TI, la alcaldía municipal de Chía adopta la arquitectura de software como un elemento estratégico de control y alineación, asegurando que los sistemas de información se diseñen y evolucionen de forma coherente con el modelo de arquitectura empresarial, la estrategia de TI y las necesidades institucionales.

### 7.16.1 Objetivo

Establecer lineamientos institucionales para la definición, documentación, implementación y control de la arquitectura de software de los sistemas de información de la alcaldía municipal de Chía, garantizando calidad, interoperabilidad, seguridad y sostenibilidad tecnológica durante su ciclo de vida.

### 7.16.2 Alcance

Estos lineamientos aplican a:

- Sistemas de información nuevos y existentes.
- Desarrollos internos y soluciones adquiridas o tercerizadas.
- Aplicaciones misionales, estratégicas y de apoyo.
- Componentes de software, integraciones y servicios tecnológicos asociados.

### 7.16.3 Principios de la arquitectura de software

- Alineación estratégica: Debe soportar los objetivos del PETIC y del MAE.
- Modularidad: Los sistemas deben estructurarse en componentes desacoplados.
- Interoperabilidad: Facilitar la integración con otros sistemas.

- Escalabilidad: Permitir crecimiento funcional y técnico.
- Seguridad por diseño: Incorporar controles desde la arquitectura.
- Sostenibilidad: Facilitar mantenimiento y evolución.
- Gobernanza: Las decisiones arquitectónicas deben ser controladas.

#### 7.16.4 Lineamientos para la definición de la arquitectura de software

- Todo sistema de información debe contar con una arquitectura de software definida y documentada.
- La arquitectura debe:
  - Responder a requerimientos funcionales y no funcionales.
  - Incorporar atributos de calidad definidos institucionalmente.
- Las decisiones arquitectónicas críticas deben:
  - Justificarse.
  - Documentarse.
  - Ser aprobadas por la Oficina TIC.

#### 7.16.5 Lineamientos de estilos y patrones arquitectónicos

- La selección del estilo arquitectónico debe basarse en:
  - Complejidad del sistema.
  - Criticidad del proceso soportado.
  - Necesidades de integración y escalabilidad.
- Se podrán adoptar, entre otros:
  - Arquitecturas en capas.
  - Arquitecturas orientadas a servicios.
  - Arquitecturas basadas en eventos.
- No se permite la adopción de estilos que generen dependencias tecnológicas no controladas.

#### 7.16.6 Lineamientos para la documentación de la arquitectura

La arquitectura de software debe documentarse incluyendo, como mínimo:

- Descripción general del sistema.
- Diagramas de arquitectura (lógica y física).
- Componentes y responsabilidades.
- Flujos de información e integración.
- Tecnologías utilizadas.
- Consideraciones de seguridad y calidad.

La documentación debe mantenerse actualizada durante todo el ciclo de vida.

#### 7.16.7 Lineamientos de integración e interoperabilidad

- La arquitectura debe facilitar:
  - Integración con otros sistemas institucionales.
  - Intercambio seguro de información.
- Se deben usar estándares definidos por la Oficina TIC.
- Las integraciones deben documentarse y versionarse.

#### 7.16.8 Lineamientos de seguridad en la arquitectura

- La arquitectura debe incorporar:
  - Control de accesos por roles.
  - Segregación de ambientes.
  - Protección de datos sensibles.
- Las decisiones de seguridad deben alinearse con:
  - Políticas de seguridad de la información
  - Políticas de seguridad digital.

#### 7.16.9 Lineamientos de escalabilidad y rendimiento

- La arquitectura debe considerar:
  - Crecimiento en número de usuarios.
  - Incremento en volumen de datos.
- Debe permitir ajustes sin rediseños completos.
- Los mecanismos de escalabilidad deben documentarse.

#### 7.16.10 Lineamientos para el control de cambios arquitectónicos

Todo cambio significativo en la arquitectura debe:

- Gestionarse mediante la gestión de cambios.
- Evaluar impacto técnico y de negocio.
- Actualizar la documentación arquitectónica.

#### 7.16.11 Lineamientos de roles y responsabilidades

- Oficina TIC:
  - Define estándares arquitectónicos.
  - Aprueba arquitecturas y cambios relevantes.
- Arquitectos / equipos de desarrollo / proveedores:
  - Diseñan e implementan la arquitectura conforme a los lineamientos.

- Dueños del sistema:
  - Validan la alineación de la arquitectura con el proceso.

#### 7.16.12 Seguimiento y mejora continua

La Oficina TIC deberá:

- Evaluar periódicamente la adecuación de las arquitecturas.
- Identificar obsolescencia tecnológica.
- Promover la estandarización y reutilización.
- Ajustar lineamientos conforme a la madurez institucional.

#### 7.16.13 Representación conceptual arquitectura por capas

Los sistemas de información de la alcaldía de Chía se estructuran por capas, garantizando separación de responsabilidades, seguridad, escalabilidad y sostenibilidad.

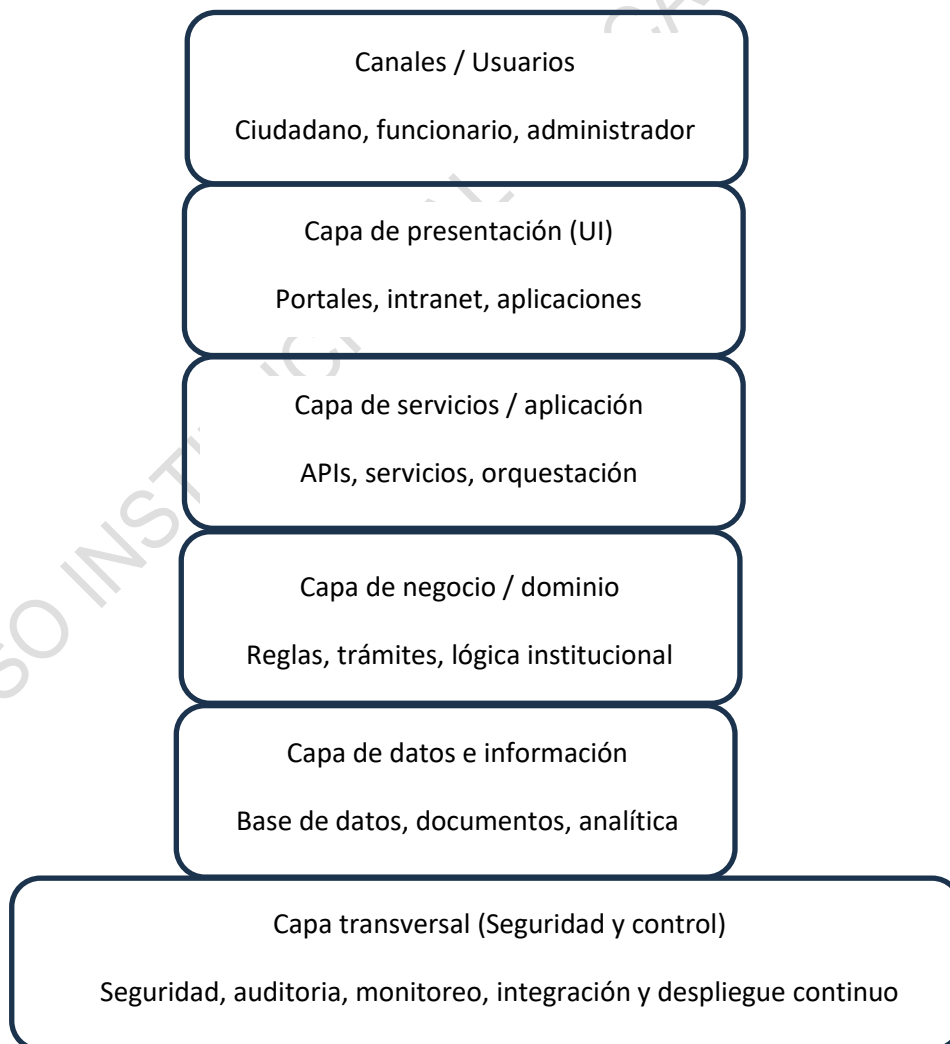


Ilustración No. 2. Representación arquitectura por capas (Elaboración propia)

7.16.14 Representación arquitectura por componentes

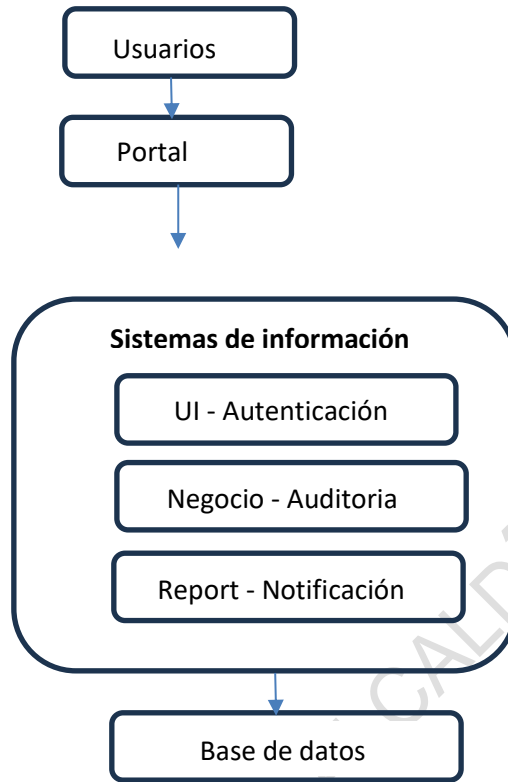


Ilustración No. 3. Representación arquitectura por componentes (Elaboración propia)

7.16.15 Arquitectura de integración e interoperabilidad

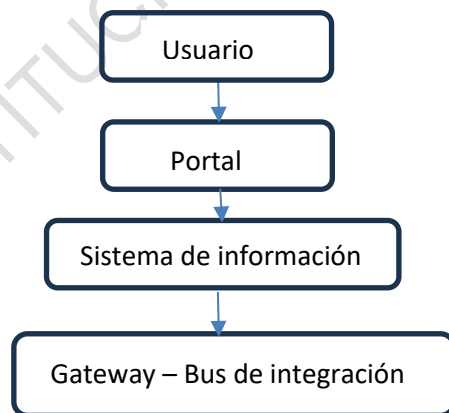


Ilustración No. 4. Representación arquitectura de integración

## 8 Gestión de servicios TI

La gestión de servicios de tecnologías de la información (TI) constituye un componente esencial del modelo de gestión y gobierno TI de la alcaldía municipal de Chía, teniendo en cuenta que permite garantizar que los servicios tecnológicos sean planeados, diseñados, entregados, soportados y mejorados de manera estructurada, eficiente y alineada con los objetivos institucionales y las necesidades de los ciudadanos y usuarios internos.

En el marco del gobierno digital y la arquitectura empresarial, la gestión de servicios de TI trasciende la operación técnica de la infraestructura y los sistemas de información, para consolidarse como un enfoque orientado a la generación de valor público, donde la tecnología actúa como habilitador estratégico de los procesos misionales, estratégicos y de apoyo de la entidad, estableciendo los lineamientos para administrar el ciclo de vida de los servicios de TI, desde su identificación y estructuración en el catálogo de servicios TI, pasando por la transición, operación y soporte, hasta el seguimiento al cumplimiento de los acuerdos de niveles de servicios definidos teniendo en cuenta la disponibilidad, capacidad, seguridad y continuidad de los servicios TI.

La gestión de servicios de TI en la alcaldía de Chía se fundamenta en un modelo orientado a las buenas prácticas internacionales reconocidas como ITIL y COBIT, y adaptado al contexto institucional, al nivel de madurez de la oficina TIC y a las directrices establecidas por el ministerio de tecnologías de la información y las comunicaciones (MinTIC), buscando promover la estandarización, la trazabilidad, la mejora continua y la optimización del uso de los recursos tecnológicos, contribuyendo a una prestación de servicios confiable, transparente y sostenible.

La gestión de servicios TI, se articula de manera directa con el catálogo de servicios de la Oficina TIC, el cual constituye el instrumento central para la identificación, clasificación y comunicación de la oferta de servicios tecnológicos disponibles para la entidad, permitiendo una gestión clara de responsabilidades, expectativas y niveles de servicio, y fortaleciendo la relación entre la Oficina TIC y las demás dependencias de la administración municipal, orientado a mejorar la experiencia del usuario, asegurar la continuidad operativa, reducir riesgos tecnológicos y apoyar de manera efectiva la transformación digital y la modernización institucional.

### 8.1 Lineamientos generales para la gestión de los servicios de TI

La gestión de servicios de tecnologías de la información (TI), permite asegurar que los servicios tecnológicos de la alcaldía municipal de Chía sean definidos, entregados, soportados y mejorados de manera estructurada, garantizando su alineación con los objetivos institucionales, la continuidad operativa y la satisfacción de los usuarios internos y externos.

Se debe reconocer a la tecnología como un habilitador del valor público, donde los servicios de TI se deben adoptar y responder de forma eficiente, oportuna y segura a las necesidades de los procesos misionales, estratégicos y de apoyo de la entidad, así como a los compromisos de gobierno digital.



Ilustración No.5 Ciclo de vida de adopción de TI (Elaboración propia)

#### 8.1.1 Objetivo de la gestión de servicios de TI

Establecer lineamientos institucionales para planificar, diseñar, entregar, operar, controlar y mejorar los servicios de TI de la alcaldía municipal de Chía, asegurando calidad, disponibilidad, seguridad, trazabilidad y alineación la estrategia institucional.

#### 8.1.2 Alcance

La gestión de servicios de TI aplica a:

- Todos los servicios tecnológicos prestados por la Oficina TIC.
- Servicios orientados a usuarios internos y externos.
- Servicios asociados a infraestructura, sistemas de información, soporte, seguridad digital y de la información e integración.
- Servicios prestados directamente por la entidad o a través de terceros.

#### 8.1.3 Principios de la gestión de servicios de TI

- Orientación al servicio: La tecnología se gestiona en función del valor que presta a la entidad y al ciudadano.
- Alineación estratégica: Los servicios de TI deben apoyar los objetivos institucionales.

- Calidad y continuidad: Los servicios deben ser confiables y disponibles.
- Transparencia: Los servicios, responsabilidades y niveles de atención deben ser claros.
- Gobernanza: La gestión de servicios se realiza bajo reglas, roles y controles definidos.
- Mejora continua: Los servicios deben evaluarse y evolucionar permanentemente.

#### 8.1.4 Definición lineamientos generales

- Todos los servicios de TI deben estar formalmente definidos en el catálogo de servicios de tecnología.
- La gestión de servicios debe cubrir todo el ciclo de vida, desde la definición hasta su mejora continua.
- Ningún servicio tecnológico podrá prestarse de manera informal o no documentada.
- Los servicios críticos deben contar con niveles de servicio definidos y monitoreados.

#### 8.1.5 Lineamientos para el ciclo de vida de los servicios de TI

##### 8.1.5.1 Definición y diseño del servicio

- Todo servicio debe:
  - Tener un propósito claro.
  - Estar alineado con los procesos institucionales.
- Deben definirse:
  - Alcance del servicio.
  - Usuarios beneficiarios.
  - Requisitos técnicos y operativos.

##### 8.1.5.2 Transición del servicio

Los servicios nuevos o modificados deben:

- Pasar por pruebas y validaciones.
- Contar con aprobación formal antes de su puesta en operación.
- La transición debe minimizar impactos operativos.

##### 8.1.5.3 Entrega y operación del servicio

- Los servicios deben prestarse conforme a lo definido en el catálogo.
- La operación debe:
  - Garantizar disponibilidad y desempeño.

- Gestionar incidentes y solicitudes de manera controlada.

#### 8.1.5.4 Soporte y control del servicio

Se deben establecer:

- Canales oficiales de atención.
- Procedimientos de escalamiento.
- Los incidentes y solicitudes deben registrarse y analizarse.

#### 8.1.5.5 Evaluación y mejora continua

Los servicios deben evaluarse periódicamente mediante:

- Indicadores de desempeño.
- Retroalimentación de usuarios.
- Los resultados deben generar acciones de mejora.

#### 8.1.5.6 Lineamientos para la gestión de niveles de servicio

- Los servicios TIC, deben contar con acuerdos de niveles de servicio (ANS).
- Los ANS deben definir:
  - Tiempos de respuesta y solución.
  - Horarios de atención.
  - Responsabilidades.
- El cumplimiento de los ANS debe ser monitoreado y reportado.

#### 8.1.5.7 Lineamientos para la gestión de incidentes y solicitudes

- Todos los incidentes y solicitudes deben:
  - Registrarse en los sistemas definidos.
  - Clasificarse y priorizarse.
- Los incidentes recurrentes deben analizarse para prevenir fallas futuras.

#### 8.1.5.8 Lineamientos para la gestión de proveedores de servicios

- Los servicios prestados por terceros deben:
  - Estar alineados con el catálogo de servicios.
  - Cumplir los ANS definidos.
- El desempeño de los proveedores debe evaluarse periódicamente.

#### 8.1.5.9 Lineamientos de roles y responsabilidades

- Oficina TIC:
  - Administra y supervisa la gestión de servicios de TI.
  - Define estándares y niveles de servicio.
- Dependencias usuarias:
  - Solicitan y utilizan los servicios conforme al catálogo.
  - Proveen retroalimentación sobre la calidad del servicio.
- Proveedores (cuando aplique):
  - Prestan los servicios conforme a los acuerdos establecidos.

#### 8.1.5.10 Seguimiento y control

La Oficina TIC deberá:

- Monitorear el desempeño de los servicios.
- Evaluar tendencias y niveles de demanda.
- Reportar resultados.
- Ajustar los servicios conforme a la evolución institucional.

## 8.2 Catálogo de servicios de tecnología

El catálogo de servicios de tecnología es el instrumento central de la gestión de servicios de TI que permite identificar, estructurar, comunicar y gestionar de manera formal la oferta de servicios tecnológicos que la Oficina TIC pone a disposición de las dependencias de la alcaldía municipal de Chía.

En el marco del modelo de gestión y gobierno TI, el catálogo constituye un mecanismo clave para orientar la gestión tecnológica a servicios, facilitar la relación entre la Oficina TIC y las áreas usuarias, establecer expectativas claras de atención y garantizar que los servicios de TI contribuyan de manera efectiva al cumplimiento de los objetivos institucionales y a la generación de valor público.

### 8.2.1 Objetivo del catálogo de servicios de tecnología

Establecer lineamientos institucionales para la definición, estructuración, administración, actualización y uso del catálogo de servicios de tecnología, asegurando claridad, estandarización, trazabilidad y alineación con el gobierno TI y la estrategia institucional.

### 8.2.2 Alcance

Estos lineamientos aplican a:

- Todos los servicios tecnológicos prestados por la Oficina TIC.
- Servicios orientados a usuarios internos y externos.
- Servicios asociados a infraestructura, sistemas de información, soporte, seguridad digital y plataformas tecnológicas.
- Servicios provistos directamente o a través de terceros.

### 8.2.3 Principios del catálogo de servicios de tecnología

El catálogo de servicios de tecnología se rige por los siguientes principios:

- Orientación a servicios: La tecnología se gestiona como un servicio, no como un activo aislado.
- Transparencia: Los servicios deben ser claramente conocidos por los usuarios.
- Estandarización: Los servicios deben definirse bajo una estructura común.
- Valor público: Los servicios deben aportar al cumplimiento de los objetivos institucionales.
- Gobernanza: La gestión del catálogo es responsabilidad de la Oficina TIC.
- Mejora continua: El catálogo debe evolucionar según necesidades y madurez institucional.

### 8.2.4 Lineamientos para la estructuración del catálogo

El catálogo de servicios de tecnología debe estructurarse, como mínimo, con la siguiente información por cada servicio:

- Nombre del servicio.
- Descripción clara y comprensible.
- Tipo de servicio (misional, de apoyo, transversal).
- Usuarios o dependencias beneficiarias.
- Responsable del servicio.
- Modalidad de atención.
- Requisitos para la solicitud.
- Niveles de servicio (ANS/SLA) cuando aplique.

No se considerará servicio tecnológico aquel que no se encuentre formalmente registrado en el catálogo.

### 8.2.5 Clasificación de los servicios de tecnología

Los servicios del catálogo deben clasificarse, al menos, en las siguientes categorías:

- Servicios de infraestructura tecnológica.

- Servicios de soporte y atención al usuario.
- Servicios de seguridad de la información y seguridad digital.
- Servicios de sistemas de información.
- Servicios de integración e interoperabilidad.
- Servicios de desarrollo de software.

#### 8.2.6 Lineamientos para la definición de niveles de servicio

- Los servicios críticos deben contar con acuerdos de nivel de servicio (ANS) definidos.
- Los ANS deben incluir:
  - Horarios de atención.
  - Tiempos de respuesta y solución.
  - Canales de atención.
- Los niveles de servicio deben ser realistas y acordes con la capacidad institucional.

#### 8.2.7 Lineamientos para la gestión y actualización del catálogo

- El catálogo de servicios debe:
  - Mantenerse actualizado.
  - Revisarse periódicamente.
- Toda modificación debe:
  - Estar justificada.
  - Ser aprobada por el jefe de la Oficina TIC.
- Los servicios obsoletos deben ser:
  - Evaluados.
  - Ajustados o retirados formalmente.

#### 8.2.8 Lineamientos para la comunicación y uso del catálogo

- El catálogo debe estar disponible para:
  - Funcionarios.
  - Contratistas.
  - Usuarios autorizados.
- Debe ser el medio oficial para:
  - Solicitar servicios de TI.
  - Conocer responsabilidades y alcances.
- No se deben atender solicitudes de servicios que no estén catalogados, salvo excepciones justificadas.

#### 8.2.9 Lineamientos de roles y responsabilidades

- Oficina TIC:
  - Define, administra y actualiza el catálogo.
  - Supervisa el cumplimiento de los niveles de servicio.
- Dependencias usuarias:
  - Utilizan el catálogo para solicitar servicios.
  - Retroalimentan sobre la calidad del servicio.
- Proveedores (cuando aplique)
  - Prestan servicios conforme a lo definido en el catálogo y los ANS.

#### 8.2.10 Seguimiento y mejora continua

La Oficina TIC deberá:

- Medir el desempeño de los servicios del catálogo.
- Analizar tendencias de demanda.
- Identificar oportunidades de mejora.
- Ajustar el catálogo conforme a la evolución tecnológica y organizacional.

### 8.3 Acceso a servicios en la nube

El acceso a servicios en la nube constituye un habilitador estratégico dentro de la gestión de servicios de TI de la alcaldía municipal de Chía, en la medida en que permite disponer de capacidades tecnológicas flexibles, escalables y seguras para soportar los sistemas de información, los servicios digitales al ciudadano y los procesos institucionales.

En el marco del modelo de gestión y gobierno TI, el acceso a servicios en la nube debe gestionarse bajo principios de gobernanza, seguridad, control y alineación estratégica, garantizando que su adopción contribuya a la eficiencia operativa, la continuidad del servicio, la optimización de recursos y el cumplimiento de la normativa vigente.

#### 8.3.1 Objetivo

Establecer los lineamientos institucionales para regular, controlar y administrar el acceso a servicios en la nube, asegurando que su uso sea seguro, autorizado, alineado con el catálogo de servicios de tecnología y coherente con la arquitectura tecnológica y de seguridad de la información de la alcaldía municipal de Chía.

#### 8.3.2 Alcance

Estos lineamientos aplican a:

- Servicios de nube pública, privada o híbrida utilizados por la entidad.

- Plataformas de correo institucional, almacenamiento, respaldo, contingencia, hosting, colaboración y aplicaciones en la nube.
- Accesos realizados por funcionarios, contratistas, operadores tecnológicos y terceros autorizados.
- Servicios en la nube incluidos en el catálogo de servicios de tecnología o contratados a través de proveedores externos.

### 8.3.3 Principios para el acceso a servicios en la nube

- **Gobernanza:** Todo acceso debe estar regulado y autorizado por la Oficina TIC.
- **Seguridad por diseño:** El acceso debe garantizar la confidencialidad, integridad y disponibilidad de la información.
- **Control de identidades:** El acceso se otorga según roles y responsabilidades.
- **Trazabilidad:** Todas las actividades deben ser registradas y auditables.
- **Alineación al servicio:** Solo se permitirá el acceso a servicios formalmente catalogados.
- **Uso responsable:** Los recursos en la nube deben utilizarse de manera eficiente y conforme a su propósito institucional.

### 8.3.4 Lineamientos para la habilitación del acceso

- El acceso a servicios en la nube debe:
  - Estar asociado a un servicio definido en el catálogo de servicios de tecnología.
  - Contar con una justificación funcional y operativa.
- Ningún funcionario o dependencia podrá habilitar servicios en la nube de manera autónoma sin aprobación de la Oficina TIC.
- Los accesos deben gestionarse a través de los mecanismos institucionales definidos (mesa de servicios, formularios, flujos de aprobación).

### 8.3.5 Lineamientos de gestión de identidades y accesos

- Todo acceso a servicios en la nube debe:
  - Asociarse a una identidad institucional.
  - Estar basado en roles y perfiles previamente definidos.
- Se debe implementar:
  - Autenticación fuerte (MFA) para servicios críticos.
  - Principio de mínimo privilegio.
- Los accesos deben:
  - Revisarse periódicamente.
  - Ser revocados de manera inmediata ante desvinculación o cambio de rol.

Tabla No. 15 Clasificación de niveles de acceso

Nivel de Acceso	Descripción
Sin acceso	No autorizado
Lectura	Consulta de información
Escritura	Creación y modificación de información
Usuario	Uso estándar del servicio
Usuario avanzado	Uso funcional ampliado
Operador	Gestión operativa controlada
Administrador	Configuración total del servicio
Temporal	Acceso limitado por tiempo

### 8.3.6 Lineamientos de seguridad de la información

- Los servicios en la nube deben cumplir con:
  - La política de seguridad de la información.
  - La política de seguridad digital.
- Se deben garantizar:
  - Cifrado de la información en tránsito y en reposo.
  - Protección contra accesos no autorizados.
- La información sensible o crítica debe:
  - Tener controles adicionales de acceso.
  - Estar sujeta a esquemas de respaldo y recuperación.

Tabla No. 16 Matriz de riesgos asociados al acceso CLOUD

Riesgo	Servicio	Impacto	Control Asociado
Acceso no autorizado	Almacenamiento	Alto	MFA + logs
Uso indebido de privilegios	Consola CLOUD	Alto	Segregación funciones
Fuga de información	Plataformas CLOUD	Alto	Cifrado + DLP
Dependencia del proveedor	Servicios SaaS	Medio	Contrato + respaldo

### 8.3.7 Lineamientos para el acceso remoto y conectividad

- El acceso a servicios en la nube desde redes externas debe:

Carrera 7 N° 12-100  
 PBX: (601) 884 4444 Ext. 2300-2301  
 oficinatic@chia.gov.co  
 www.chia-cundinamarca.gov.co

- Realizarse a través de mecanismos seguros (VPN, autenticación reforzada).
- No se permitirá el acceso a servicios críticos desde dispositivos no autorizados.
- La Oficina TIC deberá definir:
  - Políticas de acceso por tipo de usuario y ubicación.

Tabla No. 17 Matriz de control de acceso a servicios en la nube

Rol	Servicio en la Nube	Tipo de Servicio	Nivel de Acceso	Controles de Seguridad	Responsable del Control	Evidencia
Funcionario	Correo institucional en la nube	Colaboración	Usuario	Autenticación MFA, políticas de contraseña	Oficina TIC	Registro IAM
Funcionario	Almacenamiento en la nube	Información	Lectura escritura	Cifrado, control por carpetas	Oficina TIC	Logs de acceso
Líder de Proceso	Plataforma de trámites en la nube	Sistema de información	Usuario avanzado	MFA, control por rol, auditoría	Oficina TIC	Bitácora
Administrador TI	Plataforma CLOUD (IaaS / PaaS)	Infraestructura	Administrador	MFA, acceso restringido, monitoreo	Oficina TIC	Registro accesos
Analista TI	Consola de monitoreo CLOUD	Gestión TI	Operador	Acceso limitado, logs	Oficina TIC	Reportes
Proveedor	Plataforma CLOUD contratada	Servicio tercerizado	Temporal restringido	Acceso temporal, MFA	Oficina TIC	Acta autorización
Auditor	Herramientas de reportes CLOUD	Control	Solo lectura	Acceso de solo lectura, trazabilidad	Oficina TIC	Registro accesos
Seguridad TI	Consola de seguridad CLOUD	Seguridad	Administrador	MFA, segregación de funciones	Oficina TIC	Logs SIEM

### 8.3.8 Lineamientos para el uso de servicios en la nube por terceros

- Los proveedores o terceros que requieran acceso a servicios en la nube deben:
  - Contar con autorización expresa.

- Firmar compromisos de confidencialidad y seguridad.
- Los accesos de terceros deben:
  - Ser temporales.
  - Estar limitados al alcance del contrato o servicio.

#### 8.3.9 Lineamientos de monitoreo y control

- El acceso a servicios en la nube debe ser:
  - Monitoreado continuamente.
  - Registrado mediante logs y auditorías.
- La Oficina TIC debe:
  - Analizar eventos de acceso.
  - Detectar comportamientos anómalos.
  - Tomar acciones correctivas cuando aplique.

#### 8.3.10 Lineamientos de continuidad y disponibilidad

- Los servicios en la nube críticos deben:
  - Contar con esquemas de respaldo y recuperación.
  - Integrarse al plan de continuidad de TIC y DRP.
- Se deben definir:
  - Niveles de disponibilidad esperados.
  - Procedimientos ante fallas del proveedor.

#### 8.3.11 Roles y responsabilidades

- Oficina TIC:
  - Autoriza, administra y controla el acceso a servicios en la nube.
  - Define estándares de seguridad y uso.
- Dependencias usuarias:
  - Solicitan el acceso conforme a los lineamientos.
  - Usan los servicios de manera responsable.
- Proveedores:
  - Garantizan el cumplimiento de los acuerdos de servicio y seguridad.

### 8.4 Continuidad y disponibilidad de los servicios de TI

La continuidad y disponibilidad de los servicios de tecnologías de la información (TI) se establece sobre elementos críticos para garantizar la operación permanente de los procesos institucionales, la prestación de servicios al ciudadano y la confianza en la gestión

pública. La indisponibilidad de los servicios de TI puede generar impactos significativos en la atención a la ciudadanía, el cumplimiento normativo y la eficiencia administrativa.

En el marco del modelo de gestión y gobierno TI, la alcaldía municipal de Chía establece estos lineamientos con el fin de asegurar que los servicios de TI sean planificados, diseñados y operados con criterios de continuidad, resiliencia y alta disponibilidad, minimizando interrupciones y asegurando una recuperación oportuna ante incidentes, fallas o eventos disruptivos.

#### 8.4.1 Objetivo

Establecer lineamientos institucionales para garantizar la continuidad y disponibilidad de los servicios de TIC, asegurando que los servicios definidos en el catálogo de servicios de tecnología se mantengan operativos, confiables y alineados con los niveles de servicio comprometidos por la alcaldía municipal de Chía.

#### 8.4.2 Alcance

Estos lineamientos aplican a:

- Todos los servicios de TI definidos en el catálogo de servicios de tecnología.
- Servicios críticos, estratégicos y de apoyo.
- Servicios prestados por la Oficina TIC o a través de terceros.
- Infraestructura, plataformas, sistemas de información y servicios en la nube asociados.

#### 8.4.3 Principios de continuidad y disponibilidad

- Orientación al servicio: La continuidad se gestiona en función del impacto al proceso y al ciudadano.
- Prevención: Priorizar acciones que reduzcan la probabilidad de interrupciones.
- Resiliencia: Capacidad de los servicios para resistir y recuperarse ante fallas.
- Prioridad basada en criticidad: Los servicios críticos reciben mayor nivel de protección.
- Gobernanza: La continuidad y disponibilidad se gestionan bajo control institucional.
- Mejora continua: Los controles deben evaluarse y ajustarse periódicamente.

#### 8.4.4 Lineamientos para la identificación de servicios críticos

La Oficina TIC debe clasificar los servicios de TI según su criticidad, considerando:

- Impacto en procesos misionales.

- Impacto en la atención al ciudadano.
- Impacto legal, reputacional y financiero.
- Los servicios críticos deben:
  - Contar con niveles de disponibilidad definidos.
  - Tener planes de continuidad y recuperación específicos.

#### 8.4.5 Lineamientos para la disponibilidad de los servicios de TI

- Todo servicio de TI debe:
  - Contar con un nivel de disponibilidad definido (ANS).
  - Estar sujeto a monitoreo continuo.
- La disponibilidad debe gestionarse mediante:
  - Infraestructura adecuada.
  - Redundancia cuando aplique.
  - Ventanas de mantenimiento planificadas.
- Las indisponibilidades programadas deben comunicarse oportunamente a los usuarios.

#### 8.4.6 Lineamientos para la continuidad de los servicios de TI

- Los servicios críticos deben contar con:
  - Planes de continuidad de TIC.
  - Procedimientos de recuperación documentados.
- Los planes de continuidad deben:
  - Definir roles y responsabilidades.
  - Establecer tiempos de recuperación (RTO) y puntos de recuperación (RPO).
- La continuidad debe integrarse con el plan de continuidad institucional.

Tabla No. 18 Matriz de continuidad y disponibilidad de servicios de TI

Servicio de TI	Proceso que Soporta	Criticidad	Nivel de Disponibilidad	RTO (Tiempo Máx. de Recuperación)	RPO (Punto Máx. de Pérdida de Datos)	Tipo de Servicio	Responsable
Plataforma de trámites en línea	Atención al ciudadano	Alta	>= 99.5%	4 horas	30 minutos	Sistema de información	Atención al ciudadano / Oficina TIC

Servicio de TI	Proceso que Soporta	Criticidad	Nivel de Disponibilidad	RTO (Tiempo Máx. de Recuperación)	RPO (Punto Máx. de Pérdida de Datos)	Tipo de Servicio	Responsable
Sistema PQRS	Atención al ciudadano	Alta	>= 99%	6 horas	1 hora	Sistema de información	Atención al ciudadano / Oficina TIC
Correo institucional	Comunicación institucional	Alta	>= 99.9%	2 horas	15 minutos	Servicio en la nube	Oficina TIC
Sistema financiero	Gestión financiera	Alta	>= 99%	4 horas	30 minutos	Sistema de información	Sec. Hacienda / Oficina TIC
Sistema documental	Gestión documental	Media	>= 98%	12 horas	4 horas	Sistema de información	Dirección de servicios administrativos / Oficina TIC
Plataforma de almacenamiento en la nube	Gestión de información	Media	>= 98%	12 horas	2 horas	Servicio en la nube	Oficina TIC
Sistema de talento humano	Gestión del talento	Media	>= 97%	24 horas	8 horas	Sistema de información	Dirección de función pública / Oficina TIC
Mesa de servicios TI	Soporte institucional	Media	>= 98%	8 horas	2 horas	Servicio TI	Oficina TIC
Herramienta de analítica / BI	Planeación y control	Baja	>= 95%	48 horas	24 horas	Plataforma analítica	Oficina TIC
Plataforma de capacitación virtual	Formación	Baja	>= 95%	72 horas	24 horas	Servicio en la nube	Oficina TIC

#### 8.4.7 Lineamientos para la gestión de incidentes y fallas

- Toda interrupción del servicio debe:
  - Registrarse como incidente.

- Clasificarse según impacto y urgencia.
- Los incidentes mayores deben:
  - Activar procedimientos de continuidad.
  - Ser analizados para identificar causas raíz.
- Las lecciones aprendidas deben incorporarse a planes de mejora.

Tabla No. 19 Clasificación de criticidad

Nivel	Descripción
Alta	Impacta procesos misionales, atención al ciudadano o cumplimiento legal
Media	Impacta procesos estratégicos o de apoyo críticos
Baja	Impacto limitado, sin afectación directa al ciudadano

#### 8.4.8 Lineamientos para la gestión de proveedores y terceros

- Los servicios de TI prestados por terceros deben:
  - Contar con ANS alineados con los compromisos institucionales.
  - Incluir cláusulas de continuidad y disponibilidad.
- El desempeño de los proveedores debe:
  - Monitorearse periódicamente.
  - Evaluarse frente a los niveles de servicio acordados.

#### 8.4.9 Lineamientos de monitoreo y control

- La Oficina TIC debe:
  - Monitorear la disponibilidad de los servicios de TI.
  - Medir el cumplimiento de los ANS.
  - Generar reportes periódicos de desempeño.
- Los indicadores de continuidad y disponibilidad deben alimentar el tablero de indicadores de TIC.

#### 8.4.10 Lineamientos de roles y responsabilidades

- Oficina TIC:
  - Define los niveles de disponibilidad y continuidad.
  - Monitorea y controla el desempeño de los servicios.
- Dependencias usuarias:
  - Informan oportunamente incidentes que afecten la operación.
- Proveedores (cuando aplique):
  - Garantizan la continuidad y disponibilidad conforme a lo contratado.

#### 8.4.11 Seguimiento y mejora continua

La Oficina TIC deberá:

- Evaluar periódicamente la continuidad y disponibilidad de los servicios.
- Analizar tendencias de indisponibilidad.
- Actualizar planes y controles según resultados.
- Incorporar mejoras conforme a la evolución tecnológica y organizacional.

### 8.5 Alta disponibilidad de los servicios de TI

La alta disponibilidad de los servicios de tecnologías de la información es un elemento clave para garantizar la operación continua de los procesos institucionales y la prestación ininterrumpida de servicios digitales a los ciudadanos. La indisponibilidad de servicios críticos puede afectar de manera significativa la atención al ciudadano, el cumplimiento normativo y la imagen institucional.

En el marco del modelo de gestión y gobierno TI, la alcaldía municipal de Chía adopta la alta disponibilidad como un criterio técnico y de gestión obligatorio para los servicios de TIC clasificados como críticos o de alta criticidad, asegurando que estos cuenten con arquitecturas, controles y procedimientos que minimicen el impacto de fallas y reduzcan los tiempos de indisponibilidad.

#### 8.5.1 Objetivo

Establecer lineamientos institucionales para diseñar, implementar, operar y controlar la alta disponibilidad de los servicios de TIC, garantizando niveles elevados de disponibilidad, resiliencia y continuidad, alineados con el catálogo de servicios de tecnología y los compromisos institucionales.

#### 8.5.2 Alcance

Estos lineamientos aplican a:

- Servicios de TIC clasificados como críticos o de alta criticidad.
- Sistemas de información misionales y estratégicos.
- Infraestructura tecnológica, plataformas en la nube y servicios tercerizados.
- Servicios definidos en el catálogo de servicios de tecnología.

### 8.5.3 Principios de alta disponibilidad

- Diseño resiliente: Los servicios deben diseñarse para tolerar fallas.
- Eliminación de puntos únicos de falla.
- Automatización: Priorizar mecanismos automáticos de conmutación.
- Monitoreo continuo: Detección temprana de fallas.
- Escalabilidad: Capacidad de crecer sin afectar la disponibilidad.
- Gobernanza: La alta disponibilidad se gestiona bajo control institucional.

### 8.5.4 Lineamientos para la identificación de servicios con alta disponibilidad

- La Oficina TIC debe:
  - Identificar los servicios que requieren alta disponibilidad.
  - Priorizar aquellos con impacto directo en el ciudadano o procesos misionales.
- Los servicios con requerimientos de alta disponibilidad deben:
  - Tener niveles de disponibilidad superiores al estándar.
  - Contar con arquitectura de alta disponibilidad documentada.

Tabla No. 20 Matriz de alta disponibilidad de los servicios de TI

Servicio de TI	Proceso que Soporta	Criticidad	Arquitectura de Alta Disponibilidad (HA)	Componentes Redundantes	Nivel de Disponibilidad Objetivo	Tipo de Implementación	Responsable
Plataforma de trámites en línea	Atención al ciudadano	Alta	Arquitectura activo-activo con balanceo de carga	Frontend, Backend, BD, Red	>= 99.9%	Nube (multi-zona)	Atención al ciudadano / Oficina TIC
Sistema PQRS	Atención al ciudadano	Alta	Arquitectura activo-pasivo con failover automático	App, BD	>= 99.5%	Nube híbrido	Atención al ciudadano / Oficina TIC
Correo institucional	Comunicación institucional	Alta	Servicio administrado HA del proveedor	Servicio completo	>= 99.9%	Nube SaaS	Oficina TIC
Sistema financiero	Gestión financiera	Alta	Activo-pasivo con réplica de	App, BD	>= 99.5%	On-Premise / híbrido	Sec. Hacienda / Oficina TIC

Servicio de TI	Proceso que Soporta	Criticidad	Arquitectura de Alta Disponibilidad (HA)	Componentes Redundantes	Nivel de Disponibilidad Objetivo	Tipo de Implementación	Responsable
			base de datos				
Sistema documental	Gestión documental	Media	Clúster con almacenamiento redundante	App, almacenamiento	>= 99.0%	Nube	Dirección de servicios administrativos / Oficina TIC
Almacenamiento institucional en la nube	Gestión de información	Media	Redundancia geográfica del proveedor	Almacenamiento	>= 99.0%	Nube	Oficina TIC
Mesa de servicios TI	Soporte institucional	Media	Activo-pasivo	App, BD	>= 99.0%	Nube	Oficina TIC
Plataforma de analítica / BI	Planeación y control	Baja	Arquitectura básica con respaldo	BD	>= 98.0%	Nube	Oficina TIC
Plataforma de capacitación virtual	Formación	Baja	Activo-pasivo	App	>= 98.0%	Nube	Oficina TIC

#### 8.5.5 Lineamientos para el diseño de arquitecturas de alta disponibilidad

- Los servicios con alta disponibilidad deben:
  - Implementar redundancia en componentes críticos (servidores, red, almacenamiento).
  - Contar con balanceo de carga cuando aplique.
  - Evitar dependencias tecnológicas únicas.
- Las arquitecturas de alta disponibilidad deben:
  - Estar documentadas.
  - Ser aprobadas por la Oficina TIC.

Tabla No. 21 Tipos de arquitectura de alta disponibilidad

Arquitectura alta disponibilidad	Descripción
Activo-activo	Dos o más nodos activos simultáneamente, con balanceo de carga
Activo-pasivo	Nodo principal y nodo de respaldo con conmutación
Clúster	Conjunto de nodos que operan como una sola unidad
Alta disponibilidad administrada	Alta disponibilidad provista por el proveedor CLOUD
Básica con respaldo	Disponibilidad estándar con mecanismos de recuperación

#### 8.5.6 Lineamientos para la alta disponibilidad en servicios en la nube

- Los servicios en la nube deben:
  - Utilizar zonas de disponibilidad o regiones redundantes.
  - Implementar mecanismos de failover automático.
- Se deben aprovechar:
  - Servicios administrados con SLA elevados.
  - Capacidades nativas de resiliencia del proveedor.

#### 8.5.7 Lineamientos para la operación y monitoreo de la alta disponibilidad

- Los servicios con alta disponibilidad deben:
  - Ser monitoreados 24/7.
  - Contar con alertas tempranas.
- El monitoreo debe:
  - Detectar fallas parciales o degradación del servicio.
- Los eventos de indisponibilidad deben:
  - Registrarse y analizarse.

#### 8.5.8 Lineamientos para pruebas de alta disponibilidad

- Los servicios con alta disponibilidad deben:
  - Someterse a pruebas periódicas de conmutación y recuperación.
- Las pruebas deben:
  - Documentarse.
  - Generar acciones de mejora cuando aplique.

#### 8.5.9 Lineamientos para la gestión de proveedores

- Los servicios de alta disponibilidad prestados por terceros deben:
  - Contar con ANS que respalden los niveles de disponibilidad requeridos.
  - Incluir compromisos de soporte y recuperación.
- El desempeño del proveedor debe evaluarse periódicamente.

#### 8.5.10 Lineamientos de roles y responsabilidades

- Oficina TIC:
  - Define criterios de alta disponibilidad.
  - Supervisa su implementación y operación.
- Proveedores (cuando aplique):
  - Implementan y mantienen las arquitecturas de HA conforme a lo contratado.
- Dependencias usuarias:
  - Informan oportunamente incidentes que afecten la disponibilidad.

#### 8.5.11 Seguimiento y mejora continua

La Oficina TIC deberá:

- Evaluar periódicamente el cumplimiento de los niveles de alta disponibilidad.
- Analizar causas de indisponibilidad.
- Ajustar arquitecturas y controles según resultados.
- Incorporar lecciones aprendidas.

### 8.6 Capacidad de los servicios tecnológicos

La gestión de la capacidad de los servicios tecnológicos es un componente fundamental de la gestión de servicios de TI, ya que permite asegurar que los servicios prestados por la alcaldía municipal de Chía cuenten, en todo momento, con los recursos tecnológicos necesarios para atender la demanda actual y futura, manteniendo niveles adecuados de desempeño, disponibilidad y calidad.

Una gestión inadecuada de la capacidad puede generar degradación del servicio, indisponibilidades, sobrecostos o subutilización de recursos. Por ello, en el marco del modelo de gestión y gobierno TI, la capacidad de los servicios tecnológicos debe gestionarse de forma planificada, medible y alineada con la estrategia institucional.

#### 8.6.1 Objetivo

Establecer lineamientos institucionales para planificar, monitorear, controlar y mejorar la capacidad de los servicios tecnológicos, garantizando que estos respondan oportunamente a las necesidades de los procesos institucionales y a los niveles de servicio definidos en el catálogo de servicios de tecnología.

### 8.6.2 Alcance

Estos lineamientos aplican a:

- Todos los servicios tecnológicos definidos en el catálogo de servicios de la Oficina TIC.
- Servicios prestados sobre infraestructura propia, en la nube o híbrida.
- Servicios críticos, estratégicos y de apoyo.
- Recursos asociados a cómputo, almacenamiento, red, licenciamiento y plataformas tecnológicas.

### 8.6.3 Principios de la gestión de capacidad

- Orientación al servicio: La capacidad se gestiona en función del servicio y su impacto en el negocio.
- Planeación anticipada: Prever la demanda futura y evitar cuellos de botella.
- Eficiencia: Optimizar el uso de los recursos tecnológicos.
- Escalabilidad: Facilitar el crecimiento controlado de los servicios.
- Medición y control: Basar las decisiones en datos objetivos.
- Gobernanza: La capacidad se gestiona bajo control institucional.

### 8.6.4 Lineamientos para la planificación de la capacidad

La Oficina TIC debe elaborar y mantener un plan de capacidad de servicios tecnológicos, alineado con:

- El PETIC.
- El catálogo de servicios de tecnología.
- La clasificación de criticidad de los servicios.
- La planificación de capacidad debe considerar:
  - Crecimiento de usuarios.
  - Incremento en volúmenes de información.
  - Nuevos servicios o funcionalidades.
  - Cambios normativos o tecnológicos.

### 8.6.5 Lineamientos para la gestión de la demanda

- La demanda de los servicios tecnológicos debe:
  - Analizarse periódicamente.
  - Proyectarse en el corto, mediano y largo plazo.
- Las dependencias usuarias deben:

- Informar oportunamente cambios que impacten la demanda.
- Los servicios críticos deben contar con márgenes de capacidad adicionales.

#### 8.6.6 Lineamientos para el monitoreo de la capacidad

- La Oficina TIC debe monitorear, como mínimo:
  - Uso de CPU, memoria y almacenamiento.
  - Capacidad de red y ancho de banda.
  - Consumo de licencias y servicios en la nube.
- El monitoreo debe:
  - Realizarse de forma continua o periódica, según la criticidad.
  - Generar alertas ante umbrales definidos.

#### 8.6.7 Lineamientos para el control y ajuste de la capacidad

- Cuando se identifiquen riesgos de saturación o subutilización:
  - Se deben analizar causas.
  - Proponer acciones correctivas o preventivas.
- Los ajustes de capacidad deben:
  - Gestionarse mediante la gestión de cambios cuando aplique.
  - Documentarse y aprobarse formalmente.

#### 8.6.8 Lineamientos para la capacidad en servicios en la nube

- Los servicios en la nube deben:
  - Aprovechar capacidades de escalamiento dinámico cuando sea posible.
  - Contar con controles de consumo y costos.
- La Oficina TIC debe:
  - Definir límites y alertas de uso.
  - Monitorear el impacto financiero del crecimiento de capacidad.

#### 8.6.9 Lineamientos para la gestión de capacidad con proveedores

- Los contratos con proveedores deben:
  - Definir claramente los niveles de capacidad y escalabilidad.
  - Establecer tiempos de ampliación o ajuste de recursos.
- El desempeño del proveedor debe:
  - Evaluarse en función de la capacidad entregada frente a la demandada.

#### 8.6.10 Lineamientos de roles y responsabilidades

- Oficina TIC:
  - Planifica, monitorea y controla la capacidad de los servicios tecnológicos.
  - Define umbrales y escenarios de crecimiento.
- Dependencias usuarias:
  - Informan cambios que afecten la demanda de los servicios.
- Proveedores (cuando aplique):
  - Garantizan la capacidad conforme a lo contratado.

#### 8.6.11 Seguimiento y mejora continua

La Oficina TIC deberá:

- Evaluar periódicamente la adecuación de la capacidad de los servicios.
- Analizar tendencias de crecimiento y consumo.
- Ajustar planes de capacidad según resultados.
- Incorporar mejoras tecnológicas y de gestión.

### 8.7 Acuerdos de nivel de servicios

Los acuerdos de niveles de servicio (ANS) constituyen un instrumento esencial de la gestión de servicios de TI, ya que permiten establecer de manera clara y medible los niveles de calidad, tiempos de atención y compromisos de desempeño asociados a los servicios tecnológicos que la Oficina TIC presta a las dependencias de la alcaldía municipal de Chía.

En el marco del modelo de gestión y gobierno TI, los acuerdos de niveles de servicio facilitan la gestión transparente de expectativas, el control del desempeño de los servicios y la mejora continua, asegurando que los servicios de TI contribuyan de manera efectiva al cumplimiento de los objetivos institucionales y a la atención oportuna de las necesidades de los usuarios.

#### 8.7.1 Objetivo

Establecer los lineamientos institucionales para la definición, formalización, gestión, seguimiento y mejora de los acuerdos de niveles de servicio, garantizando que los servicios tecnológicos cuenten con compromisos claros, medibles y alineados con el catálogo de servicios de tecnología y el protocolo de la mesa de servicios.

#### 8.7.2 Alcance

Estos lineamientos aplican a:

- Todos los servicios tecnológicos definidos en el catálogo de servicios de la Oficina TIC.
- Servicios de TIC prestados a usuarios internos y externos.
- Servicios operados directamente por la Oficina TIC o por terceros.
- La atención de incidentes, solicitudes, requerimientos y eventos asociados a los servicios de TI.

### 8.7.3 Principios de los acuerdos de niveles de Servicio

- Orientación al servicio: Los acuerdos de niveles de servicio se definen desde la perspectiva del usuario.
- Claridad y transparencia: Los compromisos deben ser comprensibles y públicos.
- Medición objetiva: Los niveles de servicio deben ser medibles y verificables.
- Realismo: Los acuerdos de niveles de servicio deben corresponder a la capacidad institucional.
- Mejora continua: Los acuerdos de niveles de servicio deben ajustarse según resultados y madurez.
- Gobernanza: La definición y control de los acuerdos de niveles de servicio TIC es responsabilidad del jefe de la Oficina TIC.

### 8.7.4 Lineamientos para la definición de los acuerdos de niveles de servicio

- Todo servicio tecnológico debe:
  - Contar con acuerdos de niveles de servicio definidos.
  - Estar alineado con el catálogo de servicios de tecnología.
- Los acuerdos de niveles de servicio deben considerar:
  - Tipo de servicio.
  - Criticidad del servicio.
  - Impacto en el proceso institucional y en el ciudadano.
- La definición de los acuerdos de niveles de servicio debe apoyarse en:
  - El árbol de categorías y caracterización de servicios TIC.
  - Los niveles de prioridad definidos en el protocolo de mesa de servicios.

### 8.7.5 Lineamientos para la caracterización y priorización

- Los servicios y solicitudes deben:
  - Clasificarse según categorías y subcategorías.
  - Priorizarse considerando impacto y urgencia.
- La prioridad asignada debe:
  - Determinar los tiempos de respuesta y solución.
  - Ser coherente con los niveles de servicio comprometidos.

#### 8.7.6 Lineamientos para los componentes mínimos de los acuerdos de niveles de servicio

Todo acuerdo de nivel de servicio debe incluir, como mínimo:

- Nombre del servicio.
- Descripción del servicio.
- Horarios de atención.
- Tiempos de respuesta y solución.
- Canales de atención definidos.
- Roles y responsabilidades.
- Indicadores de desempeño.

#### 8.7.7 Lineamientos para la gestión de acuerdos de niveles de servicio con proveedores

- Los servicios prestados por terceros deben:
  - Contar con acuerdos de niveles de servicio contractuales alineados con los acuerdos de niveles de servicio institucionales.
  - Definir penalidades y acciones correctivas por incumplimiento.
- El desempeño del proveedor debe:
  - Evaluarse periódicamente frente a los acuerdos de niveles de servicio acordados.

#### 8.7.8 Lineamientos para el seguimiento y control de los acuerdos de niveles de servicio

- La Oficina TIC debe:
  - Monitorear el cumplimiento de los acuerdos de niveles de servicio.
  - Registrar los tiempos de atención y solución.
- Los resultados del seguimiento deben:
  - Alimentar el tablero de indicadores de TI.
  - Presentarse a las instancias de gobierno TI cuando aplique y al jefe de la Oficina TIC.

#### 8.7.9 Lineamientos para la revisión y mejora de los acuerdos de niveles de servicio

- Los acuerdos de niveles de servicio deben:
  - Revisarse periódicamente.
  - Ajustarse cuando existan cambios en la demanda, capacidad o criticidad.
- Los incumplimientos recurrentes deben:
  - Analizarse para identificar causas raíz.
  - Generar planes de mejora.

#### 8.7.10 Lineamientos de roles y responsabilidades

- Oficina TIC:
  - Define, administra y controla los acuerdos de niveles de servicio.
  - Supervisa el cumplimiento de los compromisos de servicio.
- Dependencias usuarias:
  - Utilizan los servicios conforme a los acuerdos de niveles de servicio definidos.
  - Reportan oportunamente incidentes y solicitudes.
- Proveedores (cuando aplique):
  - Cumplen los acuerdos de niveles de servicio contractuales establecidos.

### 8.8 Soporte a los servicios de TI

El soporte a los servicios de TI es el conjunto de actividades orientadas a garantizar la atención oportuna, controlada y de calidad de los incidentes, requerimientos y solicitudes relacionadas con los servicios tecnológicos de la alcaldía municipal de Chía. Este soporte se constituye en el principal punto de contacto entre los usuarios y la Oficina TIC, y es fundamental para asegurar la continuidad operativa, la satisfacción del usuario y el cumplimiento de los acuerdos de niveles de servicio (ANS).

En el marco del modelo de gestión y gobierno TI, el soporte a los servicios de TI se gestiona de manera centralizada, trazable y estandarizada, a través de la mesa de servicios (MDS), conforme al protocolo institucional definido.

#### 8.8.1 Objetivo

Establecer los lineamientos institucionales para la prestación del soporte a los servicios de TIC, asegurando una gestión estructurada de incidentes, requerimientos y solicitudes, alineada con el catálogo de servicios de tecnología, los acuerdos de niveles de servicio y el protocolo de la mesa de servicios.

#### 8.8.2 Alcance

Estos lineamientos aplican a:

- Todos los servicios tecnológicos definidos en el catálogo de servicios de la Oficina TIC.
- Usuarios internos (funcionarios y contratistas) de la alcaldía municipal de Chía.
- Servicios de soporte prestados directamente por la Oficina TIC o a través de terceros.

- Incidentes, requerimientos, solicitudes de servicio, desarrollos y eventos de seguridad de la información.

### 8.8.3 Principios del soporte a los servicios de TI

- Centralización: Todo soporte se gestiona a través de la mesa de servicios.
- Trazabilidad: Cada caso debe quedar registrado desde su apertura hasta su cierre.
- Estandarización: La atención sigue procedimientos y niveles definidos.
- Orientación al usuario: El soporte busca restaurar el servicio con el menor impacto posible.
- Escalamiento controlado: Los casos se atienden según niveles de soporte.
- Mejora continua: El análisis de los casos alimenta acciones de mejora.

### 8.8.4 Lineamientos generales del soporte

- Todo incidente, requerimiento o solicitud de servicio debe:
  - Registrarse obligatoriamente en la herramienta de gestión GLPI.
  - Ser categorizado y priorizado conforme a ITIL y al protocolo de la mesa de servicios.
- No se permitirá la atención informal o fuera de los canales definidos, salvo situaciones excepcionales autorizadas por la Oficina TIC.

### 8.8.5 Lineamientos para la mesa de servicios (MDS)

- La mesa de servicios es el único punto oficial de contacto para el soporte de TI.
- La mesa de servicios es responsable de:
  - Recepción y registro de solicitudes.
  - Categorización y priorización.
  - Asignación y escalamiento.
  - Seguimiento, documentación y cierre de casos.
- El soporte debe prestarse conforme a los horarios definidos institucionalmente.

### 8.8.6 Lineamientos para los niveles de soporte

El soporte a los servicios de TI se estructura en niveles, conforme al protocolo de la mesa de servicios:

#### **Primer nivel:**

- Atención remota o telefónica.

- Solución de incidentes comunes y de baja complejidad.

**Segundo nivel:**

- Atención en sitio.
- Diagnóstico y solución de fallas de hardware y software.

**Tercer nivel:**

- Soporte especializado en redes, servidores y plataformas.

**Cuarto nivel:**

- Desarrollo de software.
- Incidentes graves de seguridad de la información.

Cada nivel debe documentar las acciones realizadas y garantizar la trazabilidad del caso.

### 8.8.7 Lineamientos para la gestión de incidentes y requerimientos

- Los incidentes y requerimientos deben:
  - Clasificarse según su impacto y urgencia.
  - Atenderse conforme a los tiempos definidos en los acuerdos de niveles de servicio.
- Los incidentes recurrentes deben:
  - Analizarse para identificar causas raíz.
  - Generar acciones preventivas o correctivas.

Tabla No. 22 Matriz incidente / requerimiento

Tipo	Categoría	Nivel de Soporte	Tiempo de Respuesta	Tiempo de Solución	Responsable Principal	Escalamiento
Incidente	Caída total de sistema crítico	Nivel 3	<= 30 min	<= 4 horas	Oficina TIC – infraestructura	Proveedor / Oficina TIC
Incidente	Degradación de servicio	Nivel 2	<= 1 hora	<= 8 horas	Oficina TIC – Soporte	Nivel 3
Incidente	Falla individual de usuario	Nivel 1	<= 2 horas	<= 24 horas	Mesa de servicios	Nivel 2
Incidente	Incidente de seguridad	Nivel 4	<= 15 min	<= 4 horas	Seguridad de la información	CSIRT / Oficina TIC

Tipo	Categoría	Nivel de Soporte	Tiempo de Respuesta	Tiempo de Solución	Responsable Principal	Escalamiento
Requerimiento	Solicitud de acceso	Nivel 1	<= 4 horas	<= 48 horas	Mesa de servicios	Nivel 2
Requerimiento	Instalación de software estándar	Nivel 1	<= 8 horas	<= 3 días hábiles	Mesa de servicios	Nivel 2
Requerimiento	Cambio menor en sistema	Nivel 2	<= 1 día hábil	<= 5 días hábiles	Oficina TIC – Soporte	Comité de cambios
Requerimiento	Desarrollo / ajuste funcional	Nivel 4	<= 2 días hábiles	Según alcance	Oficina TIC // Desarrollo Proveedor	Comité de Cambios
Requerimiento	Solicitud de infraestructura	Nivel 3	<= 1 día hábil	<= 10 días hábiles	Oficina TIC – Infraestructura	Oficina TIC
Requerimiento	Consulta / orientación TI	Nivel 1	<= 4 horas	<= 24 horas	Mesa de servicios	—

#### 8.8.8 Lineamientos para el soporte en seguridad de la información

- Los eventos de seguridad deben:
  - Registrarse y gestionarse como casos especiales en la MDS.
  - Escalarse al equipo de seguridad de la información o a instancias nacionales cuando aplique.
- La gestión debe garantizar:
  - Confidencialidad.
  - Trazabilidad.
  - Documentación completa del incidente.

#### 8.8.9 Lineamientos para la comunicación y seguimiento

- El usuario debe:
  - Recibir notificaciones del estado de su solicitud.
- La Oficina TIC debe:
  - Mantener informados a los usuarios sobre avances y cierres.
- El cierre de los casos debe:
  - Incluir encuesta de satisfacción.
  - Permitir retroalimentación del usuario.

#### 8.8.10 Lineamientos para la calidad del soporte

- La calidad del soporte se mide mediante:
  - Cumplimiento de acuerdos de niveles de servicio.
  - Encuestas de satisfacción.
  - Análisis estadístico de los casos.
- Resultados deficientes deben:
  - Generar acciones de mejora documentadas.

#### 8.8.11 Lineamientos de roles y responsabilidades

- Oficina TIC:
  - Administra la mesa de servicios.
  - Garantiza el cumplimiento de los acuerdos de niveles de servicio.
  - Evalúa la calidad del soporte.
- Usuarios:
  - Registran las solicitudes por los canales definidos.
  - Proveen información clara y oportuna.
- Proveedores (cuando aplique):
  - Atienden los casos escalados conforme a lo contratado.

### 8.9 Planes de mantenimiento

Los planes de mantenimiento de los servicios de TI constituyen un instrumento fundamental para garantizar la disponibilidad, continuidad, desempeño y calidad de los servicios tecnológicos que soportan los procesos institucionales de la alcaldía municipal de Chía. El mantenimiento planificado y controlado permite prevenir fallas, reducir riesgos operativos, optimizar la capacidad instalada y extender la vida útil de los activos tecnológicos.

En el marco del modelo de gestión y gobierno TI, los planes de mantenimiento se conciben como un mecanismo de gestión preventiva, correctiva y evolutiva, articulado con la gestión de servicios TI, la gestión de la capacidad, la alta disponibilidad y los acuerdos de niveles de servicio (ANS).

#### 8.9.1 Objetivo

Establecer los lineamientos institucionales para la definición, ejecución, control y mejora de los planes de mantenimiento de los servicios de TI, asegurando que estos se realicen de manera planificada, documentada y alineada con la criticidad de los servicios y la capacidad tecnológica de la entidad.

### 8.9.2 Alcance

Estos lineamientos aplican a:

- Todos los servicios tecnológicos definidos en el catálogo de servicios de la Oficina TIC.
- Servicios soportados por infraestructura tecnológica, sistemas de información y plataformas en la nube.
- Servicios prestados directamente por la Oficina TIC o a través de terceros.
- Actividades de mantenimiento preventivo, correctivo, adaptativo y evolutivo.

### 8.9.3 Principios de los planes de mantenimiento

- Orientación al servicio: El mantenimiento se prioriza según el impacto del servicio.
- Prevención: Priorizar acciones que reduzcan la ocurrencia de incidentes.
- Planificación: Las actividades deben programarse y comunicarse oportunamente.
- Trazabilidad: Toda actividad de mantenimiento debe quedar registrada.
- Alineación a la capacidad: El mantenimiento debe considerar la capacidad y carga de los servicios.
- Mejora continua: Los resultados del mantenimiento alimentan acciones de mejora.

### 8.9.4 Lineamientos para la definición de los planes de mantenimiento

- La Oficina TIC debe elaborar y mantener planes de mantenimiento para los servicios tecnológicos, considerando:
  - Criticidad del servicio.
  - Niveles de disponibilidad y acuerdos de niveles de servicio definidos.
  - Capacidad de los servicios tecnológicos.
- Cada plan de mantenimiento debe:
  - Estar documentado.
  - Contar con aprobación formal.
  - Integrarse al calendario institucional de TI.

### 8.9.5 Tipos de mantenimiento de los servicios de TI

Los planes de mantenimiento deben contemplar, como mínimo, los siguientes tipos:

- Mantenimiento preventivo: Acciones programadas para prevenir fallas y degradación del servicio.
- Mantenimiento correctivo: Acciones para corregir fallas detectadas en la operación.
- Mantenimiento adaptativo: Ajustes derivados de cambios tecnológicos, normativos o de entorno.

- Mantenimiento evolutivo: Mejoras funcionales o técnicas orientadas a optimizar el servicio.

#### 8.9.6 Lineamientos para la planificación y programación

- El mantenimiento preventivo debe:
  - Programarse periódicamente según el tipo de servicio.
  - Considerar ventanas de mantenimiento definidas.
- Las actividades programadas deben:
  - Comunicarse oportunamente a los usuarios.
  - Minimizar el impacto en la operación institucional.

#### 8.9.7 Lineamientos para la ejecución del mantenimiento

- Toda actividad de mantenimiento debe:
  - Registrarse en la mesa de servicios o herramienta definida.
  - Contar con responsable asignado.
- Cuando el mantenimiento implique cambios significativos:
  - Debe gestionarse a través del proceso de gestión de cambios.

#### 8.9.8 Lineamientos para el mantenimiento de servicios en la nube

- Los servicios en la nube deben:
  - Ajustarse a los planes de mantenimiento del proveedor.
  - Integrarse a los planes institucionales de mantenimiento.
- La Oficina TIC debe:
  - Verificar el cumplimiento de los compromisos del proveedor.
  - Evaluar el impacto del mantenimiento en la capacidad y disponibilidad.

#### 8.9.9 Lineamientos para el control y seguimiento

- La Oficina TIC debe:
  - Realizar seguimiento al cumplimiento de los planes de mantenimiento.
  - Medir la efectividad del mantenimiento mediante indicadores.
- Los resultados deben:
  - Alimentar el tablero de indicadores de TIC.
  - Soportar la toma de decisiones de mejora.

#### 8.9.10 Lineamientos para la articulación con la capacidad y disponibilidad

- Los planes de mantenimiento deben:
  - Considerar la capacidad actual y proyectada de los servicios.
  - Evitar la saturación de recursos durante su ejecución.
- El mantenimiento debe contribuir a:
  - Mejorar la disponibilidad.
  - Reducir incidentes recurrentes.

#### 8.9.11 Lineamientos de roles y responsabilidades

- Oficina TIC:
  - Define, ejecuta y controla los planes de mantenimiento.
  - Evalúa su impacto en la capacidad y disponibilidad de los servicios.
- Dependencias usuarias:
  - Atienden las comunicaciones de mantenimiento programado.
- Proveedores (cuando aplique):
  - Ejecutan el mantenimiento conforme a lo contratado y aprobado.

#### 8.9.12 Plantilla plan de mantenimiento de servicios de tecnologías de la información (TI)

##### Información general

Campo	Descripción
Nombre del servicio	
Código del servicio (Catálogo)	
Dependencia responsable	Oficina TIC
Proceso que soporta	
Tipo de servicio	( ) Infraestructura ( ) Sistema de Información ( ) Nube ( ) Soporte
Criticidad del servicio	( ) Alta ( ) Media ( ) Baja
Nivel de disponibilidad (ANS)	
Periodo del plan	
Fecha de elaboración	
Responsable del plan	
Aprobado por	

##### Objetivo del plan de mantenimiento

Describir el objetivo del plan, indicando cómo las actividades de mantenimiento contribuyen a la disponibilidad, continuidad, capacidad y calidad del servicio.

### Alcance

Definir el alcance del mantenimiento, incluyendo:

- Componentes tecnológicos cubiertos.
- Ambientes (producción, contingencia, nube, on-premise).
- Exclusiones (si aplica).

### Caracterización del servicio

Elemento	Descripción
Arquitectura del servicio	
Componentes críticos	
Dependencias tecnológicas	
Proveedor (si aplica)	
Ventana de operación	
Ventana de mantenimiento	

### Tipos de mantenimiento aplicables

Marcar los tipos de mantenimiento incluidos en el plan:

- Mantenimiento preventivo.
- Mantenimiento correctivo.
- Mantenimiento adaptativo.
- Mantenimiento evolutivo.

### Actividades de mantenimiento

Nº	Tipo de mantenimiento	Actividad	Frecuencia	Responsable	Impacto esperado
1	Preventivo				
2	Correctivo				
3	Adaptativo				
4	Evolutivo				

**Programación del mantenimiento**

Actividad	Fecha programada	Hora inicio	Hora fin	Ventana autorizada	Comunicación requerida
				( ) Sí ( ) No	

**Impacto en la disponibilidad y continuidad**

Elemento	Descripción
Impacto en usuarios	
Afectación al ANS	( ) Sí ( ) No
Requiere plan de contingencia	( ) Sí ( ) No
Medidas de mitigación	

**Articulación con gestión de cambios**

¿Requiere gestión de cambios?	( ) Sí ( ) No
Tipo de cambio	( ) Estándar ( ) Normal ( ) Emergencia
Ticket de cambio (# asignado GLPI)	
Comité de cambios	

**Registro y trazabilidad**

Elemento	Descripción
Herramienta de registro (MDS)	GLPI
Código del ticket	
Evidencias asociadas	
Responsable de cierre	

**Indicadores de mantenimiento**

Indicador	Fórmula	Frecuencia	Meta
Cumplimiento plan de mantenimiento			
Incidentes post-mantenimiento			
Disponibilidad del servicio			

### Evaluación y mejora

Describir los resultados del mantenimiento, lecciones aprendidas y acciones de mejora propuestas.

### Roles y responsabilidades

Rol	Responsabilidad
Oficina TIC	Planificación, ejecución y control
Proveedor (si aplica)	Ejecución del mantenimiento
Dependencia usuaria	Recepción y validación

### Aprobación del plan

Nombre	Cargo	Firma	Fecha

### Control de versiones

Versión	Fecha	Descripción del cambio	Responsable
1.0		Creación del plan	

### 8.10 Control de consumo de los recursos compartidos por servicios tecnológicos

Los servicios tecnológicos de la alcaldía municipal de Chía operan sobre recursos compartidos tales como infraestructura de cómputo, almacenamiento, red, plataformas, licencias y servicios en la nube. La ausencia de controles sobre el consumo de estos recursos puede generar saturación, degradación del servicio, sobrecostos y riesgos de indisponibilidad, afectando la calidad de los servicios prestados a los usuarios y ciudadanos.

En el marco del modelo de gestión y gobierno TI, el control del consumo de los recursos compartidos se establece como un mecanismo de gobernanza y eficiencia, orientado a garantizar el uso responsable, equitativo y alineado con la capacidad tecnológica, los niveles de servicio y la planeación institucional.

#### 8.10.1 Objetivo

Establecer lineamientos institucionales para medir, controlar, analizar y optimizar el consumo de los recursos tecnológicos compartidos por los servicios de TI, asegurando su uso eficiente, sostenible y alineado con la gestión de capacidad y la gestión de servicios de TI.

#### 8.10.2 Alcance

Estos lineamientos aplican a:

- Todos los servicios tecnológicos definidos en el catálogo de servicios de la Oficina TIC.
- Recursos tecnológicos compartidos asociados a:
  - Infraestructura (servidores, red, almacenamiento).
  - Plataformas y sistemas de información.
  - Servicios en la nube.
- Licenciamiento y suscripciones.
- Servicios prestados directamente por la Oficina TIC o por terceros.

#### 8.10.3 Principios para el control del consumo

- Orientación al servicio: El consumo se analiza por servicio, no solo por infraestructura.
- Equidad: Los recursos se asignan conforme a necesidades reales y criticidad.
- Eficiencia: Se promueve el uso óptimo y responsable de los recursos.
- Transparencia: El consumo debe ser medible, visible y trazable.
- Prevención: Anticipar riesgos de saturación o sobredimensionamiento.
- Gobernanza: El control del consumo es responsabilidad institucional.

#### 8.10.4 Lineamientos para la identificación de recursos compartidos

La Oficina TIC debe identificar y documentar los recursos tecnológicos compartidos que soportan los servicios de TI, incluyendo:

- Infraestructura física y virtual.
- Plataformas comunes.

- Servicios en la nube de uso transversal.
- Cada recurso compartido debe:
  - Estar asociado a uno o varios servicios del catálogo.
  - Contar con responsables definidos.

#### 8.10.5 Lineamientos para la medición del consumo

- El consumo de recursos compartidos debe medirse, como mínimo, en:
  - Capacidad de cómputo (CPU, memoria).
  - Almacenamiento.
  - Ancho de banda y red.
  - Uso de licencias y servicios CLOUD.
- La medición debe:
  - Realizarse de forma periódica o continua según la criticidad.
  - Apoyarse en herramientas de monitoreo institucionales.

#### 8.10.6 Lineamientos para la asignación y límites de consumo

- La Oficina TIC debe definir:
  - Límites de consumo por servicio o grupo de servicios.
  - Umbrales de alerta y saturación.
- Los límites deben:
  - Basarse en la criticidad del servicio.
  - Estar alineados con la capacidad disponible.
- El sobreconsumo debe:
  - Ser analizado y justificado.
  - Gestionarse mediante acciones correctivas o de ampliación.

#### 8.10.7 Lineamientos para el control del consumo en servicios en la nube

- Los servicios en la nube deben:
  - Contar con controles de consumo y costos.
  - Tener alertas de uso configuradas.
- La Oficina TIC debe:
  - Monitorear el consumo por servicio y por dependencia.
  - Evaluar periódicamente el impacto financiero del uso de recursos CLOUD.

#### 8.10.8 Lineamientos para el análisis y optimización del consumo

- El consumo de recursos debe:
  - Analizarse periódicamente para identificar subutilización o sobreutilización.

- Se deben implementar acciones como:
  - Ajustes de capacidad.
  - Redistribución de recursos.
  - Optimización de configuraciones.
- Las decisiones deben documentarse y alinearse con la gestión de cambios cuando aplique.

#### 8.10.9 Lineamientos para la gestión de riesgos asociados al consumo

- El control del consumo debe:
  - Identificar riesgos de saturación, indisponibilidad o sobrecostos.
- Los riesgos identificados deben:
  - Registrarse.
  - Tratarse mediante planes de mitigación.

#### 8.10.10 Lineamientos de roles y responsabilidades

- Oficina TIC:
  - Define métricas, límites y umbrales de consumo.
  - Monitorea y controla el uso de los recursos compartidos.
- Dependencias usuarias:
  - Usan los servicios conforme a los lineamientos definidos.
  - Informan cambios que puedan impactar el consumo.
- Proveedores (cuando aplique):
  - Facilitan información de consumo y apoyan la optimización.

#### 8.10.11 Seguimiento y mejora continua

La Oficina TIC deberá:

- Evaluar periódicamente el consumo de los recursos compartidos.
- Ajustar límites y controles según resultados.
- Incorporar mejoras tecnológicas y de gestión.
- Reportar resultados a las instancias de gobierno TI, cuando aplique, y/o al jefe de la Oficina TIC.

### 8.11 Gestión preventiva de los servicios tecnológicos

La gestión preventiva de los servicios tecnológicos comprende el conjunto de acciones planificadas y sistemáticas orientadas a anticipar, reducir y mitigar riesgos que puedan

afectar la disponibilidad, seguridad, continuidad y calidad de los servicios de TI de la alcaldía municipal de Chía.

En el marco del modelo de gestión y gobierno TI, la gestión preventiva busca evitar incidentes antes de que ocurran, reducir la recurrencia de fallas, fortalecer la seguridad de la información y asegurar que los servicios tecnológicos operen de manera estable y confiable, alineados con los acuerdos de niveles de servicio (ANS).

#### 8.11.1 Objetivo

Establecer lineamientos institucionales para implementar una gestión preventiva integral de los servicios tecnológicos, mediante controles técnicos, operativos y organizacionales que permitan disminuir la probabilidad e impacto de incidentes, fallas operativas y eventos de seguridad de la información.

#### 8.11.2 Alcance

Estos lineamientos aplican a:

- Todos los servicios tecnológicos definidos en el catálogo de servicios de la Oficina TIC.
- Infraestructura tecnológica, sistemas de información, plataformas, redes y servicios en la nube.
- Usuarios internos, contratistas y proveedores que interactúan con los servicios de TI.
- Procesos de soporte, mantenimiento, seguridad de la información y continuidad del servicio.

#### 8.11.3 Principios de la gestión preventiva

- Prevención antes que corrección: Priorizar acciones que eviten incidentes.
- Enfoque basado en riesgos: Actuar según impacto y probabilidad.
- Seguridad por diseño y por defecto.
- Continuidad del servicio como criterio rector.
- Responsabilidad compartida entre TIC, usuarios y proveedores.
- Mejora continua sustentada en datos y lecciones aprendidas.

#### 8.11.4 Lineamientos generales de gestión preventiva

- La Oficina TIC debe implementar controles preventivos sobre:
  - Infraestructura tecnológica.
  - Sistemas de información.

- Accesos, usuarios y credenciales.
- Uso de software y licenciamiento.
- Toda acción preventiva debe:
  - Estar documentada.
  - Ser medible.

#### 8.11.5 Lineamientos de prevención asociados a la seguridad de la información

La gestión preventiva se articula directamente con los procedimientos de seguridad de la información, que establecen controles para prevenir incidentes de seguridad, incluyendo:

- Reporte oportuno de eventos e incidentes de seguridad.
- Manejo adecuado de la información institucional.
- Control del uso de medios removibles.
- Borrado seguro de información en equipos.
- Trabajo controlado en áreas seguras.
- Acceso seguro a la red corporativa.
- Instalación controlada de software.
- Uso legal y autorizado del software.

#### 8.11.6 Lineamientos preventivos en la operación de los servicios TI

- Los servicios tecnológicos deben:
  - Contar con monitoreo preventivo de desempeño y disponibilidad.
  - Tener definidos umbrales de alerta temprana.
- Los eventos detectados deben:
  - Analizarse antes de que se conviertan en incidentes.
  - Generar acciones correctivas preventivas.

#### 8.11.7 Lineamientos preventivos en mantenimiento y capacidad

- La gestión preventiva debe:
  - Integrarse a los planes de mantenimiento de servicios TI.
  - Considerar la capacidad actual y proyectada de los servicios.
- Se deben ejecutar:
  - Mantenimientos preventivos periódicos.
  - Ajustes anticipados de capacidad cuando se identifiquen tendencias de crecimiento.

#### 8.11.8 Lineamientos preventivos en el uso de recursos tecnológicos

- Se deben implementar controles para:
  - Evitar el uso indebido de recursos tecnológicos.
  - Prevenir la sobrecarga de recursos compartidos.
- El consumo anómalo debe:
  - Detectarse tempranamente.
  - Analizarse y corregirse oportunamente.

#### 8.11.9 Lineamientos de prevención mediante capacitación y concientización

- La Oficina TIC debe:
  - Capacitar periódicamente a los usuarios en buenas prácticas de uso de TI.
  - Sensibilizar sobre riesgos de seguridad y operación.
- La capacitación es un control preventivo clave para reducir errores humanos

#### 8.11.10 Lineamientos para la gestión preventiva con proveedores

- Los proveedores de servicios TI deben:
  - Cumplir los controles preventivos definidos por la alcaldía.
  - Alinear sus prácticas a los procedimientos de seguridad de la información.
- Los contratos deben:
  - Incluir obligaciones preventivas y mecanismos de control.

#### 8.11.11 Lineamientos de seguimiento y control

- La Oficina TIC debe:
  - Monitorear la efectividad de las acciones preventivas.
  - Registrar eventos, alertas y acciones realizadas.
- Los resultados deben:
  - Alimentar indicadores de gestión.
  - Servir de insumo para la mejora continua.

### 8.12 Respaldo y recuperación de los servicios tecnológicos

El respaldo y la recuperación de los servicios tecnológicos constituyen un pilar fundamental para garantizar la disponibilidad, integridad, continuidad de la información y de los servicios de TIC que soportan los procesos misionales, estratégicos y de apoyo de la alcaldía municipal de Chía.

En el marco del modelo de gestión y gobierno TI, estos lineamientos buscan asegurar que, ante incidentes operativos, fallas técnicas, eventos de seguridad de la información o desastres, la entidad cuente con mecanismos confiables y documentados que permitan

restaurar oportunamente los servicios tecnológicos y minimizar el impacto en la operación institucional y en la atención al ciudadano.

#### 8.12.1 Objetivo

Establecer los lineamientos institucionales para la planificación, ejecución, control y mejora de las actividades de respaldo y recuperación de los servicios tecnológicos, garantizando la protección de la información y la restauración oportuna de los servicios ante incidentes o eventos disruptivos.

#### 8.12.2 Alcance

Estos lineamientos aplican a:

- Todos los servicios tecnológicos definidos en el catálogo de servicios de la Oficina TIC.
- Sistemas de información, bases de datos, infraestructura, plataformas y servicios en la nube.
- Información institucional en ambientes productivos, de contingencia y respaldo.
- Servicios prestados directamente por la Oficina TIC o a través de terceros.

#### 8.12.3 Principios del respaldo y la recuperación

- Protección de la información como activo estratégico.
- Prevención y preparación ante incidentes y fallas.
- Recuperación oportuna de los servicios críticos.
- Integridad y confidencialidad de la información respaldada.
- Alineación con la continuidad del servicio.
- Gobernanza y trazabilidad de los procesos de respaldo y recuperación.

#### 8.12.4 Lineamientos para la definición de respaldos

- La Oficina TIC debe definir políticas y esquemas de respaldo que incluyan:
  - Tipo de información a respaldar.
  - Frecuencia de los respaldos.
  - Tipo de respaldo (completo, incremental, diferencial).
- Los respaldos deben priorizar:
  - Servicios críticos y de alta criticidad.
  - Información sensible o estratégica.

Tabla No. 23 Tipos de respaldo

Tipo de respaldo	Descripción
Completo	Copia total de la información
Incremental	Copia de cambios desde el último respaldo
Diferencial	Copia de cambios desde el último respaldo completo
Snapshot	Captura del estado del sistema
Replicación	Copia continua a sitio alternativo
Administrado proveedor	Respaldo nativo del servicio CLOUD

#### 8.12.5 Lineamientos para la gestión de respaldos

- Los respaldos deben:
  - Ejecutarse de forma automática cuando sea posible.
  - Verificarse periódicamente para garantizar su integridad.
- La información respaldada debe:
  - Almacenarse en ubicaciones seguras y separadas del ambiente productivo.
  - Contar con controles de acceso y cifrado cuando aplique.

#### 8.12.6 Lineamientos para respaldos en servicios en la nube

- Los servicios en la nube deben:
  - Utilizar mecanismos de respaldo ofrecidos por el proveedor o definidos por la entidad.
  - Contar con retención adecuada de la información respaldada.
- La Oficina TIC debe:
  - Verificar el cumplimiento de los compromisos de respaldo del proveedor.
  - Asegurar la disponibilidad de los respaldos ante incidentes.

#### 8.12.7 Lineamientos para la recuperación de los servicios tecnológicos

- La recuperación de servicios debe:
  - Estar alineada con los valores de RTO y RPO definidos institucionalmente.
  - Ejecutarse conforme a procedimientos documentados.
- La restauración debe incluir:
  - Validación de la integridad de la información recuperada.
  - Verificación del funcionamiento del servicio restaurado.

Tabla No. 24 Matriz de respaldo y recuperación de los servicios tecnológicos

Servicio de TI	Proceso que Soporta	Criticidad	Tipo de Respaldo	Frecuencia de Respaldo	Ubicación del Respaldo	RTO (Tiempo Máx. Recuperación)	RPO (Pérdida Máx. de Datos)	Responsable
Plataforma de trámites en línea	Atención al ciudadano	Alta	Completo + Incremental	Diario / Cada 4 horas	Nube segura / Región secundaria	4 horas	30 minutos	Atención al ciudadano / Oficina TIC
Sistema PQRS	Atención al Ciudadano	Alta	Completo + Incremental	Diario	Nube / Sitio alternativo	6 horas	1 hora	Atención al ciudadano / Oficina TIC
Correo Institucional	Comunicación institucional	Alta	Respaldo administrado proveedor	Continuo	Nube del proveedor	2 horas	15 minutos	Oficina TIC
Sistema financiero	Gestión financiera	Alta	Completo + Incremental	Diario	Sitio alternativo cifrado	4 horas	30 minutos	Sec. Hacienda / Oficina TIC
Sistema documental	Gestión documental	Media	Completo	Diario	Nube	12 horas	4 horas	Dirección de servicios administrativos / Oficina TIC
Almacenamiento institucional en la nube	Gestión de información	Media	Replicación + Snapshot	Diario	Nube / Sitio alternativo	12 horas	2 horas	Oficina TIC
Sistema de talento humano	Gestión del talento	Media	Completo	Diario	Sitio alternativo	24 horas	8 horas	Dirección de función pública / Oficina TIC
Mesa de servicios TI	Soporte institucional	Media	Completo	Diario	Nube / Sitio alternativo	8 horas	2 horas	Oficina TIC
Plataforma de analítica / BI	Planeación y control	Baja	Completo	Semanal	Nube	48 horas	24 horas	Oficina TIC

Servicio de TI	Proceso que Soporta	Criticidad	Tipo de Respaldo	Frecuencia de Respaldo	Ubicación del Respaldo	RTO (Tiempo Máx. Recuperación)	RPO (Pérdida Máx. de Datos)	Responsable
Plataforma de capacitación virtual	Formación	Baja	Completo	Semanal	Nube	72 horas	24 horas	Oficina TIC

#### 8.12.8 Lineamientos de recuperación ante incidentes de seguridad

- Ante incidentes de seguridad de la información:
  - La recuperación debe ejecutarse después de la fase de contención y erradicación.
  - Debe preservarse la evidencia cuando aplique.
- La recuperación puede implicar:
  - Restauración desde respaldos confiables.
  - Reinstalación de sistemas.
  - Endurecimiento de configuraciones para prevenir recurrencias.

#### 8.12.9 Lineamientos para pruebas de respaldo y recuperación

- La Oficina TIC debe:
  - Realizar pruebas periódicas de restauración.
  - Documentar resultados y lecciones aprendidas.
- Las pruebas deben:
  - Verificar tiempos de recuperación.
  - Validar la confiabilidad de los respaldos.

#### 8.12.10 Lineamientos para la documentación y trazabilidad

- Toda actividad de respaldo y recuperación debe:
  - Documentarse y registrarse en las herramientas institucionales.
  - Contar con responsables definidos.
- La documentación debe:
  - Servir de insumo para auditorías y procesos de mejora.

#### 8.12.11 Lineamientos de roles y responsabilidades

- Oficina TIC:

- Define, ejecuta y controla los procesos de respaldo y recuperación.
- Verifica la disponibilidad de los respaldos.
- Dependencias usuarias:
  - Informan oportunamente incidentes que afecten la información o los servicios.
- Proveedores (cuando aplique):
  - Cumplen los esquemas de respaldo y recuperación acordados contractualmente.

### 8.13 Análisis de riesgos

El análisis de riesgos es un componente transversal del gobierno TI que permite identificar, evaluar y priorizar los riesgos que puedan afectar la disponibilidad, continuidad, seguridad y calidad de los servicios tecnológicos de la alcaldía municipal de Chía.

En el marco del modelo de gestión y gobierno TI, el análisis de riesgos no se limita a un ejercicio documental, sino que se constituye en un mecanismo permanente de apoyo a la toma de decisiones, orientado a prevenir incidentes, reducir impactos operativos y fortalecer la confianza en los servicios digitales ofrecidos a la ciudadanía.

#### 8.13.1 Objetivo

Establecer los lineamientos institucionales para realizar el análisis de riesgos asociados a los servicios tecnológicos, garantizando su alineación con la gestión de servicios TI, la seguridad de la información, la continuidad del servicio y el proceso institucional de valoración de riesgos.

#### 8.13.2 Alcance

Estos lineamientos aplican a:

- Todos los servicios tecnológicos incluidos en el catálogo de servicios de la Oficina TIC.
- Los activos de información, infraestructura, plataformas, sistemas de información y servicios en la nube que soportan dichos servicios.
- Los riesgos operativos, tecnológicos, de seguridad de la información y de continuidad, asociados a la prestación de los servicios TI.

#### 8.13.3 Principios del análisis de riesgos

- Enfoque basado en riesgos: Priorización según impacto y probabilidad.

- Orientación al servicio: El análisis parte del servicio tecnológico y no solo del activo técnico.
- Prevención: Anticipación de eventos que puedan afectar la operación.
- Proporcionalidad: Los controles se definen según la criticidad del riesgo.
- Mejora continua: Revisión y actualización periódica.
- Gobernanza: Roles y responsabilidades claramente definidos.

#### 8.13.4 Lineamientos para la identificación de riesgos

- El análisis de riesgos debe iniciar con la identificación de los activos de información y servicios tecnológicos asociados a cada proceso institucional.
- Se deben identificar amenazas y vulnerabilidades considerando:
  - Tecnología.
  - Infraestructura.
  - Sistemas de información.
  - Recurso humano.
  - Proveedores y terceros.
- La identificación debe apoyarse en:
  - Historial de incidentes (Mesa de servicios / GLPI).
  - Reportes de seguridad.
  - Cambios tecnológicos y organizacionales.

#### 8.13.5 Lineamientos para el análisis y evaluación de riesgos

- Los riesgos identificados deben evaluarse considerando:
  - Probabilidad de ocurrencia.
  - Impacto potencial sobre la confidencialidad, integridad y disponibilidad.
- La evaluación debe:
  - Determinar el riesgo inherente y residual.
  - Utilizar la matriz institucional de riesgos definida por la entidad.
- Los riesgos deben clasificarse en niveles (alto, medio, bajo) para su priorización.

#### 8.13.6 Lineamientos para el tratamiento de riesgos

- Para los riesgos priorizados se debe definir un plan de tratamiento, que puede incluir:
  - Controles preventivos.
  - Controles detectivos.
  - Controles correctivos.
- Las opciones de tratamiento incluyen:
  - Mitigar.
  - Transferir.
  - Aceptar.

- Evitar.
- El tratamiento debe alinearse con:
  - Procedimientos de seguridad de la información.
  - Gestión de incidentes de seguridad.
  - Gestión preventiva de los servicios tecnológicos.

#### 8.13.7 Lineamientos para la articulación con la gestión de incidentes

- Los riesgos materializados deben:
  - Registrarse como incidentes.
  - Retroalimentar el análisis de riesgos.
- El análisis posterior al incidente debe:
  - Identificar causas raíz.
  - Ajustar controles y planes de tratamiento.

#### 8.13.8 Lineamientos para el monitoreo y seguimiento

- La Oficina TIC debe:
  - Monitorear periódicamente los riesgos identificados.
  - Verificar la efectividad de los controles implementados.
- El seguimiento debe:
  - Actualizar la matriz de riesgos.
  - Ajustar prioridades según cambios tecnológicos o institucionales.

#### 8.13.9 Lineamientos para roles y responsabilidades

- Oficina TIC:
  - Lidera el análisis de riesgos TI y de servicios tecnológicos.
  - Consolida y actualiza la matriz de riesgos.
  - Asegura la alineación con el MSPI y políticas de seguridad.
- Responsables de procesos y servicios:
  - Identifican riesgos asociados a su operación.
  - Apoyan la implementación de controles.
- Proveedores:
  - Cumplen controles y reportan riesgos asociados a los servicios prestados.

#### 8.13.10 Documentación y trazabilidad

- Todo análisis de riesgos debe:
  - Documentarse formalmente.
  - Mantener trazabilidad de decisiones y controles.
- La documentación es insumo para:

- Auditorías.
- Planeación de inversiones TI.
- Mejora continua del MGGTI.

## 8.14 Seguridad informática

La seguridad informática se encuentra alineada con el modelo de gestión de arquitectura empresarial, la política de seguridad de la información y las mejores prácticas internacionales ISO/IEC 27001:2022, garantizando de esta manera el cumplimiento normativo y el enfoque en generar valor al ciudadano, mediante la protección de la información, que confían a la entidad.

### 8.14.1 Objetivo

Establecer lineamientos para proteger la infraestructura tecnológica, los sistemas de información, las redes, los dispositivos y los servicios digitales de la alcaldía de Chía frente a amenazas internas y externas, garantizando la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información que soporta la gestión institucional y la prestación de servicios a la ciudadanía.

### 8.14.2 Alcance

Estos lineamientos aplican a todos los servicios TI, activos tecnológicos, funcionarios, contratistas, proveedores y terceros, que interactúan con los recursos informáticos de la entidad.

### 8.14.3 Enfoque de gestión

La seguridad informática se gestiona como un componente integral del modelo de seguridad y privacidad de la información (MSPI) y del gobierno TI, bajo un enfoque preventivo, basado en riesgos y de mejora continua, alineado con:

- NTC-ISO/IEC 27001:2022.
- Resolución 500 de 2021 – Seguridad digital.
- CONPES 3995 de 2020.
- Decreto 1008 de 2018 (Gobierno digital).

### 8.14.4 Lineamientos estratégicos

#### 8.14.4.1 Gobierno y responsabilidades

- La Oficina TIC es responsable de liderar, coordinar y supervisar la seguridad informática institucional.
- El comité de seguridad de la información apoya la toma de decisiones, priorización de riesgos y respuesta ante incidentes.
- Todos los funcionarios, contratistas y proveedores son corresponsables del cumplimiento de los controles de seguridad informática según su rol.

#### 8.14.4.2 Gestión de riesgos informáticos

- Identificar, analizar y valorar periódicamente los riesgos informáticos que afecten infraestructura, sistemas y servicios TIC.
- Definir y aplicar controles técnicos, administrativos y operativos para mitigar los riesgos identificados.
- Mantener actualizada la matriz de riesgos informáticos, articulada con la gestión de riesgos institucional.

#### 8.14.4.3 Control de accesos y privilegios

- Implementar controles de acceso lógico basados en roles y principio de mínimo privilegio.
- Garantizar autenticación robusta, uso de contraseñas seguras y, cuando aplique, autenticación multifactor.
- Gestionar altas, modificaciones y bajas de usuarios de forma oportuna ante cambios de rol o desvinculación.

#### 8.14.4.4 Seguridad en infraestructura y redes

- Proteger la infraestructura tecnológica mediante firewalls, segmentación de red, IDS/IPS, antivirus y monitoreo continuo.
- Mantener documentación actualizada de la arquitectura tecnológica y configuraciones críticas.
- Implementar esquemas de redundancia y alta disponibilidad para servicios críticos.

#### 8.14.4.5 Seguridad en sistemas de información

- Integrar requisitos de seguridad informática en todo el ciclo de vida de los sistemas de información (análisis, diseño, desarrollo, pruebas, producción y mantenimiento).
- Separar ambientes de desarrollo, pruebas y producción.

- Aplicar prácticas de desarrollo seguro y gestión controlada de versiones y código fuente.

#### *8.14.4.6 Gestión de incidentes de seguridad informática*

- Establecer mecanismos claros para el reporte, clasificación, atención y cierre de incidentes de seguridad informática.
- Garantizar tiempos de respuesta acordes a la criticidad del incidente.
- Documentar incidentes, evidencias, lecciones aprendidas y acciones correctivas para prevenir recurrencias.

#### *8.14.4.7 Respaldo, recuperación y continuidad*

- Asegurar respaldos periódicos de sistemas y datos críticos, conforme a la criticidad de los servicios.
- Definir y probar planes de recuperación ante incidentes y desastres (RTO/RPO).
- Integrar la seguridad informática a los planes de continuidad de los servicios TI.

#### *8.14.4.8 Seguridad con terceros y proveedores*

- Exigir cláusulas de seguridad informática y confidencialidad en los contratos con proveedores de TIC.
- Evaluar periódicamente el cumplimiento de los controles de seguridad por parte de terceros.
- Gestionar cambios tecnológicos con proveedores a través del proceso institucional de gestión de cambios.

#### *8.14.4.9 Sensibilización y cultura de seguridad*

- Desarrollar programas permanentes de capacitación y concientización en seguridad informática.
- Promover buenas prácticas en el uso de equipos, redes, sistemas y servicios digitales.
- Fortalecer la cultura de reporte oportuno de incidentes y eventos de seguridad.

#### *8.14.4.10 Seguimiento y mejora continua*

- Realizar auditorías internas periódicas sobre la seguridad informática.

- Medir el desempeño mediante indicadores de incidentes, disponibilidad, cumplimiento de controles y madurez.
- Actualizar los lineamientos ante cambios normativos, tecnológicos o resultados de auditorías e incidentes.

### 8.15 Disposición de residuos tecnológicos

La disposición de residuos tecnológicos constituye un componente esencial de la gestión responsable de los servicios de TI, orientado a garantizar el manejo adecuado, seguro y ambientalmente responsable de los equipos, dispositivos y componentes tecnológicos que han cumplido su ciclo de vida útil en la alcaldía municipal de Chía.

En el marco del modelo de gestión y gobierno TI (MGGTI), estos lineamientos buscan asegurar que la disposición de residuos tecnológicos se realice de manera controlada, trazable y alineada con la normativa ambiental y de seguridad de la información, evitando riesgos ambientales, legales y de exposición de información institucional.

#### 8.15.1 Objetivo

Establecer los lineamientos institucionales para la gestión y disposición final de los residuos tecnológicos generados por la operación de los servicios de TI, garantizando el cumplimiento normativo, la protección de la información y la sostenibilidad ambiental.

#### 8.15.2 Alcance

Estos lineamientos aplican a:

- Equipos de cómputo, periféricos y dispositivos electrónicos.
- Infraestructura tecnológica en desuso (servidores, switches, routers, UPS, etc.).
- Medios de almacenamiento (discos duros, SSD, cintas, USB).
- Componentes, partes y consumibles tecnológicos.
- Residuos generados por mantenimiento, renovación o baja de activos TI.

#### 8.15.3 Principios para la disposición de residuos tecnológicos

- Responsabilidad ambiental.
- Cumplimiento normativo.
- Protección de la información.
- Trazabilidad del proceso.
- Economía circular, cuando aplique.
- Gobernanza y control institucional.

#### 8.15.4 Lineamientos generales de gestión de residuos tecnológicos

- La disposición de residuos tecnológicos debe:
  - Realizarse de forma planificada y documentada.
  - Estar alineada con los procesos de baja de activos institucionales.
- Ningún equipo o componente tecnológico podrá:
  - Ser desechado informalmente.
  - Entregarse a terceros sin autorización institucional.

#### 8.15.5 Clasificación de residuos tecnológicos

La Oficina TIC debe liderar la clasificación adecuada de los residuos tecnológicos, incluyendo:

- Equipos reutilizables: Susceptibles de reasignación o donación institucional.
- Equipos obsoletos o dañados: Destinados a disposición final.
- Componentes peligrosos: Baterías, UPS, monitores, entre otros.
- Medios de almacenamiento: Con tratamiento especial por contener información.

#### 8.15.6 Lineamientos para la protección de la información

- Antes de la disposición de cualquier equipo o medio de almacenamiento:
  - Se debe realizar el borrado seguro de la información, conforme a los procedimientos de seguridad de la información.
- Cuando aplique:
  - Se debe realizar la destrucción física de los medios de almacenamiento.
- Todas las acciones deben:
  - Documentarse y validarse por la Oficina TIC.

#### 8.15.7 Lineamientos para la disposición ambientalmente responsable

- Los residuos tecnológicos deben:
  - Entregarse únicamente a gestores autorizados del manejo de los residuos de aparatos eléctricos y electrónicos (RAEE).
  - Cumplir la normatividad ambiental vigente.
- La Oficina TIC debe:
  - Verificar certificaciones y autorizaciones del gestor.
  - Exigir certificados de disposición final.

Tabla No. 25 Matriz de disposición de residuos tecnológicos

Equipo / activo tecnológico	Tipo de residuo	Riesgo asociado	Tratamiento requerido	Responsable principal	Soporte Evidencia /
Computador de escritorio	RAEE	Información ambiental	Borrado seguro + reciclaje RAEE	Oficina TIC	Acta de borrado + Certificado RAEE
Computador portátil	RAEE	Información ambiental	Borrado seguro + reciclaje RAEE	Oficina TIC	Acta + Certificado RAEE
Servidor físico	RAEE	Alto (datos críticos)	Destrucción de discos + reciclaje	Oficina TIC	Acta de destrucción
Disco duro / SSD	Residuo peligroso	Fuga de información	Destrucción física certificada	Oficina TIC	Certificado de destrucción
Switch / Router	RAEE	Ambiental	Reciclaje RAEE autorizado	Oficina TIC	Certificado RAEE
Impresora	RAEE	Ambiental	Reciclaje RAEE	Oficina TIC	Certificado RAEE
UPS	RAEE Peligroso	Ambiental eléctrico	Entrega a gestor RAEE especializado	Oficina TIC	Certificado RAEE
Baterías	Residuo peligroso	Ambiental	Disposición controlada	Gestor RAEE	Certificado ambiental
Monitores	RAEE	Ambiental	Reciclaje RAEE	Oficina TIC	Certificado RAEE
Teléfonos IP / móviles	RAEE	Información	Borrado + reciclaje	Oficina TIC / Sec. Gobierno	Acta + Certificado RAEE
Cámaras CCTV	RAEE	Seguridad	Borrado + reciclaje	Oficina TIC / Proveedor / Iduvi	Acta de borrado
Equipos de red obsoletos	RAEE	Ambiental	Reciclaje RAEE	Oficina TIC	Certificado RAEE
Consumibles (toner, cartuchos)	Residuo especial	Ambiental	Disposición especializada	Área administrativa	Certificado proveedor

#### 8.15.8 Lineamientos para la trazabilidad y control

- Todo proceso de disposición debe:
  - Contar con acta de baja del activo.

- Incluir inventario detallado de los residuos.
- Conservar soportes y certificados.
- La información debe:
  - Integrarse al inventario de activos TI.

#### 8.15.9 Lineamientos de roles y responsabilidades

- Oficina TIC:
  - Identifica, clasifica y autoriza la disposición de residuos tecnológicos.
  - Garantiza los medios tecnológicos para la protección de la información.
- Área Administrativa / Almacén:
  - Apoya los procesos de baja y control de activos.
- Gestores externos (RAEE):
  - Realizan la disposición final conforme a la normatividad ambiental.

#### 8.15.10 Seguimiento y mejora continua

- La Oficina TIC debe:
  - Realizar seguimiento periódico a los procesos de disposición.
  - Evaluar oportunidades de reutilización y reciclaje.
- Los resultados deben:
  - Alimentar indicadores de gestión y sostenibilidad.

#### 8.15.11 Reglas institucionales obligatorias

- Ningún equipo puede salir de la entidad sin:
  - Autorización formal.
  - Registro en inventario.
  - Tratamiento definido.
- Los equipos con almacenamiento deben:
  - Tener borrado seguro o destrucción física.
- Solo se permite disposición con:
  - Gestores RAEE autorizados.
- Todos los procesos deben:
  - Contar con evidencias documentales.

## 8.16 Gestión de problemas de TI

La gestión de problemas de TI tiene como propósito identificar, analizar y eliminar las causas raíz de los incidentes que afectan los servicios tecnológicos de la alcaldía municipal de Chía, con el fin de reducir la recurrencia de fallas, minimizar impactos en la operación institucional y mejorar de forma sostenida la calidad y estabilidad de los servicios de TI.

En el marco del modelo de gestión y gobierno TI (MGGTI), la gestión de problemas se constituye como un proceso clave de gestión preventiva y de mejora continua, complementario a la gestión de incidentes y articulado con la seguridad de la información, la continuidad del servicio y la gestión de cambios.

### 8.16.1 Objetivo

Establecer los lineamientos institucionales para la identificación, análisis, tratamiento y cierre de problemas de TI, garantizando la eliminación de causas raíz de incidentes, la reducción de riesgos operativos, el fortalecimiento de la disponibilidad y confiabilidad de los servicios tecnológicos.

### 8.16.2 Alcance

Estos lineamientos aplican a:

- Todos los servicios tecnológicos incluidos en el catálogo de servicios de la Oficina TIC.
- Incidentes recurrentes, críticos o de alto impacto.
- Fallas estructurales asociadas a infraestructura, sistemas de información, plataformas, seguridad o proveedores.
- Problemas identificados de manera reactiva o proactiva.

### 8.16.3 Principios de la gestión de problemas

- Enfoque en causa raíz, no solo en síntomas.
- Prevención de incidentes recurrentes.
- Priorización basada en impacto y riesgo.
- Trazabilidad y documentación del análisis y decisiones.
- Articulación con seguridad y continuidad.
- Mejora continua de los servicios de TI.

### 8.16.4 Definición institucional de problema

Para efectos del MGGTI, se entiende por:

- Incidente: Interrupción no planificada o degradación de un servicio.
- Problema: Causa desconocida o subyacente de uno o más incidentes, o una debilidad significativa que puede generar incidentes futuros.

#### 8.16.5 Lineamientos para la identificación de problemas

- Un problema puede originarse por:
  - Incidentes recurrentes o críticos.
  - Tendencias identificadas en la mesa de servicios (MDS).
  - Resultados de análisis de riesgos.
  - Hallazgos de auditoría o seguridad.
- La Oficina TIC debe:
  - Registrar los problemas en la herramienta institucional (GLPI).
  - Asociarlos a los incidentes relacionados.

#### 8.16.6 Lineamientos para el análisis de problemas

- Todo problema debe:
  - Contar con un responsable asignado.
  - Analizarse mediante técnicas de causa raíz (Ejemplo: 5 Porqués, Ishikawa).
- El análisis debe considerar:
  - Impacto en los servicios y procesos.
  - Riesgos de seguridad de la información.
  - Dependencias tecnológicas y de proveedores.

Tabla No. 26 Ejemplo de matriz de gestión de problemas

Código Problema	Servicio de TI afectado	Incidente(s) relacionado(s)	Causa raíz identificada	Solución temporal	Solución definitiva	Responsable	Estado
PR-001	Plataforma de trámites en línea	INC-145, INC-152	Saturación de base de datos por crecimiento no planificado	Reinicio controlado fuera de horario	Ampliación de capacidad + optimización de consultas	Oficina TIC / Infraestructura	Cerrado
PR-002	Correo institucional	INC-210, INC-218	Configuración inadecuada de filtros antispam	Ajuste manual de reglas	Reconfiguración + monitoreo continuo	Oficina TIC	Cerrado

Código Problema	Servicio de TI afectado	Incidente(s) relacionado(s)	Causa raíz identificada	Solución temporal	Solución definitiva	Responsable	Estado
PR-003	Sistema PQRS	INC-301	Error en validación de campos del formulario	Corrección manual de registros	Ajuste en código fuente y pruebas	Oficina TIC / Desarrollo	En seguimiento
PR-004	Red institucional	INC-412, INC-419	Equipo de red obsoleto	Redireccionamiento de tráfico	Renovación de switch	Oficina TIC / Infraestructura	Cerrado
PR-005	Sistema financiero	INC-522	Dependencia de proveedor externo sin redundancia	Procedimiento manual alternativo	Contrato de soporte con SLA + HA	Oficina TIC / Sec. Hacienda / Proveedor	En ejecución
PR-006	Mesa de servicios TI	INC-601	Falta de capacitación de usuarios	Apoyo telefónico extendido	Capacitación y guías de uso	Oficina TIC	Cerrado

#### 8.16.7 Lineamientos para soluciones temporales y definitivas

- Cuando no sea posible una solución inmediata:
  - Se deben definir soluciones temporales para reducir el impacto.
- Las soluciones definitivas deben:
  - Eliminar la causa raíz.
  - Documentarse y validarse técnicamente.
- Toda solución que implique cambios debe:
  - Gestionarse a través del proceso de gestión de cambios.

#### 8.16.8 Lineamientos para la articulación con la seguridad de la información

- Los problemas relacionados con seguridad deben:
  - Coordinarse con el responsable de seguridad de la información.
  - Considerar controles preventivos y correctivos definidos en los procedimientos institucionales.
- Los problemas derivados de incidentes de seguridad deben:
  - Retroalimentar el análisis de riesgos y los controles de seguridad.

#### 8.16.9 Lineamientos para el seguimiento y cierre

- Un problema solo podrá cerrarse cuando:
  - La causa raíz haya sido eliminada o mitigada.
  - Se haya verificado la efectividad de la solución.
- El cierre debe:
  - Documentar lecciones aprendidas.
  - Actualizar la base de conocimiento institucional.

#### 8.16.10 Lineamientos de roles y responsabilidades

- Oficina TIC:
  - Lidera la gestión de problemas de TI.
  - Prioriza, analiza y hace seguimiento a los problemas.
- Mesa de servicios (MDS):
  - Identifica tendencias e incidentes recurrentes.
  - Apoya la identificación de problemas.
- Responsable de seguridad de la información:
  - Participa en problemas relacionados con seguridad.
- Proveedores (cuando aplique):
  - Apoyan el análisis y solución de problemas asociados a los servicios prestados.

#### 8.16.11 Articulación con la gestión de servicios de TI

La gestión de problemas se articula con:

- Gestión de incidentes.
- Gestión preventiva de los servicios tecnológicos.
- Análisis de riesgos.
- Gestión de cambios.
- Continuidad y disponibilidad de servicios TI.
- Respaldo y recuperación de servicios TI.

#### 8.16.12 Indicadores de la gestión de problemas

Se deben definir indicadores como:

- Número de problemas identificados vs. resueltos.
- Reducción de incidentes recurrentes.
- Tiempo promedio de resolución de problemas.
- Porcentaje de problemas con causa raíz documentada.

### 8.16.13 Reglas institucionales obligatorias

- Todo problema debe:
  - Estar asociado a uno o más incidentes.
  - Tener causa raíz documentada.
- No se permite cerrar problemas sin:
  - Solución definitiva o mitigación aceptada.
- Las soluciones definitivas deben:
  - Gestionarse por gestión de cambios cuando aplique.
- Los problemas de seguridad:
  - Deben articularse con el responsable de seguridad de la información.

## 8.17 Gestión de cambios de TI

La gestión de cambios de TI tiene como propósito garantizar que todas las modificaciones que impacten los servicios tecnológicos, la infraestructura, los sistemas de información o los componentes TIC de la alcaldía municipal de Chía se realicen de manera planificada, controlada, documentada y autorizada, minimizando riesgos operativos, de seguridad de la información y de indisponibilidad de los servicios.

En el marco del modelo de gestión y gobierno TI (MGGTI), la gestión de cambios es un proceso transversal que asegura la estabilidad de los servicios TI, facilita la innovación controlada y fortalece la alineación entre la estrategia institucional, la arquitectura empresarial y la operación tecnológica.

### 8.17.1 Objetivo

Establecer los lineamientos institucionales para la identificación, evaluación, aprobación, implementación, seguimiento y cierre de los cambios de TI, garantizando trazabilidad, control del riesgo y continuidad de los servicios tecnológicos.

### 8.17.2 Alcance

Estos lineamientos aplican a:

- Todos los servicios tecnológicos incluidos en el catálogo de servicios de la Oficina TIC.
- Cambios que afecten infraestructura, redes, plataformas, sistemas de información, configuraciones, parches, licencias y servicios en la nube.
- Cambios solicitados por dependencias internas o identificados por la Oficina TIC.

- Cambios gestionados directamente por la entidad o a través de proveedores externos.

### 8.17.3 Principios de la gestión de cambios

- Control y trazabilidad de todo cambio.
- Evaluación previa del riesgo e impacto.
- Aprobación formal antes de la implementación.
- Minimización del impacto en los servicios.
- Seguridad de la información por diseño.
- Mejora continua basada en lecciones aprendidas.

### 8.17.4 Tipos de cambios de TI

La Oficina TIC debe clasificar los cambios de TI de acuerdo con la metodología institucional en:

#### 8.17.4.1 *Cambio normal*

Cambios planificados que pueden generar afectación a los servicios o infraestructura TIC y requieren evaluación y aprobación formal por el comité de cambios (CAB).

#### 8.17.4.2 *5.2 Cambio estándar*

Cambios de bajo riesgo y alta recurrencia, con procedimientos previamente aprobados, que no requieren aprobación individual del CAB.

#### 8.17.4.3 *Cambio de emergencia*

Cambios urgentes requeridos para restaurar un servicio crítico o mitigar una vulnerabilidad grave, cuya aprobación no puede esperar el ciclo regular.

### 8.17.5 Lineamientos para el registro y clasificación

- Todo cambio debe:
  - Registrarse formalmente como RFC en la mesa de servicios (GLPI).
  - Diligenciar el formato de control de cambios TIC aprobado por calidad.
- La Oficina TIC debe:
  - Clasificar el tipo de cambio.
  - Determinar impacto, prioridad y riesgo.

### 8.17.6 Lineamientos para el análisis y aprobación

- Todo cambio debe someterse a:
  - Análisis técnico y funcional.
  - Evaluación de riesgos operativos y de seguridad de la información.
- Los cambios normales y de alto impacto deben:
  - Ser evaluados y aprobados por el comité de cambios (CAB) o el jefe de la Oficina TIC.
- Los cambios rechazados deben:
  - Documentarse y cerrarse formalmente.

#### 8.17.7 Lineamientos para la planeación del cambio

Todo cambio aprobado debe contar con:

- Plan de implementación detallado.
- Identificación de riesgos y plan de tratamiento.
- Plan de pruebas.
- Plan de reversión (roll-back).
- Cronograma y responsables definidos.

#### 8.17.8 Lineamientos para la implementación

- La implementación debe:
  - Realizarse conforme al plan aprobado.
  - Minimizar el impacto en la operación institucional.
- Los cambios deben:
  - Ejecutarse preferiblemente en ventanas de mantenimiento.
  - Cumplir los controles de seguridad definidos.

#### 8.17.9 Lineamientos para pruebas y validación

- Todo cambio debe:
  - Ser probado antes de su puesta en producción.
  - Validarse funcional y técnicamente.
- Las pruebas deben:
  - Documentarse y conservar evidencias.

#### 8.17.10 Lineamientos para el cierre y documentación

- Un cambio solo podrá cerrarse cuando:
  - Se hayan completado las pruebas exitosamente.
  - Se haya actualizado la CMDB si aplica.

- Se documenten las lecciones aprendidas.
- El cierre debe:
  - Registrarse en la herramienta GLPI.

#### 8.17.11 Articulación con la seguridad de la información

- Los cambios que impacten datos, accesos o infraestructura crítica deben:
  - Contar con la validación del responsable de seguridad de la información y/o el comité de seguridad de la información.
- Los cambios de emergencia relacionados con incidentes de seguridad deben:
  - Articularse con el proceso de gestión de incidentes de seguridad

#### 8.17.12 Roles y responsabilidades

- Gestor del cambio (Oficina TIC):
  - Lidera todo el ciclo del cambio.
- Solicitante del cambio:
  - Justifica y valida el cambio.
- Equipo técnico ejecutor:
  - Implementa, prueba y documenta el cambio.
- Comité de seguridad de la información:
  - Evalúa riesgos de ciberseguridad cuando aplique.
- Área de calidad:
  - Garantiza la vigencia de formatos y procedimientos.

#### 8.17.13 Seguimiento y control

- La Oficina TIC debe:
  - Medir el desempeño de la gestión de cambios.
  - Analizar cambios fallidos o revertidos.
- Los resultados deben:
  - Alimentar indicadores del MGGTI.
  - Soportar la mejora continua.

Tabla No. 27 Matriz de gestión de cambios TI

Tipo de Cambio	Descripción del Cambio	Nivel de Riesgo	Impacto en el Servicio	Aprobador	Tiempo Máx. de Aprobación	Tiempo Máx. de Implementación
Cambio estándar	Actualización rutinaria de	Bajo	Bajo / Nulo	Oficina TIC	<= 1 día hábil	<= 2 días hábiles

Tipo de Cambio	Descripción del Cambio	Nivel de Riesgo	Impacto en el Servicio	Aprobador	Tiempo Máx. de Aprobación	Tiempo Máx. de Implementación
	software autorizado					
Cambio estándar	Creación/modificación de usuarios y accesos	Bajo	Bajo	Oficina TIC	<= 1 día hábil	<= 1 día hábil
Cambio estándar	Ajustes de configuración menores	Bajo	Bajo	Oficina TIC	<= 1 día hábil	<= 2 días hábiles
Cambio normal	Actualización de sistema de información	Medio	Medio	Comité de cambios (CAB)	<= 3 días hábiles	<= 5 días hábiles
Cambio normal	Modificación de infraestructura tecnológica	Medio	Medio Alto	Comité de cambios (CAB)	<= 3 días hábiles	<= 7 días hábiles
Cambio normal	Integración de nuevos módulos o servicios	Medio	Alto	Comité de cambios (CAB)	<= 5 días hábiles	<= 15 días hábiles
Cambio normal	Ajustes funcionales solicitados por dependencia	Medio	Medio	Comité de cambios (CAB)	<= 3 días hábiles	Según alcance
Cambio de emergencia	Restauración de servicio crítico	Alto	Alto Crítico	Jefe Oficina TIC	Inmediato	Inmediato
Cambio de emergencia	Mitigación de vulnerabilidad crítica	Alto	Crítico	Jefe Oficina TIC y/o Comité de seguridad de la información	Inmediato	Inmediato
Cambio de emergencia	Corrección urgente de error en producción	Alto	Alto	Jefe Oficina TIC	Inmediato	<= 24 horas

Tabla No. 28 Criterios de clasificación del riesgo

Nivel de Riesgo	Criterios
Bajo	Sin impacto significativo, cambios repetitivos y controlados
Medio	Impacto moderado, requiere validación técnica y funcional

Nivel de Riesgo	Criterios
Alto	Impacto crítico, riesgo para la continuidad o seguridad

### 8.18 Implementación del protocolo de internet versión 6 (IPv6)

El crecimiento sostenido de los servicios digitales, la ampliación de la infraestructura tecnológica y el aumento de dispositivos conectados hacen indispensable la adopción de un protocolo de red que garantice escalabilidad, continuidad y sostenibilidad tecnológica. Teniendo esto en cuenta, el protocolo de internet versión 6 (IPv6) se constituye como el estándar que responde al agotamiento del espacio de direccionamiento IPv4 y a los lineamientos definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.

La alcaldía municipal de Chía, a través de la Oficina TIC y en trabajo conjunto entre infraestructura y gobierno TI, adoptó, ejecutó y culminó el proceso de transición del protocolo IPv4 a IPv6, dando cumplimiento a las directrices nacionales y asegurando la continuidad de los servicios tecnológicos institucionales

#### 8.18.1 Objetivo

Incorporar dentro del modelo de gestión y gobierno TI los lineamientos de gobernanza, control y sostenibilidad del protocolo IPv6, declarando su adopción como parte del estado base de la arquitectura tecnológica institucional, y garantizando su operación segura, controlada y alineada con la gestión de servicios de TI.

#### 8.18.2 Alcance

La implementación del protocolo IPv6 aplica a:

- La infraestructura de red institucional.
- Los servicios tecnológicos incluidos en el catálogo de servicios TI.
- Los sistemas de información y plataformas tecnológicas.
- La conectividad interna y externa de la entidad.
- Los proveedores y terceros que interactúan con la red institucional.

#### 8.18.3 Estado de implementación

La alcaldía municipal de Chía:

- Ejecutó el plan de transición del servicio de IPv4 a IPv6, bajo un esquema de coexistencia controlada (Dual Stack), garantizando interoperabilidad y continuidad del servicio.
- Implementó y documentó un plan de contingencia IPv6, orientado a mitigar riesgos técnicos, operativos y de seguridad asociados al proceso de adopción.
- Verificó la compatibilidad de la infraestructura tecnológica, sistemas de información y servicios críticos con el protocolo IPv6.

Por lo tanto, el protocolo IPv6 se considera implementado, operativo y gobernado, y deja de ser una iniciativa en transición para convertirse en un componente permanente de la arquitectura de TI institucional.

#### 8.18.4 Lineamientos de gobierno para IPv6

##### 8.18.4.1 Gobierno y responsabilidad

- La Oficina TIC es responsable de la administración, operación y control del protocolo IPv6.
- Toda modificación a la configuración IPv6 debe gestionarse a través del proceso institucional de gestión de cambios de TI.

##### 8.18.4.2 Continuidad y contingencia

La operación del protocolo IPv6 se rige por el plan de contingencia IPv6, el cual debe:

- Mantenerse actualizado.
- Probarse periódicamente.
- Activarse ante eventos que afecten la conectividad o disponibilidad de los servicios tecnológicos.

#### 8.18.5 Seguridad de la información

La operación de IPv6 debe cumplir los lineamientos institucionales de:

- Seguridad informática.
- Gestión de incidentes de seguridad.
- Los controles de seguridad deben cubrir direccionamiento, enrutamiento, acceso, monitoreo y filtrado de tráfico IPv6.

#### 8.18.6 Interoperabilidad y servicios

- Todos los nuevos sistemas de información y servicios tecnológicos deben:
  - Ser compatibles con IPv6.
  - Justificar técnicamente cualquier excepción.
- Los servicios existentes deben:

- Mantener compatibilidad con el esquema IPv6 implementado.

#### 8.18.7 Relación con proveedores

- Los proveedores de servicios tecnológicos deben:
  - Garantizar compatibilidad con IPv6.
  - Cumplir los lineamientos técnicos y de seguridad definidos por la entidad.
- La compatibilidad con IPv6 se establece como requisito obligatorio en nuevos procesos contractuales de TI.

#### 8.18.8 Seguimiento y mejora continua

La Oficina TIC debe:

- Monitorear permanentemente la operación del protocolo IPv6.
- Evaluar su desempeño, disponibilidad y seguridad.
- Incorporar mejoras técnicas y operativas conforme a la evolución tecnológica y normativa.
- Reportar el estado de IPv6 dentro de los indicadores de gestión de TI cuando aplique.

Tabla No. 29 Matriz servicio IPV6

Servicio tecnológico	Dependencia de IPv6	Tipo de dependencia	Riesgo asociado	Impacto	Nivel de riesgo	Estrategia de contingencia	Responsable
Plataforma de trámites en línea	Direccionamiento IPv6	Crítica	Fallo de enrutamiento IPv6	Interrupción total del servicio	Alto	Activación dual stack // Redireccionamiento IPv4	Oficina TIC / infraestructura
Sistema PQRS	Conectividad IPv6	Alta	Incompatibilidad de componentes	Degradación del servicio	Medio	Conmutación a IPv4 según plan	Oficina TIC / Infraestructura
Correo institucional	Red IPv6 + Nube	Crítica	Error de resolución DNS IPv6	Interrupción de comunicaciones	Alto	Uso DNS IPv4 / Proveedor	Oficina TIC
Sistema financiero	Acceso seguro IPv6	Alta	Configuración errónea de firewall IPv6	Riesgo de indisponibilidad	Alto	Ajuste reglas / Retorno temporal IPv4	Oficina TIC /

Servicio tecnológico	Dependencia de IPv6	Tipo de dependencia	Riesgo asociado	Impacto	Nivel de riesgo	Estrategia de contingencia	Responsable
							Infraestructura
Sistema documental	Transporte IPv6	Media	Latencia o pérdida de paquetes	Lentitud operativa	Medio	Ruteo alternativo	Oficina TIC / Infraestructura
Mesa de servicios TI	Conectividad IPv6	Media	Falla de acceso interno	Impacto en soporte TI	Medio	Red interna de IPv4 respaldo	Oficina TIC
Plataforma de analítica / BI	Red IPv6	Baja	Bajo soporte IPv6 en cliente	Acceso parcial	Bajo	Acceso IPv4 alternativo	Oficina TIC
Servicios de videovigilancia	Red IPv6	Crítica	Pérdida de conectividad	Afectación a seguridad	Alto	Red de contingencia segregada	Oficina TIC / infraestructura
Servicios de nube institucional	IPv6 + Proveedor	Alta	Falla de interoperabilidad	Indisponibilidad parcial	Medio	Escalamiento a proveedor IPv4	Oficina TIC / infraestructura
Servicios de Integración (APIs)	IPv6	Media	Fallas de compatibilidad externa	Error en intercambio de datos	Medio	Gateway IPv4-IPv6	Oficina TIC / Desarrollo

**Tabla No. 30 Criterios del tipo de dependencia IPv6**

Nivel de Dependencia	Descripción
Crítica	El servicio no opera sin IPv6
Alta	IPv6 es el principal medio de operación
Media	IPv6 soporta parcialmente el servicio
Baja	IPv6 es complementario

#### 8.18.9 Reglas institucionales obligatorias

- Todo servicio con dependencia crítica o alta debe:
  - Tener estrategia de contingencia documentada.
  - Probar su plan de contingencia periódicamente.
- Las contingencias deben:
  - Estar alineadas con el plan de contingencia IPv6.
  - Registrarse en gestión de cambios si se activan.
- Los riesgos deben:
  - Integrarse a la matriz institucional de riesgos TIC.

USO INSTITUCIONAL - ALCALDÍA DE CHÍA

## 9 Uso y apropiación de TI

El uso y apropiación de las tecnologías de la información y las comunicaciones (TIC) constituye un pilar fundamental para la generación de valor público, la eficiencia institucional y el cumplimiento de la misionalidad de la alcaldía de Chía. Si bien la entidad realiza esfuerzos significativos en la planeación, adquisición, implementación, operación de servicios y soluciones de TI, dichos esfuerzos solo se traducen en beneficios reales cuando estas tecnologías son efectivamente utilizadas, comprendidas e incorporadas en las prácticas cotidianas de los funcionarios, contratistas y ciudadanos.

En este contexto, el componente de uso y apropiación de TI del modelo de gestión y gobierno de TI, tiene como propósito establecer las condiciones organizacionales, culturales y operativas que faciliten la adopción efectiva de los servicios, sistemas de información, herramientas tecnológicas y lineamientos institucionales. Este componente reconoce que la transformación digital no es únicamente un ejercicio tecnológico, sino un proceso de cambio organizacional que involucra personas, procesos, cultura y capacidades.

El dominio de uso y apropiación de TI, orienta la definición e implementación de estrategias de gestión del cambio, comunicación, formación y acompañamiento, que permitan sensibilizar a los grupos de interés frente a la incorporación de nuevas soluciones tecnológicas o al fortalecimiento del uso de las ya existentes. Asimismo, promueve el desarrollo de competencias digitales, la generación de conciencia sobre los beneficios y riesgos asociados al uso de la tecnología, y la consolidación de comportamientos que aseguren su integración sostenible en la cultura institucional.

De esta manera, la alcaldía municipal de Chía busca garantizar que las inversiones en TI contribuyan efectivamente a la mejora de la gestión pública, al fortalecimiento de los procesos internos, a la prestación de servicios de calidad y a una relación más cercana, eficiente y transparente con la ciudadanía, en concordancia con los lineamientos de la política de gobierno digital y el marco de referencia de arquitectura empresarial.

### 9.1 Estrategia de uso y apropiación de TI

La estrategia de uso y apropiación de TI, tiene como propósito garantizar que los servicios, sistemas de información y herramientas tecnológicas implementadas por la alcaldía municipal de Chía sean comprendidos, aceptados, utilizados y aprovechados de manera efectiva por los servidores públicos, contratistas y demás grupos de interés, de modo que contribuyan al mejoramiento de la gestión institucional y a la generación de valor público, reconociendo que la adopción tecnológica es un proceso de cambio cultural y organizacional, y no únicamente técnico.

#### 9.1.1 Alcance

La estrategia de uso y apropiación de TI aplica a:

- Todos los servicios tecnológicos del catálogo de servicios TI.
- Los sistemas de información institucionales.
- Las soluciones tecnológicas nuevas o existentes.
- Los funcionarios, contratistas y usuarios internos de la entidad.
- Los procesos institucionales soportados por TI.

### 9.1.2 Principios orientadores

- Enfoque en las personas: La tecnología se diseña y adopta en función del usuario.
- Gestión del cambio gradual: Reconocimiento de la resistencia al cambio y adopción progresiva.
- Comunicación clara y permanente.
- Aprendizaje continuo.
- Uso responsable y seguro de la tecnología.
- Generación de valor público.

### 9.1.3 Lineamientos estratégicos

#### 9.1.3.1 *Gestión del cambio organizacional*

La Oficina TIC debe articularse con las áreas responsables de talento humano y comunicaciones para:

- Gestionar la resistencia al cambio.
- Acompañar la adopción de nuevas tecnologías.
- Todo nuevo servicio o sistema debe:
  - Contar con un plan de gestión del cambio asociado.

#### 9.1.3.2 *Comunicación y sensibilización*

- Se deben definir estrategias de comunicación que:
  - Informen oportunamente sobre nuevos servicios o cambios tecnológicos.
  - Expliquen beneficios, impactos y responsabilidades.
- Los mensajes deben:
  - Adaptarse a los distintos perfiles de usuario.

#### 9.1.3.3 *Formación y fortalecimiento de capacidades*

- La entidad debe:
  - Promover el desarrollo de competencias digitales.
  - Priorizar capacitaciones prácticas y orientadas al uso real de los servicios.
- Las capacitaciones deben:
  - Ajustarse a roles y funciones.
  - Considerar distintos niveles de madurez digital.

#### 9.1.3.4 *Acompañamiento y soporte al usuario*

- La mesa de servicios TI debe:
  - Actuar como canal principal de acompañamiento.
  - Identificar dificultades recurrentes de uso.
- Los hallazgos deben:
  - Retroalimentar la mejora de los servicios y la estrategia de uso.

#### 9.1.3.5 *Diseño centrado en el usuario*

- Los servicios y sistemas de información deben:
  - Diseñarse considerando la experiencia del usuario.
  - Minimizar la complejidad operativa.
- Se debe promover:
  - La usabilidad, accesibilidad y claridad funcional.

#### 9.1.3.6 *Uso responsable y seguro de TI*

- La estrategia debe:
  - Fomentar el uso responsable de los servicios tecnológicos.
  - Incorporar lineamientos de seguridad de la información y protección de datos.
- Los usuarios deben:
  - Conocer sus responsabilidades frente al uso de TI.

#### 9.1.3.7 *Medición y mejora continua*

- La Oficina TIC debe:
  - Medir el nivel de uso y adopción de los servicios tecnológicos.
  - Identificar brechas de uso y oportunidades de mejora.
- Los resultados deben:
  - Alimentar la mejora continua del MGGTI.

#### 9.1.3.8 *Roles y responsabilidades*

- Oficina TIC:
  - Lidera la estrategia de uso y apropiación de TI.
  - Coordina acciones de comunicación, formación y acompañamiento.
- Dependencias usuarias:
  - Facilitan la participación de sus equipos.
  - Promueven el uso adecuado de los servicios tecnológicos.
- Talento Humano / Prensa (cuando aplique):
  - Apoyan la gestión del cambio y la sensibilización.

#### 9.1.4 Reglas institucionales

- Todo servicio crítico debe:

- Evaluar periódicamente su nivel de uso.
- Las acciones de apropiación deben:
  - Registrarse y tener responsables definidos.
- Las brechas identificadas deben:
  - Retroalimentar el diseño y mejora del servicio.
- Los resultados deben:
  - Integrarse a indicadores de uso y apropiación de TI

Tabla No. 31 Matriz de uso y apropiación

Servicio / Sistema de información	Tipo de usuario	Rol del usuario	Nivel de uso actual	Evidencia de uso	Brecha identificada	Acción de apropiación	Responsable	Prioridad
Plataforma de trámites en línea	Funcionario	Gestor de trámite	Alto	Registros en sistema	Vacios en el funcionamiento	Seguimiento y mejora continua	Oficina TIC	Media
Plataforma de trámites en línea	Ciudadano	Usuario final	Medio	Métricas de acceso	Dificultad en navegación	Campaña de sensibilización + guía rápida	Oficina TIC / Prensa	Alta
Sistema PQRS	Funcionario	Analista	Bajo	Reportes MDS	Desconocimiento funcional	Capacitación práctica focalizada	Atención al ciudadano / Oficina TIC	Alta
Sistema documental	Funcionario	Usuario operativo	Medio	Logs de acceso	Uso parcial de funciones	Taller de buenas prácticas	Dirección de servicios administrativos / Oficina TIC	Media
Sistema financiero	Funcionario	Usuario especializado	Alto	Reportes del sistema	Sincronización entre plataformas	Actualización periódica	Sec. Hacienda / Oficina TIC	Baja
Correo institucional	Funcionario	Usuario general	Alto	Métricas de uso	Uso inseguro ocasional	Sensibilización en seguridad	Oficina TIC	Alta
Mesa de servicios TI	Funcionario	Usuario interno	Bajo	Tickets repetitivos	Desconocimiento del canal	Campaña de uso del MDS	Oficina TIC	Alta
Plataforma de analítica / BI	Directivo	Toma de decisiones	Bajo	Accesos esporádicos	Falta de apropiación	Sesión ejecutiva guiada	Oficina TIC	Media
Herramientas colaborativas	Funcionario	Usuario general	Bajo	Métricas de adopción	Resistencia al cambio	Estrategia de gestión del cambio	Dirección de función pública / Oficina TIC	Alta

### 9.1.5 Tipos de acciones de apropiación

- Capacitación práctica y focalizada.
- Acompañamiento personalizado.
- Guías rápidas y material visual.
- Campañas de comunicación y sensibilización.
- Sesiones ejecutivas para directivos.
- Refuerzo en seguridad y uso responsable.
- Mejora de usabilidad y experiencia de usuario.

## 9.2 Esquema de incentivos

El esquema de incentivos para el uso y apropiación de TI, tiene como propósito promover la adopción efectiva, el uso responsable y el aprovechamiento de las tecnologías de la información por parte de los servidores públicos y contratistas de la alcaldía municipal de Chía, reconociendo los comportamientos positivos que contribuyen a la transformación digital, la mejora de la gestión institucional y la generación de valor público.

### 9.2.1 Objetivo

Reducir la resistencia al cambio, fortalecer la cultura digital y estimular la participación activa de los usuarios en la adopción de los servicios y soluciones tecnológicas institucionales.

### 9.2.2 Alcance

El esquema de incentivos aplica a:

- Funcionarios y contratistas de la alcaldía municipal de Chía.
- Usuarios internos de los servicios y sistemas de información institucionales.
- Dependencias que hagan uso intensivo de soluciones tecnológicas.

### 9.2.3 Principios orientadores

- Reconocimiento al esfuerzo y la adopción, no a la jerarquía.
- Equidad y transparencia en los criterios de otorgamiento.
- Enfoque no monetario, acorde con la normativa del sector público.
- Gradualidad, considerando distintos niveles de madurez digital.
- Sostenibilidad, evitando esquemas difíciles de mantener en el tiempo.
- Alineación con la gestión del desempeño institucional.

## 9.2.4 Tipología de incentivos

### 9.2.4.1 Incentivos de reconocimiento institucional

- Reconocimiento público a usuarios o dependencias con alto nivel de adopción de TI.
- Menciones destacadas en comunicaciones internas.
- Insignias digitales internas de buenas prácticas en uso de TI.

### 9.2.4.2 Incentivos de desarrollo de capacidades

- Prioridad en cupos de capacitación especializada en TI.
- Acceso preferente a talleres, pilotos o nuevas funcionalidades.
- Participación en mesas de co-creación o pruebas de nuevos servicios.

### 9.2.4.3 Incentivos organizacionales

- Reconocimiento a dependencias con mejoras demostrables en productividad mediante TIC.
- Priorización de requerimientos tecnológicos para áreas con alto nivel de adopción.
- Inclusión como casos de éxito institucionales.

### 9.2.4.4 Incentivos culturales y simbólicos

- Insignias digitales internas asociadas a competencias tecnológicas.
- Reconocimiento en eventos institucionales.

## 9.2.5 Criterios para la asignación de incentivos

Los incentivos deben asignarse con base en criterios objetivos, tales como:

- Nivel de uso efectivo de los servicios tecnológicos.
- Participación activa en procesos de capacitación.
- Cumplimiento de buenas prácticas de seguridad de la información.
- Reducción de incidentes que son por uso inadecuado de TI.
- Aporte a la mejora de procesos mediante el uso de tecnología.

Los criterios deben ser medibles, verificables y trazables.

Tabla No. 32 Matriz asignación de incentivos

Incentivo	Criterio de otorgamiento	Evidencia requerida	Responsable de validación	Periodicidad
Reconocimiento institucional	Uso efectivo y continuo de un sistema de información	Reportes de uso / métricas del sistema	Oficina TIC	Semestral

Incentivo	Criterio de otorgamiento	Evidencia requerida	Responsable de validación	Periodicidad
Insignia digital interna de buenas prácticas en TI	Cumplimiento de lineamientos de uso y seguridad	Informe de cumplimiento de checklist	Oficina TIC / Seguridad de la Información	Anual
Prioridad en capacitaciones especializadas	Participación activa en procesos de adopción	Listados de asistencia / evaluaciones	Oficina TIC / Dirección de función pública	Permanente
Acceso preferente a pilotos tecnológicos	Alto nivel de adopción y disposición al cambio	Resultados de pruebas piloto	Oficina TIC	Según proyecto
Reconocimiento a dependencia destacada	Mejora demostrable en productividad mediante TI	Indicadores de proceso / informes	Oficina TIC / Planeación	Anual
Mención en comunicaciones internas	Buenas prácticas replicables	Publicación institucional	Prensa	Trimestral
Insignia digital institucional	Desarrollo de competencias digitales	Registro de formación aprobada	Talento Humano / TIC	Permanente
Participación en mesas de co-creación	Aportes a mejora de servicios TI	Actas de sesiones	Oficina TIC	Según convocatoria
Reconocimiento por uso seguro de TI	Cumplimiento de políticas de seguridad	Reportes de auditoría / cero incidentes	Oficina TIC	Anual

### 9.2.6 Lineamientos de implementación

- La Oficina TIC lidera la definición y seguimiento del esquema.
- La implementación debe articularse con:
  - Gestión del talento humano.
  - Comunicaciones a través de medios institucionales.
- El esquema debe:
  - Divulgarse claramente a los usuarios.
  - Actualizarse periódicamente según resultados y madurez digital.

### 9.2.7 Seguimiento y evaluación

- La Oficina TIC debe:
  - Medir el impacto del esquema de incentivos en la adopción de TI.
  - Evaluar su efectividad para reducir resistencia al cambio.
- Los resultados deben:

- Alimentar indicadores del componente de uso y apropiación de TIC.
- Soportar la mejora continua del MGGTI.

### 9.2.8 Reglas institucionales obligatorias

- Todo incentivo debe:
  - Estar asociado a criterios claros y medibles.
  - Contar con evidencia verificable.
- No se permite otorgar incentivos sin:
  - Validación formal por el responsable asignado.
- Los resultados deben:
  - Registrarse y conservarse como soporte del MGGTI.
- El esquema debe:
  - Divulgarse a los usuarios internos.

## 9.3 Plan de formación

El plan de formación en uso y apropiación de TIC, tiene como propósito fortalecer las competencias digitales de los servidores públicos y contratistas, garantizando que los servicios, sistemas de información y herramientas tecnológicas institucionales sean comprendidos, utilizados de manera correcta y aprovechados de forma efectiva, contribuyendo a la mejora de la gestión pública y a la generación de valor público.

### 9.3.1 Objetivo

Reconocer que la formación es un instrumento clave de la gestión del cambio, indispensable para reducir la resistencia al uso de la tecnología y consolidar una cultura digital institucional.

### 9.3.2 Alcance

El plan de formación aplica a:

- Funcionarios y contratistas de la alcaldía municipal de Chía.
- Usuarios internos de los sistemas de información y servicios TI.
- Nuevos funcionarios que ingresen a la entidad.
- Dependencias con bajo o medio nivel de adopción tecnológica.

### 9.3.3 Principios orientadores

- Enfoque en el usuario: Formación ajustada a roles y necesidades reales.
- Aprender haciendo: Énfasis práctico y aplicado.
- Gradualidad: Niveles progresivos según madurez digital.
- Pertinencia: Contenidos alineados con procesos institucionales.
- Accesibilidad: Metodologías y materiales claros y comprensibles.
- Continuidad: Formación permanente, no eventos aislados.

#### 9.3.4 Lineamientos del plan de formación

##### 9.3.4.1 *Diagnóstico de necesidades de formación*

- La Oficina TIC debe:
  - Identificar brechas de conocimiento y uso de TI.
  - Apoyarse en la matriz de uso y apropiación.
- El diagnóstico debe:
  - Actualizarse periódicamente.

##### 9.3.4.2 *Segmentación de usuarios*

El plan debe considerar distintos perfiles de usuario, tales como:

- Usuarios básicos.
- Usuarios operativos.
- Usuarios especializados.
- Directivos y tomadores de decisión.

Cada segmento debe contar con contenidos y metodologías diferenciadas.

##### 9.3.4.3 *Contenidos de formación*

El plan de formación debe incluir, como mínimo:

- Uso funcional de sistemas de información institucionales.
- Uso del catálogo de servicios y la mesa de servicios TI.
- Buenas prácticas en el uso de herramientas tecnológicas.
- Seguridad de la información y uso responsable de TI.
- Cambios tecnológicos relevantes y nuevas funcionalidades.

#### 9.3.5 Modalidades de formación

Se deben combinar diferentes modalidades, tales como:

- Talleres presenciales prácticos.
- Capacitaciones virtuales.
- Guías rápidas y manuales de usuario.
- Videos cortos y material audiovisual.

- Acompañamiento en sitio para dependencias críticas.

### 9.3.6 Articulación con la gestión del cambio

- Toda nueva solución o servicio TIC debe:
  - Incluir actividades de formación dentro de su plan de implementación.
- La formación debe:
  - Coordinarse con acciones de comunicación y sensibilización.

### 9.3.7 Roles y responsabilidades

- Oficina TIC:
  - Lidera la definición y ejecución del plan de formación TIC.
  - Diseña contenidos y metodologías.
- Dirección de función pública:
  - Apoya la gestión de competencias y registros de formación.
- Dependencias usuarias:
  - Facilitan la participación de sus equipos.

### 9.3.8 Registro y evidencias

- Toda actividad de formación debe:
  - Contar con evidencias de ejecución (listas de asistencia, evaluaciones o encuestas de apropiación).
  - Registrarse para fines de seguimiento y auditoría.

### 9.3.9 Evaluación y mejora continua

- La Oficina TIC debe:
  - Evaluar la efectividad de la formación impartida.
  - Medir su impacto en el nivel de uso y apropiación de TIC.
- Los resultados deben:
  - Retroalimentar el plan de formación y la estrategia de uso y apropiación TIC.

### 9.3.10 Plantilla del plan anual de formación en uso y apropiación de TIC

#### 9.3.10.1 *Objetivo general*

Fortalecer las competencias digitales de los servidores públicos y contratistas de la alcaldía municipal de Chía, promoviendo el uso efectivo, seguro y responsable de los servicios, sistemas de información y herramientas tecnológicas institucionales, con el fin de mejorar la gestión pública y la generación de valor público.

#### 9.3.10.2 *Objetivos específicos*

- Incrementar el nivel de adopción de los servicios tecnológicos institucionales.
- Reducir incidentes asociados al uso inadecuado de TIC.
- Acompañar los procesos de cambio tecnológico y organizacional.
- Desarrollar capacidades digitales acordes a los roles institucionales.
- Promover una cultura de uso responsable y seguro de la tecnología.

#### 9.3.10.3 *Alcance*

Aplica a:

- Funcionarios y contratistas de la alcaldía municipal de Chía.
- Usuarios internos de los sistemas de información.
- Directivos y tomadores de decisión.
- Dependencias priorizadas según nivel de uso y apropiación.

#### 9.3.10.4 *Enfoque metodológico*

- Aprender haciendo (enfoque práctico).
- Formación diferenciada por roles.
- Modalidad mixta (presencial / virtual).
- Acompañamiento progresivo.
- Evaluación continua del impacto.

### 9.4 Evaluación del nivel de adopción de TIC

Establecer un marco institucional para medir, analizar y mejorar el nivel de adopción de las tecnologías de la información, garantizando que los servicios, sistemas de información y herramientas tecnológicas implementadas por la alcaldía de Chía sean utilizados de manera efectiva, segura y alineada con los procesos institucionales, generando valor público.

#### 9.4.1 *Objetivo*

Identificar brechas de uso, resistencia al cambio y oportunidades de mejora, y constituirse como un insumo clave para la toma de decisiones en TIC.

#### 9.4.2 *Alcance*

La evaluación del nivel de adopción de TI aplica a:

- Servicios tecnológicos incluidos en el catálogo de servicios TIC.
- Sistemas de información institucionales.
- Usuarios internos (funcionarios y contratistas).
- Dependencias y procesos apoyados por TI.

#### 9.4.3 Principios orientadores

- Objetividad: Basada en datos y evidencias verificables.
- Enfoque en el usuario: Consideración de experiencia y facilidad de uso.
- Gradualidad: Reconocimiento de distintos niveles de madurez digital.
- Transparencia: Criterios claros y comunicados.
- Mejora continua: Evaluación orientada a la acción, no al castigo.
- Articulación institucional: Alineada con otros componentes del MGGTI.

#### 9.4.4 Dimensiones de evaluación

La evaluación del nivel de adopción de TI debe considerar, como mínimo, las siguientes dimensiones:

##### 9.4.4.1 *Uso efectivo*

- Frecuencia y regularidad de uso de los servicios y sistemas.
- Uso de funcionalidades clave.
- Autonomía del usuario en el uso de la herramienta.

##### 9.4.4.2 *Apropiación funcional*

- Integración de la tecnología en los procesos de trabajo.
- Sustitución efectiva de prácticas manuales o alternas.
- Percepción de utilidad y valor del servicio.

##### 9.4.4.3 *Competencias digitales*

- Nivel de conocimiento para el uso del servicio.
- Capacidad para resolver tareas sin apoyo constante.
- Necesidad recurrente de soporte por uso inadecuado.

##### 9.4.4.4 *Experiencia del usuario*

- Facilidad de uso y usabilidad.
- Claridad de la información y funcionalidades.
- Satisfacción general del usuario.

#### 9.4.4.5 *Uso responsable y seguro*

- Cumplimiento de lineamientos de seguridad de la información.
- Reducción de incidentes asociados a malas prácticas.
- Conocimiento de responsabilidades en el uso de TI.

#### 9.4.5 Niveles de adopción de TI

La entidad debe clasificar el nivel de adopción de TI en categorías institucionales, tales como:

- Bajo: Uso esporádico, dependencia alta de soporte, resistencia al cambio.
- Medio: Uso regular con apoyo ocasional, apropiación parcial.
- Alto: Uso frecuente, autónomo y alineado con procesos.

Estos niveles deben utilizarse para priorizar acciones de mejora y formación.

#### 9.4.6 Fuentes de información para la evaluación

La evaluación del nivel de adopción debe apoyarse en fuentes como:

- Métricas de uso de sistemas de información.
- Reportes de la mesa de servicios TI.
- Resultados de encuestas de satisfacción y percepción.
- Evidencias del plan de formación y uso y apropiación.
- Resultados del esquema de incentivos.

#### 9.4.7 Periodicidad de la evaluación

La evaluación del nivel de adopción de TIC debe realizarse:

- Como mínimo una vez al año.
- De forma extraordinaria ante cambios tecnológicos relevantes.

#### 9.4.8 Roles y responsabilidades

- Oficina TIC:
  - Lidera el proceso de evaluación.
  - Consolida resultados y propone acciones de mejora.
- Dependencias usuarias:
  - Facilitan la participación de sus equipos.
  - Apoyan la recolección de información.
- Dirección de función pública / Prensa (cuando aplique):
  - Apoyan acciones derivadas de formación y gestión del cambio.

#### 9.4.9 Uso de los resultados

Los resultados de la evaluación del nivel de adopción de TI deben utilizarse para:

- Priorizar acciones del plan de formación.
- Definir o ajustar acciones del esquema de incentivos.
- Mejorar la usabilidad y funcionalidad de los servicios TIC.
- Alimentar indicadores del MGGTI.
- Apoyar la toma de decisiones de relacionadas con TIC.

### 9.5 Plan de capacitación y entrenamiento para los sistemas de información

El plan de capacitación y entrenamiento para los sistemas de información tiene como propósito asegurar que los usuarios institucionales cuenten con los conocimientos, habilidades y competencias necesarias para utilizar de manera efectiva, segura y autónoma los sistemas de información, garantizando su correcta integración a los procesos misionales, estratégicos y de apoyo de la alcaldía municipal de Chía.

#### 9.5.1 Objetivo

Constituirse como un instrumento clave para la apropiación tecnológica, la reducción de errores operativos y la generación de valor público a partir de las inversiones en TIC.

#### 9.5.2 Alcance

El plan de capacitación y entrenamiento aplica a:

- Todos los sistemas de información institucionales, nuevos o existentes.
- Funcionarios y contratistas que interactúan con dichos sistemas.
- Usuarios con roles operativos, analíticos, administrativos y directivos.
- Dependencias priorizadas según criticidad del sistema y nivel de adopción.

#### 9.5.3 Principios orientadores

- Enfoque por roles: Capacitación diferenciada según funciones y responsabilidades.
- Aprender haciendo: Entrenamiento práctico y aplicado al contexto real.
- Gradualidad y progresión: Niveles básicos, intermedios y avanzados.
- Pertinencia funcional: Contenidos alineados con los procesos institucionales.
- Accesibilidad y claridad: Materiales comprensibles y reutilizables.

- Continuidad: Capacitación permanente, no eventos aislados.

#### 9.5.4 Lineamientos para la elaboración del plan

##### 9.5.4.1 Identificación de sistemas críticos y priorización

- La Oficina TIC debe:
  - Identificar los sistemas de información críticos.
  - Priorizar aquellos con mayor impacto en la operación institucional o con bajo nivel de adopción.
- La priorización debe:
  - Articularse con la evaluación del nivel de adopción de TI.

##### 9.5.4.2 Segmentación de usuarios y roles

El plan debe definir claramente los perfiles de usuario, tales como:

- Usuarios básicos.
- Usuarios especializados.
- Administradores del sistema.
- Directivos y tomadores de decisión.

Cada perfil debe contar con contenidos y profundidad diferenciados.

##### 9.5.4.3 Contenidos mínimos de capacitación

El plan de capacitación y entrenamiento debe incluir, como mínimo:

- Funcionalidades principales del sistema de información.
- Flujos de trabajo y casos de uso reales.
- Buenas prácticas operativas.
- Manejo de errores frecuentes.
- Uso responsable y seguro de la información.
- Relación del sistema con otros servicios y procesos.

##### 9.5.4.4 Modalidades de capacitación

Se deben contemplar diversas modalidades, tales como:

- Talleres presenciales prácticos.
- Capacitaciones virtuales sincrónicas o asincrónicas.
- Manuales de usuario y guías rápidas.
- Videos tutoriales cortos.
- Entrenamiento en el puesto de trabajo.

La modalidad debe seleccionarse según el tipo de usuario y la criticidad del sistema.

#### 9.5.4.5 *Articulación con la gestión del cambio*

- Todo sistema de información nuevo o actualizado debe:
  - Incluir actividades de capacitación y entrenamiento como parte de su plan de implementación.
- La capacitación debe:
  - Coordinarse con acciones de comunicación y acompañamiento al usuario.

#### 9.5.4.6 *Responsabilidades institucionales*

- Oficina TIC:
  - Lidera la elaboración y ejecución del plan.
  - Define contenidos, metodologías y cronograma.
- Dependencias usuarias:
  - Facilitan la participación de los usuarios.
  - Apoyan la identificación de necesidades específicas.
- Dirección de función pública (cuando aplique):
  - Apoya el registro de capacitaciones y desarrollo de competencias.

#### 9.5.4.7 *Registro de evidencias*

Toda actividad de capacitación debe:

- Contar con listas de asistencia, evaluaciones o evidencias de participación.
- Registrarse para efectos de seguimiento, control y auditoría.

#### 9.5.4.8 *Evaluación de la efectividad*

- La Oficina TIC debe:
  - Evaluar el impacto de la capacitación en el uso real del sistema.
  - Medir la reducción de incidentes por errores de uso.
- Los resultados deben:
  - Retroalimentar el plan de capacitación y la estrategia de uso y apropiación.

#### 9.5.5 *Periodicidad del plan*

El plan de capacitación y entrenamiento debe:

- Elaborarse con periodicidad anual.
- Actualizarse ante cambios relevantes en los sistemas de información.

## 10 Glosario

Los **servicios SaaS** (Software como Servicio) son aplicaciones basadas en la nube que se entregan a los usuarios a través de Internet mediante suscripción, eliminando la necesidad de instalar y mantener software localmente.

**Gestión de Identidad y Acceso (IAM)**, un sistema para controlar quién accede a qué recursos digitales (usuarios, aplicaciones, datos) mediante autenticación y autorización.

**Backend** es el sistema completo "detrás de escena" (servidor, lógica, APIs) que hace funcionar una aplicación.

**PaaS (Plataforma como Servicio)** es un modelo de computación en la nube que ofrece un entorno completo para desarrollar, ejecutar y gestionar aplicaciones, incluyendo hardware, sistemas operativos, bases de datos y herramientas.

**Los Logs SIEM** (Security Information and Event Management) son los datos generados por dispositivos, aplicaciones y sistemas de una red que se recopilan, analizan y correlacionan en una plataforma centralizada para detectar, investigar y responder a amenazas de seguridad en tiempo real.

**Scrumban** es un marco ágil híbrido que fusiona la estructura de Scrum (sprints, reuniones) con la flexibilidad y visualización de flujo continuo de Kanban (tablero visual, límites de trabajo en curso - WIP).

**CRISP-DM** (Cross-Industry Standard Process for Data Mining) es una metodología estándar y probada para proyectos de minería de datos y ciencia de datos.

## 11 Referencias bibliográficas

Ministerio de tecnologías de la información, (2023). Guía dominio MGGTI.G.ES - Estrategia de TI. Versión 3.0.

Ministerio de tecnologías de la información, (2023). Guía dominio MGGTI.G.SI - Gestión de sistemas información. Versión 1.0.

Ministerio de tecnologías de la información, (2023). Guía dominio MGGTI.G.ST - Gestión de servicios de TI. Versión 1.0.

Ministerio de tecnologías de la información, (2023). Guía dominio MGGTI.G.GO - Gobierno de TI. Versión 3.0.

Ministerio de tecnologías de la información, (2023). Guía general MGGTI.G.GI – Dominio de información. Versión 1.0.

Ministerio de tecnologías de la información, (2023). Guía específica MGGTI.GE.GI.04 – Gobierno de datos. Versión 3.0.

Ministerio de tecnologías de la información, (2023). Guía dominio MGGTI.G.UA – Uso y apropiación de TI. Versión 1.0.

Ministerio de tecnologías de la información, (2022). RAE.ADM.01 – Plazos para la implementación del marco de referencia de arquitectura empresarial. Versión 1.0.

Infraestructura colombiana de datos espaciales, (2021). Marco de referencia geoespacial de la ICDE.

Archivo General de la Nación, (2017). Guía Implementación de un Sistema de Gestión de Documentos Electrónicos de Archivo-SGDEA.