PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN (PETI)

Vigencia 2026

Calle 24 #51-40, Bogotá
Capital Tower- Piso 7 y 11
Tel: **601 580 16 72** - Código Postal: 111321
Contactenos@epc.com.co
www.epc.com.co
@EPCUNDI

TABLA DE CONTENIDO

1. Introducción

El Plan Estratégico de Tecnologías de la Información para la vigencia constituye el instrumento de planeación que orienta la gestión, uso y fortalecimiento de las Tecnologías de la Información como habilitador estratégico del cumplimiento de los objetivos institucionales, la prestación eficiente de los servicios públicos y la modernización de la gestión administrativa.

El presente PETI se formula en cumplimiento de lo dispuesto en el Decreto 612 de 2018, el cual establece la integración de los planes institucionales y estratégicos al Modelo Integrado de Planeación y Gestión (MIPG), y define el Plan Estratégico de Tecnologías de la Información como un componente obligatorio de la planeación institucional, articulado con el Plan Estratégico Institucional y los lineamientos de la Política de Gobierno Digital.

El documento adopta los lineamientos vigentes del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) en materia de Gobierno Digital, seguridad digital, interoperabilidad y servicios ciudadanos digitales, así como los principios definidos por el Departamento Administrativo de la Función Pública (DAFP) para la gestión pública orientada a resultados, la transparencia y el control.

El PETI se estructura bajo un enfoque realista y verificable, acorde con el nivel de madurez tecnológica de la entidad, priorizando la sostenibilidad operativa, la seguridad de la información, la continuidad de los servicios y la correcta articulación con los procesos misionales, estratégicos y de apoyo de Empresas Públicas de Cundinamarca S.A E.S.P, en este sentido, el plan no se limita a la incorporación de herramientas tecnológicas, sino que consolida un modelo de gobernanza de TI alineado con la planeación institucional y el Sistema Integrado de Gestión.

De acuerdo con el organigrama institucional vigente, el Proceso de Tecnologías de la Información se encuentra adscrito a la Dirección de Planeación, lo que refuerza su rol como proceso de apoyo estratégico y transversal, responsable de habilitar y soportar la toma de decisiones, la gestión documental, la transparencia, la seguridad digital y la continuidad institucional, articulando de manera directa con el Plan Estratégico de Seguridad y Privacidad de la Información (PESI), el Modelo de Seguridad y Privacidad de la Información (MSPI), el Plan de Continuidad del Negocio (PCN) y el Plan de Recuperación Tecnológica (DRP), garantizando que las iniciativas tecnológicas se desarrollen bajo criterios de gestión del riesgo, protección de la información y cumplimiento normativo.

Este plan se concibe como un documento dinámico, sujeto a seguimiento, evaluación y actualización periódica, que permite a la entidad responder de manera oportuna a los cambios normativos, tecnológicos y organizacionales, y que sirve como insumo fundamental para los procesos de auditoría, Control Interno y reporte de avances en el marco del MIPG y el FURAG.

2. Marco Normativo y de Referencia

El Plan Estratégico de Tecnologías de la Información se fundamenta en el marco normativo colombiano vigente, en los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), y en estándares internacionales de buenas prácticas en gestión de tecnologías de la información, seguridad digital y continuidad del negocio.

Este marco normativo garantiza que la planeación, gestión y control de las Tecnologías de la Información se desarrollen en coherencia con el Modelo Integrado de Planeación y Gestión (MIPG), la Política de Gobierno Digital y los principios de eficiencia, transparencia, seguridad y mejora continua exigidos a las entidades públicas.

2.1 Normatividad nacional aplicable

- Decreto 612 de 2018: establece la integración de los planes institucionales y estratégicos al MIPG, definiendo el Plan Estratégico de Tecnologías de la Información como un instrumento obligatorio de planeación, articulado con el Plan Estratégico Institucional y sujeto a seguimiento y evaluación.
- Decreto 338 de 2022: adopta la Política de Gobierno Digital y define los lineamientos para la transformación digital del Estado, la interoperabilidad, la seguridad digital, la gestión de la información y la prestación de servicios ciudadanos digitales.
- Ley 1341 de 2009 y Ley 1978 de 2019: establecen los principios de la sociedad de la información y el marco general para el desarrollo del sector TIC en Colombia.
- Ley 1581 de 2012 y sus decretos reglamentarios: regulan la protección de datos personales, los derechos de los titulares y las obligaciones de los responsables y encargados del tratamiento de la información.
- Ley 1712 de 2014: desarrolla el derecho fundamental de acceso a la información pública, estableciendo obligaciones en materia de transparencia activa y pasiva.

- Ley 594 de 2000: Ley General de Archivos, que regula la gestión documental, la organización, conservación y disposición de los documentos institucionales, en concordancia con las Tablas de Retención Documental (TRD).
- Decreto 1083 de 2015 y normas concordantes: regulan el Modelo Integrado de Planeación y Gestión (MIPG), del cual hace parte la planeación estratégica de las Tecnologías de la Información.
- Decreto 2157 de 2017: establece disposiciones para la gestión de la continuidad del negocio en las entidades públicas, aplicable a la planeación de la continuidad y recuperación tecnológica.

2.2 Lineamientos y políticas institucionales y sectoriales

- El PETI se articula con los siguientes lineamientos y documentos de referencia:
- Política de Gobierno Digital – MinTIC, vigente.
- Lineamientos de Arquitectura Empresarial TIC del Estado.
- Lineamientos para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).
- Guías y orientaciones del Departamento Administrativo de la Función Pública (DAFP) en materia de planeación, control y evaluación.
- Plan Estratégico Institucional (PEI) vigente.
- Plan Estratégico de Seguridad y Privacidad de la Información (PESI).
- Modelo de Seguridad y Privacidad de la Información (MSPI).
- Plan de Continuidad del Negocio (PCN).
- Plan de Recuperación Tecnológica (DRP).
- Sistema Integrado de Gestión (SIG).
- Tablas de Retención Documental (TRD) institucionales.

2.3 Estándares y buenas prácticas de referencia

Para fortalecer la gestión de las Tecnologías de la Información y asegurar su alineación con estándares reconocidos, el PETI toma como referencia las siguientes normas internacionales, en la medida en que resultan aplicables al contexto y nivel de madurez de la entidad:

- ISO/IEC 27001:2022: Sistema de Gestión de Seguridad de la Información.
- ISO/IEC 27005: Gestión de riesgos de seguridad de la información.
- ISO/IEC 27031: Directrices para la preparación en continuidad y recuperación de tecnologías de la información.
- ISO 22301:2019: Sistema de Gestión de Continuidad del Negocio.

- ISO 31000:2018: Gestión del riesgo.
- Buenas prácticas de gobierno y gestión de TI aplicables al sector público.

El uso de estos referentes no implica la adopción automática de esquemas de certificación, sino la aplicación progresiva de buenas prácticas que contribuyan a fortalecer la gobernanza, la seguridad, la continuidad y la sostenibilidad de las Tecnologías de la Información en Empresas Públicas de Cundinamarca S.A E.S.P.

3. Glosario de Términos y Acrónimos

Arquitectura de TI: Estructura que define los componentes tecnológicos, de información y sistemas de información de la entidad, así como sus relaciones, con el fin de soportar los procesos institucionales y la estrategia organizacional.

Continuidad del Negocio (PCN): Conjunto de lineamientos y procedimientos orientados a garantizar la continuidad de los procesos críticos de la entidad ante eventos disruptivos que afecten la operación.

Control Interno: Sistema integrado de políticas, normas, métodos y procedimientos adoptados por la entidad para proporcionar una seguridad razonable sobre el logro de los objetivos institucionales.

DRP – Plan de Recuperación Tecnológica: Plan que establece las acciones, responsables y tiempos necesarios para restablecer los servicios tecnológicos y sistemas de información tras un incidente o interrupción.

FURAG – Formulario Único de Reporte de Avances de la Gestión: Herramienta mediante la cual las entidades públicas reportan el avance en la implementación del Modelo Integrado de Planeación y Gestión (MIPG).

Gobierno de TI: Conjunto de estructuras, procesos y mecanismos que permiten dirigir, evaluar y controlar el uso de las Tecnologías de la Información, asegurando su alineación con los objetivos institucionales.

Gestión de TI: Actividades operativas y administrativas orientadas a planear, implementar, operar y mantener los servicios y recursos tecnológicos de la entidad.

MDA – Mesa de Ayuda: Instancia encargada de brindar soporte técnico, registrar incidentes y atender requerimientos relacionados con los servicios tecnológicos institucionales.

MIPG – Modelo Integrado de Planeación y Gestión: Marco de referencia que integra los sistemas de planeación, gestión y control de las entidades públicas, orientado a generar valor público.

MSPI – Modelo de Seguridad y Privacidad de la Información: Conjunto de lineamientos definidos por MinTIC para la gestión de la seguridad y privacidad de la información en las entidades públicas.

PETI – Plan Estratégico de Tecnologías de la Información: Instrumento de planeación que define la estrategia, objetivos, iniciativas y acciones de Tecnologías de la Información alineadas con la planeación institucional.

PESI – Plan Estratégico de Seguridad y Privacidad de la Información: Documento que establece las estrategias, acciones y controles para proteger la información institucional y gestionar los riesgos asociados.

Seguridad Digital: Capacidad del Estado para proteger la información, los activos digitales y los servicios tecnológicos frente a riesgos y amenazas, garantizando la confidencialidad, integridad y disponibilidad.

Sistema de Información: Conjunto de componentes tecnológicos, datos, procesos y personas que permiten capturar, procesar, almacenar y distribuir información para apoyar la gestión institucional.

TI – Tecnologías de la Información: Conjunto de recursos tecnológicos utilizados para el procesamiento, almacenamiento, transmisión y gestión de la información.

TRD – Tablas de Retención Documental: Instrumento archivístico que define los tiempos de conservación y disposición final de los documentos producidos por la entidad.

Glosario MinTIC: https://www.mintic.gov.co/portal/inicio/Glosario/

4. Objetivo del Plan Estratégico de Tecnologías de la Información

El Plan Estratégico de Tecnologías de la Información tiene como objetivo orientar de manera estratégica la gestión, uso y fortalecimiento de las Tecnologías de la Información durante la vigencia 2026, asegurando su alineación con el Plan

Estratégico Institucional, el Modelo Integrado de Planeación y Gestión (MIPG) y los lineamientos de la Política de Gobierno Digital.

El PETI busca consolidar a las Tecnologías de la Información como un habilitador estratégico de la gestión institucional, contribuyendo a la eficiencia operativa, la seguridad de la información, la continuidad de los servicios, la transparencia y el cumplimiento de las obligaciones normativas aplicables a la entidad.

Así mismo, el plan tiene como propósito establecer un marco claro de gobernanza de TI, definiendo roles, responsabilidades y mecanismos de articulación institucional que permitan una adecuada planeación, ejecución, seguimiento y control de las iniciativas tecnológicas, en coherencia con la adscripción del Proceso de Tecnologías de la Información a la Dirección de Planeación.

El PETI orienta la priorización de iniciativas y proyectos tecnológicos bajo criterios de riesgo, sostenibilidad, viabilidad técnica y capacidad institucional, evitando la adopción de soluciones que no correspondan al nivel real de madurez tecnológica de Empresas Públicas de Cundinamarca S.A E.S.P, y garantizando que cada acción definida sea verificable, ejecutable y defendible ante procesos de auditoría, Control Interno y evaluación del desempeño institucional.

El objetivo del PETI es asegurar que las Tecnologías de la Información respalden de manera efectiva los procesos misionales, estratégicos y de apoyo de la entidad, fortaleciendo la seguridad digital, la gestión documental, la protección de los datos personales, la continuidad del negocio y la confianza de los ciudadanos en la gestión pública.

5. Alcance

El Plan Estratégico de Tecnologías de la Información define su alcance de manera institucional, transversal y realista, comprendiendo todos los procesos, áreas, funcionarios, contratistas y proveedores que intervienen en la planeación, adquisición, implementación, operación, uso y control de las Tecnologías de la Información durante la vigencia 2026, se extiende a los procesos estratégicos, misionales y de apoyo de la entidad, en coherencia con su adscripción a la Dirección de Planeación y su articulación con el Sistema Integrado de Gestión, el Modelo Integrado de Planeación y Gestión (MIPG) y la Política de Gobierno Digital.

Desde el punto de vista tecnológico, el PETI comprende:

- La infraestructura tecnológica institucional, incluyendo equipos de cómputo, servidores, redes de comunicaciones, servicios de conectividad, plataformas de almacenamiento, servicios en la nube de carácter básico y los elementos que soportan la operación diaria de la entidad.
- Los sistemas de información y aplicaciones que apoyan los procesos administrativos, financieros, contractuales, documentales, operativos y de atención al usuario, considerando únicamente aquellas soluciones que se encuentran efectivamente implementadas o en uso en la entidad.
- La gestión de la información institucional, abarcando su generación, procesamiento, almacenamiento, acceso, conservación y disposición final, en cumplimiento de la Ley 594 de 2000, las Tablas de Retención Documental (TRD) y la normativa vigente en materia de transparencia y acceso a la información pública.
- La seguridad digital y la protección de la información, integrando los lineamientos definidos en el Plan Estratégico de Seguridad y Privacidad de la Información (PESI), el Modelo de Seguridad y Privacidad de la Información (MSPI), la gestión de riesgos de TI y los planes de continuidad y recuperación tecnológica.
- La planeación y gestión de la contratación de bienes y servicios tecnológicos, incluyendo la definición de requerimientos técnicos, la incorporación de cláusulas de seguridad y continuidad, la supervisión técnica de los contratos y la evaluación del desempeño de los proveedores TIC.

El PETI no contempla el diseño ni la implementación de plataformas tecnológicas que no correspondan al nivel de madurez institucional ni a las capacidades reales de Empresas Públicas de Cundinamarca S.A E.S.P, tales como sistemas avanzados de relacionamiento con clientes u otras soluciones no existentes a la fecha, las iniciativas tecnológicas se priorizan bajo criterios de viabilidad, sostenibilidad, riesgo y alineación con los objetivos institucionales.

El alcance del PETI no sustituye los planes operativos anuales ni los procedimientos técnicos específicos, sino que establece el marco estratégico que orienta la toma de decisiones, la asignación de recursos y el seguimiento de la gestión de Tecnologías de la Información, sirviendo como insumo para los procesos de auditoría, Control Interno y reporte de avances en el marco del MIPG y el FURAG.

6. Contexto Estratégico Institucional

Empresas Públicas de Cundinamarca S.A. E.S.P., en su calidad de empresa prestadora de servicios públicos, desarrolla su gestión en un entorno que exige altos

niveles de eficiencia operativa, transparencia, control, seguridad de la información y continuidad en la prestación de los servicios, en este contexto, las Tecnologías de la Información se consolidan como un habilitador estratégico para el cumplimiento de los objetivos institucionales y la modernización de la gestión pública.

El Plan Estratégico de Tecnologías de la Información se formula en coherencia con el Plan Estratégico Institucional vigente y se integra al Modelo Integrado de Planeación y Gestión (MIPG), en cumplimiento de lo establecido en el Decreto 612 de 2018, esta articulación permite que la planeación tecnológica no se gestione de manera aislada, sino como parte del ciclo institucional de planeación, ejecución, seguimiento y mejora continua.

De acuerdo con el organigrama institucional vigente, el Proceso de Tecnologías de la Información se encuentra adscrito a la Dirección de Planeación, lo que posiciona a TI como un proceso de apoyo estratégico con responsabilidad transversal sobre todos los procesos de la entidad, esta ubicación fortalece el rol de TI en la toma de decisiones, la gestión del riesgo, la seguridad digital, la gestión documental, la transparencia y el soporte a los procesos misionales y administrativos.

El contexto estratégico del PETI también se encuentra determinado por los lineamientos de la Política de Gobierno Digital, que orienta a las entidades públicas hacia la transformación digital, la interoperabilidad, la protección de la información, el uso eficiente de los recursos tecnológicos y la prestación de servicios centrados en el ciudadano, en este sentido, Empresas Públicas de Cundinamarca S.A E.S.P orienta su planeación tecnológica a fortalecer capacidades institucionales reales, priorizando la estabilidad operativa, la seguridad de la información y la continuidad de los servicios, considerando como insumos estratégicos los resultados de auditorías internas, las evaluaciones de Control Interno, los compromisos derivados del MIPG y los reportes del Formulario Único de Reporte de Avances de la Gestión (FURAG), los cuales permiten identificar brechas, riesgos y oportunidades de mejora en la gestión de Tecnologías de la Información.

El contexto institucional reconoce, igualmente, la necesidad de articular la planeación tecnológica con los instrumentos específicos de seguridad y continuidad, tales como el Plan Estratégico de Seguridad y Privacidad de la Información (PESI), el Modelo de Seguridad y Privacidad de la Información (MSPI), el Plan de Continuidad del Negocio (PCN) y el Plan de Recuperación Tecnológica (DRP), garantizando que la transformación digital se desarrolle bajo criterios de control, resiliencia y cumplimiento normativo.

En este marco, el PETI se concibe como un instrumento estratégico que permite alinear las Tecnologías de la Información con la planeación institucional, fortalecer la gobernanza de TI, gestionar de manera adecuada los riesgos tecnológicos y apoyar el cumplimiento de los objetivos misionales de Empresas Públicas de Cundinamarca S.A E.S.P, asegurando una gestión pública eficiente, segura y orientada a resultados.

7. Alineación del PETI

El Plan Estratégico de Tecnologías de la Información se encuentra alineado de manera directa y estructural con el Plan Estratégico Institucional (PEI), el Modelo Integrado de Planeación y Gestión (MIPG) y el Decreto 612 de 2018, garantizando la integración de la planeación tecnológica al sistema institucional de planeación, seguimiento y control.

El Decreto 612 de 2018 establece que los planes estratégicos y operativos de las entidades públicas deben integrarse en un único marco de planeación institucional, articulado al MIPG, en este contexto, el PETI se constituye como el instrumento que orienta la gestión estratégica de las Tecnologías de la Información, asegurando que las decisiones tecnológicas respondan a los objetivos institucionales y a las prioridades definidas por la alta dirección.

La alineación con el Plan Estratégico Institucional se materializa mediante la identificación de iniciativas tecnológicas que soportan el cumplimiento de los objetivos estratégicos de Empresas Públicas de Cundinamarca S.A E.S.P, en especial aquellos relacionados con la eficiencia administrativa, la sostenibilidad operativa, la transparencia, la seguridad de la información y la mejora continua en la prestación de los servicios público, el PETI prioriza acciones que fortalecen los procesos misionales, estratégicos y de apoyo, evitando la adopción de soluciones tecnológicas desconectadas de las necesidades reales de la entidad.

Desde la perspectiva del Modelo Integrado de Planeación y Gestión (MIPG), el PETI contribuye de manera transversal a varias de sus dimensiones, en particular a las relacionadas con la gestión con valores para resultados, la planeación institucional, el control interno, la gestión del conocimiento, la innovación y la seguridad digital. La planeación tecnológica se integra así a los ciclos de planeación, ejecución, seguimiento y evaluación definidos por el MIPG.

La adscripción del Proceso de Tecnologías de la Información a la Dirección de Planeación fortalece esta alineación, al garantizar que la planeación tecnológica se articule directamente con los procesos de planeación estratégica, el Sistema Integrado de Gestión y los mecanismos de seguimiento institucional. Esta ubicación permite una mayor coherencia entre las prioridades institucionales y las iniciativas de TI, así como una adecuada trazabilidad de las decisiones tecnológicas.

El PETI se alinea con los lineamientos de la Política de Gobierno Digital, asegurando que las Tecnologías de la Información contribuyan a la transformación digital del Estado, la protección de la información, la interoperabilidad, el fortalecimiento de la transparencia y la mejora en la atención a los ciudadanos, dentro de un marco de control y cumplimiento normativo, esta alineación garantiza que el PETI no sea un documento aislado, sino un componente integral de la planeación institucional de Empresas Públicas de Cundinamarca S.A E.S.P, que facilita la rendición de cuentas, el seguimiento por parte de Control Interno y la evaluación de resultados en el marco del FURAG, fortaleciendo la gobernanza y la gestión estratégica de las Tecnologías de la Información.

8. Ubicación del Proceso de Tecnologías de la Información

El Proceso de Tecnologías de la Información (TI) en Empresas Públicas de Cundinamarca S.A. E.S.P. se encuentra adscrito directamente a la Dirección de Planeación, de conformidad con el organigrama institucional vigente, esta ubicación responde a la naturaleza estratégica y transversal de la gestión de Tecnologías de la Información dentro de la entidad.

La adscripción del Proceso TI a la Dirección de Planeación posiciona a las Tecnologías de la Información como un proceso de apoyo estratégico, responsable de habilitar la planeación institucional, la toma de decisiones, la gestión del conocimiento, la seguridad digital, la continuidad del negocio y el cumplimiento de los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG) y la Política de Gobierno Digital.

Desde esta ubicación organizacional, el Proceso TI articula de manera transversal con todos los procesos estratégicos, misionales y de apoyo de Empresas Públicas de Cundinamarca S.A E.S.P, brindando soporte tecnológico y asegurando que las soluciones implementadas se alineen con los objetivos institucionales, las capacidades reales de la entidad y las exigencias normativas vigentes.

El Proceso de Tecnologías de la Información mantiene una relación funcional y permanente con la Dirección de Control Interno, en lo relacionado con la gestión de riesgos tecnológicos, la implementación de controles, el seguimiento a los planes de mejoramiento y la atención de auditorías internas y externas. Así mismo, articula con la Dirección Jurídica y la Dirección de Gestión Contractual para asegurar que los procesos de adquisición y contratación de bienes y servicios tecnológicos incorporen criterios técnicos, de seguridad digital, continuidad y cumplimiento normativo.

El Proceso TI se articula con la Dirección de Finanzas, Presupuesto, Contabilidad y Tesorería para la planeación y ejecución de los recursos destinados a Tecnologías de la Información, garantizando la sostenibilidad financiera de las iniciativas tecnológicas y su alineación con el presupuesto institucional.

En el ámbito operativo y misional, el Proceso TI brinda soporte transversal a la Subgerencia General, la Subgerencia Técnica y Operativa y las Direcciones misionales, asegurando la disponibilidad, integridad y confidencialidad de la información que soporta la prestación de los servicios públicos y la gestión de proyectos institucionales.

Esta ubicación organizacional fortalece la gobernanza de las Tecnologías de la Información, permite una mayor coherencia entre la planeación estratégica y la gestión tecnológica, y asegura que el PETI se ejecute como un instrumento institucional integrado, verificable y alineado con los principios de eficiencia, control, seguridad y transparencia exigidos a Empresas Públicas de Cundinamarca S.A E.S.P.

9. Diagnóstico del Estado Actual de las Tecnologías de la Información

El diagnóstico del estado actual de las Tecnologías de la Información en Empresas Públicas de Cundinamarca S.A. E.S.P. constituye la base para la formulación del Plan Estratégico de Tecnologías de la Información (PETI), este diagnóstico se realiza a partir del análisis de la infraestructura tecnológica existente, los sistemas de información en operación, los procesos de gestión de TI, la seguridad digital, la continuidad del negocio y los resultados de auditorías y evaluaciones institucionales.

El ejercicio diagnóstico tiene un enfoque realista y verificable, orientado a identificar fortalezas, debilidades, riesgos y oportunidades de mejora, en coherencia con el nivel de madurez tecnológica de la entidad y con los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG) y la Política de Gobierno Digital.

En términos de infraestructura tecnológica, la entidad cuenta con una base operativa que soporta los procesos administrativos, financieros, contractuales, documentales y operativos, no obstante, se identifican retos asociados a la capacidad de crecimiento, la estandarización de la infraestructura, la gestión de respaldos, la documentación técnica y la implementación de esquemas de continuidad y recuperación tecnológica de manera formal y sistemática.

En relación con los sistemas de información, Empresas Públicas de Cundinamarca S.A E.S.P dispone de aplicaciones que apoyan procesos institucionales clave; sin embargo, se evidencian limitaciones en la interoperabilidad entre sistemas, la automatización de procesos y la integración de la información, la gestión de los sistemas se orienta principalmente a la operación, lo que hace necesario fortalecer la planeación, la documentación, la gestión de cambios y el control de versiones, evitando dependencias críticas de terceros y riesgos operativos.

Desde la perspectiva de la seguridad digital, la entidad ha avanzado en la adopción de lineamientos básicos de seguridad de la información y protección de datos personales, aun así, se requiere consolidar la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), fortalecer la gestión de riesgos de TI, mejorar los controles de acceso, la gestión de incidentes y la sensibilización de los usuarios, con el fin de reducir la exposición a riesgos tecnológicos y de seguridad.

En cuanto a la continuidad del negocio y la recuperación tecnológica, se identifican avances incipientes en la definición de respaldos y procedimientos de recuperación; no obstante, se requiere fortalecer la formalización, documentación, pruebas periódicas y articulación de estos mecanismos con el Plan de Continuidad del Negocio (PCN) y el Plan de Recuperación Tecnológica (DRP), en cumplimiento de la normativa vigente.

El diagnóstico también considera los resultados de auditorías internas, los informes de Control Interno y los compromisos derivados del MIPG y el FURAG, los cuales evidencian la necesidad de mejorar la trazabilidad de la gestión de TI, el control de proveedores tecnológicos, la documentación de procesos y la generación de evidencias que soporten el cumplimiento normativo.

Empresas Públicas de Cundinamarca S.A E.S.P cuenta con una base tecnológica funcional que permite el desarrollo de sus procesos institucionales; sin embargo, el diagnóstico evidencia la necesidad de fortalecer la planeación estratégica de TI, la gobernanza, la seguridad digital, la continuidad operativa y la articulación

institucional, aspectos que son abordados de manera progresiva y realista en el PETI 2026.

9.1. Consistencia de cifras institucionales

La gestión de Tecnologías de la Información se desarrolla con una estructura organizacional ajustada a la naturaleza y tamaño de la entidad, el soporte tecnológico es atendido mediante el Proceso de Tecnologías de la Información, liderado por el Coordinador TIC y apoyado operativamente por la Mesa de Ayuda (MDA), los sistemas de información en operación corresponden principalmente a herramientas de apoyo administrativo, financiero, documental y operativo, así como a plataformas ofimáticas y servicios tecnológicos básicos, los cuales soportan los procesos estratégicos, misionales y de apoyo, no se cuenta actualmente con plataformas empresariales robustas tipo ERP o CRM, situación que es reconocida en el presente diagnóstico y considerada en la definición de iniciativas futuras.

9.2. Riesgos tecnológicos identificados

A partir del análisis del contexto tecnológico y operativo, se identifican los siguientes riesgos tecnológicos relevantes:

- Dependencia de infraestructura tecnológica básica con limitadas capacidades de escalabilidad.
- Riesgos asociados a la seguridad de la información y a posibles incidentes de ciberseguridad.
- Dependencia de proveedores externos para la prestación de algunos servicios tecnológicos.
- Riesgos operativos derivados de interrupciones en los servicios tecnológicos críticos.
- Limitaciones en la automatización de procesos y en la integración de sistemas de información.

Estos riesgos son gestionados de manera articulada con el Modelo de Seguridad y Privacidad de la Información (MSPI), la gestión de riesgos institucional y los lineamientos de Control Interno.

9.3. Brechas de madurez tecnológica

El análisis de madurez tecnológica evidencia brechas principalmente en los siguientes aspectos:

- Nivel de formalización del gobierno de TI.

- Grado de automatización de procesos institucionales.
- Integración entre sistemas de información.
- Capacidades de monitoreo y seguimiento continuo de servicios tecnológicos.
- Apropiación y uso eficiente de las tecnologías por parte de los usuarios internos.

Estas brechas constituyen insumos clave para la formulación del portafolio de iniciativas estratégicas de TI y el plan de implementación.

9.4. Incidentes tecnológicos recientes y lecciones aprendidas

Durante la vigencia anterior se han presentado incidentes tecnológicos de baja criticidad, principalmente asociados a fallas operativas, requerimientos de soporte y eventos relacionados con seguridad de la información, la atención de estos incidentes ha permitido identificar lecciones aprendidas orientadas a:

- Fortalecer el registro y gestión de incidentes.
- Mejorar los tiempos de respuesta y recuperación.
- Reforzar las medidas preventivas de seguridad digital.
- Sensibilizar a los usuarios en el uso adecuado de los recursos tecnológicos.

Las lecciones aprendidas son incorporadas en las acciones de mejora definidas en los planes asociados de seguridad y continuidad.

10. Principios Rectores

El Plan Estratégico de Tecnologías de la Información se rige por un conjunto de principios que orientan la planeación, ejecución, seguimiento y control de las Tecnologías de la Información durante la vigencia, estos principios aseguran que la gestión tecnológica se desarrolle de manera coherente con los objetivos institucionales, el marco normativo vigente y las capacidades reales de la entidad.

Alineación estratégica: Las Tecnologías de la Información deben estar alineadas con el Plan Estratégico Institucional, el Modelo Integrado de Planeación y Gestión (MIPG) y los lineamientos de la Política de Gobierno Digital, garantizando que las decisiones tecnológicas contribuyan de manera directa al logro de los objetivos institucionales.

Eficiencia y sostenibilidad: La gestión de TI debe orientarse al uso eficiente de los recursos, priorizando soluciones viables, sostenibles y acordes con la capacidad financiera, técnica y operativa de la entidad, evitando reprocesos y sobrecostos.

Seguridad de la información y protección de datos personales: Toda iniciativa tecnológica debe garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información, en cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI), la Ley 1581 de 2012 y la normativa aplicable.

Continuidad del negocio: Las Tecnologías de la Información deben apoyar la continuidad de los procesos institucionales críticos, mediante la implementación progresiva de planes de continuidad y recuperación tecnológica que reduzcan el impacto de incidentes o fallas.

Transparencia y acceso a la información: La gestión tecnológica debe facilitar el cumplimiento de las obligaciones en materia de transparencia y acceso a la información pública, fortaleciendo la publicación, disponibilidad y trazabilidad de la información institucional.

Gestión del riesgo: La planeación y ejecución de las iniciativas de TI deben incorporar un enfoque de gestión del riesgo, identificando, evaluando y tratando los riesgos tecnológicos y de seguridad de la información de manera sistemática.

Articulación institucional: El Proceso de Tecnologías de la Información actúa de manera transversal, articulándose con todos los procesos de la entidad y con las instancias de control, para asegurar coherencia, coordinación y efectividad en la gestión tecnológica.

Mejora continua: La gestión de TI se concibe como un proceso dinámico, sujeto a seguimiento, evaluación y mejora continua, incorporando lecciones aprendidas, resultados de auditoría y cambios normativos o tecnológicos relevantes.

Estos principios rectores constituyen la base para la definición de los objetivos estratégicos, las iniciativas y los mecanismos de seguimiento del PETI 2026, asegurando una gestión de Tecnologías de la Información coherente, controlada y orientada a resultados.

11. Objetivos Estratégicos de Tecnologías de la Información

Los objetivos estratégicos de Tecnologías de la Información definidos en la gestión tecnológica durante la vigencia, asegurando su contribución directa al cumplimiento de los objetivos institucionales, la eficiencia operativa, la seguridad digital y la continuidad del negocio.

Estos objetivos se formulan en coherencia con el Plan Estratégico Institucional, el Modelo Integrado de Planeación y Gestión (MIPG), la Política de Gobierno Digital y el Decreto 612 de 2018, y se encuentran alineados con el nivel real de madurez tecnológica de la entidad.

Objetivo estratégico 1. Fortalecer la gobernanza de las Tecnologías de la Información: Consolidar un modelo de gobierno de TI alineado con la Dirección de Planeación, que defina roles, responsabilidades y mecanismos de articulación institucional claros, permitiendo una adecuada planeación, priorización, ejecución y control de las iniciativas tecnológicas.

Objetivo estratégico 2. Garantizar la seguridad de la información y la protección de los datos personales: Fortalecer la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) y del Plan Estratégico de Seguridad y Privacidad de la Información (PESI), asegurando la aplicación de controles que protejan la confidencialidad, integridad, disponibilidad y privacidad de la información institucional.

Objetivo estratégico 3. Asegurar la continuidad operativa y la resiliencia tecnológica: Implementar y fortalecer de manera progresiva los mecanismos de continuidad del negocio y recuperación tecnológica, mediante la formalización, documentación y prueba del Plan de Continuidad del Negocio (PCN) y el Plan de Recuperación Tecnológica (DRP), reduciendo el impacto de incidentes tecnológicos sobre los procesos institucionales.

Objetivo estratégico 4. Optimizar la infraestructura tecnológica y los servicios de TI: Mejorar la disponibilidad, estabilidad y sostenibilidad de la infraestructura tecnológica institucional, priorizando la estandarización, el control operativo, la gestión de respaldos y el uso eficiente de los recursos tecnológicos.

Objetivo estratégico 5. Fortalecer el soporte a los procesos misionales y administrativos: Asegurar que las Tecnologías de la Información soporten de manera efectiva los procesos misionales, estratégicos y de apoyo de Empresas Públicas de Cundinamarca S.A E.S.P, facilitando la gestión documental, la operación institucional, la atención al usuario y la toma de decisiones.

Objetivo estratégico 6. Mejorar la gestión de riesgos tecnológicos: Integrar la gestión de riesgos de Tecnologías de la Información al sistema institucional de gestión del

riesgo, identificando, evaluando y tratando de manera sistemática los riesgos tecnológicos y de seguridad de la información.

Objetivo estratégico 7. Fortalecer la transparencia y el cumplimiento normativo: Apoyar el cumplimiento de las obligaciones de transparencia, acceso a la información pública y rendición de cuentas, mediante el adecuado uso, administración y control de las Tecnologías de la Información y del sitio web institucional.

Estos objetivos estratégicos orientan la definición de las iniciativas, proyectos, indicadores y mecanismos de seguimiento del PETI 2026, garantizando una gestión tecnológica coherente, controlada y alineada con los principios de la gestión pública.

12. Gobierno y Gestión de Tecnologías de la Información

El gobierno y la gestión de las Tecnologías de la Información en Empresas Públicas de Cundinamarca S.A. E.S.P. se estructuran con el propósito de asegurar que las decisiones tecnológicas se encuentren alineadas con la planeación institucional, generen valor público, gestionen adecuadamente los riesgos y garanticen el cumplimiento normativo vigente.

El modelo de gobierno de TI se fundamenta en los principios del Modelo Integrado de Planeación y Gestión (MIPG), los lineamientos de la Política de Gobierno Digital y las buenas prácticas de gestión de tecnologías de la información aplicables al sector público, adoptando un enfoque proporcional al nivel de madurez tecnológica de la entidad.

11.1 Gobierno de Tecnologías de la Información

El gobierno de TI establece las estructuras de decisión, roles y responsabilidades que permiten orientar estratégicamente la gestión tecnológica, en este marco:

- La Dirección de Planeación ejerce la orientación estratégica del Proceso de Tecnologías de la Información, asegurando su alineación con el Plan Estratégico Institucional, el Sistema Integrado de Gestión y las prioridades institucionales.
- El Proceso de Tecnologías de la Información, a través del Coordinador de TI, es responsable de liderar la planeación, ejecución, seguimiento y control de las iniciativas tecnológicas definidas en el PETI, garantizando su coherencia técnica, su viabilidad operativa y su cumplimiento normativo.
- La Dirección de Control Interno realiza el seguimiento y evaluación independiente del gobierno y la gestión de TI, verificando la eficacia de los

controles, la gestión de riesgos tecnológicos y el cumplimiento de los compromisos establecidos en el PETI.
- Las demás Direcciones y Subgerencias participan como actores articulados, definiendo necesidades, priorizando requerimientos y apoyando la implementación de las iniciativas tecnológicas que soportan sus procesos.

Este esquema de gobierno permite que las decisiones en materia de Tecnologías de la Información se adopten de manera coordinada, documentada y verificable, reduciendo riesgos y evitando reprocesos.

11.2 Gestión de Tecnologías de la Información

La gestión de TI comprende el conjunto de procesos y actividades orientadas a la operación, mantenimiento y mejora de los servicios tecnológicos que soportan la gestión institucional. Esta gestión se desarrolla bajo los siguientes lineamientos:

- Planeación y priorización de iniciativas tecnológicas conforme al PETI, considerando criterios de riesgo, impacto institucional, viabilidad técnica y disponibilidad de recursos.
- Gestión operativa de la infraestructura tecnológica, los sistemas de información y los servicios de soporte, asegurando niveles adecuados de disponibilidad, estabilidad y continuidad.
- Administración de cambios tecnológicos, garantizando su documentación, evaluación de impacto y control, con el fin de minimizar riesgos operativos.
- Gestión de incidentes y requerimientos a través de la Mesa de Ayuda, asegurando trazabilidad, tiempos de atención definidos y generación de evidencias.
- Supervisión técnica de proveedores y contratos tecnológicos, en articulación con la Dirección de Gestión Contractual y la Dirección Jurídica, verificando el cumplimiento de obligaciones, niveles de servicio y cláusulas de seguridad y continuidad.

11.3 Articulación con el Sistema de Control Interno

El gobierno y la gestión de TI se articulan con el Sistema de Control Interno, integrando la identificación, evaluación y tratamiento de riesgos tecnológicos al mapa de riesgos institucional, los resultados de auditorías internas, evaluaciones de Control Interno y revisiones periódicas del PETI constituyen insumos para la mejora continua de la gestión tecnológica.

En este contexto, el gobierno y la gestión de las Tecnologías de la Información se consolidan como un componente esencial de la planeación institucional, asegurando que la tecnología contribuya de manera efectiva, segura y controlada al cumplimiento de los objetivos de Empresas Públicas de Cundinamarca S.A E.S.P.

13. Arquitectura Tecnológica y de Sistemas de Información

La arquitectura tecnológica y de sistemas de información constituye el marco que orienta la organización, evolución y uso de las Tecnologías de la Información, con el fin de asegurar su alineación con los procesos institucionales, la planeación estratégica y los lineamientos de la Política de Gobierno Digital.

La definición de la arquitectura tecnológica se realiza bajo un enfoque progresivo y realista, acorde con el nivel de madurez institucional, priorizando la estabilidad operativa, la seguridad de la información, la continuidad del servicio y la sostenibilidad de las soluciones tecnológicas.

1. Enfoque de arquitectura tecnológica

La arquitectura tecnológica de Empresas Públicas de Cundinamarca S.A E.S.P se fundamenta en los siguientes lineamientos:

- Alineación con los procesos estratégicos, misionales y de apoyo de la entidad, asegurando que las soluciones tecnológicas respondan a necesidades institucionales reales.
- Aplicación de principios de estandarización, interoperabilidad y control, conforme a los lineamientos definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).
- Priorización de soluciones tecnológicas sostenibles, escalables de manera controlada y acordes con la capacidad operativa y financiera de la entidad.
- Enfoque en la seguridad digital y la protección de la información como componentes transversales de la arquitectura.

2. Infraestructura tecnológica

La infraestructura tecnológica institucional comprende los recursos físicos y lógicos que soportan la operación de los sistemas de información y los servicios tecnológicos de Empresas Públicas de Cundinamarca S.A E.S.P, incluyendo equipos de cómputo,

servidores, redes de comunicaciones, servicios de conectividad, plataformas de almacenamiento y servicios en la nube de carácter básico.

La gestión de la infraestructura se orienta a garantizar niveles adecuados de disponibilidad, integridad y continuidad, mediante prácticas de mantenimiento, control de configuraciones, gestión de respaldos y documentación técnica, el PETI prioriza el fortalecimiento de la infraestructura existente, evitando la adopción de soluciones que no correspondan a las capacidades reales de la entidad.

3. Sistemas de información

Los sistemas de información de Empresas Públicas de Cundinamarca S.A E.S.P apoyan procesos administrativos, financieros, contractuales, documentales, operativos y de atención al usuario, la arquitectura de sistemas se orienta a:

- Asegurar la operación estable y controlada de los sistemas existentes.
- Fortalecer la gestión de accesos, roles y perfiles de usuario.
- Mejorar progresivamente la integración y el intercambio de información entre sistemas, en la medida en que sea técnica y operativamente viable.
- Garantizar la trazabilidad de la información y el control de versiones de las aplicaciones y sus componentes.

El PETI no contempla la implementación de plataformas tecnológicas avanzadas que no se encuentren actualmente en operación o que no correspondan al nivel de madurez institucional, tales como sistemas de gestión de relacionamiento con clientes u otras soluciones similares.

4. Servicios en la nube

La adopción de servicios en la nube se considera de manera gradual y controlada, priorizando aquellos servicios que aporten beneficios claros en términos de disponibilidad, respaldo y continuidad, y que cumplan con los requisitos de seguridad, protección de datos personales y control definidos por la entidad.

La contratación y uso de servicios en la nube deberán incorporar criterios de seguridad de la información, localización de datos, continuidad del servicio y reversibilidad, en articulación con el Modelo de Seguridad y Privacidad de la Información (MSPI) y la normativa vigente.

5. Arquitectura y gestión de la información

La arquitectura tecnológica se articula con la gestión de la información institucional y la gestión documental, garantizando que los sistemas de información y las plataformas tecnológicas soporten el cumplimiento de la Ley 594 de 2000, las Tablas de Retención Documental (TRD) y los lineamientos de transparencia y acceso a la información pública.

En este sentido, la arquitectura tecnológica contribuye a la adecuada conservación, disponibilidad y disposición final de la información institucional, fortaleciendo la trazabilidad, la seguridad y el control de los documentos y datos gestionados por Empresas Públicas de Cundinamarca S.A E.S.P.

14. Seguridad Digital y Protección de la Información

La seguridad digital y la protección de la información constituyen un eje transversal del Plan Estratégico de Tecnologías de la Información orientado a garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información institucional, en cumplimiento del marco normativo vigente y de los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

La gestión de la seguridad digital se articula con la Política de Gobierno Digital, el Modelo Integrado de Planeación y Gestión (MIPG) y los instrumentos específicos definidos por la entidad, en especial el Plan Estratégico de Seguridad y Privacidad de la Información (PESI) y el Modelo de Seguridad y Privacidad de la Información (MSPI).

1 Enfoque de seguridad digital

La seguridad digital en Empresas Públicas de Cundinamarca S.A E.S.P se concibe como un proceso continuo y sistemático, integrado a la planeación, ejecución y control de las Tecnologías de la Información, y no como un conjunto de acciones aisladas, en este sentido, toda iniciativa tecnológica definida en el PETI debe incorporar criterios de seguridad desde su fase de planeación, bajo un enfoque preventivo y basado en riesgos.

El enfoque adoptado prioriza la protección de los activos de información, la gestión adecuada de accesos, la reducción de vulnerabilidades, la detección y respuesta a incidentes, y la generación de evidencias que soporten el cumplimiento normativo y los procesos de auditoría.

2 Modelo de Seguridad y Privacidad de la Información

Empresas Públicas de Cundinamarca S.A E.S.P adopta el Modelo de Seguridad y Privacidad de la Información (MSPI) como marco de referencia para la gestión de la seguridad digital, el MSPI define los roles, responsabilidades, políticas, procedimientos y controles necesarios para proteger la información institucional, en coherencia con la normativa nacional y las buenas prácticas internacionales.

La implementación del MSPI se orienta a fortalecer, de manera progresiva, los siguientes aspectos:

- Identificación y clasificación de los activos de información.
- Definición y aplicación de controles de seguridad acordes con el nivel de riesgo.
- Gestión de accesos y privilegios de usuarios.
- Protección de datos personales en cumplimiento de la Ley 1581 de 2012.
- Gestión de incidentes de seguridad de la información.
- Sensibilización y capacitación en seguridad digital.

3 Protección de datos personales

La entidad garantiza la protección de los datos personales que administra, en cumplimiento de la Ley 1581 de 2012 y sus normas reglamentarias, el PETI 2026 incorpora acciones orientadas a fortalecer el cumplimiento de las obligaciones como responsable del tratamiento de datos, asegurando que los sistemas de información, procesos tecnológicos y servicios contratados incluyan medidas adecuadas de seguridad y privacidad.

La protección de datos personales se integra a la gestión de riesgos de TI, a la contratación de servicios tecnológicos y a la administración del sitio web institucional, garantizando la confidencialidad y el uso adecuado de la información de los titulares.

4 Gestión de incidentes de seguridad

La gestión de incidentes de seguridad de la información se desarrolla bajo procedimientos definidos, que permiten la detección, registro, análisis, atención y

cierre de los incidentes que puedan afectar los activos de información o los servicios tecnológicos de la entidad.

El Proceso de Tecnologías de la Información, a través del Coordinador de TI y la Mesa de Ayuda, es responsable de coordinar la atención de los incidentes, generar las evidencias correspondientes y articular las acciones necesarias con la Dirección de Control Interno y las demás áreas involucradas, cuando sea aplicable.

5 Seguridad en la contratación tecnológica y servicios tercerizados

Los procesos de contratación de bienes y servicios tecnológicos incorporan criterios de seguridad digital y protección de la información, incluyendo cláusulas relacionadas con confidencialidad, protección de datos personales, continuidad del servicio, gestión de incidentes y responsabilidades frente a fallas o vulneraciones de seguridad.

La supervisión técnica de los contratos tecnológicos verifica el cumplimiento de estas obligaciones y contribuye a reducir los riesgos asociados a la tercerización de servicios tecnológicos.

En conjunto, este enfoque de seguridad digital permite que el PETI fortalezca la protección de la información institucional, reduzca la exposición a riesgos tecnológicos y garantice el cumplimiento de las obligaciones legales y normativas aplicables a Empresas Públicas de Cundinamarca S.A E.S.P.

6 Acciones de capacitación y sensibilización en seguridad digital

Con el fin de fortalecer la cultura institucional en materia de seguridad digital y protección de la información, Empresas Públicas de Cundinamarca S.A. E.S.P. implementará acciones de capacitación y sensibilización dirigidas a funcionarios, contratistas y usuarios con acceso a los activos de información y servicios tecnológicos de la entidad.

Las acciones estarán orientadas a prevenir incidentes de seguridad de la información, reducir riesgos asociados al factor humano y promover el uso responsable de las Tecnologías de la Información, en concordancia con los lineamientos institucionales.

Las principales acciones previstas son:

- Jornadas de sensibilización en seguridad digital, enfocadas en buenas prácticas de uso de los recursos tecnológicos, manejo de contraseñas, protección de la información y prevención de incidentes.
- Difusión periódica de comunicaciones internas relacionadas con alertas de seguridad, recomendaciones y lineamientos institucionales.
- Capacitación básica en protección de datos personales y tratamiento de la información, conforme a la Ley 1581 de 2012.
- Socialización de los roles y responsabilidades frente a la seguridad de la información, especialmente para usuarios con funciones críticas.
- Inclusión de contenidos de seguridad digital en los procesos de inducción y reinducción, cuando aplique.

La ejecución de estas acciones será coordinada por el Proceso de Tecnologías de la Información, en articulación con las áreas de Gestión Humana y Control Interno, y su implementación se realizará de manera gradual, de acuerdo con la capacidad institucional y la disponibilidad de recursos.

El seguimiento a las actividades de capacitación y sensibilización se efectuará mediante registros de asistencia, evidencias de divulgación y certificados digitales emitidos por el ente capacitador, los cuales servirán como insumo para la mejora continua de la gestión de seguridad digital.

15. Gestión de Riesgos de Tecnologías de la Información

La gestión de riesgos de Tecnologías de la Información en Empresas Públicas de Cundinamarca S.A. E.S.P. constituye un componente fundamental del Plan Estratégico de Tecnologías de la Información, orientado a identificar, analizar, evaluar y tratar los riesgos tecnológicos que puedan afectar el cumplimiento de los objetivos institucionales, la seguridad de la información y la continuidad de los servicios.

La gestión de riesgos de TI se desarrolla en coherencia con el Modelo Integrado de Planeación y Gestión (MIPG), la Política de Administración del Riesgo institucional, el Modelo de Seguridad y Privacidad de la Información (MSPI) y las buenas prácticas establecidas en normas internacionales como ISO 31000 e ISO/IEC 27005, aplicadas de manera proporcional al nivel de madurez de la entidad.

1 Enfoque de gestión del riesgo en Tecnologías de la Información

El enfoque adoptado por Empresas Públicas de Cundinamarca S.A E.S.P reconoce que los riesgos tecnológicos deben gestionarse de forma integral, considerando tanto los riesgos asociados a la operación de la infraestructura tecnológica y los sistemas de información, como aquellos relacionados con la seguridad de la información, la continuidad del negocio, la contratación de servicios tecnológicos y el factor humano.

La gestión del riesgo de TI se integra al ciclo institucional de planeación, ejecución, seguimiento y mejora continua, asegurando que las decisiones tecnológicas se adopten con criterios de prevención, control y sostenibilidad.

2 Identificación y evaluación de riesgos tecnológicos

La identificación de riesgos tecnológicos se realiza de manera periódica, considerando, entre otros, los siguientes aspectos:

- Indisponibilidad de servicios tecnológicos críticos.
- Incidentes de seguridad de la información y pérdida de datos.
- Fallas de infraestructura tecnológica o de servicios tercerizados.
- Deficiencias en la gestión de respaldos y recuperación de información.

- Vulnerabilidades asociadas a accesos no autorizados o uso inadecuado de los sistemas.
- Dependencia excesiva de proveedores tecnológicos.
- Falta de documentación, procedimientos o capacitación del personal.

Los riesgos identificados son evaluados en términos de probabilidad e impacto, y se incorporan al mapa de riesgos institucional y al mapa de riesgos del Proceso de Tecnologías de la Información, garantizando su trazabilidad y seguimiento.

3 Tratamiento y seguimiento de riesgos de TI

Para cada riesgo tecnológico identificado, se definen acciones de tratamiento orientadas a su mitigación, transferencia, aceptación o eliminación, según corresponda, estas acciones se articulan con los planes de acción institucionales, los planes de mejoramiento derivados de auditorías y los instrumentos de seguridad y continuidad definidos por la entidad.

El seguimiento a los riesgos de TI se realiza de manera periódica, a través de reportes al interior del Proceso de Tecnologías de la Información y en articulación con la Dirección de Planeación y la Dirección de Control Interno, los resultados de este seguimiento constituyen insumo para la revisión y actualización del PETI, el PESI y el MSPI.

4 Articulación con auditoría y Control Interno

La gestión de riesgos de Tecnologías de la Información se encuentra articulada con los procesos de auditoría interna y Control Interno, permitiendo la verificación independiente de la eficacia de los controles implementados y la identificación de oportunidades de mejora.

Las observaciones y recomendaciones derivadas de auditorías son incorporadas a los planes de mejoramiento y al ciclo de mejora continua de la gestión tecnológica, fortaleciendo la gobernanza y la resiliencia institucional.

En este marco, la gestión de riesgos de TI se consolida como un pilar del PETI 2026, asegurando una administración responsable, controlada y alineada con los objetivos estratégicos de Empresas Públicas de Cundinamarca S.A E.S.P y con las exigencias normativas vigentes.

16. Continuidad del Negocio y Recuperación Tecnológica

La continuidad del negocio y la recuperación tecnológica constituyen un componente esencial del Plan Estratégico de Tecnologías de la Información de Empresas Públicas de Cundinamarca S.A. E.S.P, orientado a garantizar la prestación ininterrumpida de los servicios institucionales y la protección de los activos de información frente a eventos disruptivos.

La gestión de la continuidad se desarrolla en coherencia con el Modelo Integrado de Planeación y Gestión (MIPG), la Política de Administración del Riesgo institucional, el Modelo de Seguridad y Privacidad de la Información (MSPI) y las disposiciones establecidas en el Decreto 2157 de 2017, así como con las buenas prácticas definidas en las normas ISO 22301 e ISO/IEC 27031.

1 Enfoque de continuidad del negocio

Empresas Públicas de Cundinamarca S.A E.S.P adopta un enfoque preventivo y progresivo para la gestión de la continuidad del negocio, reconociendo que la

interrupción de los servicios tecnológicos puede afectar de manera directa el cumplimiento de los objetivos institucionales, la prestación de los servicios públicos y la confianza de los ciudadanos.

La continuidad del negocio se concibe como un proceso transversal que involucra a todas las áreas de la entidad y que se articula con la planeación estratégica, la gestión de riesgos y la seguridad de la información.

2 Plan de Continuidad del Negocio (PCN)

El Plan de Continuidad del Negocio (PCN) establece los lineamientos, responsabilidades y procedimientos necesarios para garantizar la continuidad de los procesos institucionales críticos ante eventos que puedan afectar la operación normal de la entidad.

El PETI 2026 orienta el fortalecimiento del PCN mediante:

- La identificación y priorización de los procesos críticos soportados por las Tecnologías de la Información.
- La definición de estrategias de continuidad acordes con las capacidades institucionales.
- La asignación de roles y responsabilidades para la gestión de situaciones de contingencia.
- La articulación del PCN con los planes de seguridad de la información y gestión del riesgo.

3 Plan de Recuperación Tecnológica (DRP)

El Plan de Recuperación Tecnológica (DRP) define los procedimientos técnicos para la restauración de los servicios tecnológicos, los sistemas de información y los activos tecnológicos, una vez se presente una interrupción o incidente que afecte la operación.

El DRP se orienta a:

- Establecer mecanismos de respaldo y restauración de la información.
- Definir tiempos objetivos de recuperación acordes con la criticidad de los servicios.
- Documentar procedimientos de recuperación tecnológica claros y verificables.

- Garantizar la disponibilidad de evidencias que soporten la ejecución de las acciones de recuperación.

La ejecución operativa del DRP es responsabilidad del Proceso de Tecnologías de la Información, a través del Coordinador de TI y la Mesa de Ayuda, en articulación con las áreas involucradas según la naturaleza del incidente.

4 Pruebas, seguimiento y mejora continua

El PETI promueve la realización de pruebas periódicas de los planes de continuidad y recuperación tecnológica, con el fin de verificar su efectividad, identificar brechas y fortalecer la capacidad de respuesta institucional frente a eventos disruptivos.

Los resultados de las pruebas, los incidentes atendidos y las observaciones derivadas de auditorías y evaluaciones de Control Interno constituyen insumos para la actualización del PCN, el DRP y el PETI, asegurando su vigencia y mejora continua.

En este marco, la continuidad del negocio y la recuperación tecnológica se consolidan como elementos clave para la resiliencia organizacional de Empresas Públicas de Cundinamarca S.A E.S.P, permitiendo reducir los impactos operativos, financieros y reputacionales asociados a la materialización de riesgos tecnológicos.

5 Periodicidad y alcance de pruebas de continuidad y recuperación tecnológica

Con el propósito de garantizar la resiliencia tecnológica y la continuidad de los servicios soportados por Tecnologías de la Información, Empresas Públicas de Cundinamarca S.A. E.S.P. define la periodicidad y el alcance de las pruebas asociadas al Plan de Continuidad del Negocio (PCN) y al Plan de Recuperación Tecnológica (DRP), en concordancia con el Decreto 2157 de 2017, el Modelo de Seguridad y Privacidad de la Información (MSPI) y las buenas prácticas aplicables.

Las pruebas de continuidad y recuperación tecnológica tendrán como objetivos principales validar la efectividad de los procedimientos definidos, identificar oportunidades de mejora y asegurar la capacidad de respuesta ante incidentes que afecten la disponibilidad de los servicios tecnológicos.

Periodicidad de las pruebas:

- Se realizará, como mínimo, una prueba anual de los procedimientos de continuidad y recuperación tecnológica.

- Adicionalmente, se podrán ejecutar pruebas extraordinarias cuando se presenten cambios significativos en la infraestructura tecnológica, en los sistemas de información, en la estructura organizacional o cuando ocurra un incidente relevante.
- Las pruebas se programarán y documentarán dentro del plan anual de actividades del Proceso de Tecnologías de la Información.

Alcance de las pruebas:

- Verificación de los procedimientos de respaldo y restauración de información.
- Validación de la disponibilidad de los servicios tecnológicos considerados críticos.
- Evaluación de los tiempos de respuesta y recuperación definidos.
- Revisión de roles y responsabilidades durante la atención de eventos disruptivos.
- Comprobación de los mecanismos de comunicación interna durante la contingencia.

Las pruebas podrán ejecutarse mediante ejercicios de escritorio, simulaciones controladas o pruebas técnicas parciales, de acuerdo con la criticidad de los servicios y la capacidad operativa de la entidad, evitando afectar la prestación normal de los servicios institucionales.

Seguimiento y mejora:
Los resultados de las pruebas serán documentados mediante actas o informes, en los cuales se consignarán las observaciones, hallazgos y acciones de mejora identificadas, dichos insumos serán utilizados para actualizar el PCN, el DRP y los procedimientos asociados, y servirán como evidencia para los procesos de auditoría y Control Interno.

17. Relación con Proveedores y Contratación

La relación con proveedores y la contratación de bienes y servicios tecnológicos en Empresas Públicas de Cundinamarca S.A. E.S.P. se gestionan como un componente estratégico del Plan Estratégico de Tecnologías de la Información (PETI), orientado a garantizar la continuidad de los servicios, la seguridad de la información, el cumplimiento normativo y el uso eficiente de los recursos públicos.

La gestión contractual en materia de Tecnologías de la Información se desarrolla en articulación con la Dirección de Gestión Contractual, la Dirección Jurídica, la Dirección de Planeación y la Dirección de Control Interno, asegurando que los procesos de contratación respondan a las necesidades institucionales reales y se ejecuten bajo criterios de transparencia, legalidad y control.

1 Enfoque de contratación tecnológica

La contratación de bienes y servicios tecnológicos se orienta por los principios de planeación, eficiencia, responsabilidad y sostenibilidad, priorizando soluciones acordes con el nivel de madurez tecnológica de la entidad y evitando la adquisición de herramientas o plataformas que no puedan ser operadas, soportadas o controladas adecuadamente.

Toda contratación tecnológica debe estar previamente alineada con el PETI, el presupuesto institucional y los lineamientos de la Política de Gobierno Digital, garantizando que las decisiones de adquisición respondan a una necesidad institucional debidamente identificada y priorizada.

2 Requerimientos técnicos y criterios de seguridad

Los procesos de contratación de servicios tecnológicos incorporan requerimientos técnicos claros, definidos por el Proceso de Tecnologías de la Información, que permiten asegurar la calidad, funcionalidad y sostenibilidad de las soluciones contratadas.

Así mismo, los contratos de TI incluyen cláusulas relacionadas con:

- Seguridad de la información y protección de datos personales.
- Confidencialidad de la información institucional.
- Continuidad del servicio y recuperación ante incidentes.
- Responsabilidades frente a fallas, incidentes o incumplimientos.
- Niveles de servicio y tiempos de respuesta, cuando aplique.

Estos criterios permiten reducir los riesgos asociados a la tercerización de servicios tecnológicos y fortalecen la capacidad de supervisión técnica de la entidad.

3 Supervisión y control de proveedores tecnológicos

La supervisión técnica de los contratos de Tecnologías de la Información es ejercida por el Proceso de Tecnologías de la Información, a través del Coordinador de TI, en articulación con la Dirección de Gestión Contractual y la Dirección Jurídica.

La supervisión se orienta a verificar el cumplimiento de las obligaciones contractuales, los requerimientos técnicos, los compromisos de seguridad digital y los acuerdos de nivel de servicio establecidos, generando las evidencias necesarias para los procesos de auditoría y Control Interno.

En caso de identificarse desviaciones, incumplimientos o riesgos relevantes, se activan los mecanismos contractuales y administrativos correspondientes, con el fin de proteger los intereses de la entidad y garantizar la continuidad de los servicios tecnológicos.

4 Evaluación y mejora en la gestión de proveedores

El PETI promueve la evaluación periódica del desempeño de los proveedores tecnológicos, considerando criterios de calidad del servicio, cumplimiento contractual, gestión de incidentes y capacidad de respuesta.

Los resultados de estas evaluaciones constituyen insumo para la toma de decisiones futuras en materia de contratación, la definición de planes de mejora y la mitigación de riesgos asociados a la dependencia de terceros.

La relación con proveedores y la contratación de servicios tecnológicos se consolidan como un proceso controlado, transparente y alineado con la planeación estratégica de Empresas Públicas de Cundinamarca S.A E.S.P, contribuyendo a una gestión responsable y segura de las Tecnologías de la Información.

5 Evaluación y retroalimentación a proveedores tecnológicos

Con el fin de asegurar la calidad, continuidad y seguridad de los servicios tecnológicos contratados, se establece un proceso de evaluación y retroalimentación a los proveedores tecnológicos, articulado con los lineamientos institucionales de contratación, control interno y gestión de riesgos.

La evaluación de proveedores tecnológicos tiene como objetivo verificar el cumplimiento de las obligaciones contractuales, la adecuada prestación de los

servicios, el cumplimiento de los requisitos de seguridad de la información y la contribución efectiva al logro de los objetivos institucionales.

Criterios de evaluación: La evaluación de los proveedores tecnológicos podrá considerar, entre otros, los siguientes aspectos:

- Cumplimiento de los niveles de servicio acordados.
- Calidad y oportunidad en la atención de incidentes y requerimientos.
- Cumplimiento de los lineamientos de seguridad y privacidad de la información.
- Disponibilidad y continuidad de los servicios prestados.
- Cumplimiento de los compromisos contractuales y normativos aplicables.

Periodicidad de la evaluación:

- La evaluación se realizará de manera periódica, conforme a la duración y naturaleza del contrato.
- Adicionalmente, se podrán realizar evaluaciones extraordinarias cuando se presenten incidentes relevantes, incumplimientos o cambios significativos en los servicios contratados.

Retroalimentación y mejora:
Los resultados de la evaluación serán comunicados al proveedor correspondiente y, cuando aplique, se definirán acciones de mejora o ajustes en la prestación del servicio, la retroalimentación se documentará y se articulará con los procesos de supervisión contractual, Gestión Contractual y Control Interno.

Este proceso de evaluación y retroalimentación constituye un insumo para la toma de decisiones relacionadas con la continuidad, ajuste o finalización de los servicios tecnológicos, y contribuye a la mejora continua de la gestión de Tecnologías de la Información en la entidad.

18. Portafolio de Iniciativas y Proyectos Estratégicos de TI

El portafolio de iniciativas y proyectos estratégicos de Tecnologías de la Información para la vigencia constituye el instrumento mediante el cual se materializan los objetivos definidos en el Plan Estratégico de Tecnologías de la Información (PETI), asegurando una gestión tecnológica coherente, priorizada y alineada con la planeación institucional.

El portafolio se estructura bajo un enfoque realista y ejecutable, considerando el nivel de madurez tecnológica de la entidad, la disponibilidad de recursos, los riesgos identificados y las prioridades institucionales definidas por la Dirección de Planeación y la alta dirección.

1 Criterios de priorización

Las iniciativas y proyectos estratégicos de TI se priorizan con base en los siguientes criterios:

- Alineación con el Plan Estratégico Institucional y el MIPG.
- Contribución a la seguridad de la información y la continuidad del negocio.
- Impacto en los procesos misionales, estratégicos y de apoyo.
- Nivel de riesgo asociado a la no implementación.
- Viabilidad técnica, operativa y financiera.
- Capacidad institucional para su ejecución y sostenimiento.
- Requerimientos normativos y compromisos derivados de auditoría y Control Interno.

2. Líneas estratégicas del portafolio

El portafolio de proyectos de TI se organiza en las siguientes líneas estratégicas:

Fortalecimiento de la gobernanza y gestión de TI: Iniciativas orientadas a consolidar el modelo de gobierno de TI, fortalecer la planeación, la documentación de procesos, la gestión de cambios y la articulación con Planeación, Control Interno y las demás áreas de la entidad.

Seguridad digital y protección de la información: Proyectos dirigidos a fortalecer la implementación del MSPI y el PESI, la gestión de riesgos de TI, la protección de datos personales, la gestión de incidentes y la sensibilización en seguridad digital.

Infraestructura tecnológica y servicios de TI: Iniciativas orientadas a mejorar la disponibilidad, estabilidad y control de la infraestructura tecnológica, la gestión de respaldos, la estandarización de equipos y la optimización de los servicios de soporte.

Continuidad del negocio y recuperación tecnológica: Proyectos orientados a la formalización, actualización y prueba del Plan de Continuidad del Negocio (PCN) y

del Plan de Recuperación Tecnológica (DRP), asegurando su articulación con la gestión de riesgos y la seguridad de la información.

Soporte a procesos institucionales y transparencia: Iniciativas que fortalecen el soporte tecnológico a los procesos administrativos, misionales y de atención al ciudadano, incluyendo la gestión documental, el sitio web institucional y el cumplimiento de las obligaciones de transparencia y acceso a la información pública.

3. Gestión y seguimiento del portafolio

La gestión del portafolio de iniciativas y proyectos de TI es responsabilidad del Proceso de Tecnologías de la Información, bajo la orientación de la Dirección de Planeación, el seguimiento se realiza de manera periódica, verificando el avance, los resultados alcanzados, los riesgos asociados y la generación de evidencias que soporten la ejecución de las iniciativas.

Los resultados del seguimiento al portafolio constituyen insumo para la toma de decisiones, la priorización de recursos, la actualización del PETI y la rendición de cuentas ante los procesos de auditoría, Control Interno y evaluación institucional.

En este marco, el portafolio de iniciativas y proyectos estratégicos de TI permite traducir la planeación estratégica en acciones concretas, controladas y alineadas con los objetivos institucionales de Empresas Públicas de Cundinamarca S.A E.S.P para la vigencia 2026.

3 Proyectos estratégicos de TI

ID	Nombre del proyecto	Objetivo del proyecto	Alcance principal	Responsable	Áreas involucradas
1	Fortalecimiento del Gobierno de TI	Consolidar el gobierno y la gestión de TI alineados con la planeación institucional y el MIPG.	Definición y actualización de lineamientos, roles, responsabilidades y mecanismos de seguimiento de TI.	Coordinador TIC	Dirección de Planeación, Control Interno, Gestión de Calidad
2	Actualización y seguimiento del PETI	Garantizar la actualización, validación y seguimiento del PETI	Ajuste del documento, control de cambios, socialización, seguimiento anual.	Coordinador TIC	Planeación, Control Interno, Gestión de Calidad

		conforme al Decreto 612 de 2018.			
3	Fortalecimiento de la Seguridad y Privacidad de la Información	Reducir los riesgos asociados a la seguridad de la información y proteger los activos de información institucionales.	Actualización del MSPI, PESI, gestión de incidentes, sensibilización y capacitación.	Coordinador TIC	Control Interno, Jurídica, Gestión Humana
4	Gestión de Riesgos de TI	Identificar, analizar y tratar los riesgos tecnológicos de manera articulada con la gestión de riesgos institucional.	Actualización de la matriz de riesgos TI y seguimiento a controles.	Coordinador TIC	Control Interno, Planeación
5	Continuidad del Negocio y Recuperación Tecnológica	Asegurar la continuidad de los servicios tecnológicos críticos ante eventos disruptivos.	Actualización del PCN y DRP, ejecución de pruebas y seguimiento.	Coordinador TIC	Subgerencia Técnica y Operativa, Control Interno
6	Fortalecimiento del Soporte Tecnológico y Mesa de Ayuda	Mejorar la atención de incidentes y requerimientos tecnológicos internos.	Organización del registro de incidentes, tiempos de respuesta y evidencias de atención.	Coordinador TIC	Mesa de Ayuda (MDA)
7	Gestión de Proveedores Tecnológicos	Mejorar el control y seguimiento a los proveedores de servicios tecnológicos.	Definición de criterios de evaluación, retroalimentación y seguimiento contractual.	Coordinador TIC	Gestión Contractual, Jurídica, Control Interno
8	Gestión Documental y Transparencia Digital	Garantizar la correcta publicación y gestión de documentos TI conforme a la normativa vigente.	Publicación de documentos en repositorio institucional y componente de transparencia.	Coordinador TIC	Gestión de Calidad, Planeación

9	Sensibilización y apropiación de TI	Fortalecer el uso adecuado y responsable de las tecnologías por parte de los usuarios internos.	Jornadas de sensibilización, comunicaciones internas y apoyo a usuarios.	Coordinador TIC	Gestión Humana
10	Monitoreo y seguimiento de indicadores de TI	Medir el desempeño de la gestión de TI para la toma de decisiones y reporte institucional.	Definición, medición y seguimiento de indicadores de TI y seguridad digital.	Coordinador TIC	Planeación, Control Interno

19. Plan de Implementación y Cronograma

El Plan de Implementación del Plan Estratégico de Tecnologías de la Información establece las directrices para la ejecución ordenada, controlada y verificable de las iniciativas y proyectos estratégicos definidos, asegurando su alineación con la planeación institucional, la disponibilidad de recursos y las capacidades operativas de la entidad.

El plan de implementación se concibe como un instrumento dinámico, sujeto a ajustes conforme a los resultados del seguimiento, los cambios normativos, las prioridades institucionales y las recomendaciones derivadas de auditorías internas y evaluaciones de Control Interno.

1 Enfoque de implementación

La implementación del PETI se desarrolla bajo un enfoque progresivo y realista, priorizando aquellas iniciativas que fortalecen la gobernanza de TI, la seguridad de la información, la continuidad del negocio y la estabilidad operativa de los servicios tecnológicos.

La ejecución de las iniciativas se articula con el ciclo institucional de planeación, ejecución, seguimiento y evaluación, conforme a lo establecido en el Modelo Integrado de Planeación y Gestión (MIPG) y el Decreto 612 de 2018.

2 Responsables de la implementación

La responsabilidad de la implementación del PETI recae en el Proceso de Tecnologías de la Información, bajo la orientación estratégica de la Dirección de Planeación. En este marco:

- El Coordinador de Tecnologías de la Información lidera la ejecución técnica de las iniciativas, coordina los recursos necesarios y realiza el seguimiento al cumplimiento de los objetivos definidos.
- La Mesa de Ayuda ejecuta las actividades operativas asociadas a la implementación, operación y soporte de las soluciones tecnológicas.
- Las Direcciones y Subgerencias participan de manera articulada, facilitando la implementación de las iniciativas que soportan sus procesos y aportando información para el seguimiento y evaluación.

3 Cronograma general de implementación

El cronograma de implementación del PETI se estructura de manera anual, considerando las siguientes fases:

- Fase de planeación y priorización: definición detallada de las iniciativas a ejecutar, asignación de responsables y articulación con el presupuesto institucional.
- Fase de ejecución: desarrollo e implementación de las iniciativas priorizadas, asegurando la documentación, el control de cambios y la generación de evidencias.
- Fase de seguimiento y control: verificación periódica del avance, identificación de desviaciones, gestión de riesgos y adopción de acciones correctivas.
- Fase de evaluación y ajuste: análisis de resultados, incorporación de lecciones aprendidas y ajuste de prioridades para el siguiente ciclo de planeación.

El detalle del cronograma, con tiempos específicos y responsables, se definirá en los planes operativos anuales del Proceso de Tecnologías de la Información, en coherencia con el PETI y el presupuesto aprobado.

4 Seguimiento a la implementación

El seguimiento a la implementación del PETI se realizará mediante informes periódicos presentados a la Dirección de Planeación y a las instancias de Control Interno, los cuales incluirán el estado de avance de las iniciativas, los riesgos identificados, las acciones de mitigación y las evidencias de ejecución.

Los resultados del seguimiento constituyen insumo para la rendición de cuentas, la evaluación del desempeño institucional en el marco del MIPG y el reporte de avances a través del FURAG.

En este marco, el Plan de Implementación y Cronograma del PETI, permite asegurar una ejecución ordenada, controlada y alineada con los objetivos estratégicos de Empresas Públicas de Cundinamarca S.A E.S.P, fortaleciendo la gobernanza y la gestión de las Tecnologías de la Información.

5 Cronograma visual de implementación (Diagrama de Gantt)

ID	Actividad / Proyecto	Responsable	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov
1	Revisión normativa y alineación con MIPG y Gobierno Digital	Coordinador TIC	■	■								
2	Diagnóstico del estado actual de TI (riesgos, brechas, incidentes)	Coordinador TIC	■	■	■							
3	Actualización del PETI y documentos asociados (MSPI, PESI, PCN, DRP)	Coordinador TIC		■	■	■	■					
4	Fortalecimiento del Gobierno de TI	Coordinador TIC			■	■	■	■				
5	Gestión de riesgos de TI y seguridad de la información	Coordinador TIC			■	■	■	■	■			
6	Gestión de incidentes de seguridad de la información	Coordinador TIC	■	■	■	■	■	■	■	■	■	■
7	Continuidad del negocio y recuperación tecnológica (PCN / DRP)	Coordinador TIC				■	■	■	■			
8	Ejecución de pruebas de continuidad y recuperación tecnológica	Coordinador TIC						■	■			
9	Sensibilización y capacitación en seguridad digital	Coordinador TIC				■	■	■	■	■		
10	Gestión y evaluación de proveedores tecnológicos	Coordinador TIC					■	■	■	■		
11	Definición y seguimiento de indicadores de TI	Coordinador TIC				■	■	■	■	■	■	

12	Socialización del PETI con Direcciones y Subgerencias	Coordinador TIC					■	■	■	■		
13	Incorporación de observaciones y ajustes al PETI	Coordinador TIC						■	■	■		
14	Revisión por Gestión de Calidad	Coordinador TIC								■	■	
15	Publicación del PETI y documentos asociados	Coordinador TIC									■	■

20. Indicadores de Seguimiento y Evaluación

El seguimiento y la evaluación del Plan Estratégico de Tecnologías de la Información se realizan mediante un conjunto de indicadores que permiten medir el avance, la efectividad y el impacto de la gestión de Tecnologías de la Información, en coherencia con el Modelo Integrado de Planeación y Gestión (MIPG) y los lineamientos del Decreto 612 de 2018.

Los indicadores definidos permiten verificar el cumplimiento de los objetivos estratégicos de TI, facilitar la toma de decisiones, identificar desviaciones oportunamente y generar evidencias para los procesos de Control Interno, auditoría y reporte de avances institucionales, incluyendo el Formulario Único de Reporte de Avances de la Gestión (FURAG).

1. Enfoque de medición y seguimiento

El sistema de indicadores del PETI se fundamenta en un enfoque práctico y verificable, alineado con la capacidad real de medición de la entidad y orientado a resultados, los indicadores se definen de manera clara, con responsables identificados y fuentes de información confiables, evitando métricas que no puedan ser soportadas con evidencias objetivas.

El seguimiento a los indicadores se integra al ciclo institucional de planeación, ejecución y evaluación, permitiendo la articulación con los informes de gestión, los reportes de Control Interno y los procesos de evaluación del desempeño institucional.

2. Tipología de indicadores

Los indicadores del PETI se agrupan en las siguientes categorías:

Indicadores estratégicos: Miden el grado de avance global del PETI y su alineación con el Plan Estratégico Institucional y el MIPG, permiten evaluar el cumplimiento de los objetivos estratégicos de Tecnologías de la Información y la contribución de TI a los resultados institucionales.

Indicadores operativos: Evalúan la eficiencia y efectividad de la gestión operativa de TI, incluyendo la disponibilidad de los servicios tecnológicos, la atención de incidentes, la ejecución de respaldos, la implementación de controles de seguridad y la ejecución de las iniciativas definidas en el PETI.

Indicadores de seguridad y riesgo: Miden el avance en la implementación del MSPI, la gestión de riesgos de TI, la atención de incidentes de seguridad de la información y el cumplimiento de las acciones definidas en los planes de tratamiento de riesgos.

Indicadores de continuidad: Permiten evaluar el nivel de preparación de la entidad frente a eventos disruptivos, considerando la actualización y prueba del Plan de Continuidad del Negocio (PCN) y del Plan de Recuperación Tecnológica (DRP).

3. Seguimiento, reporte y uso de resultados

El seguimiento a los indicadores del PETI es responsabilidad del Proceso de Tecnologías de la Información, bajo la orientación de la Dirección de Planeación, los resultados se consolidan en informes periódicos que son presentados a la Dirección de Planeación y a las instancias de Control Interno, y que sirven como insumo para la toma de decisiones y la priorización de acciones de mejora.

Los resultados de los indicadores alimentan los reportes institucionales en el marco del MIPG y el FURAG, así como los procesos de auditoría interna y externa, garantizando la trazabilidad y la transparencia de la gestión de Tecnologías de la Información.

En este sentido, los indicadores de seguimiento y evaluación del PETI se constituyen como una herramienta clave para asegurar una gestión tecnológica controlada, orientada a resultados y alineada con los objetivos estratégicos de Empresas Públicas de Cundinamarca S.A E.S.P.

4. Metas cuantitativas e identificación de responsables de reporte

Con el fin de asegurar el seguimiento efectivo, la medición de resultados y la toma de decisiones informada, se definen metas cuantitativas para los indicadores clave de Tecnologías de la Información, así como los responsables de su medición, análisis y reporte.

Las metas se establecen con base en la línea base identificada en el diagnóstico, la capacidad institucional y los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG), garantizando indicadores realistas, medibles y verificables.

ID	Indicador	Línea base	Meta 2026	Frecuencia de medición	Responsable de medición	Responsable de reporte
1	Avance en la implementación del PETI	PETI en proceso de validación institucional	100 % del PETI validado, aprobado y publicado	Trimestral	Coordinador TIC	Dirección de Planeación
2	Proyectos estratégicos de TI en ejecución	Proyectos definidos sin seguimiento formal	≥ 80 % de proyectos ejecutándose conforme al cronograma	Trimestral	Coordinador TIC	Dirección de Planeación
3	Cumplimiento del plan de implementación del PETI	Sin medición formal	≥ 85 % de actividades ejecutadas	Trimestral	Coordinador TIC	Control Interno
4	Incidentes de seguridad de la información registrados y gestionados	Registro parcial de incidentes	100 % de incidentes registrados, atendidos y cerrados	Mensual	Coordinador TIC	Control Interno
5	Actualización de documentos de seguridad (MSPI, PESI)	Documentos vigentes sin actualización 2026	100 % de documentos actualizados y publicados	Semestral	Coordinador TIC	Dirección de Planeación

6	Ejecución de acciones de capacitación en seguridad digital	Acciones no formalizadas	≥ 80 % de acciones de capacitación y sensibilización ejecutadas	Semestral	Coordinador TIC	Gestión Humana
7	Ejecución de pruebas de continuidad y recuperación tecnológica	Pruebas no formalizadas	100 % de pruebas programadas ejecutadas	Anual	Coordinador TIC	Control Interno
8	Tiempo de recuperación de servicios tecnológicos críticos	No documentado	Tiempo de recuperación definido y validado en pruebas	Anual	Coordinador TIC	Dirección de Planeación
9	Atención oportuna de incidentes de TI	Medición informal	≥ 80 % de incidentes atendidos dentro del tiempo definido	Mensual	Coordinador TIC	Subgerencia General
10	Nivel de satisfacción de usuarios internos con el soporte TI	No medido	Nivel medio–alto de satisfacción	Anual	Coordinador TIC	Dirección de Planeación

21. Articulación con Auditoría Interna, Control Interno y FURAG

El Plan Estratégico de Tecnologías de la Información se articula de manera directa y permanente con los procesos de auditoría interna, Control Interno y los mecanismos de evaluación del desempeño institucional, garantizando la trazabilidad, el control y la mejora continua de la gestión de Tecnologías de la Información.

Esta articulación se desarrolla en coherencia con el Modelo Integrado de Planeación y Gestión (MIPG), los lineamientos del Decreto 612 de 2018 y las disposiciones vigentes en materia de control y evaluación de la gestión pública.

1. Articulación con Control Interno

El Proceso de Tecnologías de la Información mantiene una articulación permanente con la Dirección de Control Interno, orientada a:

- Integrar los riesgos tecnológicos y de seguridad de la información al mapa de riesgos institucional.
- Verificar la implementación y efectividad de los controles definidos para la gestión de TI.
- Realizar seguimiento a los planes de mejoramiento derivados de evaluaciones y auditorías.
- Garantizar la generación y conservación de evidencias que soporten el cumplimiento normativo y la gestión del riesgo.

La información generada en el marco del PETI constituye insumo para las evaluaciones de Control Interno y fortalece la toma de decisiones orientadas a la mejora continua.

2. Auditoría interna y externa

El PETI sirve como marco de referencia para las auditorías internas y externas relacionadas con la gestión de Tecnologías de la Información, la seguridad de la información, la continuidad del negocio y la contratación de servicios tecnológicos.

Las auditorías internas permiten evaluar el grado de cumplimiento del PETI, la eficacia de los controles implementados y la alineación de la gestión de TI con los objetivos institucionales, las auditorías externas, por su parte, verifican el cumplimiento de la normativa aplicable, la correcta ejecución de los recursos y la adecuada administración de los activos tecnológicos y de información.

Las observaciones, hallazgos y recomendaciones derivadas de los procesos de auditoría son analizadas y atendidas por el Proceso de Tecnologías de la Información, en articulación con la Dirección de Planeación y las demás áreas involucradas, y se incorporan a los planes de mejoramiento institucional.

3. Articulación con el FURAG

Los avances y resultados de la gestión de Tecnologías de la Información definidos en el PETI se reflejan en el Formulario Único de Reporte de Avances de la Gestión (FURAG), como parte del seguimiento al MIPG y a la planeación institucional.

La información reportada en el FURAG se soporta en evidencias verificables generadas por el Proceso de Tecnologías de la Información, incluyendo indicadores de gestión, avances de proyectos, implementación de controles de seguridad y acciones de mejora.

Esta articulación permite garantizar la coherencia entre la planeación estratégica, la ejecución y el reporte de resultados, fortaleciendo la transparencia, la rendición de cuentas y la evaluación del desempeño institucional, la articulación del PETI con Auditoría Interna, Control Interno y FURAG consolida un enfoque de gestión tecnológica basado en el control, la evidencia y la mejora continua, en coherencia con las exigencias normativas y los principios de la gestión pública.

22. Mecanismos de Seguimiento, Revisión y Actualización

El Plan Estratégico de Tecnologías de la Información se concibe como un instrumento dinámico de planeación, sujeto a seguimiento, revisión y actualización permanente, con el fin de asegurar su vigencia, pertinencia y coherencia frente a los cambios normativos, organizacionales y tecnológicos.

Los mecanismos definidos en este capítulo permiten garantizar que el PETI se mantenga alineado con el Plan Estratégico Institucional, el Modelo Integrado de Planeación y Gestión (MIPG), la Política de Gobierno Digital y las prioridades estratégicas de la entidad.

1. Seguimiento al PETI

El seguimiento a la ejecución del PETI es responsabilidad del Proceso de Tecnologías de la Información, bajo la orientación de la Dirección de Planeación, este seguimiento se realiza de manera periódica, mediante la revisión del avance de las iniciativas y proyectos definidos, el análisis de los indicadores de gestión y la verificación de la implementación de los controles establecidos.

Los resultados del seguimiento se documentan en informes de avance, los cuales constituyen insumo para la toma de decisiones, la gestión de riesgos, el reporte institucional y los procesos de auditoría y Control Interno.

2. Revisión periódica del PETI

La revisión del PETI se realiza como mínimo de manera anual, en el marco del ciclo de planeación institucional definido por el Decreto 612 de 2018, esta revisión permite

evaluar la pertinencia de los objetivos estratégicos, la vigencia de las iniciativas definidas y la coherencia del plan con los cambios organizacionales, normativos o tecnológicos que puedan presentarse.

La revisión del PETI se articula con:

- La evaluación del desempeño institucional en el marco del MIPG.
- Los resultados de auditorías internas y externas.
- Los reportes y compromisos derivados del FURAG.
- Las recomendaciones de la Dirección de Control Interno.

3. Actualización del PETI

La actualización del PETI podrá realizarse de manera ordinaria o extraordinaria, las actualizaciones ordinarias corresponden a los ajustes derivados de la revisión anual del plan y de la planeación institucional, las actualizaciones extraordinarias se podrán realizar cuando se presenten cambios normativos relevantes, modificaciones en la estructura organizacional, incidentes tecnológicos de alto impacto o recomendaciones de entes de control que así lo exijan.

Toda actualización del PETI debe ser debidamente documentada, contar con trazabilidad y ser aprobada por las instancias institucionales competentes, garantizando su coherencia con el Sistema Integrado de Gestión y la planeación estratégica de la entidad.

En este marco, los mecanismos de seguimiento, revisión y actualización del PETI aseguran que la planeación estratégica de Tecnologías de la Información se mantenga vigente, controlada y alineada con los objetivos institucionales de Empresas Públicas de Cundinamarca S.A E.S.P, fortaleciendo la gobernanza y la gestión responsable de la tecnología.

23. Documentos Relacionados

El Plan Estratégico de Tecnologías de la Información se articula con un conjunto de documentos institucionales que soportan la planeación, gestión, control y evaluación de las Tecnologías de la Información, asegurando coherencia documental, trazabilidad y cumplimiento normativo.

Los documentos relacionados constituyen insumos fundamentales para la formulación, ejecución y seguimiento del PETI, y hacen parte del Sistema Integrado de Gestión de la entidad.

Entre los principales documentos relacionados se encuentran:

- Plan Estratégico Institucional (PEI) vigente.
- Modelo Integrado de Planeación y Gestión (MIPG).
- Plan Estratégico de Seguridad y Privacidad de la Información (PESI).
- Modelo de Seguridad y Privacidad de la Información (MSPI).
- Plan de Continuidad del Negocio (PCN).
- Plan de Recuperación Tecnológica (DRP).
- Política de Seguridad de la Información institucional.
- Política de Administración del Riesgo institucional.
- Mapa de Riesgos Institucional y Mapa de Riesgos del Proceso de Tecnologías de la Información.
- Sistema Integrado de Gestión (SIG).
- Tablas de Retención Documental (TRD) institucionales.
- Procedimientos y lineamientos del Proceso de Tecnologías de la Información.
- Informes de auditoría interna y externa relacionados con Tecnologías de la Información.
- Planes de mejoramiento derivados de auditorías y evaluaciones de Control Interno.
- Lineamientos y guías vigentes del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Estos documentos permiten asegurar que el PETI no opere de manera aislada, sino como parte integral de la planeación institucional, facilitando la articulación entre los procesos, la gestión del riesgo, la seguridad de la información y la rendición de cuentas ante los organismos de control.

24. Matriz FODA del Proceso de TI

La presente matriz FODA permite identificar los factores internos y externos que inciden en la gestión del Proceso de Tecnologías de la Información de Empresas Públicas de Cundinamarca S.A. E.S.P., y constituye un insumo para la definición de estrategias, iniciativas y acciones de mejora contempladas en el PETI.

	Fortalezas	**Debilidades**
Oportunidades	• Adscripción del Proceso de Tecnologías de la Información a la Dirección de Planeación, lo que facilita la alineación estratégica. • Existencia de instrumentos de planeación y control. • Conocimiento institucional del marco normativo aplicable a TI, seguridad digital y protección de datos personales. • Articulación funcional con Control Interno y Gestión de Calidad. • Capacidad para operar y sostener servicios tecnológicos básicos de manera continua. • Registro y atención de incidentes tecnológicos a través de la Mesa de Ayuda.	• Bajo nivel de automatización e integración de sistemas de información. • Dependencia de herramientas ofimáticas y soluciones no integradas. • Infraestructura tecnológica con capacidades limitadas de escalabilidad. • Necesidad de fortalecer la apropiación tecnológica por parte de los usuarios internos. • Dependencia de proveedores externos para algunos servicios tecnológicos.

Amenazas	• Lineamientos, guías y herramientas metodológicas emitidas por MinTIC para la planeación de TI. • Disponibilidad de soluciones tecnológicas en la nube con esquemas de pago por uso. • Marco normativo que impulsa la transformación digital y la seguridad digital. • Posibilidad de fortalecimiento de capacidades mediante capacitación y asistencia técnica externa. • Uso de estándares y buenas prácticas como referencia para la mejora continua. • Articulación del PETI con MIPG, FURAG y procesos de auditoría.	• Incremento de amenazas y riesgos asociados a la ciberseguridad. • Cambios frecuentes en la normativa aplicable a TI y seguridad digital. • Restricciones presupuestales que limitan la implementación de nuevas soluciones tecnológicas. • Obsolescencia acelerada de la infraestructura tecnológica. • Dependencia de proveedores tecnológicos externos. • Aumento de las expectativas de los ciudadanos frente a servicios digitales.

25. Disposiciones Finales

El Plan Estratégico de Tecnologías de la Información es de obligatorio cumplimiento para todas las dependencias, procesos, funcionarios, contratistas y proveedores que intervienen en la planeación, gestión, uso y control de las Tecnologías de la Información de la entidad.

La implementación, seguimiento y control del PETI se encuentran a cargo del Proceso de Tecnologías de la Información, bajo la orientación estratégica de la Dirección de Planeación, en articulación con las demás áreas institucionales y las instancias de Control Interno, cada dependencia deberá facilitar la información, los recursos y la colaboración necesarios para el cumplimiento de las iniciativas definidas en el presente plan.

El PETI deberá ser considerado como referente obligatorio en los procesos de planeación, contratación y ejecución de bienes y servicios tecnológicos, garantizando que toda iniciativa de Tecnologías de la Información se encuentre alineada con los objetivos institucionales, el presupuesto aprobado y el marco normativo vigente.

El presente documento será divulgado a través de los medios institucionales definidos por la entidad y estará disponible para consulta de los servidores públicos, los organismos de control y la ciudadanía, en cumplimiento de las disposiciones de transparencia y acceso a la información pública.

Cualquier situación no prevista en el presente PETI será analizada y resuelta en el marco de la planeación institucional, el Sistema Integrado de Gestión y las normas aplicables, garantizando la coherencia, el control y la sostenibilidad de la gestión de Tecnologías de la Información.

26. Control de Cambios

CONTROL DE CAMBIOS				
VERSIÓN	**FECHA**	**DESCRIPCIÓN DEL CAMBIO**	**RESPONSABLE**	**CARGO**
0	31/10/2025	Versión inicial	Diego Ernesto Guevara	Director de Planeación
1	26/01/2026	Actualización	Diego Ernesto Guevara	Director de Planeación

PROYECTÓ	**REVISÓ**	**APROBÓ**
Nombre: Héctor Gil	Nombre: Carlos Garavito	Nombre: Diego Guevara
Cargo: Coordinador TI – Planeación	Cargo: Contratista-Planeación	Cargo: Director de Planeación
Dirección: Planeación	Subgerencia y/o Dirección: Planeación	Dirección: Planeación
Fecha: 28/01/2026	Fecha: 28/01/2026	Fecha: 28/01/2026

PLAN DE TRABAJO
Plan Estratégico de Tecnologías de la Información (PETI)

OBJETIVO	Validar, actualizar y formalizar el Plan Estratégico de Tecnologías de la Información (PETI), mediante su socialización con las Direcciones y Subgerencias con injerencia directa.
JUSTIFICACIÓN	La actualización del Plan Estratégico de Tecnologías de la Información (PETI) es necesaria para asegurar que el documento cuente con la validación de las Direcciones y Subgerencias con injerencia directa, garantizando su coherencia institucional, correcta aplicación y alineación con la planeación estratégica, en cumplimiento del Decreto 612 de 2018 y el Modelo Integrado de Planeación y Gestión (MIPG).
LIDER	Coordinador TIC
EQUIPO	Dirección de Planeación

Item	Acción	Responsable	Producto	Fecha inicio	Fecha Fin	26/1/2026 DIAS PARA EL CUMPLIMIENTO
1	Revisar el marco normativo vigente y los lineamientos institucionales aplicables a la Seguridad y Privacidad de la Información.	Coordinador TIC	Documento o matriz de revisión normativa	1/02/2026	28/02/2026	33
2	Consolidar y analizar los documentos institucionales existentes	Coordinador TIC	Inventario y diagnóstico documental	1/02/2026	31/03/2026	64
3	Definir el alcance, estructura y criterios de actualización de los componentes del documento, con base en el diagnóstico previo.	Coordinador TIC	Alcance y criterios de actualización definidos	1/03/2026	31/03/2026	64
4	Revisar y verificar los componentes del documento relacionados	Coordinador TIC	Componentes verificados y observaciones internas	1/04/2026	31/07/2026	186
5	Elaborar y/o actualizar los componentes del documento conforme a los lineamientos definidos	Coordinador TIC	Documento actualizado con control de cambios	1/05/2026	31/08/2026	217
6	Socializar el documento actualizado con las Direcciones y Subgerencias con injerencia directa, otorgando un plazo para el envío de observaciones y sugerencias.	Coordinador TIC	Correos de socialización y constancia de plazo otorgado	1/06/2026	30/09/2026	247
7	Consolidar, analizar e incorporar las observaciones y sugerencias recibidas por parte de las dependencias; en caso de no recibirse comentarios dentro del plazo establecido, se entenderá validado el contenido del documento.	Coordinador TIC	Matriz de observaciones y versión ajustada del documento	1/07/2026	31/10/2026	278
8	Remitir el documento consolidado a Gestión de Calidad para su revisión, verificación y control documental.	Coordinador TIC	Correo u oficio de remisión a Gestión de Calidad	1/10/2026	15/11/2026	293
9	Incorporar los ajustes solicitados por Gestión de Calidad, en caso de presentarse.	Coordinador TIC	Documento ajustado conforme a observaciones de Calidad	16/10/2026	15/11/2026	293
10	Gestionar la aprobación final y la publicación del documento en el repositorio institucional y, cuando aplique, en el componente de Transparencia.	Coordinador TIC	Constancia de publicación institucional y en Transparencia	1/11/2026	30/11/2026	308