

EMPRESA DE DESARROLLO Y RENOVACIÓN URBANA E.I.C.E
RESOLUCIÓN No. 10.15-013-2026

(30 de enero de 2026)

**“POR LA CUAL SE ADOPTA LOS PLANES INSTITUCIONALES DISPUESTOS EN EL
DECRETO 612 DE 2018, DE LA EMPRESA DE DESARROLLO Y RENOVACION
URBANA EDRU EICE”**

La Gerente General de la Empresa de Desarrollo y Renovación Urbana E.I.C.E. – EDRU E.I.C.E. en uso de sus atribuciones constitucionales, legales y en especial lo descrito en la Ley 872 de 2003, modificada por el Decreto 1499 de 2017, el Decreto 1083 de 2015 y el artículo 23 de la Resolución de Junta Directiva No. 20.15.1-001-2024 del 18 de julio de 2024, así como las demás normas que las modifiquen, desarrollen o complementen, y

CONSIDERANDO:

Que, el Decreto 1499 de 2017, en su artículo 1°, sustituyó el Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015 - Único Reglamentario del Sector de Función Pública, con el fin de reglamentar el alcance del Sistema de Gestión y su articulación con el Sistema de Control Interno de que trata el artículo 133 de la Ley 1753 de 2015, actualizando el Modelo Integrado de Planeación y Gestión.

Que, la EDRU, mediante Resolución No. 10.15-029-2018 adoptó el Modelo Integrado de Planeación y Gestión- MIPG, articulado con el Modelo Estándar de Control Interno – MECI 2014, y creó el Comité Institucional de Gestión y Desempeño, según lo estipulado en el Decreto Nacional 1499 de 2017.

Que, de conformidad con lo establecido en el artículo 25 de la Constitución Política de Colombia, que señala que *“El trabajo es un derecho y una obligación social y goza, en todas sus modalidades, de la especial protección del Estado. Toda persona tiene derecho a un trabajo en condiciones dignas y justas.”* Que, la Ley 909 de 2004 en el numeral 2, literales a) y b) del artículo 15 y en el numeral 1 del artículo 17, señala que las entidades deberán formular y adoptar anualmente los planes estratégicos de talento humano, anual de vacantes y de previsión de recursos humanos, sin consagrar fecha para el efecto.

Que, el Decreto ley 1567 de 1998 en el artículo 3 literal c) consagra que las entidades, con el propósito de organizar la capacitación interna, deberán formular con una periodicidad mínima de un año su plan institucional de capacitación; en el artículo 34 señala que el jefe de cada entidad deberá adoptar y desarrollar internamente planes anuales de incentivos institucionales, de acuerdo con la ley y los reglamentos, sin indicar plazo para su adopción.

Que, el Decreto 1072 de 2015 en el artículo 2.2.4.6.8 numeral 7 consagra, que los empleadores deben desarrollar un plan de trabajo anual para alcanzar cada uno de los objetivos propuestos en el Sistema de Gestión de la Seguridad y Salud en el Trabajo (SGSST), sin indicar plazo para su adopción.

Que, el artículo 2.2.10.1 del Decreto 1083 de 2015, expedido por la Presidencia de la República, establece que *“Las entidades deberán organizar programas de estímulos con el fin de motivar el desempeño eficaz y el compromiso de sus empleados. Los estímulos se implementarán a través de programas de bienestar social”*.

Que, el artículo 2.2.10.6 del Decreto 1083 de 2015, indica que: *“Los programas de Bienestar responderán a estudios técnicos que permitan, a partir de la identificación de necesidades y expectativas de los empleados, determinar actividades y grupos de beneficiarios bajo criterio de equidad, eficiencia mayor cobertura institucional”*.

EMPRESA DE DESARROLLO Y RENOVACIÓN URBANA E.I.C.E
RESOLUCIÓN No. 10.15-013-2026

(30 de enero de 2026)

**“POR LA CUAL SE ADOPTA LOS PLANES INSTITUCIONALES DISPUESTOS EN EL
DECRETO 612 DE 2018, DE LA EMPRESA DE DESARROLLO Y RENOVACION
URBANA EDRU EICE”**

Que, el artículo 2.2.10.9 del Decreto 1083 de 2015, indica que: *“Plan de incentivos institucionales. El jefe de cada entidad adoptará anualmente el plan de incentivos institucionales y señalará en él los incentivos no pecuniarios que se ofrecerán al mejor empleado de carrera de la entidad, a los mejores empleados de carrera de cada nivel jerárquico y al mejor empleado de libre nombramiento y remoción de la entidad, así como los incentivos pecuniarios y no pecuniarios para los mejores equipos de trabajo. Dicho plan se elaborará de acuerdo con los recursos institucionales disponibles para hacerlos efectivos. En todo caso los incentivos se ajustarán a lo establecido en la Constitución Política y la ley”.*

Que, el artículo 2.2.9.1 del Decreto 1083 de 2015, indica que: *“Planes de capacitación. Los planes de capacitación de las entidades públicas deben responder a estudios técnicos que identifiquen necesidades y requerimientos de las áreas de trabajo y de los empleados, para desarrollar los planes anuales institucionales y las competencias laborales.*

Que, el artículo 2.8.2.5.8 del Decreto 1080 de 2015, reglamenta las Leyes 594 de 2000 y 1437 de 2011, incluye de los instrumentos archivísticos para la gestión documental el Plan Institucional de Archivos – PINAR; el cual es un instrumento que permitirá planear, hacer seguimiento y articular con los planes estratégicos, la función archivística de acuerdo con las necesidades, debilidades, riesgos y oportunidades.

Que, el Decreto 1122 del agosto 30 de 2024, *“Por el cual se reglamenta el artículo 73 de la Ley 1474 de 2011, modificado por el artículo 31 de la Ley 2195 de 2022, en lo relacionado con los Programas de Transparencia y Ética Pública”* en su artículo 2.1.4.4.1.1. *Ámbito de aplicación. “Las entidades obligadas del orden nacional, departamental y municipal, cualquiera que sea su régimen de contratación, deberán implementar Programas de Transparencia y Ética Pública con las características, estándares, elementos, requisitos, procedimientos y controles mínimos que para tales efectos establezca la Secretaría de Transparencia de la Presidencia de la República”.*

Que, el Programa de Transparencia y Ética Pública (PTEP) es un instrumento obligatorio de gestión diseñado para prevenir riesgos de corrupción, lavado de activos y soborno en entidades públicas, fundamentado principalmente en la Ley 2195 de 2022 y el Decreto 1122 de 2024. Este programa establece la debida diligencia, gestión de riesgos y la cultura de integridad (antisoborno) como pilares fundamentales para la administración pública, integrándose con el modelo Integrado de Planeación y Gestión (MIPG).

Que, el Decreto 1008 de 2018, Establecen los Lineamientos Generales de la Política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

Que, dentro de la Política de Gobierno Digital, se encuentra contemplado el Plan Estratégico de Tecnología de la Información - PETI, el cual debe ser adoptado por la entidad, con el fin de garantizar la armonía en la articulación y en el desarrollo de la Política de Gobierno Digital.

Que, de acuerdo con el artículo 2.2.9.1.2.1 del Decreto 1078 de 2015 (DUR-TIC), por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la

EMPRESA DE DESARROLLO Y RENOVACIÓN URBANA E.I.C.E
RESOLUCIÓN No. 10.15-013-2026

(30 de enero de 2026)

**“POR LA CUAL SE ADOPTA LOS PLANES INSTITUCIONALES DISPUESTOS EN EL
DECRETO 612 DE 2018, DE LA EMPRESA DE DESARROLLO Y RENOVACION
URBANA EDRU EICE”**

Información y las Comunicaciones, la política de gobierno digital' será definida por, MinTIC y se desarrollará a través de componentes y habilitadores transversales que, acompañados de lineamientos y estándares, permitirán el logro de propósitos que generarán valor público en un entorno de confianza digital a partir del aprovechamiento de las TIC.

Que, según el numeral 2, del artículo anteriormente citado, los habilitadores transversales de la política de gobierno digital, son los elementos fundamentales de seguridad y privacidad de la información, arquitectura y servicios ciudadanos digitales, que permiten el desarrollo de los componentes y el logro de los propósitos de dicha política.

Que, la Resolución 00500 del 10 de marzo del 2021 *“Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”*

Que, la Resolución 0448 de 2022, por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías, de la Información y las Comunicaciones, se definen lineamientos frente al uso y manejo de la información y se deroga la resolución 2256 de 2020.

Que, el Decreto 612 de 2018, adicionó al Capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, los siguientes artículos:

“2.2.22.3.14. Integración de los planes institucionales y estratégicos al Plan de Acción. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año”:

1. *Plan Institucional de Archivos de la Entidad PINAR*
2. *Plan Anual de Adquisiciones*
3. *Plan Anual de Vacantes*
4. *Plan de Previsión de Recursos Humanos*
5. *Plan Estratégico de Talento Humano*
6. *Plan Institucional de Capacitación*
7. *Plan de Incentivos Institucionales*
8. *Plan de Trabajo Anual en Seguridad y Salud en el Trabajo*
9. *Plan Anticorrupción y de Atención al Ciudadano*
10. *Plan Estratégico de Tecnologías de la Información y las Comunicaciones -PETI*

Que, en sesión llevada a cabo el 29 de enero de 2026, por el Comité Institucional de Gestión y Desempeño se revisaron y se aprobaron los siguientes planes institucionales que le aplican a la EDRU E.I.C.E.:

1. Plan Institucional de Archivos de la Entidad PINAR
2. Plan Estratégico de Talento Humano
3. Plan Institucional de Capacitación

EMPRESA DE DESARROLLO Y RENOVACIÓN URBANA E.I.C.E
RESOLUCIÓN No. 10.15-013-2026

(30 de enero de 2026)

“POR LA CUAL SE ADOPTA LOS PLANES INSTITUCIONALES DISPUESTOS EN EL DECRETO 612 DE 2018, DE LA EMPRESA DE DESARROLLO Y RENOVACION URBANA EDRU EICE”

4. Plan de Incentivos Institucionales
5. Plan de Trabajo Anual en Seguridad y Salud en el Trabajo
6. Programa de Transparencia y Ética Publica
7. Plan Estratégico de Tecnologías de la Información y las Comunicaciones -PETI
8. Plan de tratamiento de riesgos de seguridad y privacidad de la información
9. Plan de seguridad y privacidad de la información
10. Plan de acción institucional

Que, con fundamento en lo antes expuesto, la Empresa de Desarrollo y Renovación Urbana –EDRU E.I.C.E.

RESUELVE:

ARTÍCULO PRIMERO: Adoptar los planes institucionales para la vigencia 2026 que se relacionan a continuación:

1. Plan Institucional de Archivos de la Entidad PINAR
2. Plan Estratégico de Talento Humano
3. Plan Institucional de Capacitación
4. Plan de Incentivos Institucionales
5. Plan de Trabajo Anual en Seguridad y Salud en el Trabajo
6. Programa de Transparencia y Ética Publica
7. Plan Estratégico de Tecnologías de la Información y las Comunicaciones -PETI
8. Plan de tratamiento de riesgos de seguridad y privacidad de la información
9. Plan de seguridad y privacidad de la información
10. Plan de acción institucional

ARTÍCULO SEGUNDO: Estos planes son aplicables a los funcionarios y contratistas de la Empresa de Desarrollo y Renovación Urbana EDRU EICE y tendrán que ser socializados a través de la página web, capacitaciones, inducciones y reinducciones que se programen, de acuerdo a las temáticas definidas en su contenido.

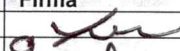
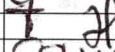

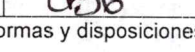


ARTÍCULO TERCERO: La presente Resolución rige a partir de la fecha de su expedición.

Se expide en Santiago de Cali el 30 de enero de 2026.

COMUNIQUESE Y CUMPLASE


MARÍA ALEXANDRA PACHECO MUÑOZ.
Gerente General

Empresa de Desarrollo y Renovación Urbana - EDRU E.I.C.E.

	nombre	Cargo / Actividad	Firma
Proyectó	Julian Gomez Alarcón	Contratista Oficina de Planeación	
Proyectó	Adriana Millan Azcarate	Contratista Oficina de Planeación	
Revisó	Jorge Andrés Martínez Zambrano	Jefe Oficina de Planeación	
Revisó	Carolina Soto Flórez	Jefe Oficina Jurídica	
Revisó	Sandra Idali Arévalo Peña	Directora Administrativa	
Aprobó	Ana Maria Gil Rodríguez	Secretaria General	

Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para firma.



PLAN ESTRATÉGICO DE
TECNOLOGÍAS DE LA
INFORMACIÓN Y LAS
COMUNICACIONES PETI

2026


 <p>Gestión Administrativa, Documental y TIC Dirección Administrativa</p>	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

TABLA DE CONTENIDO

		Pág.
1	INTRODUCCIÓN	1
1.1	Objetivo del Documento	1
1.2	Alcance	1
1.3	Metodología de Actualización	2
2	MARCO NORMATIVO Y POLÍTICO	2
2.1	Normatividad Aplicable.....	3
2.2	Políticas y Lineamientos de Gobierno Digital.....	3
2.3	Estándares y Mejores Prácticas Internacionales	4
3	DIAGNÓSTICO ESTRATÉGICO	4
3.1	Diagnóstico Organizacional (ciberseguridad, brechas y recomendaciones iniciales). Ciberseguridad	5
3.1.1	Brechas	5
3.1.2	Recomendaciones.....	5
3.2	Diagnóstico de Tecnologías de la Información	5
3.3	Análisis FODA en Tecnologías de la Información.....	6
3.4	Estado Actual de la Arquitectura Empresarial.....	6
3.5	Evaluación de Madurez Digital.....	7
4	ARQUITECTURA EMPRESARIAL DE TI.....	8
4.1	Visión Actual de la Arquitectura	8
4.2	Arquitectura Objetivo (Futura).....	9
4.3	Hoja de Ruta de Evolución	10
5	ACTUALIZACIÓN DE LA VISIÓN Y OBJETIVOS ESTRATÉGICOS DE TI	10
5.1	Objetivos Estratégicos.....	11
5.1.1	Fortalecer la seguridad de la información y la ciberseguridad.....	11
5.1.2	Optimizar la gestión de la información y los datos.....	11
5.1.3	Modernizar la infraestructura tecnológica y los servicios de TI.	11
5.1.4	Impulsar la transformación digital y los servicios ciudadanos digitales.	11
5.1.5	Fortalecer las capacidades institucionales y la cultura TIC.	11
5.2	Alineación con los dominios de gobierno digital (MinTIC).	12
5.3	Matriz de Articulación entre el PETI y los Objetivos Estratégicos Institucionales.....	12
5.4	Indicadores Estratégicos (KPIs).	13
5.4.1	Seguridad de la información.	13
5.4.2	Indicador 2 – calidad de datos institucionales.....	13
5.4.3	Nivel de satisfacción posterior a la capacitación.....	14
5.4.4	Reducción de incidentes de seguridad asociados a error humano:	15
5.4.5	Grado de adopción de nuevos sistemas.....	15
6	PORTAFOLIO DE INICIATIVAS DE TI	16
6.1	Criterios de Priorización	16
6.2	Iniciativas Estratégicas.....	17
6.3	Fichas Técnicas de Iniciativas.....	18
6.4	Gobernanza del Portafolio.....	18
7	GESTIÓN DE RIESGOS TI	19
7.1	Principios de la Gestión de Riesgos.....	20
7.2	Metodología de Gestión de Riesgos	20
7.3	Clasificación de Riesgos TI	22
7.4	Matriz de Riesgos de TI	22
7.5	Controles Recomendados (ISO 27001:2022 / NIST).....	22
7.6	Gobernanza del Riesgo.....	23
8	PLAN DE CAPACITACIÓN Y GESTIÓN DEL CAMBIO	23
8.1	Objetivos del Plan	24
8.2	Estrategia de Capacitación.	24



Gestión Administrativa,
Documental y TIC
Dirección Administrativa

SISTEMA DE GESTIÓN INTEGRADO


Código:
PLI-GDO-03-01

Versión:
3

PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI

Fecha de entrada en
vigencia:
30-ene-2026

8.3	Contenidos Formativos	24
8.4	Medición de Resultados	25
8.4.1	Ficha Técnica de indicadores del PETI.....	25
8.5	Gobernanza del Plan.....	26
9	ESTRATEGIA DE SEGURIDAD DE LA INFORMACIÓN	26
9.1	Objetivos de la Estrategia	26
9.2	Principios Rectores	27
9.3	Componentes de la Estrategia.....	27
9.3.1	Política de seguridad de la información.	28
9.3.2	Gestión de activos de información.	28
9.3.3	Gestión de riesgos de seguridad	28
9.3.4	Controles técnicos y administrativos (ISO 27002:2022).	29
9.3.5	Gestión de incidentes de seguridad.	29
9.3.6	Concienciación y capacitación.	29
9.3.7	Continuidad del negocio y recuperación ante desastres.	29
9.4	Indicadores de Seguridad de la Información (KPIs).....	30
9.5	Gobernanza y Seguimiento	30
10	PLAN DE CONTINUIDAD DEL NEGOCIO (PCN) EN TI	31
10.1	Objetivos del PCN	31
10.2	Alcance.....	31
10.3	Metodología.....	32
10.3.1	Análisis de Impacto al Negocio (BIA)	32
10.3.2	Evaluación de Riesgos de Continuidad	32
10.3.3	Estrategias de Continuidad y Recuperación	32
10.3.4	Planes de Respuesta y Procedimientos	32
10.3.5	Pruebas, Ejercicios y Simulaciones	32
10.4	Estrategias Tecnológicas de Resiliencia.....	33
10.5	Roles y Responsabilidades	33
10.6	Indicadores de Desempeño (KPIs).	34
10.7	Gobernanza y Seguimiento.....	34
11	ESTRATEGIA DE FINANCIAMIENTO Y SOSTENIBILIDAD	35
11.1	Planeación Financiera TIC	35
11.2	Fuentes de Financiamiento	36
11.3	Sostenibilidad Financiera.	36
11.4	Indicadores Financieros.	37
11.5	Gobernanza Financiera.....	37
12	INDICADORES DE DESEMPEÑO (KPIs) Y SEGUIMIENTO	37
12.1	Dimensiones de Medición.	37
12.2	Indicadores Estratégicos (KPIs).	38
12.2.1	Gobernanza TIC.....	38
12.2.2	Seguridad de la información.	38
12.2.3	Gestión de proyectos TIC.....	38
12.2.4	Capacitación y cultura digital.	38
12.3	Herramientas de seguimiento.	38
12.4	Gobernanza del Seguimiento.....	39
13	CONCLUSIONES Y RECOMENDACIONES	39
13.1	Conclusiones.....	39
13.2	Recomendaciones.....	40
14	CRONOGRAMA DE ACTIVIDADES - PETI.....	41
15	ANEXOS.....	44
15.1	Normatividad Aplicable.....	45
15.2	Formatos y Plantillas.	46
16	TÉRMINOS Y DEFINICIONES.....	46
17	CONTROL DE CAMBIOS	49

	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

1. INTRODUCCIÓN

1.1 Objetivo del Documento


El Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETI) constituye la hoja de ruta institucional que orienta la planeación, implementación y seguimiento de las iniciativas tecnológicas necesarias para el cumplimiento de la misión, visión y objetivos estratégicos de la entidad. Se trata de un instrumento dinámico y flexible, sujeto a revisiones y actualizaciones periódicas, con el fin de adaptarse a los cambios del entorno tecnológico, normativo, estratégico y organizacional.

El PETI de la EDRU E.I.C.E. Se encuentra plenamente alineado con la Política de Seguridad de la Información y con el Sistema de Gestión de Seguridad de la Información (SGSI), adoptado bajo el estándar internacional ISO/IEC 27001:2022. De esta manera, se asegura que todas las iniciativas tecnológicas se desarrollen dentro de un marco que garantice la confidencialidad, integridad y disponibilidad de la información.

Asimismo, el plan se encuentra articulado con la Estrategia de Gobierno Digital definida por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), garantizando la interoperabilidad, la provisión de servicios ciudadanos digitales, la gestión eficiente de las TIC y el aprovechamiento estratégico de los datos. De igual forma, se integra con el Plan Anticorrupción y de Atención al Ciudadano (PAAC), fortaleciendo la transparencia, la rendición de cuentas y la mejora continua en la prestación de los servicios institucionales.

1.2 Alcance

El presente Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETI) comprende:

 <p>Gestión Administrativa, Documental y TIC Dirección Administrativa</p>	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

- Todas las áreas funcionales de la EDRU E.I.C.E., los procesos estratégicos, misionales, de apoyo y control que dependen del uso de plataformas tecnológicas.
- La infraestructura tecnológica de la Entidad, incluyendo hardware, software, redes y servicios en la nube.
- La gestión, protección y seguridad de la información institucional.
- Los proyectos TIC en ejecución y los planificados durante la vigencia del plan.

En este sentido, el PETI se configura como una herramienta estratégica para la planificación, priorización y ejecución de iniciativas tecnológicas, orientadas a fortalecer la eficiencia institucional, optimizar la experiencia de los usuarios y garantizar el cumplimiento de la normatividad vigente.


1.3 Metodología de Actualización

La actualización del Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETI) se llevó a cabo en tres fases:

- Diagnóstico: Análisis integral del estado actual de las TIC en la Entidad, considerando la infraestructura tecnológica, las aplicaciones, los procesos y el talento humano disponible.
- Actualización Estratégica: Formulación de los objetivos estratégicos de TI, definición de iniciativas prioritarias y aseguramiento de la alineación con la planeación institucional.
- Implementación y Seguimiento: Conformación del portafolio de proyectos, establecimiento de indicadores de gestión y diseño de la estrategia de monitoreo y control.

2 MARCO NORMATIVO Y POLÍTICO

El Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETI) de la EDRU E.I.C.E. Se sustenta en el cumplimiento de la normativa vigente en materia de gestión

	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

de las TIC, protección de datos personales, seguridad de la información y gobierno digital. Asimismo, incorpora estándares y buenas prácticas internacionales que garantizan la eficiencia, la transparencia y la calidad en la prestación de los servicios institucionales.

Este marco normativo y político asegura que todas las iniciativas, proyectos y operaciones tecnológicas de la entidad se desarrollen en un entorno regulado, en armonía con los lineamientos definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), contribuyendo de manera efectiva a la transformación digital de la administración pública.


2.1 Normatividad Aplicable

La actualización del PETI se sustenta en el marco legal y normativo vigente, así como en los lineamientos institucionales y de política pública, entre los cuales se destacan:

- Ley 1712 de 2014 – Ley de Transparencia y del Derecho de Acceso a la Información Pública.
- Decreto 1008 de 2018 – Estrategia de Gobierno Digital.
- CONPES 3854 – Política Nacional de Explotación de Datos (Big Data).
- Ley 1581 de 2012 – Protección de Datos Personales.
- Decreto 1377 de 2013 – Reglamenta aspectos de la Ley 1581 de 2012.
- Decreto 620 de 2020 – Lineamientos de la Estrategia de Gobierno Digital.
- Ley 594 de 2000 – Ley General de Archivos.
- Decreto 1081 de 2015 – Decreto Único Reglamentario del Sector Presidencia.
- Política de Seguridad y Privacidad de la Información definida por la EDRU.
- Programa de Transparencia y Ética Pública - PTEP.

2.2 Políticas y Lineamientos de Gobierno Digital

La actualización del PETI se fundamenta en los lineamientos de la Estrategia de Gobierno Digital, liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones

 <p>EDRU Empresa de Desarrollo y Renovación Urbana</p> <p>Gestión Administrativa, Documental y TIC Dirección Administrativa</p>	<p>SISTEMA DE GESTIÓN INTEGRADO</p>	Código: PLI-GDO-03-01
		Versión: 3
	<p>PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI</p>	Fecha de entrada en vigencia: 30-ene-2026

(MinTIC), cuyo propósito es fomentar el uso estratégico de las TIC para optimizar la gestión pública, fortalecer la transparencia y mejorar la provisión de servicios a la ciudadanía.

En este sentido, el PETI mantiene coherencia y articulación con:

- El Plan Estratégico Institucional.
- El Programa de Transparencia y Ética Pública
- Las Políticas de Seguridad de la Información adoptadas por la EDRU.
- Las estrategias de interoperabilidad y gobierno abierto definidas por el MinTIC.

2.3 Estándares y Mejores Prácticas Internacionales.


Con el fin de garantizar la calidad, seguridad y continuidad de las iniciativas TIC de la entidad, el PETI adopta como marco de referencia los siguientes estándares y buenas prácticas internacionales:

- ISO/IEC 27001:2022 – Sistema de Gestión de Seguridad de la Información (SGSI).
- ISO/IEC 27002:2022 – Directrices y controles para la seguridad de la información.
- ISO 22301:2019 – Gestión de la Continuidad del Negocio.
- ISO/IEC 20000-1:2018 – Gestión de Servicios de Tecnologías de la Información.
- TOGAF – Marco de referencia para el diseño y gestión de la Arquitectura Empresarial.

3 DIAGNÓSTICO ESTRATÉGICO

El diagnóstico estratégico del PETI constituye la base para definir las acciones y proyectos que permitan cerrar brechas, potenciar capacidades y garantizar que las tecnologías de la información y las comunicaciones de la Empresa de Desarrollo y Renovación Urbana E.I.C.E. - EDRU E.I.C.E, estén alineadas con los objetivos institucionales, la normatividad vigente y las mejores prácticas internacionales.

Este diagnóstico se elaboró a partir de:

 <p>Gestión Administrativa, Documental y TIC Dirección Administrativa</p>	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

- Entrevistas con líderes de procesos y responsables de áreas.
- Evaluación de madurez digital según el Modelo de Gobierno Digital de MinTIC.
- Revisión de la infraestructura tecnológica, software, políticas y procedimientos.
- Análisis de riesgos y oportunidades desde la perspectiva de la ISO/IEC 27001:2022.

3.1 Diagnóstico Organizacional (ciberseguridad, brechas y recomendaciones iniciales). Ciberseguridad

Identificar: Falta un registro centralizado y categorizado de activos de información.

Proteger: Ausencia de controles formales para clasificación y etiquetado de la información.

Detectar: Monitoreo de eventos de seguridad no automatizados.

Responder: No existe un plan documentado y probado de respuesta a incidentes.

Recuperar: Procesos de respaldo y restauración dispersos y no estandarizados.

3.1.1 Brechas.

- Gestión de Activos: Inventario incompleto de hardware, software y licencias.
- Seguridad de la Información: Falta formalizar y aprobar el SGSI bajo ISO 27001:2022.
- Monitoreo y Control: Ausencia de KPIs y tablero de control para el seguimiento de proyectos TIC.


3.1.2 Recomendaciones.

- Formalizar el SGSI bajo ISO 27001:2022.
- Definir y publicar un Tablero de Control de KPIs TIC.

3.2 Diagnóstico de Tecnologías de la Información

Se llevó a cabo una evaluación de los principales componentes que conforman el ecosistema tecnológico de la entidad, abarcando los siguientes aspectos:

- Infraestructura tecnológica: hardware, redes y centros de datos.
- Sistemas de información y aplicaciones corporativas.

 <p>Gestión Administrativa, Documental y TIC Dirección Administrativa</p>	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

- Gestión de datos y analítica.
- Seguridad de la información.
- Talento humano especializado en TI.

3.3 Análisis FODA en Tecnologías de la Información


El análisis de Fortalezas, Oportunidades, Debilidades y Amenazas (FODA) se desarrolló con las áreas líderes de la entidad, permitiendo identificar factores internos y externos que influyen en la gestión de las Tecnologías de la Información.

Fortalezas	Oportunidades
Plataforma tecnológica actualizada	Nuevas políticas de Gobierno Digital
Infraestructura básica de red y conectividad estable en todas las sedes.	Lineamientos y programas de Gobierno Digital ofrecidos por MinTIC.
Compromiso de la Dirección Administrativa con la transformación digital.	Disponibilidad de tecnologías en la nube para optimizar costos y escalabilidad.
Experiencia previa en implementación de sistemas administrativos.	Posibilidad de interoperar con otras entidades para mejorar procesos.
Debilidades	Amenazas
Baja cultura digital interna	Pérdida de control de las credenciales de acceso.
Ausencia de un inventario unificado y actualizado de activos TIC (CMDB).	Riesgos de fuga de información.
Políticas y procedimientos de seguridad de la información en proceso de formalización.	Obsolescencia tecnológica en equipos y sistemas.
Falta de métricas de desempeño (KPIs) para los servicios TIC.	Cambios normativos que exigen adaptaciones rápidas.

3.4 Estado Actual de la Arquitectura Empresarial

La arquitectura empresarial de la EDRU E.I.C.E constituye el marco que articula los procesos, las aplicaciones, los datos y la infraestructura tecnológica que respalda la operación institucional. A partir del diagnóstico realizado, se documentó el estado actual de cada uno de

Página 6 de 49

	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

sus dominios, identificando componentes obsoletos, duplicados o con requerimientos de modernización. Este análisis permite definir una hoja de ruta de transformación tecnológica alineada con los objetivos estratégicos de la entidad, los lineamientos del Gobierno Digital y las mejores prácticas de ISO 27001:2022 en materia de seguridad de la información.

Hallazgos principales por dominio:


- **Procesos:** Se evidencia una limitada alineación entre procesos institucionales y la estrategia de Gobierno Digital.
- **Datos e Información:** No se cuenta con controles de seguridad robustos (cifrado, control de accesos, trazabilidad), lo que dificulta el cumplimiento de los requisitos establecidos en ISO 27001:2022.
- **Tecnología e Infraestructura:** Se identifican deficiencias en la aplicación de controles de seguridad, ausencia en monitoreo continuo y falta de políticas de virtualización.

Conclusiones:

- La arquitectura empresarial de la EDRU E.I.C.E requiere un proceso de modernización integral que abarque los ámbitos de procesos, aplicaciones, datos e infraestructura.
- Es indispensable establecer un marco de gobernanza TIC que garantice la alineación de la arquitectura con la estrategia institucional, los lineamientos de Gobierno Digital, las exigencias regulatorias y los estándares de seguridad de la información definidos en la norma ISO 27001:2022.
- La identificación de componentes obsoletos y duplicados representa una oportunidad para optimizar el uso de recursos, reducir costos operativos y fortalecer tanto la seguridad como la continuidad de los servicios tecnológicos.

3.5 Evaluación de Madurez Digital

De acuerdo con el Modelo de Gobierno Digital de MinTIC, la EDRU E.I.C.E presenta los siguientes niveles de madurez:

	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

- Gestión de TIC: Nivel intermedio. Se cuenta con procesos documentados, aunque aún no se encuentran plenamente integrados ni optimizados.
- Seguridad y Privacidad de la Información: Nivel inicial. Existen políticas en fase de diseño y controles en proceso de implementación.
- Gestión de Datos y Analítica: Nivel básico. No se dispone de una estrategia formal para la gestión y aprovechamiento de los datos como activo institucional.

4 ARQUITECTURA EMPRESARIAL DE TI.


La Arquitectura Empresarial de Tecnologías de la Información constituye el marco de referencia que orienta la alineación de los recursos tecnológicos con los objetivos estratégicos de la EDRU E.I.C.E. Su finalidad es asegurar que los procesos, la información, las aplicaciones y la infraestructura tecnológica se encuentren organizados, integrados y orientados a generar valor tanto para la entidad como para la ciudadanía.

La actualización de esta arquitectura se enmarca en la Estrategia de Gobierno Digital del MinTIC, fomentando la seguridad, la eficiencia y el uso responsable de los recursos tecnológicos.

4.1 Visión Actual de la Arquitectura

La arquitectura empresarial de la Empresa de Desarrollo y Renovación Urbana – EDRU E.I.C.E., está conformada actualmente por un ecosistema de aplicaciones, infraestructura tecnológica y procesos de negocio que soportan la prestación de servicios a la ciudadanía, entidades asociadas y usuarios internos.

- Procesos: Los procesos misionales se respaldan en aplicaciones independientes, con limitada integración entre las áreas administrativas y misionales.
- Información: Existen bases de datos aisladas, sin un modelo centralizado de gestión de la información ni un catálogo institucional de datos.

	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

- **Aplicaciones:** Varias aplicaciones cumplen funciones operativas, aunque presentan restricciones en escalabilidad, integración y cobertura de necesidades institucionales.
- **Seguridad:** La seguridad se gestiona de manera básica, sin controles avanzados ni monitoreo centralizado.

4.2 Arquitectura Objetivo (Futura)

La visión futura de la arquitectura de TI de la EDRU E.I.C.E está orientada a evolucionar hacia un modelo seguro, escalable e integrado, con un enfoque centrado en el ciudadano y plenamente articulado con los lineamientos de Gobierno Digital.


Procesos: Implementación de procesos estandarizados y automatizados mediante plataformas de Business Process Management (BPM), que aseguren eficiencia, trazabilidad y mejora continua.

Información: Creación de un Catálogo Institucional de Datos, con adopción de principios de datos abiertos, gobernanza de datos y gestión integral de metadatos.

Aplicaciones: Consolidación de un portafolio integrado de aplicaciones, priorizando soluciones alineadas con los estándares de Gobierno Digital y orientadas a la prestación de servicios digitales al ciudadano.

Infraestructura tecnológica: Migración progresiva hacia un modelo híbrido (servidores locales combinados con nube pública y privada), que garantice mayor disponibilidad, resiliencia y escalabilidad.

Seguridad: Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO 27001:2022, acompañado de controles avanzados (MFA, cifrado, SIEM) y planes de gestión de incidentes.

 <p>Gestión Administrativa, Documental y TIC Dirección Administrativa</p>	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

4.3 Hoja de Ruta de Evolución

Corto plazo (0-12 meses):

- Realizar el levantamiento detallado del inventario de aplicaciones y activos tecnológicos.
- Actualizar la infraestructura de red y los servidores críticos.
- Iniciar la construcción del Catálogo Institucional de Datos.

Mediano plazo (1-3 años):

- Implementar soluciones de interoperabilidad entre los sistemas internos.
- Avanzar en la migración progresiva hacia una infraestructura híbrida (nube + local).
- Automatizar los procesos prioritarios de la entidad.


Largo plazo (3-5 años):

- Implementar de manera completa el Sistema de Gestión de Seguridad de la Información (SGSI) bajo la norma ISO 27001:2022.
- Alcanzar un nivel de madurez digital alta, conforme a los lineamientos del MinTIC.

5 ACTUALIZACIÓN DE LA VISIÓN Y OBJETIVOS ESTRATÉGICOS DE TI.

La visión del Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETI) de la EDRU E.I.C.E es consolidar a la entidad como una organización moderna, segura y eficiente, que aprovecha las TIC como motor de transformación digital. Este enfoque busca garantizar la transparencia, la seguridad de la información y la calidad en la prestación de servicios a la ciudadanía.

La actualización del PETI establece objetivos estratégicos que orientan la planeación, inversión y ejecución de proyectos tecnológicos, asegurando que las TIC no solo respalden las operaciones institucionales, sino que también impulsen su misión y contribuyan al cumplimiento de la Estrategia de Gobierno Digital.

 <p>Gestión Administrativa, Documental y TIC Dirección Administrativa</p>	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

5.1 Objetivos Estratégicos

Los objetivos estratégicos de la EDRU E.I.C.E en materia de Tecnologías de la Información y las Comunicaciones se estructuran en cinco ejes fundamentales, entre ellos:

5.1.1 Fortalecer la seguridad de la información y la ciberseguridad.

- Implementar un Sistema de Gestión de Seguridad de la Información (SGSI) conforme con la norma ISO/IEC 27001:2022.
- Proteger la confidencialidad, integridad y disponibilidad de la información institucional.
- Promover una cultura organizacional orientada a la seguridad digital.

5.1.2 Optimizar la gestión de la información y los datos.

- Desarrollar un Catálogo Institucional de Datos y adoptar prácticas de datos abiertos.
- Fortalecer la calidad, interoperabilidad y disponibilidad de la información.
- Potenciar el uso de analítica de datos para la toma de decisiones estratégicas.

5.1.3 Modernizar la infraestructura tecnológica y los servicios de TI.


- Avanzar progresivamente hacia un modelo de infraestructura híbrida (nube + local).
- Implementar soluciones tecnológicas escalables, resilientes y sostenibles en el tiempo.

5.1.4 Impulsar la transformación digital y los servicios ciudadanos digitales.

- Digitalizar y automatizar los procesos institucionales.
- Integrar la entidad al ecosistema de servicios ciudadanos digitales promovido por MinTIC.
- Garantizar servicios digitales accesibles, disponibles y fáciles de usar para todos los ciudadanos.

5.1.5 Fortalecer las capacidades institucionales y la cultura TIC.

- Desarrollar programas de capacitación y gestión del cambio organizacional.
- Fomentar la innovación y el uso estratégico de las TIC en todas las áreas de la entidad.
- Consolidar un modelo de gobernanza TIC alineado con el PETI.

	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026


5.2 Alineación con los dominios de gobierno digital (MinTIC).

Los objetivos estratégicos de la EDRU E.I.C.E en materia de TIC se articulan directamente con los ejes de la política de Gobierno Digital, de la siguiente manera:

- Servicios Ciudadanos Digitales: Objetivo 4
- Seguridad y Privacidad de la Información: Objetivo 1
- Gestión de las TIC: Objetivos 3 y 5
- Uso y Aprovechamiento de Datos: Objetivo 2
- Interoperabilidad: Objetivos 2 y 4

5.3 Matriz de Articulación entre el PETI y los Objetivos Estratégicos Institucionales

Eje del PETI / Gobierno Digital	Objetivo TIC del PETI	Objetivo Estratégico Institucional que Apoya	Tipo de Contribución Estratégica	KPI Asociado (PETI)
1. Servicios Ciudadanos Digitales	Mejorar la experiencia y acceso a servicios digitales para el ciudadano y actores urbanos.	Objetivo 1 y Objetivo 2	Facilita acceso a trámites, mejora comunicación en zonas priorizadas y agiliza servicios para procesos de renovación urbana.	<ul style="list-style-type: none"> • Tasa de digitalización de servicios • Nivel de satisfacción del usuario digital
2. Seguridad y Privacidad de la Información	Garantizar la confidencialidad, integridad y disponibilidad de la información urbana, jurídica y administrativa.	Objetivo 3	Asegura continuidad tecnológica para macroproyectos urbanos y mitiga riesgos críticos de infraestructura y datos.	<ul style="list-style-type: none"> • % incidentes críticos atendidos < 72h • Cumplimiento de controles SGSI
3. Gestión de las TIC	Modernizar la infraestructura tecnológica y fortalecer la capacidad operativa de TI.	Objetivo 3 y Objetivo 4	Provee soporte tecnológico a macroproyectos de renovación e integración inmobiliaria, y mejora la eficiencia institucional.	<ul style="list-style-type: none"> • % ejecución del portafolio PETI • Disponibilidad de servicios TI
4. Uso y Aprovechamiento de Datos	Mejorar la calidad, disponibilidad y análisis de datos para la toma de	Objetivo 2 y Objetivo 3	Permite planeación urbana basada en datos confiables y soporte analítico	<ul style="list-style-type: none"> • Índice de calidad de datos • % de datos actualizados

 <p>Gestión Administrativa, Documental y TIC Dirección Administrativa</p>	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

	decisiones urbanas.		para macroproyectos.	
5. Interoperabilidad	Conectar sistemas internos y externos para facilitar el intercambio seguro de información.	Objetivo 1, 2 y 4	Acelera procesos de renovación urbana mediante intercambio de información con entidades externas (Catastro, Planeación, Jurídica, etc.).	<ul style="list-style-type: none"> • % servicios interoperables • Tiempo promedio de intercambio de datos

La matriz anterior evidencia la trazabilidad directa entre los ejes del PETI, los objetivos TIC y los cuatro objetivos estratégicos de la EDRU, dando cumplimiento a los lineamientos de MIPG y Gobierno Digital.

5.4 Indicadores Estratégicos (KPIs).

5.4.1 Seguridad de la información.

Indicador 1 – Seguridad de la Información

Nombre: % de incidentes críticos de seguridad atendidos en menos de 72 horas

Definición: Mide el porcentaje de incidentes clasificados como críticos que fueron gestionados y cerrados dentro de un tiempo máximo de 72 horas.

Fórmula:

$(\text{Incidentes críticos atendidos} \leq 72\text{h} / \text{Total incidentes críticos reportados}) \times 100$

Unidad de medida: Porcentaje (%)

Línea base: Por definir con la oficina de planeación

Meta anual: $\geq 90\%$

Fuente de información: Registro de incidentes - Mesa de Servicios TI


Periodicidad: Mensual / Trimestral

Responsable: Equipo TIC – Seguridad de la Información

5.4.2 Indicador 2 – calidad de datos institucionales

Nombre: Índice de Calidad de Datos Institucionales

Tipo: Cuantitativo compuesto

 <p>Gestión Administrativa, Documental y TIC Dirección Administrativa</p>	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

Definición: Evalúa el nivel de calidad de los datos institucionales en términos de confiabilidad, disponibilidad y actualización.

Variables:

Variable	Definición	Método de medición
Confiabilidad	Grado en que los datos están completos, sin inconsistencias ni errores.	% de registros validados sin inconsistencias.
Disponibilidad	Acceso oportuno a la información que necesitan los procesos.	% de bases de datos con acceso operativo sin interrupciones.
Actualización	Frecuencia con la que los datos son actualizados según el ciclo definido por el proceso.	% de datos actualizados dentro del periodo establecido.

Fórmula del indicador general:

$$\frac{(\text{Confiabilidad}\% + \text{Disponibilidad}\% + \text{Actualización}\%)}{3}$$

3

Unidad de medida: Índice 0–100%

Línea base: Por definir

Meta: ≥ 85%

Fuente: Inventario y evaluaciones de activos de información

Periodicidad: Trimestral

Responsable: Oficina TIC / Responsable de Datos

5.4.3 Nivel de satisfacción posterior a la capacitación


Nombre del Indicador: Nivel de satisfacción posterior a la capacitación TIC.

Objetivo: Evaluar la percepción y satisfacción de los funcionarios después de participar en actividades de capacitación TIC.

Descripción: Promedio del nivel de satisfacción reportado en encuestas posteriores a la capacitación.

Fórmula de Cálculo: (Suma de calificaciones en encuestas / Número total de encuestas diligenciadas)

Variables: Variable 1 -Calificación de satisfacción, Variable 2 - Número de encuestas diligenciadas

	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

Línea Base: Pendiente (se definirá con la primera medición oficial).

Meta Anual (2025) $\geq 4.0 / 5.0$

Unidad: Puntaje

Periodicidad: Trimestral

Fuente: Encuestas posteriores a la capacitación.

Responsable: Talento Humano

5.4.4 Reducción de incidentes de seguridad asociados a error humano:

Indicador 4: Reducción de incidentes de seguridad asociados a error humano

Nombre del Indicador: Reducción de incidentes de seguridad asociados a error humano.

Objetivo: Reducir incidentes de seguridad digital derivados de fallas operativas del personal.

Descripción: Mide el porcentaje de disminución anual de incidentes de seguridad asociados al factor humano.

Fórmula: $(\text{Incidentes año anterior} - \text{Incidentes año actual}) / \text{Incidentes año anterior} \times 100$

Variables: Variable 1 -Incidentes año anterior, Variable 2 - Incidentes año actual

Línea Base: Por definir (requiere histórico del SGSI).

Meta Anual (2025): Reducción $\geq 20\%$

Unidad: Porcentaje (%)

Periodicidad: Semestral

Fuente: Registro de incidentes

Sistema SGSI: Reportes de la Oficina TIC

Responsable: Oficina TIC – Seguridad de la Información

5.4.5 Grado de adopción de nuevos sistemas


Indicador 5: Grado de adopción de nuevos sistemas

Nombre del Indicador: Grado de adopción de nuevos sistemas institucionales.

Objetivo: Medir qué tan efectivamente los funcionarios utilizan los sistemas implementados recientemente.

Descripción: Porcentaje de usuarios activos sobre el total de usuarios habilitados en un nuevo sistema institucional.

Fórmula de Cálculo: $(\text{Usuarios activos} / \text{Usuarios habilitados}) \times 100$

	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

Variables: Variable 1 - usuarios activos, Variable 2 - Usuarios habilitados

Línea Base: Por definir (primera medición).

Meta Anual (2025): $\geq 70\%$

Unidad: Porcentaje (%)

Periodicidad: Trimestral

Fuente: Logs de acceso

Análítica de uso: Reportes del sistema

Responsable: Oficina TIC

6 PORTAFOLIO DE INICIATIVAS DE TI


El portafolio de iniciativas reúne los proyectos estratégicos de Tecnologías de la Información priorizados por la EDRU E.I.C.E para garantizar el cumplimiento de los objetivos definidos en el PETI. Cada iniciativa responde a una necesidad institucional específica y se encuentra alineada con los lineamientos de Gobierno Digital, la normativa vigente y las mejores prácticas internacionales en gestión de proyectos y seguridad de la información.

Este portafolio se estructura en tres horizontes de tiempo: corto plazo (0-12 meses), mediano plazo (1-3 años) y largo plazo (3-5 años), lo que permite trazar una hoja de ruta progresiva, ordenada y sostenible.

6.1 Criterios de Priorización

Las iniciativas del PETI se priorizan considerando los siguientes criterios:

- Contribución directa al cumplimiento de la misión institucional y de los objetivos estratégicos.
- Cumplimiento normativo: Nivel de alineación con la normativa vigente (MinTIC, ISO/IEC 27001:2022, Ley 1581 de Protección de Datos, entre otras).
- Valor al ciudadano: Grado de mejora en la experiencia y satisfacción de los usuarios internos y externos.

 <p>EDRU Empresa de Desarrollo y Renovación Urbana</p> <p>Gestión Administrativa, Documental y TIC Dirección Administrativa</p>	<p>SISTEMA DE GESTIÓN INTEGRADO</p>	Código: PLI-GDO-03-01
		Versión: 3
	<p>PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI</p>	Fecha de entrada en vigencia: 30-ene-2026

- Riesgo mitigado: Capacidad de la iniciativa para reducir vulnerabilidades tecnológicas y de seguridad de la información.


6.2 Iniciativas Estratégicas.

Corto Plazo (0-12 meses):

- Implementar un tablero básico de analítica para procesos misionales prioritarios.
- Diseñar y aprobar la hoja de ruta de implementación del SGSI basado en ISO 27001 - 2022.
- Actualizar la infraestructura tecnológica crítica (servidores, redes y sistemas de respaldo).
- Publicar el inventario inicial de datos institucionales y su clasificación (incluyendo el listado preliminar de datos abiertos exigidos por el PTEP).
- Definir y aprobar fichas técnicas de indicadores TIC con Planeación y construir el tablero mínimo viable.
 - ✓ Fase 1: Definir fichas técnicas (30 días)
 - ✓ Fase 2: Implementar tablero (2–3 meses)

- Mediano Plazo (1-3 años):

- ✓ Realizar el estudio técnico de viabilidad para adopción de infraestructura híbrida.
- ✓ Implementar herramientas avanzadas de analítica y explotación de datos.
- ✓ Identificar y priorizar los dos primeros procesos candidatos a automatización.
- ✓ Realizar diagnóstico de adopción de Servicios Ciudadanos Digitales y plan de integración.
- ✓ Desarrollar e implementar un sistema de gestión documental electrónico.
- ✓ Implementar el Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001-2022.

	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

La implementación del SGSI se realizará conforme a los lineamientos establecidos por la ISO/IEC 27001-2022. Esta adopción será soportada mediante actas de aprobación, lineamientos internos y procedimientos documentados del SGSI.

Largo Plazo (3-5 años):

- Incrementar el nivel de madurez digital según modelo MinTIC.

6.3 Fichas Técnicas de Iniciativas.

Cada proyecto debe documentarse con el formato FOR-GDO-03-04 FICHA TÉCNICA DE PROYECTOS TIC, elaborada conforme a los lineamientos institucionales:

- Nombre del proyecto.
- Objetivo.
- Descripción del alcance.
- Responsable.
- Duración estimada.
- Riesgos asociados.
- Indicadores de éxito (KPIs).


Los documentos FOR-GDO-03-04 FICHA TÉCNICA DE PROYECTOS TIC y FOR-GDO-03-09 BANCO DE INICIATIVAS TIC se integran al Procedimiento PRO-GDO-03-01 - GESTIÓN DE INICIATIVAS Y PROYECTOS TIC.

La Oficina TIC mantendrá actualizadas estas fichas y las usará como base para seguimiento, socialización y evaluación de proyectos.

6.4 Gobernanza del Portafolio.

La gestión del portafolio TIC se realizará bajo el siguiente esquema:

Supervisión del Portafolio

 <p>Gestión Administrativa, Documental y TIC Dirección Administrativa</p>	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

La supervisión del portafolio estará a cargo del Comité Institucional de Gestión y Desempeño (CIGD), instancia responsable de validar el avance estratégico, revisar los resultados y tomar decisiones sobre priorización, continuidad o ajuste de las iniciativas TIC, conforme al Modelo Integrado de Planeación y Gestión (MIPG).

Administración del Portafolio

La Oficina de Planeación será la encargada de la administración del portafolio TIC, incluyendo:

- consolidación de la información del portafolio;
- Revisión trimestral del avance de iniciativas;
- Verificación de alineación con el Plan Estratégico y el PETI;
- Elaboración de informes institucionales.


Ejecución Técnica

La Dirección Administrativa y su equipo TIC, serán responsables de la gestión técnica, operativa y documental de las iniciativas y proyectos TIC que integran el portafolio, garantizando la actualización de fichas técnicas, cronogramas e informes de avance.

7 GESTIÓN DE RIESGOS TI

Se adopta un enfoque alineado con las mejores prácticas y estándares internacionales, complementado con la normativa nacional vigente, entre los que se destacan:

- ISO 31000:2018 – Principios y directrices para la gestión de riesgos.
- ISO/IEC 27005:2022 – Gestión de riesgos en seguridad de la información.
- Guía para la Gestión del Riesgo – Versión 7 (DAFP), Capítulo V, lineamiento oficial del Modelo Integrado de Planeación y Gestión (MIPG) para la administración del riesgo institucional.

	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

- ISO/IEC 27001:2022 – Requisitos para el Sistema de Gestión de Seguridad de la Información (SGSI).
- Lineamientos de Gobierno Digital – MinTIC sobre gestión de riesgos TIC y ciberseguridad en entidades públicas.

7.1 Principios de la Gestión de Riesgos


- Integralidad: Se consideran riesgos estratégicos, operativos, regulatorios, tecnológicos y de ciberseguridad.
- Enfoque preventivo: Se prioriza la anticipación frente a la reacción.
- Alineación estratégica: La gestión de riesgos se realiza en coherencia con los objetivos institucionales y el PETI.
- Mejora continua: El proceso se revisa y ajusta de manera periódica para garantizar su eficacia.
- Transparencia: Los resultados se documentan y se presentan en los comités directivos.

7.2 Metodología de Gestión de Riesgos

El ciclo de gestión de riesgos de TI en la EDRU E.I.C.E se desarrolla en cinco fases principales:

Identificación:

- Elaboración del inventario de activos tecnológicos (hardware, software, datos y procesos), en el formato FOR-GDO-03-06 PLANILLA DE INVENTARIO DE ACTIVOS DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES – TIC.
- Detección de amenazas potenciales (ciberataques, fallas técnicas, errores humanos, desastres naturales, obsolescencia tecnológica).
- Reconocimiento de vulnerabilidades existentes (ausencia de controles, configuraciones inadecuadas, falta de capacitación, inexistencia de planes de continuidad).

	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

Análisis:

- Valoración del impacto en la organización (operativo, reputacional, financiero, legal y estratégico).
- Estimación de la probabilidad de ocurrencia de cada riesgo identificado.

Evaluación:


- Clasificación de riesgos por niveles (bajo, medio, alto, crítico).
- Priorización de riesgos en función de su impacto sobre la misión institucional y la continuidad de los servicios.

Tratamiento:

- Evitar: Suprimir o no ejecutar actividades que generen un riesgo alto no controlable.
- Mitigar: Implementar controles técnicos, administrativos y de seguridad.
- Transferir: Externalizar el riesgo mediante seguros, contratos de servicios gestionados u outsourcing.
- Aceptar: Asumir el riesgo cuando el costo de mitigación sea superior al impacto potencial.

Monitoreo y Revisión:

- Realizar seguimiento trimestral a los riesgos identificados y a la efectividad de los controles implementados.
- Actualizar anualmente la matriz de riesgos de TI, incorporando cambios en el entorno tecnológico y organizacional.
- Incluir la revisión de la gestión de riesgos en las auditorías internas y externas, garantizando la verificación y mejora continua del proceso.

 <p>Gestión Administrativa, Documental y TIC Dirección Administrativa</p>	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

7.3 Clasificación de Riesgos TI.


- Riesgos de Ciberseguridad: Incluyen amenazas como malware, phishing, ransomware y fugas de información.
- Riesgos Operativos: Relacionados con fallas de hardware o software, interrupciones en los servicios y problemas de disponibilidad en la red.
- Riesgos Regulatorios: Asociados al incumplimiento de la normativa vigente, como la Ley 1581 de 2012, el Decreto 620 de 2020 y la Ley 1712 de 2014.
- Riesgos Estratégicos: Derivados de la falta de alineación de los proyectos de TI con el Plan Estratégico de Tecnologías de la Información (PETI) y los objetivos institucionales.
- Riesgos de Proveedores: Vinculados a la dependencia de terceros, incumplimiento de acuerdos de nivel de servicio (SLA) y brechas contractuales.

7.4 Matriz de Riesgos de TI

Ver el formato FOR-GDO-03-01 MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACION.

7.5 Controles Recomendados (ISO 27001:2022 / NIST)

- Autenticación multifactor (MFA).
- Segmentación de red y firewalls de próxima generación.
- Cifrado de información sensible en reposo y en tránsito.
- Monitoreo centralizado con herramientas SIEM (Gestión de Eventos e Información de Seguridad).
- Copias de seguridad cifradas y probadas periódicamente.
- Políticas de gestión de identidades y accesos (IAM).
- Programas de concienciación en ciberseguridad.

 <p>Gestión Administrativa, Documental y TIC Dirección Administrativa</p>	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026


7.6 Gobernanza del Riesgo

- **El Comité Institucional de Gestión y Desempeño (CIGD)** es el órgano responsable de la supervisión de la gestión del riesgo en la EDRU E.I.C.E., conforme al Modelo Integrado de Planeación y Gestión (MIPG). Este comité está conformado por la Gerencia General, Subgerencia, Secretaría General, Dirección Administrativa, Dirección Financiera, Oficina Jurídica, Oficina de Planeación, Coordinación de Seguimiento y Control, Dirección de Planes Parciales, Dirección de Proyectos y Dirección de Desarrollo.
- **La Oficina de Control Interno** valida metodológicamente la matriz de riesgos TIC - FOR-GDO-03-01, verifica su consistencia con la Guía para la Gestión del Riesgo – Versión 7 del DAFP y apoya la consolidación del Mapa de Riesgos Institucional.
- **La Matriz de Riesgos TIC se incorpora al Mapa de Riesgos Institucional**, garantizando su alineación con la gestión global del riesgo y su reporte en el marco del MIPG.

8 PLAN DE CAPACITACIÓN Y GESTIÓN DEL CAMBIO

El éxito del Plan Estratégico de Tecnologías de la Información (PETI) no depende únicamente de la implementación de infraestructura y soluciones tecnológicas, sino también de la adecuada adopción y uso por parte de los funcionarios, contratistas y la ciudadanía. En este sentido, la EDRU E.I.C.E implementará un Plan de Capacitación y Gestión del Cambio, orientado a:

- Fortalecer las competencias digitales de los colaboradores.
- Fomentar una cultura organizacional de seguridad de la información.
- Facilitar la apropiación de los nuevos procesos y servicios digitales.

	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

8.1 Objetivos del Plan

- Fortalecer las competencias digitales del personal en todos los niveles de la organización, garantizando un uso eficiente y seguro de las herramientas tecnológicas.
- Fomentar una cultura de seguridad de la información que asegure el cumplimiento de la norma ISO 27001:2022 y de las políticas institucionales.
- Asegurar la apropiación de nuevas tecnologías y procesos digitales, disminuyendo la resistencia al cambio y facilitando su adopción.
- Promover la innovación y el uso estratégico de las TI, en coherencia con el PETI y la Estrategia de Gobierno Digital.

8.2 Estrategia de Capacitación.


La estrategia de capacitación se desarrollará de forma progresiva y diferenciada, atendiendo a las responsabilidades y funciones de cada nivel de la organización:

- Nivel Directivo: Formación en Gobierno Digital, uso estratégico de las TIC para la gestión institucional, gestión de riesgos y toma de decisiones basada en datos.
- Nivel Administrativo y Técnico: Capacitación en herramientas tecnológicas de uso cotidiano, interoperabilidad de sistemas, uso seguro de la información y cumplimiento normativo.
- Nivel Operativo: Talleres prácticos en competencias digitales básicas, seguridad de contraseñas, uso del correo institucional y manejo de trámites digitales.

8.3 Contenidos Formativos

Los contenidos del plan de capacitación estarán enfocados en fortalecer las competencias digitales y de seguridad de la información, incluyendo:

- Cultura Digital y lineamientos de Gobierno Digital (MinTIC).
- Seguridad de la Información y Ciberseguridad, con énfasis en la norma ISO/IEC 27001:2022.

	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

- Protección de Datos Personales (Ley 1581 de 2012 y normativa complementaria).
- Gestión Documental Electrónica e Interoperabilidad de sistemas.
- Analítica de Datos y toma de decisiones basadas en evidencia.
- Gestión del Cambio y adopción de nuevas herramientas digitales.

8.4 Medición de Resultados


8.4.1 Ficha Técnica de indicadores del PETI

En cumplimiento de los lineamientos del MIPG, el DAFP y la Política de Gobierno Digital, los indicadores definidos para medir los resultados del PETI cuentan con su respectiva ficha técnica, FOR-GAC-08 FICHA TÉCNICA PARA FORMULACIÓN DE INDICADORES, la cual incluye:

- Nombre del indicador
- Objetivo del indicador
- Fórmula de cálculo
- Definición de variables
- Unidad de medida
- Línea base
- Meta anual
- Frecuencia de medición
- Responsable del reporte
- Medios de verificación
- Fuente de información

A continuación, se presentan los indicadores definidos para el seguimiento del PETI:

- Porcentaje de funcionarios capacitados en competencias TIC.
- Porcentaje de funcionarios certificados en seguridad de la información.
- Nivel de satisfacción obtenido en encuestas posteriores a la capacitación.
- Reducción de incidentes de seguridad asociados a errores humanos.
- Grado de adopción de nuevos sistemas, medido por métricas de acceso y transacciones realizadas.

 <p>Gestión Administrativa, Documental y TIC Dirección Administrativa</p>	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

8.5 Gobernanza del Plan

Responsable:

La Oficina de Planeación es la encargada del seguimiento, monitoreo y consolidación de los avances del PETI, de acuerdo con el Manual de Funciones institucional y los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG). Esta dependencia reporta los resultados al Comité Institucional de Gestión y Desempeño (CIGD) para su análisis y toma de decisiones. La Oficina TIC y el Área de Talento Humano brindarán apoyo operativo y técnico cuando corresponda, especialmente en actividades de capacitación, fortalecimiento de competencias y adopción de nuevas tecnologías.

El Comité Institucional de Gestión y Desempeño se reunirá semestralmente para revisar avances y validar el cumplimiento de los objetivos del PETI.


9 ESTRATEGIA DE SEGURIDAD DE LA INFORMACIÓN

La Estrategia de Seguridad de la Información de la EDRU E.I.C.E tiene como propósito proteger la confidencialidad, integridad, disponibilidad y trazabilidad de la información institucional, asegurando el cumplimiento normativo y fortaleciendo la confianza digital.

Este componente del PETI se implementa en el marco del Sistema de Gestión de Seguridad de la Información (SGSI), conforme a los lineamientos de la norma ISO/IEC 27001:2022, los controles de la ISO/IEC 27002 y las políticas de Gobierno Digital definidas por el MinTIC.

9.1 Objetivos de la Estrategia

- Implementar y mantener un SGSI formal en la EDRU.
- Garantizar el cumplimiento de la normativa nacional en materia de protección de datos personales (Ley 1581 de 2012, Decreto 1377 de 2013).
- Prevenir, detectar y responder de manera eficaz ante incidentes de seguridad y ciberataques.

 <p>Gestión Administrativa, Documental y TIC Dirección Administrativa</p>	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

- Fomentar una cultura organizacional orientada a la seguridad de la información.
- Asegurar la continuidad operativa de los procesos misionales soportados en TIC.

9.2 Principios Rectores


La Estrategia de Seguridad de la Información se fundamenta en los siguientes principios:

- Seguridad por diseño y por defecto en todos los sistemas y servicios TIC.
- Cumplimiento normativo de la Ley 1581 de 2012, la Ley 1712 de 2014 y los lineamientos del MinTIC.
- Gestión del riesgo de seguridad con enfoque preventivo, de acuerdo con la norma ISO/IEC 27005.
- Mejora continua del SGSI, en concordancia con el ciclo PHVA (Planear, Hacer, Verificar, Actuar).
- Conciencia y corresponsabilidad de todos los funcionarios y contratistas en la protección de la información.

Principios de Gestión Integral del Riesgo (Guía V7 – DAFP)

- Enfoque integral del riesgo, articulado con el Modelo Integrado de Planeación y Gestión (MIPG).
- Coordinación entre dependencias para la identificación, valoración y tratamiento del riesgo.
- Gestión preventiva basada en evidencia y análisis de causas.
- Responsabilidad de todos los niveles directivos y operativos en la gestión del riesgo.
- Transparencia y trazabilidad en el registro, seguimiento y reporte del riesgo.
- Inclusión del riesgo TIC en el Mapa de Riesgos Institucional.
- Mejora continua del modelo de riesgo mediante revisión periódica y lecciones aprendidas.

9.3 Componentes de la Estrategia

 <p>Gestión Administrativa, Documental y TIC Dirección Administrativa</p>	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

9.3.1 Política de seguridad de la información.

La Política de Seguridad de la Información constituye la declaración oficial de compromiso institucional frente a la protección de los activos de información, se encuentra integrada al sistema de gestión integrado con el código POL-GDO-03-01 POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN y contempla:

- Aprobación por parte del Comité Institucional de Gestión y Desempeño.
- Definición de roles y responsabilidades, a cargo de las áreas de Gestión Administrativa, Gestión Documental, TIC y el Comité Institucional de Gestión y Desempeño.
- Publicación y socialización interna obligatoria, garantizando el conocimiento y apropiación por parte de todos los miembros de la organización.

9.3.2 Gestión de activos de información.


La gestión de activos busca garantizar el control, la protección y el uso adecuado de los recursos de información de la organización mediante:

- Inventario actualizado de activos (hardware, software, datos y procesos).
- Clasificación de la información según su nivel de sensibilidad y criticidad.
- Políticas de acceso fundamentadas en el principio de mínimo privilegio.

9.3.3 Gestión de riesgos de seguridad

La gestión de riesgos se orienta a identificar y mitigar amenazas que puedan comprometer la información institucional, a través de:

- Identificación, evaluación y tratamiento de riesgos TIC.
- Integración con la matriz de riesgos institucional.
- Revisión anual o cada vez que ocurra un cambio significativo en procesos, sistemas o normatividad.

 <p>Gestión Administrativa, Documental y TIC Dirección Administrativa</p>	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

9.3.4 Controles técnicos y administrativos (ISO 27002:2022).

Se implementan controles de seguridad en línea con la norma ISO/IEC 27002:2022, que incluyen:

- Autenticación multifactor (MFA).
- Gestión de identidades y accesos (IAM).
- Segmentación de red y uso de firewalls de próxima generación.
- Cifrado de datos en tránsito y en reposo.
- Respaldo automatizado con pruebas periódicas de restauración.
- Seguridad física y ambiental en centros de datos.

9.3.5 Gestión de incidentes de seguridad.

Se establece un marco para prevenir, detectar y responder a incidentes de seguridad, mediante:

- Plan de Respuesta a Incidentes, interno o tercerizado.
- Registro, clasificación y análisis de incidentes.
- Procedimientos de comunicación interna y externa.
- Ejercicios de simulación y procesos de mejora continua.

9.3.6 Concienciación y capacitación.


La cultura de seguridad se fortalece a través de:

- Programas periódicos de formación en seguridad digital.
- Campañas de phishing simulado para medir vulnerabilidad.
- Políticas de uso aceptable de los recursos TIC.

9.3.7 Continuidad del negocio y recuperación ante desastres.

La organización garantizará la disponibilidad de los servicios críticos mediante la implementación de estrategias de continuidad y recuperación, que incluyen:

- Integración con el Plan de Continuidad del Negocio (BCP) y el Plan de Recuperación ante Desastres (DRP).
- Definición de objetivos de recuperación: RTO (Recovery Time Objective) y RPO (Recovery Point Objective), alineados con la criticidad de los procesos.

 <p>Gestión Administrativa, Documental y TIC Dirección Administrativa</p>	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

- Ejecución de pruebas anuales de restauración y recuperación de servicios críticos, con registro de resultados y aplicación de mejoras.

9.4 Indicadores de Seguridad de la Información (KPIs)


La efectividad de la estrategia de seguridad será medida a través de indicadores clave de desempeño, entre los que se destacan:

- % de incidentes críticos gestionados.
- % de cumplimiento de controles ISO 27001:2022, verificado en auditorías internas.
- % de funcionarios y contratistas capacitados en seguridad de la información.
- % de sistemas críticos con respaldos verificados de manera exitosa.

9.5 Gobernanza y Seguimiento.

La gobernanza del Sistema de Gestión de Seguridad de la Información (SGSI) se fundamentará en:

- Responsable: La Oficina de Planeación será la encargada del seguimiento, monitoreo y consolidación de los avances del SGSI, en cumplimiento del Manual de Funciones y del Modelo Integrado de Planeación y Gestión (MIPG).
- El Área TIC y el Área de Talento Humano brindarán apoyo operativo y técnico en las actividades relacionadas con seguridad de la información, formación y gestión del cambio.
- Seguimiento trimestral: La Oficina de Planeación realizará seguimiento trimestral al avance del SGSI y presentará los informes correspondientes al Comité Institucional de Gestión y Desempeño (CIGD) para la toma de decisiones.
- Publicación de resultados: Se elaborarán informes trimestrales y semestrales para el Comité Institucional, acompañados de la publicación de resultados relevantes en el portal institucional, en cumplimiento de la política de Gobierno Abierto.
- Auditorías anuales: Se efectuarán auditorías anuales de cumplimiento ISO 27001 -2022, reforzadas con revisiones de los entes de control cuando sea necesario.

 <p>Gestión Administrativa, Documental y TIC Dirección Administrativa</p>	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

10 PLAN DE CONTINUIDAD DEL NEGOCIO (PCN) EN TI.

El Plan de Continuidad del Negocio (PCN) de la EDRU E.I.C.E tiene como propósito garantizar la resiliencia institucional y la capacidad de la entidad para asegurar la operación de sus servicios críticos frente a interrupciones, desastres o incidentes de seguridad de la información.

Este plan se encuentra alineado con la Política de Seguridad de la Información, el PETI y la norma ISO 22301:2019, integrando tanto la dimensión organizacional como la tecnológica, y asegurando la preparación, respuesta y recuperación efectiva ante contingencias.

10.1 Objetivos del PCN


El Plan de Continuidad del Negocio (PCN) en Tecnologías de la Información tiene como objetivos principales:

- Garantizar la disponibilidad y recuperación oportuna de los servicios TIC críticos de la EDRU E.I.C.E, minimizando el impacto de interrupciones o desastres.
- Establecer procedimientos claros y estandarizados para la respuesta, recuperación y restablecimiento de los servicios tecnológicos.
- Asegurar el cumplimiento de la normatividad nacional vigente en materia de seguridad de la información y continuidad del negocio, incluyendo los lineamientos del MinTIC, la Ley 1712 de 2014 (Transparencia) y la Ley 1581 de 2012 (Protección de Datos Personales).

10.2 Alcance

El Plan de Continuidad del Negocio (PCN) aplica a los siguientes componentes:

- Procesos misionales y de soporte que dependen de los servicios TIC.
- Activos tecnológicos críticos, incluyendo servidores, aplicaciones, bases de datos y redes.

	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

- Instalaciones físicas y personal clave de la entidad.
- Proveedores estratégicos de servicios tecnológicos, cuyo funcionamiento es esencial para la operación institucional.

10.3 Metodología.

El Plan de Continuidad del Negocio (PCN) se desarrolla bajo el enfoque del ciclo PHVA (Planear, Hacer, Verificar, Actuar), siguiendo los lineamientos de las normas ISO 22301:2019 e ISO 27031:2025, e incluye las siguientes fases:

10.3.1 Análisis de Impacto al Negocio (BIA)

- Identificación y clasificación de los procesos críticos de la organización.
- Priorización de funciones esenciales según su impacto operativo y estratégico.

10.3.2 Evaluación de Riesgos de Continuidad

- Identificación de amenazas relevantes: desastres naturales, fallas técnicas, ciberataques y errores humanos.
- Análisis de vulnerabilidades y definición de escenarios potenciales de interrupción.

10.3.3 Estrategias de Continuidad y Recuperación


- Implementación de infraestructura tecnológica redundante.
- Automatización de respaldos y replicación de datos en entornos de nube.
- Diseño de mecanismos que aseguren la rápida recuperación de servicios esenciales.

10.3.4 Planes de Respuesta y Procedimientos

- Plan de Respuesta a Incidentes de Seguridad de la Información.
- Plan de Recuperación ante Desastres (DRP).
- Procedimientos de comunicación interna y externa en situaciones de crisis.

10.3.5 Pruebas, Ejercicios y Simulaciones

- Ejecución periódica de pruebas y simulaciones de recuperación de sistemas críticos.
- Registro y análisis de resultados, incorporando lecciones aprendidas.
- Implementación de mejoras continuas en los procedimientos de continuidad.

 <p>Gestión Administrativa, Documental y TIC Dirección Administrativa</p>	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

10.4 Estrategias Tecnológicas de Resiliencia.

- Migración progresiva hacia una infraestructura híbrida (on-premise + nube).
- Implementación de soluciones de alta disponibilidad (HA) y balanceo de carga.
- Uso de herramientas de monitoreo 24/7 para la detección y respuesta temprana ante incidentes.
- Garantía de redundancia en comunicaciones y suministro eléctrico (UPS, plantas de energía).
- Respaldo de información cifrada y replicada en múltiples ubicaciones seguras.

10.5 Roles y Responsabilidades.

Comité Institucional de Gestión y Desempeño (CIGD):

Responsable de aprobar, supervisar y coordinar la implementación del PCN, asegurando su alineación con los objetivos estratégicos y misionales de la entidad.

Área de Tecnologías de la Información (TI):


Encargada de ejecutar el Plan de Recuperación ante Desastres (DRP), garantizar la disponibilidad y seguridad de la infraestructura tecnológica, así como mantener la continuidad operativa de los sistemas críticos.

Gestores de procesos:

Responsables de activar y aplicar los procedimientos de continuidad en sus áreas, asegurando la protección y restablecimiento oportuno de los procesos misionales y de soporte.

Oficina de Comunicaciones:

Encargada de diseñar, coordinar y ejecutar la estrategia de comunicación institucional durante situaciones de crisis, asegurando la difusión de información clara, precisa, oportuna y coherente tanto a nivel interno como externo.

 <p>Gestión Administrativa, Documental y TIC Dirección Administrativa</p>	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

10.6 Indicadores de Desempeño (KPIs).

Los siguientes indicadores permitirán evaluar el desempeño del Plan de Continuidad y Gestión de Respaldo.

Cada indicador contará con su Ficha Técnica, definida según los lineamientos del DAFP y del Modelo Integrado de Planeación y Gestión (MIPG), incluyendo: objetivo, fórmula, variables, línea base, meta, fuente de verificación, periodicidad y responsable, para ello se utilizará el formato FOR-GAC-08 FICHA TÉCNICA PARA FORMULACIÓN DE INDICADORES.


Indicadores definidos:

- Porcentaje de pruebas de respaldo y restauración exitosas.
- Tiempo promedio de recuperación ante incidentes críticos.
- Porcentaje de funcionarios clave capacitados en el PCN.
- Nivel de cumplimiento de las auditorías internas y externas.

10.7 Gobernanza y Seguimiento.

La gobernanza del Plan de Continuidad del Negocio (PCN) se fundamentará en los siguientes lineamientos:

- Responsable: La Oficina de Planeación será la dependencia encargada del seguimiento, monitoreo y consolidación de los avances del PCN, en cumplimiento del Manual de Funciones institucional, del MIPG y de los lineamientos del DAFP.
- La Oficina TIC y las demás áreas involucradas brindarán apoyo operativo y técnico en la ejecución, mantenimiento y actualización del PCN.
- Revisión del PCN: El PCN será revisado y actualizado de manera anual, o antes, en caso de presentarse cambios significativos en procesos, riesgos o estructura organizacional. Su gestión estará articulada con la Matriz de Riesgos TIC y el Mapa de Riesgos Institucional, garantizando coherencia en la administración del riesgo.

	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

- Auditorías de verificación: La efectividad del plan será evaluada mediante auditorías internas y externas, así como revisiones de control interno y verificación del cumplimiento de las acciones del plan.
- Seguimiento trimestral: La Oficina de Planeación presentará informes trimestrales al Comité Institucional de Gestión y Desempeño (CIGD), incluyendo el estado de avances, brechas identificadas y acciones correctivas.
- Transparencia y publicación: Se presentarán informes semestrales y se publicarán los avances relevantes en el portal web institucional, en cumplimiento de los lineamientos de Gobierno Abierto

11 ESTRATEGIA DE FINANCIAMIENTO Y SOSTENIBILIDAD

La Estrategia de Financiamiento y Sostenibilidad tiene como propósito garantizar que la implementación y el mantenimiento del PETI de la EDRU E.I.C.E sean financieramente viables en el corto, mediano y largo plazo. Con ello se busca prevenir la obsolescencia tecnológica y asegurar la continuidad y calidad de los servicios digitales.


Este enfoque se apoya en tres pilares fundamentales:

- ✓ Planeación financiera estratégica.
- ✓ Optimización del gasto en TIC.
- ✓ Diversificación de fuentes de financiamiento.

11.1 Planeación Financiera TIC.

La planeación financiera del PETI se estructura en dos categorías principales:

- **CAPEX (Gastos de Capital): Adquisición de hardware, software y licencias.**
 - ✓ Implementación de infraestructura tecnológica crítica.
 - ✓ Ejecución de proyectos de transformación digital de alto impacto.

	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

- **OPEX (Gastos Operativos):**
 - ✓ Servicios en la nube (SaaS, IaaS).
 - ✓ Contratos de soporte, mantenimiento y actualizaciones.
 - ✓ Capacitación, gestión del cambio y auditorías externas.
 - ✓ Servicios especializados de ciberseguridad.

11.2 Fuentes de Financiamiento

La financiación del PETI se soporta en las siguientes fuentes:

- Presupuesto interno de la EDRU: Recursos propios asignados anualmente para el funcionamiento y fortalecimiento de la infraestructura tecnológica, la operación de servicios TIC y la ejecución de proyectos estratégicos.

Teniendo en cuenta que algunos valores dependen del ciclo presupuestal vigente, el PETI incorporará la información cuantitativa en los siguientes documentos:


- PLAN ANUAL DE ADQUISICIONES 2026
- PLAN DE ACCION INSTITUCIONAL 2026

Enlace de referencia: <https://edru.gov.co/transparencia/planeacion-estrategica/>

11.3 Sostenibilidad Financiera.

La sostenibilidad financiera busca garantizar la continuidad de las tecnologías en el mediano y largo plazo, evitando la dependencia exclusiva de una única fuente de financiación o de recursos coyunturales.

Se propone integrar el PETI en el marco de la planeación financiera institucional, con el objetivo de asegurar recursos estables, suficientes y sostenibles para el cumplimiento de sus metas.

 <p>Gestión Administrativa, Documental y TIC Dirección Administrativa</p>	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

Resultado esperado: Garantizar la ejecución permanente de los objetivos del PETI, fortaleciendo la capacidad tecnológica y la innovación de la entidad.

11.4 Indicadores Financieros.

- Porcentaje de ejecución presupuestal TIC frente al plan anual.

11.5 Gobernanza Financiera.

- Integración del presupuesto TIC con el Plan Financiero Institucional.
- Revisiones trimestrales de ejecución presupuestal.
- Transparencia en la gestión de recursos, con publicación de informes en el portal de Gobierno Abierto.


12 INDICADORES DE DESEMPEÑO (KPIs) Y SEGUIMIENTO

El cumplimiento y la efectividad del PETI de la EDRU E.I.C.E., requieren un sistema integral de monitoreo, seguimiento y evaluación continua, que permita a la Oficina de Planeación y a los órganos de control:

- Verificar los avances.
- Medir resultados.
- Identificar desviaciones.
- Tomar decisiones oportunas para la mejora continua.

Para ello se definen Indicadores Clave de Desempeño (KPIs), organizados en dimensiones estratégicas alineadas con los objetivos institucionales y el PETI.

12.1 Dimensiones de Medición.

 <p>Gestión Administrativa, Documental y TIC Dirección Administrativa</p>	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

- **Gobernanza TIC:** Garantizar que las Tecnologías de la Información estén alineadas con la estrategia institucional.
- **Seguridad de la Información:** Evaluar la eficacia de los controles implementados en el SGSI.
- **Gestión de Proyectos TIC:** Medir el cumplimiento en términos de tiempo, costo, alcance y calidad.
- **Capacitación y Cultura Digital:** Evaluar la apropiación tecnológica por parte de funcionarios y contratistas.

12.2 Indicadores Estratégicos (KPIs).

12.2.1 Gobernanza TIC.

- Porcentaje de iniciativas del PETI alineadas con el Plan Estratégico Institucional.
- Nivel de madurez en Gobierno Digital (según autoevaluación MinTIC).

12.2.2 Seguridad de la información.

- Porcentaje de cumplimiento en auditorías ISO 27001.
- Porcentaje de incidentes críticos de seguridad gestionados dentro del tiempo definido (SLA).

12.2.3 Gestión de proyectos TIC.


- Nivel de satisfacción de usuarios internos con nuevos sistemas.

12.2.4 Capacitación y cultura digital.

- Porcentaje de funcionarios capacitados en competencias digitales.
- Nivel de adopción de nuevas herramientas digitales (% de uso efectivo).

12.3 Herramientas de seguimiento.

- **Tablero de Control (Dashboard PETI):** Monitoreo en tiempo real de los KPIs mediante herramientas de Business Intelligence.
- **Informes Trimestrales de Avance:** Consolidación de indicadores y logros alcanzados.

	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

- Evaluaciones Anuales de Madurez Digital: Según los lineamientos de la Guía MinTIC de Gobierno Digital.
- Auditorías Internas y Externas: Verificación del cumplimiento de la norma ISO 27001 y demás estándares aplicables.


12.4 Gobernanza del Seguimiento.

- Los indicadores serán reportados trimestralmente a la Oficina de Planeación.
- Los resultados relevantes se publicarán en el portal institucional, garantizando transparencia bajo el enfoque de Gobierno Abierto.
- Los KPIs serán revisados y ajustados anualmente para mantener su pertinencia y efectividad.

13 CONCLUSIONES Y RECOMENDACIONES

13.1 Conclusiones.


- El Plan Estratégico de Tecnologías de la Información (PETI) de la EDRU E.I.C.E., se consolida como una herramienta estratégica y transversal, orientada a garantizar la alineación de las TIC con la misión institucional, los objetivos de desarrollo y las políticas públicas de Gobierno Digital.
- La actualización periódica del plan permite a la entidad avanzar hacia un estado de madurez tecnológica progresiva, fortaleciendo la eficiencia operativa, la calidad en la prestación de los servicios y la transparencia frente a la ciudadanía.
- La adopción de estándares internacionales como ISO/IEC 27001, ISO 22301, ISO 27005 y COBIT, junto con los lineamientos del MinTIC, proporciona un marco integral de gobernanza, seguridad de la información y gestión de riesgos.

	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

- La implementación de mecanismos de seguimiento y medición mediante KPIs estratégicos facilita la evaluación continua del progreso, asegurando la mejora permanente y la trazabilidad de los logros alcanzados.
- Finalmente, el énfasis en la cultura organizacional y en la gestión del cambio fortalece el compromiso de los funcionarios y contratistas con la transformación digital, garantizando que la tecnología sea utilizada de manera adecuada, segura y centrada en el cumplimiento normativo.


13.2 Recomendaciones.

- Fortalecer la infraestructura tecnológica mediante un enfoque en servicios en la nube híbrida, esquemas de alta disponibilidad y redundancia, asegurando la continuidad de los servicios críticos de la entidad.
- Consolidar el modelo de Gobierno Digital, promoviendo la apertura y aprovechamiento de datos institucionales como herramienta de transparencia, innovación y valor público.
- Implementar un programa de capacitación continua en competencias digitales y seguridad de la información, dirigido a todos los niveles de la entidad, para fomentar la apropiación tecnológica y la cultura digital.
- Mantener la revisión y actualización periódica del PETI, al menos cada dos años, integrando las lecciones aprendidas de auditorías, la evolución tecnológica y los cambios en el marco regulatorio.
- Esta revisión será coordinada por la Oficina de Planeación en articulación con la Oficina TIC y el Comité Institucional de Gestión y Desempeño (CIGD), en cumplimiento del MIPG y los lineamientos del DAFP.


	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

14 CRONOGRAMA DE ACTIVIDADES - PETI


Actividad	Fecha de inicio	Fecha fin	Responsable	Tipo de actividad	Meta	Documentos / Evidencias esperadas
Levantamiento de información TIC y SGSI	Enero	Marzo	Gestión Administrativa, Documental y TIC.	Diagnóstico.	Identificar el estado actual.	Informe de diagnóstico inicial, inventario de sistemas.
Evaluación de cumplimiento normativo (ISO 27001, MinTIC, Ley 1581, Ley 1712)	Enero	Marzo	Oficina Jurídica / Gestión Administrativa, Documental y TIC.	Diagnóstico.	Establecer línea base normativa.	Matriz de cumplimiento normativo.
Análisis de brechas de seguridad de la información.	Enero	Febrero	Gestión Administrativa, Documental y TIC.	Diagnóstico.	Identificar brechas frente a ISO 27001.	Informe de brechas y plan preliminar.
Redacción y aprobación del PETI actualizado	Enero.	Enero.	Dirección Administrativa / Gestión Administrativa, Documental y TIC.	Planeación estratégica.	Aprobación del PETI v3.	Documento PETI aprobado y acta de comité.
Definición de objetivos estratégicos TIC y KPIs.	Enero	Febrero.	Gestión Administrativa, Documental y TIC.	Planeación estratégica.	Establecer metas claras y medibles.	Tablero de indicadores definido.
Actualización de políticas TIC (seguridad, uso aceptable, protección de datos).	Febrero.	Febrero.	Oficina Jurídica / Gestión Administrativa, Documental y TIC.	Normativa.	Políticas aprobadas y socializadas.	Políticas actualizadas y divulgadas.
Clasificación e inventario de activos de información.	Febrero	Marzo	Gestión Administrativa, Documental y TIC.	Implementación.	Inventario con clasificación por criticidad.	Matriz de activos clasificados.

	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

Actividad	Fecha de inicio	Fecha fin	Responsable	Tipo de actividad	Meta	Documentos / Evidencias esperadas
Desarrollo de la Matriz de Riesgos TIC y plan de tratamiento.	Febrero	Marzo	Gestión Administrativa, Documental y TIC.	Implementación.	Riesgos identificados y tratados.	Matriz de riesgos TIC + plan de tratamiento.
Capacitación en Seguridad de la Información (ISO 27001, phishing, datos).	Marzo	Diciembre	Gestión Administrativa, Documental y TIC.	Capacitación.	Funcionarios capacitados.	Listas de asistencia, material de capacitación.
Implementación de controles técnicos (MFA, cifrado, SIEM, respaldos).	Marzo	Mayo	Gestión Administrativa, Documental y TIC.	Implementación.	Controles de seguridad aplicados.	Reportes técnicos, evidencias de configuración.
Integración con PAAC y Estrategia de Gobierno Digital.	Marzo	Junio	Gestión Administrativa, Documental y TIC.	Articulación.	Alineación con política pública.	Informe de integración y actas.
Implementación del tablero de control de KPIs.	Abril	Abril	Gestión Administrativa, Documental y TIC.	Seguimiento.	Tablero activo y actualizado.	Dashboard en Excel/Power BI.
Auditoría interna del PETI y SGSI.	Junio	Junio	Oficina de planeación.	Auditoría.	Evaluar cumplimiento.	Informe de auditoría interna.

	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

Actividad	Fecha de inicio	Fecha fin	Responsable	Tipo de actividad	Meta	Documentos / Evidencias esperadas
Revisión por la Dirección (ajustes y mejoras).	Julio	Julio.	Dirección Administrativa / Gestión Administrativa, Documental y TIC.	Revisión.	PETI actualizado.	Acta de revisión por la dirección.
Actualización anual del PETI.	Cuando se requiera	Cuando se requiera	Dirección Administrativa / Gestión Administrativa, Documental y TIC.	Mejora continua.	PETI ajustado a cambios.	Documento PETI actualizado, acta de comité.

	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

15 ANEXOS

Los anexos constituyen un complemento esencial del Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETI), al aportar herramientas prácticas y evidencias documentales que fortalecen su implementación, seguimiento y auditoría.

- **Matriz de Riesgos TIC**

FOR-GDO-03-01 MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

- **Inventario de Activos de TI.**

Se registrará en el formato FOR-GDO-03-06 PLANILLA DE INVENTARIO DE ACTIVOS DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - TIC., matriz oficial de Inventario de Activos TIC, que incluirá hardware, software, licencias, servicios tecnológicos, recursos en la nube y activos de información.

Esta matriz permitirá mantener actualizada la información conforme a los lineamientos de ISO/IEC 27001:2022 (control A.5.9 – Inventario de Activos) y la política de Seguridad y Privacidad de la Información.


El inventario se actualizará trimestralmente por la Oficina TIC y será validado por la Oficina de Planeación y Control Interno.

Inventario actualizado de hardware, software, licencias y servicios contratados.

- **Fichas de Proyectos TIC (Modelo).**

Cada iniciativa o proyecto TIC deberá documentarse mediante el formato FOR-GDO-03-04 FICHA TÉCNICA DE PROYECTOS TIC., codificada en el Sistema Integrado de Gestión Documental (SGI), de acuerdo con los lineamientos de Gobierno Digital y la Oficina de Planeación.

✓ La ficha incluirá como mínimo:

 <p>Gestión Administrativa, Documental y TIC Dirección Administrativa</p>	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

- ✓ Nombre del proyecto
- ✓ Código del documento
- ✓ Objetivo
- ✓ Alcance
- ✓ Responsable
- ✓ Duración
- ✓ Costos estimados
- ✓ Fuente de financiación
- ✓ Riesgos asociados
- ✓ Indicadores (KPIs)
- ✓ Relación con objetivos del PETI
- ✓ Dependencias involucradas
- ✓ Estado del proyecto


- **Matriz de Indicadores de Desempeño (KPIs).**

La Entidad contará con un tablero de control en formato Excel, adoptado como anexo oficial del PETI, que consolida todos los indicadores definidos para el seguimiento y evaluación del plan. Este tablero incluirá: nombre del indicador, objetivo, fórmula de cálculo, línea base, meta, responsable, frecuencia de medición, fuente de información y estado de cumplimiento. FOR-GDO-03-07 MATRIZ INTEGRAL DE INDICADORES DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES.

El tablero será actualizado periódicamente para garantizar la trazabilidad, medición continua del desempeño institucional y cumplimiento de los lineamientos establecidos por Gobierno Digital, MIPG y la gestión por resultados.

15.1 Normatividad Aplicable.

- ISO/IEC 27001:2022 – Seguridad de la Información.
- Ley 1581 de 2012 – Protección de Datos Personales.
- Ley 1712 de 2014 – Transparencia y Acceso a la Información Pública.

	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

- Política de Gobierno Digital (Decreto 1008 de 2018 y Resolución MinTIC 1519 de 2020).
- Plan Anticorrupción y de Atención al Ciudadano (PAAC).

15.2 Formatos y Plantillas.

La Entidad contará con los siguientes formatos, los cuales han sido desarrollados y adoptados conforme al Sistema de Gestión Integrado:

Formato FOR-GDO-03-07 MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN


Formato FOR-GDO-03-05 MATRIZ PLAN DE TRABAJO DE RIESGOS DE TECNOLOGÍAS DE LA INFORMACION Y LAS COMUNICACIONES - TIC. Documento independiente que detalla acciones, responsables y fechas de tratamiento según ISO/IEC 27005.

Formato FOR-GDO-03-02 SEGUIMIENTO Y EVALUACIÓN DE RIESGOS. Documento independiente destinado al registro y seguimiento de incidentes de seguridad, articulado con el SGSI.


Los tres formatos serán anexados oficialmente al PETI como parte del paquete de documentos de soporte.

16 TÉRMINOS Y DEFINICIONES

- Activo de Información: Recurso de la organización que contiene, procesa o transmite datos y que requiere protección (ejemplo: bases de datos, aplicaciones, equipos).
- Alta Disponibilidad (HA): Capacidad de un sistema para mantenerse operativo con mínimas interrupciones gracias a redundancia de infraestructura.

 <p>Gestión Administrativa, Documental y TIC Dirección Administrativa</p>	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

- Autenticación Multifactor (MFA): Mecanismo de seguridad que requiere más de un método de validación (ej. contraseña + token).
- Backup (Copia de Seguridad): Procedimiento de duplicar información con el fin de recuperarla en caso de pérdida o desastre.
- CAPEX (Capital Expenditure): Inversión de capital en infraestructura y equipos TIC.
- Ciberseguridad: Conjunto de medidas y controles para proteger sistemas y datos frente a ataques digitales.
- Cloud Computing (Computación en la Nube): Modelo de prestación de servicios TIC a través de internet, en modalidad SaaS o IaaS.
- Confidencialidad: Principio de seguridad que asegura que la información solo sea accesible por personal autorizado.
- Disponibilidad: Principio de seguridad que garantiza el acceso oportuno y confiable a la información y sistemas.
- DRP (Disaster Recovery Plan): Plan de recuperación de infraestructura tecnológica tras un desastre.
- Gobierno Digital: Estrategia MinTIC para modernizar el Estado a través de TIC, promoviendo servicios ciudadanos digitales, interoperabilidad y apertura de datos.
- Indicador Clave de Desempeño (KPI): Métrica utilizada para medir el logro de objetivos estratégicos.
- Integridad: Principio de seguridad que asegura que la información no sea alterada de forma no autorizada.

 <p>Gestión Administrativa, Documental y TIC Dirección Administrativa</p>	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

- ISO 27001:2022: Norma internacional para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI).
- Mapa de Actores: Herramienta que identifica a los participantes internos y externos que intervienen en la ejecución del PETI.
- MinTIC: Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.
- OPEX (Operational Expenditure): Gastos operativos recurrentes para mantener servicios TIC (soporte, nube, licencias).
- PETI: Plan Estratégico de Tecnologías de la Información y las Comunicaciones. Documento que alinea la estrategia tecnológica con los objetivos institucionales.
- Plan Anticorrupción y de Atención al Ciudadano (PAAC): Instrumento de política pública en Colombia que busca prevenir riesgos de corrupción y mejorar la atención al ciudadano.
- RPO (Recovery Point Objective): Punto de recuperación aceptable en términos de pérdida de datos.
- RTO (Recovery Time Objective): Tiempo máximo permitido para recuperar un proceso o sistema tras una interrupción.
- SGSI (Sistema de Gestión de Seguridad de la Información): Conjunto de políticas, procedimientos y controles para proteger la información bajo ISO 27001.
- Transformación Digital: Proceso de integración de tecnología en procesos institucionales para mejorar eficiencia y servicio al ciudadano.

 <p>Gestión Administrativa, Documental y TIC Dirección Administrativa</p>	SISTEMA DE GESTIÓN INTEGRADO	Código: PLI-GDO-03-01
		Versión: 3
	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - PETI	Fecha de entrada en vigencia: 30-ene-2026

17 CONTROL DE CAMBIOS

FICHA CONTROL DE CAMBIOS		
Versión	Fecha	Descripción de la Modificación
1	31-ene-2025	Versión inicial. Aprobado a través del acta de Comité Institucional de Gestión y Desempeño No. 10.1.2.001-2025 del 31 de enero de 2025. Resolución de adopción No. 10.15-014-2025 del 31 de enero de 2025
2	10-dic-2025	Actualización del contenido del documento para dar cumplimiento al plan de mejoramiento establecido por la Oficina de Control Interno. Aprobado a través de acta de Comité Institucional de Gestión y Desempeño No. 10.1.2.007-2025 del 5 de diciembre de 2025. Resolución de adopción No. 10.15-115-2025 del 10 de diciembre de 2025
3	30-ene-2026	Revisión y actualización del documento, aprobado a través del acta de Comité Institucional de Gestión y Desempeño No. 10.1.2.001-2026 del 29 de enero de 2026. Resolución de adopción No. 10.15-013-2026 del 29 de enero de 2026.

Elaborado por:	Revisado por:	Comité Institucional de Gestión y Desempeño		Resolución de Adopción	
Diana Marcela Orozco Jaramillo Contratista – TIC Dirección Administrativa	-Sandra Idalí Arévalo Peña – Director Administrativo -Julián Eduardo Gómez Alarcón – Contratista – Planes Institucionales – Oficina de Planeación -Adriana Millán Azcárate -Contratista - Aseguramiento de la Calidad – Oficina de Planeación. -Jorge Andrés Martínez Zambrano - Jefe Oficina de Planeación	No Acta. 10.1.2.001-2026	Fecha: 29-ene-2026	No.: 10.15-013-2026	Fecha de expedición: 30-ene-2026