TABLA DE CONTENIDO

INTRODUCCIÓN 2
OBJETIVO 3
OBJETIVO GENERAL 3
OBJETIVOS ESPECÍFICOS 3
ALCANCE 3
MARCO NORMATIVO Y DE REFERENCIA 4
PRINCIPIOS RECTORES DEL PETI 6
CONTEXTO ESTRATÉGICO INSTITUCIONAL 7
DIAGNÓSTICO DE TECNOLOGÍAS DE LA INFORMACIÓN 8
ALINEACIÓN CON EL PLAN ESTRATÉGICO INSTITUCIONAL (PEI) Y EL MIPG 9
OBJETIVOS ESTRATÉGICOS DEL PETI 10
ESTRATEGIAS DE TRANSFORMACIÓN DIGITAL 11
MODELO DE GOBIERNO DE TI 12
ARQUITECTURA EMPRESARIAL Y DE SISTEMAS DE INFORMACIÓN 13
GOBERNANZA Y TRES LÍNEAS DE DEFENSA 14
SEGURIDAD DIGITAL Y ARTICULACIÓN CON EL PESI Y EL MSPI 15
PLAN DE GESTIÓN DE RIESGOS TECNOLÓGICOS 16
PLAN DE RELACIÓN CON PROVEEDORES Y SERVICIOS TECNOLÓGICOS 17
PORTAFOLIO DE PROYECTOS ESTRATÉGICOS DE TI 2025–2027 18
PLAN DE IMPLEMENTACIÓN Y CRONOGRAMA 19
SOSTENIBILIDAD DIGITAL Y GESTIÓN AMBIENTAL DE TIC 21
INDICADORES DE SEGUIMIENTO Y EVALUACIÓN 21
ARTICULACIÓN CON AUDITORÍAS INTERNAS Y EXTERNAS 22
MECANISMOS DE VERIFICACIÓN, REVISIÓN Y ACTUALIZACIÓN DEL PETI 23
DOCUMENTOS INTERNOS RELACIONADOS 24
DISPOSICIONES FINALES 25

Introducción

El Plan Estratégico de Tecnologías de la Información (PETI) 2025–2027 de Empresas Públicas de Cundinamarca S.A. E.S.P. (EPC) constituye la hoja de ruta institucional para orientar la planeación, implementación y seguimiento de las iniciativas tecnológicas que respaldan la prestación de servicios públicos, la gestión administrativa y el fortalecimiento de la transformación digital.

Este documento se fundamenta en la normatividad vigente en materia de Gobierno Digital, en los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y en estándares internacionales de referencia en gestión de TI, seguridad digital y continuidad de negocio, el PETI integra la estrategia tecnológica con el Plan Estratégico Institucional (PEI), asegurando que las tecnologías de la información se conviertan en un habilitador clave para alcanzar los objetivos misionales de EPC.

El plan responde a las exigencias establecidas por el Decreto 338 de 2022, la Política de Gobierno Digital, el Modelo Integrado de Planeación y Gestión (MIPG) y los compromisos derivados del FURAG 2024, articulando las acciones tecnológicas con la gestión de riesgos, la seguridad y privacidad de la información, la transparencia y la confianza ciudadana.

El PETI 2025–2027 no se limita a la incorporación de nuevas tecnologías; también busca consolidar un modelo de gobernanza de TI, promover la sostenibilidad digital y garantizar que cada proyecto tecnológico tenga impacto directo en la eficiencia institucional, en la continuidad de los servicios y en la satisfacción de los usuarios y ciudadanos.

Así mismo, el documento reconoce la importancia de la articulación con el Plan Estratégico de Seguridad y Privacidad de la Información (PESI) y con el Modelo de Seguridad y Privacidad de la Información (MSPI), asegurando que la inversión en tecnologías esté acompañada de controles adecuados que garanticen resiliencia digital y cumplimiento normativo.

El PETI se convierte, en este sentido, en un instrumento de gestión estratégica que permite priorizar proyectos, asignar recursos, gestionar proveedores y coordinar esfuerzos interinstitucionales, consolidando a EPC como una entidad moderna,

confiable y orientada a la mejora continua en el marco de la transformación digital pública.

Objetivo

Objetivo General

Definir la estrategia de gestión y aprovechamiento de las tecnologías de la información en Empresas Públicas de Cundinamarca S.A. E.S.P. (EPC) para el periodo 2025–2027, asegurando que su implementación contribuya al cumplimiento de los objetivos institucionales, a la modernización tecnológica, a la prestación eficiente de los servicios públicos y al fortalecimiento de la transformación digital, en coherencia con la normatividad nacional y los lineamientos del MinTIC.

Objetivos Específicos

1. Integrar la planeación tecnológica con el Plan Estratégico Institucional (PEI), el Modelo Integrado de Planeación y Gestión (MIPG) y los compromisos derivados del FURAG, garantizando la alineación entre la estrategia digital y la gestión institucional.
2. Establecer un portafolio de proyectos estratégicos de TI que fortalezca la infraestructura tecnológica, impulse la interoperabilidad y promueva la innovación, bajo principios de eficiencia, sostenibilidad y seguridad digital.
3. Articular el PETI con el Plan Estratégico de Seguridad y Privacidad de la Información (PESI) y el Modelo de Seguridad y Privacidad de la Información (MSPI), asegurando que la adopción tecnológica esté acompañada de controles efectivos de gestión de riesgos, protección de datos personales y continuidad de negocio.

Alcance

El Plan Estratégico de Tecnologías de la Información (PETI) se aplica a todos los procesos, áreas, funcionarios, contratistas y proveedores que intervienen en la planeación, adquisición, implementación, uso y supervisión de tecnologías de la información dentro de la entidad, su cobertura es de carácter institucional y transversal, integrándose como parte del Sistema Integrado de Gestión.

El alcance del PETI comprende:

- Infraestructura tecnológica: incluye servidores, redes de telecomunicaciones, equipos de usuario final, sistemas de almacenamiento, plataformas en la nube y servicios de conectividad que soportan la operación institucional.
- Sistemas de información y aplicaciones: abarca las soluciones tecnológicas que gestionan procesos misionales, de apoyo y de control, incluyendo sistemas de facturación, gestión de usuarios, contratación, talento humano y archivo electrónico.
- Gestión de la información: contempla el ciclo de vida de la información institucional, desde su generación y almacenamiento hasta su publicación y disposición final, en cumplimiento de la Ley 594 de 2000 y la Ley 1712 de 2014.
- Procesos de contratación tecnológica: cubre la definición de requerimientos, inclusión de cláusulas de seguridad digital, seguimiento a proveedores y verificación del cumplimiento de acuerdos de nivel de servicio (SLA).
- Seguridad digital y gestión de riesgos: se integra con el PESI y el MSPI, garantizando que toda iniciativa tecnológica incluya medidas de protección de datos, gestión de incidentes, continuidad de negocio y resiliencia digital.
- Relación con partes interesadas: considera la interacción con ciudadanos, entes de control, administraciones municipales, Gobernación de Cundinamarca, prestadores de servicios públicos y demás actores identificados en la Matriz de Partes Interesadas – TI.

Este plan no abarca la ejecución operativa de cada proyecto en detalle, sino la definición estratégica que guiará la priorización, asignación de recursos, cronogramas y mecanismos de seguimiento. Las acciones específicas se desarrollarán a través de planes operativos anuales, portafolios de proyectos y contratos tecnológicos formalizados por la entidad.

Marco Normativo y de Referencia

El Plan Estratégico de Tecnologías de la Información (PETI) se sustenta en la normatividad nacional aplicable, en los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y en estándares internacionales de gestión de TI y seguridad digital.

Normatividad nacional aplicable

- Ley 1341 de 2009 y Ley 1978 de 2019: definen los principios de la sociedad de la información y el marco para el desarrollo del sector TIC en Colombia.
- Ley 1273 de 2009: tipifica los delitos informáticos y protege la información y los datos.
- Ley 1581 de 2012 y Decreto 1377 de 2013: regulan la protección de datos personales y los derechos de los titulares.
- Ley 1712 de 2014 y Decreto 103 de 2015: regulan el derecho de acceso a la información pública y la transparencia.
- Ley 594 de 2000: Ley General de Archivos, que regula la gestión documental y conservación de información.
- Decreto 1008 de 2018 y Decreto 338 de 2022: regulan la Política de Gobierno Digital, estableciendo lineamientos para la interoperabilidad, seguridad digital y servicios ciudadanos digitales.
- Decreto 2157 de 2017: reglamenta la gestión de continuidad de negocio y recuperación ante desastres.
- Conpes 3975 de 2019 y Conpes 4070 de 2021: orientan la política de transformación digital e inteligencia artificial en Colombia.
- Conpes 3995 de 2020 y la Estrategia Nacional de Confianza y Seguridad Digital 2025–2027: establecen la hoja de ruta para fortalecer la seguridad digital y la confianza en los servicios tecnológicos del Estado.

Normatividad institucional de referencia

- Plan Estratégico Institucional (PEI) 2024–2028.
- Política General de Seguridad de la Información – EPC 2025.
- Plan Estratégico de Seguridad y Privacidad de la Información (PESI) 2025.
- Modelo de Seguridad y Privacidad de la Información (MSPI) 2025.
- Mapa de Riesgos de Gestión y de TI.
- Normograma de Gestión de TI.
- Inventario y Clasificación de Activos de Información.

Marcos y estándares internacionales de referencia

- ISO/IEC 27001:2022: sistema de gestión de seguridad de la información.
- ISO/IEC 27005: gestión de riesgos en seguridad de la información.
- ISO/IEC 27017 y 27018: seguridad y privacidad en servicios en la nube.
- ISO/IEC 27031:2025: continuidad de negocio en entornos de TI.
- ISO 22301:2019: gestión de continuidad del negocio.
- ISO 31000:2018: gestión del riesgo.
- COBIT 2019: gobernanza y gestión de TI.
- ITIL v4: buenas prácticas en gestión de servicios de TI.

- NIST Cybersecurity Framework 2.0: marco de gestión de riesgos en ciberseguridad.

Este marco normativo y de referencia garantiza que el PETI se ejecute en conformidad con la legislación colombiana, bajo lineamientos claros del MinTIC y con respaldo de estándares internacionales, asegurando una gestión tecnológica integral, trazable y alineada con la transformación digital del Estado.

Principios Rectores del PETI

El Plan Estratégico de Tecnologías de la Información (PETI) se orienta bajo un conjunto de principios que guían la planeación, implementación y seguimiento de las iniciativas tecnológicas en Empresas Públicas de Cundinamarca S.A. E.S.P. (EPC). Estos principios aseguran que las decisiones en materia tecnológica estén alineadas con los objetivos institucionales, la normativa vigente y las expectativas de los ciudadanos.

El primer principio es la eficiencia, que implica utilizar los recursos tecnológicos de manera óptima para mejorar los procesos internos y garantizar la sostenibilidad financiera. Las inversiones en TI deben generar valor agregado para la entidad y traducirse en mejores servicios para la ciudadanía.

El segundo principio es la innovación, entendida como la incorporación de soluciones digitales modernas que fortalezcan la gestión institucional y promuevan la transformación digital. El PETI fomenta la exploración de tecnologías emergentes y su aplicación responsable en los procesos de EPC.

La seguridad digital constituye un eje central. Todas las iniciativas del PETI deben garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información (CIDP), articulándose con el Plan Estratégico de Seguridad y Privacidad de la Información (PESI) y el Modelo de Seguridad y Privacidad de la Información (MSPI).

La sostenibilidad también orienta el plan. La gestión tecnológica debe incorporar prácticas responsables con el medio ambiente, como la reducción del consumo de papel, la disposición adecuada de residuos electrónicos (RAEE) y el uso eficiente de

la infraestructura tecnológica, contribuyendo a los Objetivos de Desarrollo Sostenible (ODS).

Otro principio rector es la interoperabilidad, que asegura la integración entre sistemas internos y la conexión con plataformas del Estado, garantizando la coherencia de la información y la eficiencia en los trámites digitales.

Finalmente, la transparencia y confianza ciudadana guían la gestión tecnológica, asegurando que los servicios digitales cumplan con la Ley 1712 de 2014 de Transparencia y Acceso a la Información Pública, y que cada acción en el marco del PETI fortalezca la relación de confianza entre EPC y la comunidad.

Estos principios rectores permiten que el PETI se consolide como un instrumento estratégico, garantizando que la gestión tecnológica esté orientada a la excelencia institucional, la seguridad digital, la sostenibilidad y la confianza ciudadana.

Contexto Estratégico Institucional

EPC, como empresa prestadora de servicios públicos domiciliarios, gestiona información sensible de carácter técnico, administrativo, financiero y ciudadano, que requiere altos niveles de protección, disponibilidad y trazabilidad, en este contexto, las tecnologías de la información se convierten en un habilitador estratégico para garantizar eficiencia operativa, sostenibilidad, innovación y confianza ciudadana.

El PETI se articula con el Plan Estratégico Institucional 2024–2028, asegurando que las iniciativas tecnológicas se alineen con la misión, visión y objetivos institucionales, asimismo, se integra al Modelo Integrado de Planeación y Gestión (MIPG), garantizando que la planeación digital contribuya al fortalecimiento de la gestión pública y al cumplimiento de los compromisos de modernización del Estado.

El contexto normativo y de control también impacta directamente el PETI, los compromisos derivados del FURAG, las observaciones de la Revisoría Fiscal y los resultados de las Auditorías Internas 2025 constituyen insumos fundamentales para orientar las prioridades de inversión y gestión tecnológica.

En paralelo, el plan reconoce la necesidad de mantener coherencia con los instrumentos específicos de seguridad digital: el Plan Estratégico de Seguridad y

Privacidad de la Información (PESI) y el Modelo de Seguridad y Privacidad de la Información (MSPI), estos documentos establecen los lineamientos de ciberseguridad, gestión de riesgos y protección de datos personales, que son transversales a la gestión tecnológica definida en el PETI.

Finalmente, el PETI incorpora los retos de la transformación digital, impulsada por la Política de Gobierno Digital (Decreto 338 de 2022), los Conpes 4070 de 2021 y 3995 de 2020, y la Estrategia Nacional de Confianza y Seguridad Digital 2025–2027, garantizando que la modernización tecnológica de EPC no solo responda a necesidades internas, sino también a los compromisos nacionales en materia de digitalización, interoperabilidad, transparencia y sostenibilidad.

De esta manera, el PETI se configura como un instrumento estratégico que vincula la gestión tecnológica con la planeación institucional, los compromisos de control y la política pública nacional, consolidando a EPC como una entidad moderna, confiable y resiliente en el ecosistema digital.

Diagnóstico de Tecnologías de la Información

El diagnóstico constituye la base para la formulación del Plan, a través de este ejercicio se identificaron fortalezas, debilidades, oportunidades y riesgos en el ecosistema tecnológico institucional, integrando los resultados de auditorías internas, autodiagnósticos, revisiones de control y observaciones de entes externos.

Fortalezas identificadas

EPC cuenta con un inventario consolidado de activos tecnológicos y de información, lo cual permite visibilizar los recursos disponibles y priorizar su protección, se han implementado controles básicos de seguridad digital, tales como antivirus corporativo, firewall perimetral, respaldos periódicos y autenticación en los sistemas principales, además, se dispone de una política de seguridad de la información actualizada y de un PESI articulado con el MSPI, lo que evidencia un avance significativo en la formalización de la gestión tecnológica.

Debilidades actuales

Pese a los avances, persisten brechas importantes. La infraestructura tecnológica presenta limitaciones en escalabilidad y redundancia, lo que impacta la continuidad

de los servicios, el nivel de automatización de procesos es aún bajo y la interoperabilidad entre sistemas requiere fortalecimiento, la capacitación en seguridad digital no ha alcanzado cobertura total entre funcionarios y contratistas, asimismo, la supervisión de proveedores tecnológicos aún no es sistemática, lo que representa riesgos de cumplimiento contractual y de continuidad de los servicios.

Oportunidades de mejora

El marco normativo vigente, en especial la Política de Gobierno Digital (Decreto 338 de 2022), el Conpes 4070 de 2021 y la Estrategia Nacional de Confianza y Seguridad Digital 2025–2027, ofrecen lineamientos y herramientas para fortalecer la transformación digital en EPC, existen oportunidades para migrar progresivamente a servicios en la nube con estándares de seguridad internacionales, implementar soluciones de monitoreo centralizado de eventos de seguridad (SIEM), y avanzar en la automatización de trámites ciudadanos con un enfoque de eficiencia y transparencia.

Riesgos y amenazas

El entorno tecnológico enfrenta riesgos derivados de ciberataques, fallas de infraestructura, desastres naturales y brechas de seguridad asociadas al error humano, el Mapa de Riesgos de TI identifica como prioritarios los riesgos relacionados con pérdida de disponibilidad de servicios críticos, incidentes de seguridad de la información y deficiencias en la supervisión de terceros, estos riesgos requieren atención prioritaria a través de planes de tratamiento, continuidad de negocio y fortalecimiento de la cultura digital institucional.

El diagnóstico permite concluir que EPC cuenta con una base organizacional sólida, pero requiere acelerar la modernización tecnológica y la consolidación de su modelo de seguridad digital, con el fin de responder a las exigencias normativas, mejorar la eficiencia operativa y garantizar la confianza ciudadana en los servicios públicos que presta.

Alineación con el Plan Estratégico Institucional (PEI) y el MIPG

El PETI se articula directamente con el Plan Estratégico Institucional (PEI) 2024–2028, asegurando que las iniciativas tecnológicas apoyen de manera efectiva los

objetivos misionales y las líneas estratégicas definidas por la organización, esta alineación garantiza que las inversiones en TI no se gestionen de forma aislada, sino como un componente integrado a la planeación corporativa.

Asimismo, el plan se enmarca en el Modelo Integrado de Planeación y Gestión (MIPG), el cual promueve la eficiencia administrativa, la transparencia y la mejora continua en la gestión pública, en este contexto, la gestión tecnológica se convierte en un habilitador transversal que permite cumplir con las dimensiones del modelo, en especial aquellas relacionadas con la gestión del conocimiento, la innovación, la seguridad digital y la atención al ciudadano.

Los compromisos derivados del FURAG, las observaciones de la Revisoría Fiscal y los resultados de las auditorías internas también han sido incorporados en la planeación estratégica de TI, asegurando que los proyectos definidos respondan no solo a las necesidades operativas, sino también a los requerimientos de control y supervisión institucional.

De esta forma, el PETI se consolida como el puente entre la planeación institucional y la estrategia tecnológica, asegurando coherencia, trazabilidad y sostenibilidad en la gestión de las tecnologías de la información.

Objetivos Estratégicos del PETI

Los objetivos estratégicos de este plan se orientan a consolidar la tecnología como un habilitador de la gestión institucional, la seguridad digital y la confianza ciudadana, no se trata únicamente de adquirir o renovar infraestructura, sino de transformar la manera en que los procesos y servicios se soportan en soluciones digitales confiables, seguras y sostenibles.

El primer objetivo busca garantizar que la planeación tecnológica esté alineada con la estrategia institucional, de modo que cada proyecto, inversión o iniciativa en TI aporte valor directo al cumplimiento de la misión y a los compromisos definidos en el PEI, esto implica priorizar recursos en función de su impacto y asegurar la trazabilidad entre la estrategia corporativa y los resultados en materia tecnológica.

Un segundo objetivo se centra en fortalecer la infraestructura y los sistemas de información para asegurar continuidad, escalabilidad y capacidad de respuesta frente a las crecientes demandas de los procesos internos y de los ciudadanos, aquí

se incluye la adopción de servicios en la nube bajo estándares de seguridad, la modernización de plataformas existentes y la integración de sistemas para mejorar la interoperabilidad.

El tercer objetivo estratégico consiste en consolidar la seguridad digital como principio transversal, integrando la gestión de riesgos, la protección de datos personales y la respuesta ante incidentes en cada iniciativa tecnológica. Este enfoque asegura que los avances en transformación digital se desarrollen en un entorno de confianza y resiliencia.

Finalmente, se plantea como objetivo impulsar una cultura organizacional orientada a la innovación y el uso responsable de las tecnologías, esto se traduce en programas de capacitación, campañas de sensibilización y proyectos que promuevan la sostenibilidad digital, reduciendo la brecha tecnológica y fortaleciendo la participación ciudadana en entornos digitales seguros y transparentes.

En conjunto, estos objetivos garantizan que la gestión de TI trascienda la perspectiva operativa y se convierta en un instrumento estratégico para la modernización institucional y la mejora continua.

Estrategias de Transformación Digital

La transformación digital en la entidad se concibe como un proceso integral que no solo incorpora nuevas herramientas tecnológicas, sino que redefine la forma en que se gestionan los procesos, se prestan los servicios y se relaciona la organización con los ciudadanos y partes interesadas.

La primera estrategia está orientada a la modernización de la infraestructura tecnológica, garantizando que los sistemas y plataformas institucionales cuenten con la capacidad, seguridad y flexibilidad necesarias para responder a las demandas actuales y futuras, esto incluye la actualización de servidores y redes, la adopción progresiva de servicios en la nube bajo estándares internacionales y la implementación de soluciones de respaldo y continuidad que reduzcan la vulnerabilidad frente a fallas o incidentes.

Una segunda estrategia se centra en la automatización y digitalización de procesos, con el objetivo de mejorar la eficiencia administrativa y reducir los tiempos de

respuesta en la prestación de servicios. La implementación de sistemas integrados y la interoperabilidad entre plataformas permitirá disminuir la duplicidad de esfuerzos y facilitar la trazabilidad de la información institucional.

La tercera estrategia consiste en el fortalecimiento de la seguridad digital, articulando el PETI con el PESI y el MSPI, cada proyecto tecnológico debe integrar controles de seguridad desde su diseño, aplicando prácticas de gestión de riesgos, protección de datos personales y mecanismos de monitoreo que garanticen la resiliencia frente a ciber amenazas.

Otro eje estratégico es la orientación al ciudadano, que implica diseñar y consolidar servicios digitales accesibles, confiables y transparentes, esto no solo se traduce en trámites en línea más ágiles, sino también en una mayor participación de los usuarios a través de plataformas que promuevan la confianza y la transparencia en la gestión pública.

Finalmente, la sostenibilidad digital constituye una línea prioritaria. El uso eficiente de los recursos tecnológicos, la reducción del consumo de papel, la gestión adecuada de residuos electrónicos (RAEE) y la promoción de prácticas de teletrabajo y gobierno en la nube se convierten en componentes esenciales de una estrategia responsable con el medio ambiente y alineada con los Objetivos de Desarrollo Sostenible (ODS).

Estas estrategias, integradas en el horizonte del plan, permiten que la gestión de TI se proyecte como un pilar de la transformación institucional, garantizando innovación, eficiencia, seguridad y sostenibilidad.

Modelo de Gobierno de TI

El gobierno de TI en la entidad se concibe como el conjunto de estructuras, procesos y mecanismos de control que permiten asegurar que las tecnologías de la información se gestionen de manera alineada con la estrategia institucional y generen valor sostenible para la organización y la ciudadanía.

La responsabilidad principal recae en la alta dirección, que establece las prioridades estratégicas y aprueba las inversiones tecnológicas en coherencia con los objetivos del PEI. El Comité de Gestión y Desempeño Institucional actúa como instancia de

decisión y supervisión, revisando periódicamente los avances del PETI, validando proyectos estratégicos y garantizando que la gestión de TI esté alineada con el MIPG y con los compromisos derivados de auditorías y entes de control.

El Coordinador de TI asume el rol de líder operativo y técnico del gobierno de TI, articulando la ejecución del plan con las demás áreas de la organización, entre sus responsabilidades se encuentran la priorización de iniciativas, la supervisión de proveedores, la gestión de riesgos tecnológicos y la integración del PETI con el PESI y el MSPI.

La Mesa de Ayuda (MDA) se constituye en el soporte operativo que implementa los controles técnicos, gestiona incidentes y brinda acompañamiento a los usuarios, asegurando que las decisiones estratégicas se reflejen en una operación tecnológica eficiente y segura.

La rendición de cuentas en materia de TI se materializa a través de informes de avance, que incluyen el estado de los proyectos estratégicos, los indicadores de desempeño y el cumplimiento de los compromisos derivados de auditorías, revisiones de control interno y reportes en el FURAG.

El modelo de gobierno también incorpora la supervisión de proveedores tecnológicos, asegurando que los contratos incluyan cláusulas de seguridad digital, niveles de servicio (SLA) verificables y compromisos de confidencialidad y continuidad.

Este esquema de gobernanza asegura que la gestión tecnológica no dependa únicamente de soluciones técnicas, sino que se integre como parte del ciclo de planeación estratégica, con reglas claras de responsabilidad, control y transparencia.

Arquitectura Empresarial y de Sistemas de Información

La arquitectura empresarial constituye el marco que permite alinear los procesos institucionales con las tecnologías de la información, garantizando que la evolución de las plataformas digitales responda a las necesidades misionales, administrativas y de control de la entidad.

En este sentido, la arquitectura de sistemas de información se basa en principios de interoperabilidad, integración y sostenibilidad, de acuerdo con los lineamientos de la Política de Gobierno Digital y los estándares definidos por MinTIC, el objetivo es reducir la fragmentación tecnológica, optimizar el uso de recursos y asegurar que los sistemas funcionen de manera articulada, facilitando la trazabilidad de la información y la toma de decisiones.

Actualmente, los sistemas de información cubren procesos clave como gestión de usuarios, facturación, contratación, talento humano y archivo electrónico, sin embargo, se identifican brechas en automatización e interoperabilidad, lo que hace necesario avanzar en la consolidación de una arquitectura que soporte la modernización de los procesos y la prestación de servicios ciudadanos digitales.

El plan establece la adopción gradual de plataformas integradas, el fortalecimiento de soluciones existentes y la implementación de servicios en la nube bajo estándares internacionales de seguridad (ISO/IEC 27017 y 27018), asimismo, se promoverá el uso de herramientas de análisis de datos (Big Data, BI y analítica predictiva) que permitan generar valor agregado a partir de la información institucional, mejorando la eficiencia y anticipando necesidades ciudadanas.

La arquitectura empresarial también contempla la estandarización de procesos de desarrollo y adquisición de software, aplicando buenas prácticas como ITIL v4 para la gestión de servicios y COBIT 2019 para la gobernanza de TI, con ello, se busca garantizar que cada nueva solución tecnológica sea interoperable, segura y sostenible en el tiempo.

De esta manera, la arquitectura empresarial y de sistemas de información se convierte en el eje que conecta la planeación institucional con la transformación digital, permitiendo que los proyectos estratégicos definidos en el PETI evolucionen en un marco de coherencia, control y valor agregado para la entidad y la ciudadanía.

Gobernanza y Tres Líneas de Defensa

La gobernanza se sustenta en el marco del Modelo Integrado de Planeación y Gestión (MIPG), que establece un enfoque de control y supervisión basado en el esquema de tres líneas de defensa, este modelo garantiza claridad en los roles,

independencia en la supervisión y efectividad en la gestión de los riesgos tecnológicos y de seguridad digital.

- **Primera línea de defensa:** conformada por el Coordinador de TI y la Mesa de Ayuda (MDA). Son responsables de la gestión operativa del PETI, ejecutando proyectos, implementando controles técnicos, administrando la infraestructura tecnológica y atendiendo incidentes, en esta línea se asegura el cumplimiento cotidiano de los procedimientos y controles establecidos.
- **Segunda línea de defensa**: integrada por las áreas de Planeación Estratégica, Jurídica, Contratación y Gestión de Calidad, que realizan la supervisión y monitoreo del cumplimiento de políticas, normas y lineamientos institucionales, esta línea evalúa la alineación de las acciones del PETI con el PEI, el PESI, el MSPI y con las obligaciones normativas vigentes, generando directrices para fortalecer la gestión tecnológica.
- **Tercera línea de defensa:** corresponde a la Oficina de Control Interno o quien haga sus veces, encargada de brindar aseguramiento independiente y objetivo sobre la eficacia de la implementación del PETI y del sistema de control interno, sus auditorías permiten identificar brechas, emitir recomendaciones y verificar la efectividad de los planes de mejora, alimentando los procesos de retroalimentación y transparencia institucional.

Este esquema de gobernanza asegura que la implementación del PETI se realice con un enfoque integral, equilibrando la gestión operativa, la supervisión normativa y el aseguramiento independiente, lo que contribuye a la transparencia y confiabilidad en la administración de los recursos tecnológicos.

Seguridad Digital y Articulación con el PESI y el MSPI

La seguridad digital es un eje transversal del presente plan, concebida no como un conjunto de acciones aisladas, sino como un componente estructural que acompaña todas las iniciativas tecnológicas de la entidad, su gestión se orienta por los lineamientos del Plan Estratégico de Seguridad y Privacidad de la Información (PESI) y del Modelo de Seguridad y Privacidad de la Información (MSPI), documentos que definen los principios, roles, controles y mecanismos de seguimiento para garantizar la protección integral de los activos de información.

Cada proyecto definido en el PETI deberá incorporar desde su fase de diseño los criterios de confidencialidad, integridad, disponibilidad y privacidad (CIDP), asegurando que la innovación y la modernización tecnológica se desarrollen en un entorno de confianza, esto incluye la definición de controles de acceso, esquemas de autenticación robusta, monitoreo permanente de la infraestructura y gestión de incidentes bajo procedimientos institucionales establecidos.

La articulación con el PESI permite priorizar las acciones en materia de seguridad y privacidad, de modo que las inversiones en TI estén acompañadas de mecanismos de prevención, detección y respuesta. A su vez, el MSPI asegura la trazabilidad y gobernanza del sistema, integrando la seguridad digital a los ciclos de planeación, ejecución y mejora continúa definidos en el MIPG.

El PETI también incorpora la supervisión de la seguridad en la contratación tecnológica y en la relación con proveedores, garantizando que cada contrato incluya cláusulas específicas de protección de datos personales, continuidad de negocio y cumplimiento de estándares internacionales como ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 y ISO/IEC 27031.

De esta manera, la seguridad digital no solo respalda la operación tecnológica de la entidad, sino que fortalece la confianza de los ciudadanos en los servicios digitales ofrecidos, al tiempo que asegura el cumplimiento de la normativa nacional en materia de protección de datos, transparencia y Gobierno Digital.

Plan de Gestión de Riesgos Tecnológicos

La gestión de riesgos tecnológicos constituye un componente esencial para garantizar la continuidad, seguridad y eficiencia de los procesos institucionales. El plan parte de la identificación y valoración de riesgos asociados al uso, administración y evolución de las tecnologías de la información, integrando este análisis al Mapa de Riesgos de TI y al Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

El enfoque metodológico adoptado se alinea con la ISO/IEC 27005 y la ISO 31000:2018, asegurando un proceso sistemático que comprende la identificación, análisis, evaluación, tratamiento y monitoreo de los riesgos, la valoración se realiza

considerando tanto la probabilidad de ocurrencia como el impacto en los procesos misionales, administrativos y de atención al ciudadano.

Dentro de los riesgos más relevantes identificados se encuentran: la indisponibilidad de servicios críticos por fallas en la infraestructura, incidentes de ciberseguridad que afecten datos sensibles, deficiencias en la interoperabilidad de sistemas, incumplimientos contractuales por parte de proveedores tecnológicos y vulnerabilidades asociadas a la falta de capacitación de usuarios.

El plan establece medidas de tratamiento que incluyen la mitigación mediante controles técnicos y organizacionales, la transferencia a terceros a través de contratos o seguros, la aceptación en casos de riesgos residuales de bajo impacto y la eliminación cuando el riesgo pueda suprimirse mediante la descontinuación de activos obsoletos.

El seguimiento de los riesgos se realizará generando informes consolidados que serán presentados al Comité de Gestión y Desempeño Institucional, adicionalmente, los resultados alimentarán el ciclo de mejora continua del PETI y se articularán con los reportes en el FURAG y las auditorías internas.

De esta manera, el plan de gestión de riesgos tecnológicos asegura que las iniciativas contempladas en el PETI se desarrollen bajo un marco de control, resiliencia y confianza, reduciendo vulnerabilidades y fortaleciendo la capacidad institucional frente a incidentes o contingencias.

Plan de Relación con Proveedores y Servicios Tecnológicos

La relación con proveedores de bienes y servicios tecnológicos constituye un factor determinante para garantizar la eficiencia, seguridad y continuidad de las operaciones institucionales. En este marco, la gestión de proveedores se integra como un componente estratégico del PETI, asegurando que cada contratación tecnológica se alinee con los principios de transparencia, calidad y protección de la información.

Los contratos de TI deberán incorporar cláusulas de seguridad digital que aseguren la confidencialidad de la información institucional, el cumplimiento de la Ley 1581 de 2012 en materia de protección de datos personales, la disponibilidad de los

servicios y la responsabilidad frente a incidentes o fallas que puedan afectar la operación, asimismo, se establecerán acuerdos de nivel de servicio (SLA) que definan métricas claras de desempeño, tiempos de respuesta y mecanismos de verificación.

El Coordinador de TI será responsable de la supervisión técnica de los contratos, verificando el cumplimiento de las obligaciones en materia de seguridad, continuidad y calidad de servicio, la Mesa de Ayuda (MDA) apoyará en la gestión operativa, reportando desviaciones y generando los registros necesarios para evidenciar la trazabilidad del proceso.

El plan también contempla la evaluación periódica de proveedores, que se realizará a través de auditorías, reportes de cumplimiento y revisiones conjuntas. En casos de incumplimiento, se aplicarán las medidas establecidas en los contratos, incluyendo sanciones, terminaciones anticipadas o la inclusión en listas restrictivas.

En lo que respecta a servicios en la nube, se adoptarán los lineamientos de las normas ISO/IEC 27017 y ISO/IEC 27018, asegurando que los proveedores garanticen la localización segura de los datos, la protección de la privacidad y la portabilidad de la información en caso de migración o finalización del contrato.

Este plan fortalece la gobernanza tecnológica de la entidad, asegurando que la tercerización de servicios no implique pérdida de control, sino que se convierta en una oportunidad para mejorar la capacidad tecnológica, mantener altos niveles de seguridad y garantizar la continuidad de los servicios públicos.

Portafolio de Proyectos Estratégicos de TI 2025–2027

El portafolio de proyectos estratégicos constituye el núcleo operativo del PETI, al traducir las directrices estratégicas en iniciativas concretas que fortalecen la infraestructura tecnológica, modernizan los procesos y garantizan la prestación segura y eficiente de los servicios, este portafolio se construyó a partir del diagnóstico institucional, las observaciones de auditorías, los compromisos derivados del FURAG y las prioridades establecidas en el Plan Estratégico Institucional.

Los proyectos se priorizan con base en tres criterios principales: su aporte directo a la misión institucional, el nivel de criticidad de los procesos que soportan y el impacto

en la satisfacción de los ciudadanos y usuarios, adicionalmente, se consideran los riesgos asociados a la no ejecución, la disponibilidad de recursos y la alineación con el PESI y el MSPI.

Dentro de las líneas estratégicas del portafolio se destacan, en primer lugar, los proyectos de modernización de infraestructura tecnológica, que incluyen la actualización de servidores, la ampliación de la capacidad de almacenamiento, la implementación de redes más seguras y la consolidación de centros de datos con esquemas de redundancia.

En segundo lugar, se priorizan los proyectos de automatización e interoperabilidad de procesos, cuyo propósito es reducir los tiempos de respuesta administrativa, mejorar la trazabilidad de la información y facilitar la integración con las plataformas del Estado bajo la Política de Gobierno Digital.

Una tercera línea corresponde a los proyectos de seguridad digital y gestión de riesgos, que abarcan la implementación de sistemas de monitoreo de eventos de seguridad (SIEM), programas de capacitación en ciberseguridad, fortalecimiento de la protección de datos personales y actualización de los planes de continuidad y recuperación ante desastres.

Finalmente, el portafolio incluye proyectos orientados a la sostenibilidad digital y la innovación, tales como la migración progresiva a servicios en la nube, la adopción de herramientas de analítica de datos, la digitalización de trámites ciudadanos y la gestión responsable de residuos electrónicos (RAEE).

El portafolio no es un listado rígido, sino un instrumento dinámico que se revisará y actualizará de manera anual, en coherencia con la planeación estratégica y los resultados de auditorías y evaluaciones, de esta manera, se asegura que cada proyecto contribuya de manera efectiva a la modernización institucional y al fortalecimiento de la confianza ciudadana.

Plan de Implementación y Cronograma

La implementación del PETI requiere un esquema organizado que permita ejecutar los proyectos estratégicos de manera ordenada, garantizando el uso eficiente de los recursos y el cumplimiento de los plazos establecidos, el cronograma se concibe

como un instrumento dinámico, sujeto a ajustes según la disponibilidad presupuestal, la priorización de iniciativas y los resultados de auditorías o revisiones institucionales.

La ejecución se desarrollará en tres fases principales, la primera corresponde a la planificación y preparación, en la que se definen los proyectos a ejecutar en el corto plazo, se asignan los responsables y se gestionan los recursos necesarios para su puesta en marcha, esta fase incluye la estructuración de los proyectos de modernización de infraestructura crítica y el fortalecimiento de la seguridad digital, considerados prioritarios por su impacto en la operación y continuidad de los servicios.

La segunda fase corresponde a la implementación progresiva, donde se despliegan las iniciativas priorizadas en el portafolio, garantizando su articulación con el PESI, el MSPI y el Plan Estratégico Institucional, durante esta fase se ejecutarán proyectos de automatización de procesos, interoperabilidad con plataformas estatales, adopción de servicios en la nube y despliegue de programas de capacitación en seguridad digital.

La tercera fase es la de consolidación y mejora continua, en la cual se evalúan los resultados alcanzados, se integran las lecciones aprendidas y se ajustan los proyectos en curso para asegurar su sostenibilidad. En esta etapa también se incluirán nuevos proyectos derivados de necesidades emergentes, cambios normativos o innovaciones tecnológicas relevantes.

El cronograma general del PETI abarca el periodo 2025–2027, con revisiones anuales que permitirán ajustar tiempos y prioridades, el Coordinador de TI será el encargado de liderar la implementación, apoyado por la Mesa de Ayuda (MDA) en la ejecución operativa, los informes de avance se presentarán de manera trimestral al Comité de Gestión y Desempeño Institucional, garantizando la trazabilidad y el control de cada iniciativa.

Este enfoque permite que la implementación no sea una ejecución fragmentada de proyectos, sino un proceso planificado y coherente que asegura continuidad, resiliencia y generación de valor en cada etapa del PETI.

Sostenibilidad Digital y Gestión Ambiental de TIC

El PETI incorpora el principio de sostenibilidad digital, reconociendo que la gestión tecnológica debe contribuir no solo a la eficiencia institucional, sino también a la protección del medio ambiente y a la mitigación del cambio climático.

Las acciones estratégicas de este componente incluyen:

- **Gestión de residuos electrónicos (RAEE):** establecimiento de protocolos para la disposición final y reciclaje de equipos de cómputo, periféricos y dispositivos tecnológicos en cumplimiento de la normatividad ambiental y lineamientos del Ministerio de Ambiente y Desarrollo Sostenible.
- **Eficiencia energética en infraestructura tecnológica:** adopción de prácticas como la virtualización de servidores, migración a servicios en la nube certificados y adquisición de equipos de bajo consumo energético.
- **Digitalización de procesos institucionales:** implementación de trámites electrónicos, uso de la firma digital, sistemas de gestión documental y plataformas de colaboración en línea que reduzcan el consumo de papel y recursos físicos.
- **Compras sostenibles en TIC:** inclusión de criterios ambientales en la adquisición de hardware, software y servicios, privilegiando proveedores que cumplan con estándares de ecoeficiencia y certificaciones ambientales.
- **Sensibilización institucional:** desarrollo de programas de capacitación para funcionarios y contratistas en el uso racional de recursos tecnológicos y en el adecuado manejo de equipos obsoletos.

Este enfoque asegura que el PETI contribuya a los Objetivos de Desarrollo Sostenible (ODS), en especial al ODS 12 (producción y consumo responsables) y al ODS 13 (acción por el clima), fortaleciendo la responsabilidad social y ambiental de EPC.

Indicadores de Seguimiento y Evaluación

El seguimiento y evaluación del PETI se fundamenta en un sistema de indicadores que permite medir la efectividad de los proyectos estratégicos, verificar el cumplimiento de los objetivos planteados y garantizar la mejora continua de la gestión tecnológica, estos indicadores se estructuran en tres dimensiones: estratégica, operativa y cultural.

En el nivel estratégico, los indicadores permiten evaluar el grado de avance global del plan, la alineación con el Plan Estratégico Institucional y el cumplimiento de los compromisos derivados del MIPG y del FURAG, algunos de los más relevantes son el porcentaje de ejecución del portafolio de proyectos estratégicos, el nivel de madurez alcanzado en la gestión de TI y el grado de integración del PETI con otros instrumentos como el PESI y el MSPI.

En el nivel operativo, los indicadores miden la eficiencia de la gestión de TI y el impacto directo en la prestación de los servicios, aquí se incluyen métricas como el porcentaje de sistemas críticos con pruebas exitosas de continuidad y recuperación, el tiempo promedio de atención de incidentes tecnológicos, el porcentaje de proveedores con cumplimiento de SLA y el nivel de interoperabilidad alcanzado entre sistemas institucionales y plataformas del Estado.

En el nivel cultural y de talento humano, los indicadores reflejan el compromiso de funcionarios y contratistas con la transformación digital y la seguridad de la información, se destacan el porcentaje de personal capacitado en competencias digitales y seguridad, el número de campañas de sensibilización realizadas y el nivel de participación en iniciativas de innovación tecnológica.

El monitoreo de los indicadores se realizará con reportes presentados al Comité de Gestión y Desempeño Institucional, los resultados también serán insumo para el reporte en el FURAG, las auditorías internas y las revisiones anuales del PETI.

De esta manera, los indicadores se convierten en una herramienta clave no solo para verificar resultados, sino también para orientar decisiones estratégicas, identificar brechas y asegurar que la gestión tecnológica genere valor para la entidad y para la ciudadanía.

Articulación con Auditorías Internas y Externas

El seguimiento y evaluación del PETI requiere de mecanismos de control confiables que permitan verificar el cumplimiento de los objetivos estratégicos y la implementación efectiva de los proyectos tecnológicos. Para tal fin, el plan se articula con las auditorías internas y externas, asegurando trazabilidad, independencia y mejora continua.

- Auditorías internas: realizadas por la Oficina de Control Interno, permiten evaluar el grado de cumplimiento del PETI, la eficacia de los controles

aplicados y la coherencia con el MSPI, PESI y la Política General de Seguridad de la Información, estas auditorías alimentan los procesos de gestión de riesgos y los planes de mejora institucional.

- Auditorías externas: incluyen las revisiones adelantadas por la Revisoría Fiscal, entes de control sectoriales y organismos como la Superintendencia de Servicios Públicos y la SIC, que verifican la conformidad normativa, la correcta ejecución contractual y la adecuada administración de los recursos tecnológicos.
- FURAG y reportes nacionales: los avances y resultados del PETI se reflejan en el Formulario Único de Reporte de Avances de la Gestión (FURAG), lo que permite dar cumplimiento a los lineamientos de la Función Pública en materia de Gobierno Digital y seguridad de la información.
- Revisión por la dirección: el Comité de Gestión y Desempeño Institucional analiza los informes de auditoría y seguimiento, estableciendo decisiones correctivas y preventivas para garantizar la mejora continua.

Con esta articulación, el PETI se convierte en un instrumento verificable, auditable y transparente, asegurando que los avances en transformación digital y gestión tecnológica estén alineados con los estándares de gobernanza pública y con los compromisos de transparencia y rendición de cuentas de EPC.

Mecanismos de Verificación, Revisión y Actualización del PETI

El PETI es un instrumento dinámico que debe ajustarse a los cambios normativos, tecnológicos y organizacionales, para ello, se establecen mecanismos de verificación y revisión que aseguran su vigencia, pertinencia y efectividad en el tiempo.

La verificación se realizará mediante informes de avance presentados al Comité de Gestión y Desempeño Institucional, estos informes incluirán el estado de ejecución de los proyectos, los resultados de los indicadores de seguimiento y las observaciones derivadas de auditorías internas y de control externo, el objetivo de esta verificación es asegurar la trazabilidad y el cumplimiento de los compromisos establecidos.

La revisión del PETI será de carácter anual, articulándose con el ciclo de planeación institucional y con la evaluación de resultados en el FURAG, esta revisión permitirá identificar desviaciones, actualizar prioridades y proponer nuevos proyectos

estratégicos, el Coordinador de TI liderará el proceso, con apoyo de la Mesa de Ayuda en la recolección de información y de las áreas misionales y de apoyo en la validación de avances.

La actualización extraordinaria del plan se llevará a cabo en casos de cambios normativos relevantes, emergencias tecnológicas, incidentes de seguridad de alto impacto, transformaciones en la infraestructura institucional o recomendaciones de entes de control que así lo exijan. en tales escenarios, el documento será ajustado y aprobado por el Comité de Gestión y Desempeño Institucional antes de su publicación oficial.

La validación final de cada actualización corresponderá al Grupo de Gestión de Calidad, que verificará la coherencia del documento con el Sistema Integrado de Gestión y coordinará su divulgación en los canales institucionales.

Con estos mecanismos, se garantiza que el PETI sea un plan vivo, en permanente evolución, capaz de responder a los desafíos tecnológicos y de seguridad digital de la entidad y de alinearse con las mejores prácticas de gobernanza en el sector público.

Documentos Internos Relacionados

El PETI se articula con un conjunto de documentos internos que definen, soportan y orientan la gestión tecnológica de la entidad, estos instrumentos constituyen la base documental que asegura la coherencia entre la planeación estratégica, la gestión de riesgos, la seguridad digital y el control institucional.

Dentro de los documentos de referencia se destacan, en primer lugar, aquellos de carácter estratégico: el Plan Estratégico Institucional (PEI) 2024–2028, la Política General de Seguridad de la Información, el Plan Estratégico de Seguridad y Privacidad de la Información (PESI) y el Modelo de Seguridad y Privacidad de la Información (MSPI), los cuales establecen lineamientos transversales que deben integrarse en cada proyecto tecnológico.

En segundo lugar, se encuentran los instrumentos de gestión de riesgos y continuidad, entre ellos el Mapa de Riesgos de Gestión – Área de TI, el Mapa de Riesgos Institucionales, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad

de la Información y el Plan de Contingencia y Recuperación en Seguridad Informática, que aportan insumos fundamentales para la priorización de proyectos y la adopción de medidas preventivas.

También se consideran documentos de soporte técnico y de contexto, como el Inventario y Clasificación de Activos de Información, la Caracterización del Proceso de Gestión de TI (GTI-C026), la Matriz de Contexto Estratégico de TI (PDE-F368) y la Matriz de Partes Interesadas del Área de TI (PDE-F369), que fortalecen la trazabilidad y el control de la gestión tecnológica.

Finalmente, se incluyen instrumentos normativos y de control como el Normograma de Gestión de TI (GJ-F209) y la Política de Operación del Riesgo, que aseguran el cumplimiento de la normatividad nacional y las mejores prácticas en materia de gobernanza de tecnologías de la información.

La integración de estos documentos garantiza que el PETI no sea un plan aislado, sino un componente coherente del Sistema Integrado de Gestión, articulado con las políticas, procedimientos y planes que orientan la gestión institucional.

Disposiciones Finales

El presente plan es de aplicación obligatoria para todas las áreas, funcionarios, contratistas y proveedores que intervienen en la gestión tecnológica de la entidad, su cumplimiento busca garantizar que las iniciativas en tecnologías de la información se desarrollen bajo principios de eficiencia, seguridad, sostenibilidad y transparencia, en concordancia con la normatividad nacional y los estándares internacionales adoptados.

La responsabilidad de coordinar su implementación y seguimiento recae en el Coordinador de TI, con apoyo operativo de la Mesa de Ayuda (MDA), el Comité de Gestión y Desempeño Institucional será la instancia encargada de aprobar actualizaciones, validar avances y definir acciones estratégicas frente a riesgos o desviaciones identificadas en la ejecución.

El plan será publicado en el repositorio institucional y en la página web oficial, en cumplimiento de la Ley 1712 de 2014 sobre Transparencia y Acceso a la Información Pública, garantizando su disponibilidad para la ciudadanía y los entes de control.

Las actualizaciones ordinarias se realizarán de forma anual, mientras que las modificaciones extraordinarias podrán efectuarse en cualquier momento ante cambios normativos, emergencias tecnológicas, incidentes de seguridad de alto impacto o recomendaciones de auditoría, toda modificación deberá ser aprobada por el Comité de Gestión y Desempeño Institucional y validada por el Grupo de Gestión de Calidad.

El incumplimiento de las disposiciones aquí establecidas podrá dar lugar a acciones administrativas, contractuales o disciplinarias, según lo dispuesto en la normatividad vigente y la gravedad de la falta.

Con la adopción de este documento, la entidad reafirma su compromiso con la modernización tecnológica, la seguridad digital, la mejora continua y la confianza ciudadana en la prestación de los servicios públicos.

CONTROL DE CAMBIOS				
VERSIÓN	**FECHA**	**DESCRIPCION DEL CAMBIO**	**RESPONSABLE**	**CARGO**
0	dd/mm/aaaa	Versión inicial		planeación