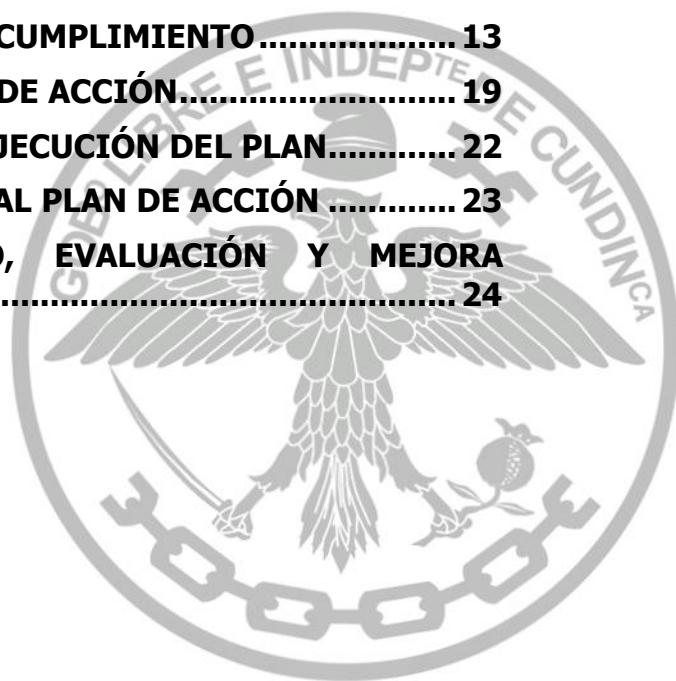


	Plan de Acción Gestión de Tecnologías de la Información	Código: GTI-PI021
		Versión:00
		Fecha: 16/12/2025

TABLA DE CONTENIDO

1. INTRODUCCIÓN.....	2
2. OBJETIVO.....	3
3. ALCANCE	3
4. MARCO NORMATIVO Y REFERENCIAL.....	4
5. GLOSARIO	5
6. CONTEXTO INSTITUCIONAL.....	7
7. PRINCIPIOS RECTORES DEL PLAN DE ACCIÓN	8
8. ESTRUCTURA DE GOBERNANZA Y RESPONSABILIDADES	9
9. EJES ESTRATÉGICOS DEL ÁREA DE TI.....	10
10. PLAN DE ACCIÓN	11
11. INDICADORES DE SEGUIMIENTO Y CUMPLIMIENTO.....	13
12. CRONOGRAMA GENERAL DEL PLAN DE ACCIÓN.....	19
13. RECURSOS NECESARIOS PARA LA EJECUCIÓN DEL PLAN.....	22
14. GESTIÓN DE RIESGOS ASOCIADOS AL PLAN DE ACCIÓN	23
15. MECANISMOS DE SEGUIMIENTO, EVALUACIÓN Y MEJORA CONTINUA.....	24



	Plan de Acción Gestión de Tecnologías de la Información	Código: GTI-PI021
		Versión:00
		Fecha: 16/12/2025

1. Introducción

El Plan de Acción del Área de Tecnologías de la Información de Empresas Públicas de Cundinamarca S.A. E.S.P. es el instrumento técnico que orienta la planificación, ejecución y seguimiento de las actividades requeridas para fortalecer la infraestructura tecnológica, garantizar la seguridad y privacidad de la información, asegurar la continuidad operativa de los servicios institucionales y apoyar la transformación digital de la entidad.

Su elaboración se fundamenta en los lineamientos del Plan Estratégico de Tecnologías de la Información (PETI), 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), el Plan de Recuperación ante Desastres (DRP), los instrumentos del Sistema Integrado de Gestión (SIG) y la normatividad vigente del Estado colombiano en materia de seguridad digital, gestión documental y administración pública.

Este documento recoge la misión y función estratégica del Área de TI dentro de la Dirección de Planeación, resaltando su papel como habilitador tecnológico de los procesos misionales, estratégicos y de apoyo que permiten a EPC cumplir con su objeto social. El plan se estructura bajo un enfoque de gestión basada en riesgo, alineado con las normas ISO/IEC 27001, ISO/IEC 27005, ISO/IEC 27031 y ISO 22301, garantizando que las acciones propuestas respondan a criterios de disponibilidad, integridad, confidencialidad, continuidad y eficiencia operativa.

El contenido del plan comprende los ejes estratégicos del área, las acciones asociadas, los indicadores de seguimiento, los responsables, los recursos necesarios y los mecanismos de mejora continua, su propósito es consolidar un marco operativo que facilite la toma de decisiones, fortalezca la resiliencia tecnológica y contribuya al cumplimiento de los objetivos institucionales, bajo los principios de transparencia, trazabilidad, efectividad y compromiso con la prestación eficiente de los servicios públicos que ofrece EPC.

Este documento es dinámico y evolutivo; su actualización deberá realizarse conforme a los cambios tecnológicos, regulatorios y organizacionales que impacten la operación de la entidad, manteniendo siempre la alineación con las políticas nacionales de seguridad digital, los lineamientos de MinTIC y las mejores prácticas internacionales en gestión de tecnologías de la información.

	Plan de Acción Gestión de Tecnologías de la Información	Código: GTI-PI021
		Versión:00
		Fecha: 16/12/2025

2. Objetivo

El Plan de Acción del Área de Tecnologías de la Información tiene como objetivo establecer las directrices, actividades estratégicas y acciones operativas que permitan fortalecer la gestión tecnológica de Empresas Públicas de Cundinamarca S.A. E.S.P., garantizando la disponibilidad, integridad y confidencialidad de la información institucional, la continuidad y resiliencia de los servicios tecnológicos, el cumplimiento de la normatividad vigente en materia de seguridad digital, y la adecuada articulación con los instrumentos de planeación institucional adoptados por la entidad.

El plan busca orientar, de manera ordenada y verificable, la ejecución de actividades prioritarias en materia de infraestructura, soporte, seguridad digital, gestión del riesgo, continuidad del negocio, gobierno digital y modernización tecnológica, asegurando que la operación tecnológica soporte eficientemente los procesos estratégicos, misionales y de apoyo, y contribuya al logro de los objetivos del Plan Estratégico Institucional, el PETI, el PESI, el MSPI, el PCN y el DRP.

Su propósito final es consolidar un marco de acción técnico y alineado con estándares internacionales (ISO/IEC 27001, ISO/IEC 27005, ISO/IEC 27031, ISO 22301 e ISO 31000) que permita a EPC anticipar, responder y recuperarse frente a incidentes tecnológicos, mejorar la prestación de los servicios institucionales y asegurar la confianza de los usuarios, partes interesadas y entes de control.

3. Alcance

Aplica a todas las actividades, procesos, recursos y servicios tecnológicos administrados, en el marco de las funciones asignadas al Área de TI dentro de la Dirección de Planeación, su alcance comprende la planificación, ejecución, seguimiento y mejora de las acciones orientadas al mantenimiento, fortalecimiento y modernización de la infraestructura tecnológica; la gestión de la seguridad y privacidad de la información, la continuidad operativa de los sistemas institucionales, y la prestación eficiente de servicios de soporte y atención a los usuarios internos.

El plan cubre las dimensiones tecnológicas, administrativas y operativas relacionadas con la gestión de sistemas de información, redes, servidores, plataformas de colaboración, almacenamiento, respaldo y recuperación, aplicaciones institucionales, servicios en nube, telecomunicaciones y soluciones de seguridad digital, también abarca la coordinación con proveedores, la supervisión de contratos tecnológicos, la administración del Sistema de Gestión de Incidentes, la gestión documental asociada

	Plan de Acción Gestión de Tecnologías de la Información	Código: GTI-PI021
		Versión:00
		Fecha: 16/12/2025

y los mecanismos de articulación con los procesos estratégicos, misionales y de apoyo de la entidad.

Este plan es aplicable a todos los servidores públicos, contratistas y proveedores que interactúan con los activos de información y servicios tecnológicos de EPC, quienes deben cumplir los lineamientos definidos en el PETI, PESI, MSPI, PCN, DRP y en las políticas institucionales de seguridad digital, el alcance del plan se extiende a las sedes administrativas y operativas de la entidad, así como a los entornos tecnológicos gestionados mediante servicios en la nube, infraestructura híbrida o soluciones de terceros que soporten procesos institucionales.

El Plan de Acción no reemplaza procedimientos técnicos específicos ni documentos normativos existentes, sino que los articula y complementa para asegurar coherencia, trazabilidad y efectividad en la gestión tecnológica institucional. Su implementación debe entenderse como un componente transversal del Sistema Integrado de Gestión y del Sistema de Gestión de Seguridad y Privacidad de la Información, garantizando una visión integral de la gestión tecnológica en beneficio de la operación y continuidad de los servicios públicos a cargo de EPC.

4. Marco Normativo y Referencial

La gestión tecnológica se desarrolla bajo un marco normativo que integra disposiciones nacionales, lineamientos sectoriales y estándares internacionales aplicables a la seguridad digital, la continuidad operativa y la gestión estratégica de TI. Este apartado consolida las normas y referentes que orientan la planificación y ejecución de las acciones del área.

En el ámbito nacional, se destacan la Política de Seguridad Digital del Estado, la Política de Gobierno Digital, la Ley de Protección de Datos Personales, la Ley de Transparencia, la Ley General de Archivos, el Decreto Único Reglamentario del Sector TIC y la Guía para la Gestión Integral del Riesgo del DAFP, que establecen directrices para la administración responsable de la información pública, el tratamiento de datos personales, la gestión del riesgo institucional y la prestación eficiente y segura de los servicios tecnológicos.

Desde la perspectiva sectorial, los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones, en especial el Modelo de Seguridad y Privacidad de la Información (MSPI) y las orientaciones de Gobierno Digital, constituyen la base para consolidar un sistema de gestión que asegure la protección de los activos de información, la continuidad operativa y la adopción de buenas prácticas en materia de tecnologías de la información.

	Plan de Acción Gestión de Tecnologías de la Información	Código: GTI-PI021
		Versión:00
		Fecha: 16/12/2025

En cuanto a referentes internacionales, se adoptan los estándares ISO/IEC 27001, ISO/IEC 27005, ISO/IEC 27031, ISO 22301 e ISO 31000, que proporcionan marcos técnicos para la gestión de la seguridad de la información, la evaluación y tratamiento del riesgo tecnológico, la continuidad de las tecnologías de la información y la resiliencia organizacional, asimismo, se consideran buenas prácticas de marcos como COBIT 2019 y NIST para fortalecer los procesos de control, gobernanza y operación tecnológica.

A nivel institucional, las acciones del área se encuentran alineadas con el Plan Estratégico Institucional (PEI), el Plan Estratégico de Tecnologías de la Información (PETI), el Plan Estratégico de Seguridad y Privacidad de la Información (PESI), el Modelo de Seguridad y Privacidad de la Información, el Plan de Continuidad del Negocio (PCN), el Plan de Recuperación ante Desastres (DRP), las matrices de riesgos GTI-F457, PDE-F368 y PDE-F369, y las políticas internas adoptadas por la entidad en materia de gestión documental y seguridad de la información.

Este marco normativo y referencial garantiza coherencia, trazabilidad y conformidad con los requisitos legales y técnicos aplicables, permitiendo que las decisiones y acciones en materia tecnológica respondan a criterios de responsabilidad, transparencia, seguridad y eficiencia en beneficio de la operación institucional y de los ciudadanos atendidos por EPC.

5. Glosario

Para efectos de interpretación y aplicación del presente documento, se adoptan los siguientes términos, definidos en concordancia con la normativa nacional, los estándares internacionales de seguridad y continuidad, y los instrumentos institucionales vigentes:

Activo de información: Cualquier dato, sistema, servicio, infraestructura, proceso o recurso que soporte la operación institucional y cuyo valor es esencial para el cumplimiento de los objetivos estratégicos.

Análisis de Impacto al Negocio (BIA): Proceso que identifica las consecuencias operativas, legales, financieras y reputacionales derivadas de la interrupción de un proceso crítico, estableciendo prioridades de recuperación y parámetros como RTO y RPO.

	Plan de Acción Gestión de Tecnologías de la Información	Código: GTI-PI021
		Versión:00
		Fecha: 16/12/2025

Ciberseguridad: Conjunto de medidas técnicas, operativas y administrativas destinadas a prevenir, detectar y responder a incidentes que comprometan la confidencialidad, integridad o disponibilidad de la información.

Continuidad del negocio: Capacidad institucional para mantener las operaciones esenciales dentro de niveles aceptables durante y después de un evento disruptivo.

Disponibilidad: Propiedad de la información o de un servicio tecnológico que garantiza que esté accesible cuando sea requerido por un usuario autorizado.

DRP (Disaster Recovery Plan): Conjunto de procedimientos técnicos y operativos orientados a restaurar los sistemas de información, infraestructura tecnológica y servicios críticos después de un incidente mayor.

Evento disruptivo: Suceso no planificado que afecta la operación, compromete la infraestructura tecnológica o interrumpe los servicios institucionales.

Gestión del riesgo: Proceso sistemático para identificar, analizar, valorar y tratar riesgos que puedan afectar la operación institucional o la seguridad de la información.

Integridad: Propiedad que asegura que los datos no han sido alterados o destruidos de manera no autorizada, manteniendo su exactitud y completitud.

Mesa de Ayuda (MDA): Equipo técnico responsable de la atención de incidentes, soporte a usuarios, mantenimiento de infraestructura y ejecución operativa de actividades asociadas al PCN y DRP.

Modelo de Seguridad y Privacidad de la Información (MSPI): Lineamiento emitido por el MinTIC que orienta a las entidades públicas en la gestión de seguridad digital, protección de datos y tratamiento de riesgos asociados a las TIC.

PCN (Plan de Continuidad del Negocio): Instrumento institucional que define los mecanismos para asegurar la continuidad operativa de los procesos y servicios críticos ante incidentes que afecten la operación normal.

RPO (Recovery Point Objective): Tiempo máximo permitido de pérdida de datos aceptable para un proceso o sistema, medido desde el último punto de respaldo válido.

	Plan de Acción Gestión de Tecnologías de la Información	Código: GTI-PI021
		Versión:00
		Fecha: 16/12/2025

RTO (Recovery Time Objective): Tiempo máximo permitido para restablecer un proceso, sistema o servicio tras una interrupción.

Seguridad de la información: Conjunto de políticas, controles y procedimientos destinados a proteger la confidencialidad, integridad y disponibilidad de la información institucional.

SGSPI: Sistema de Gestión de Seguridad y Privacidad de la Información adoptado por la entidad, alineado con el MSPI y estándares como ISO/IEC 27001.

Sistema de información: Conjunto de componentes, aplicaciones, bases de datos y servicios que permiten procesar, almacenar y transmitir información institucional.

6. Contexto Institucional

El Área de Tecnologías de la Información forma parte de la Dirección de Planeación y actúa como habilitador estratégico para los procesos misionales, de apoyo y de evaluación, su función principal consiste en asegurar que la infraestructura tecnológica, los sistemas de información, los servicios digitales y los mecanismos de seguridad operen de manera confiable, eficiente y alineada con los objetivos institucionales.

La operación de la entidad depende de plataformas críticas como el ERP contable y financiero, el Sistema SIG de planeación, el Sistema de Gestión de Proyectos (SIA), el Sistema Comercial, el Sistema de Gestión Documental y el correo institucional, estos sistemas requieren una infraestructura robusta compuesta por un CPD con servidores físicos y virtualizados, almacenamiento redundante, servicios de respaldo y recuperación, conectividad LAN/WAN, soluciones de colaboración en la nube, seguridad perimetral y herramientas de monitoreo continuo.

El Área TI asume la responsabilidad de administrar esta infraestructura, prestar servicios de soporte, gestionar incidentes y mantener los controles asociados al Sistema de Gestión de Seguridad y Privacidad de la Información, la Mesa de Ayuda (MDA) cumple un rol operativo fundamental en la atención de usuarios, la gestión de incidentes, la recuperación de servicios y la ejecución de actividades preventivas y correctivas.

Las funciones del área se desarrollan bajo los lineamientos del PETI, PESI, MSPI, PCN y DRP, los cuales definen el marco estratégico y operativo para la planeación tecnológica, la seguridad digital, la continuidad del negocio y la recuperación ante

	Plan de Acción Gestión de Tecnologías de la Información	Código: GTI-PI021
		Versión:00
		Fecha: 16/12/2025

desastres, su ejecución debe mantenerse articulada con los procesos institucionales y con las exigencias de las entidades de control, garantizando la trazabilidad de las acciones y el cumplimiento de la normativa vigente.

El contexto actual se caracteriza por una dependencia creciente de los servicios digitales, el incremento de amenazas cibernéticas, la necesidad de garantizar continuidad operativa y la obligación de adoptar buenas prácticas de gobierno digital, en este entorno, el Área TI desempeña un rol esencial para sostener la operación institucional y asegurar la prestación eficiente de los servicios públicos a cargo de la entidad, bajo criterios de disponibilidad, integridad, confidencialidad y resiliencia tecnológica.

7. Principios Rectores del Plan de Acción

La gestión tecnológica de la entidad se orienta por un conjunto de principios que aseguran que las acciones ejecutadas respondan a criterios de eficiencia, seguridad, continuidad y cumplimiento normativo, estos principios son la base para la toma de decisiones técnicas, la priorización de actividades y la ejecución coordinada con los procesos institucionales.

El primer principio es la gestión basada en el riesgo, que implica planificar y ejecutar las acciones tecnológicas considerando la criticidad de los procesos, las amenazas identificadas y las vulnerabilidades presentes en los sistemas de información. Este enfoque permite anticipar incidentes, fortalecer los controles y asegurar la continuidad operativa.

El segundo principio es la seguridad y protección de la información, garantizando que todos los servicios, sistemas y actividades cumplan los criterios de confidencialidad, integridad y disponibilidad, en coherencia con el MSPI, la normativa nacional de seguridad digital y los estándares internacionales aplicables.

El tercer principio es la resiliencia tecnológica, entendida como la capacidad institucional para anticipar, resistir, responder y recuperarse frente a fallas, incidentes cibernéticos o eventos que comprometan la operación, este principio se materializa mediante la redundancia de infraestructura, la gestión de respaldos, los planes de contingencia y los mecanismos de recuperación ante desastres.

El cuarto principio es la coordinación institucional, asegurando que todas las acciones tecnológicas se articulen con las áreas misionales, de apoyo y de control, y que

	Plan de Acción Gestión de Tecnologías de la Información	Código: GTI-PI021
		Versión:00
		Fecha: 16/12/2025

exista claridad sobre responsabilidades, flujos de comunicación y escalamiento durante incidentes o interrupciones de servicio.

El quinto principio es la eficiencia y sostenibilidad, que orienta la optimización de recursos tecnológicos, el aprovechamiento de la infraestructura existente, la priorización de inversiones y la adopción de soluciones costo-efectivas, alineadas con los objetivos del PETI y las necesidades reales de la entidad.

El sexto principio es la trazabilidad y transparencia, mediante la documentación adecuada de las actividades, registros de soporte, informes de gestión, indicadores y evidencias, lo cual permite responder a auditorías internas y externas, y cumplir con los estándares del Sistema Integrado de Gestión.

Finalmente, se adopta el principio de mejora continua, que exige evaluar permanentemente el desempeño tecnológico, revisar los resultados de auditorías, simulacros e incidentes, y actualizar los procesos, controles y estrategias conforme a la evolución del entorno digital y los riesgos emergentes.

8. Estructura de Gobernanza y Responsabilidades

La gestión tecnológica se desarrolla bajo un modelo de gobernanza alineado con el Sistema Integrado de Gestión, el Modelo de Seguridad y Privacidad de la Información, y las directrices estratégicas definidas por la Dirección, este modelo define los niveles de autoridad, las responsabilidades y los mecanismos de coordinación que permiten orientar, supervisar y ejecutar las acciones tecnológicas de manera eficiente, segura y conforme a la normativa vigente.

La Dirección fija las directrices estratégicas, aprueba los instrumentos de planeación tecnológica y supervisa el cumplimiento de los objetivos establecidos en el PETI, PESI y en los planes de continuidad y recuperación, asimismo, ejerce el rol de patrocinador institucional para proyectos tecnológicos, asignación de recursos y adopción de lineamientos de seguridad digital.

El Área de Tecnologías de la Información lidera la ejecución técnica y operativa de las actividades, administra la infraestructura tecnológica, gestiona los servicios de información, implementa controles de seguridad, coordina la continuidad y recuperación de los sistemas, supervisa a los proveedores tecnológicos y asegura el cumplimiento de las políticas internas y los estándares internacionales.

La Mesa de Ayuda (MDA) cumple funciones operativas esenciales, brindando soporte técnico a los usuarios, gestionando incidentes, aplicando controles preventivos y correctivos, ejecutando procedimientos de recuperación, manteniendo la infraestructura y generando la documentación técnica requerida para evidenciar la operación y recuperación de los servicios.

Los líderes de proceso participan en la identificación de activos de información, validan la criticidad de sus sistemas, colaboran en la gestión de riesgos y aseguran la aplicación de los procedimientos de continuidad cuando se presenten interrupciones que afecten su operación.

Las áreas jurídicas, administrativas, financieras y de control interno aportan soporte transversal, validando el cumplimiento normativo, verificando registros, acompañando auditorías, supervisando la gestión documental y fortaleciendo los procesos de transparencia y control institucional.

Este esquema de gobernanza permite que la operación tecnológica se ejecute bajo criterios de responsabilidad compartida, coordinación efectiva y trazabilidad permanente, consolidando un entorno controlado, seguro y preparado para responder ante incidentes o eventos que comprometan la prestación de los servicios institucionales.

9. Ejes Estratégicos del Área de TI

La gestión tecnológica se orienta a partir de ejes estratégicos que permiten estructurar las acciones necesarias para mantener una operación segura, eficiente y alineada con los objetivos institucionales, estos ejes consolidan las prioridades del área frente a la evolución tecnológica, la seguridad digital, la continuidad operativa y la gestión de infraestructura.

El primer eje corresponde al fortalecimiento de la seguridad y privacidad de la información, orientado a garantizar la protección de los activos institucionales bajo los lineamientos del MSPI, la normativa nacional en seguridad digital y estándares como ISO/IEC 27001 y 27005 este eje prioriza la implementación de controles, la gestión del riesgo tecnológico y la adopción de prácticas que aseguren la confidencialidad, integridad y disponibilidad de la información.

El segundo eje se centra en la continuidad operativa y recuperación tecnológica, asegurando que los sistemas y servicios críticos permanezcan disponibles o puedan restablecerse dentro de los tiempos definidos en el BIA, el PCN y el DRP, incluye

actividades de prevención, preparación, respuesta y mejora continua que permitan a la entidad operar con resiliencia frente a incidentes, fallas técnicas o eventos disruptivos.

El tercer eje abarca la gestión, modernización y optimización de la infraestructura tecnológica, garantizando que los equipos, servidores, redes, plataformas de colaboración, almacenamiento y servicios en la nube se mantengan actualizados, seguros y con niveles de servicio adecuados a las necesidades de la operación institucional.

El cuarto eje se orienta a la gestión de servicios tecnológicos y soporte al usuario, fortaleciendo la Mesa de Ayuda, mejorando los tiempos de respuesta, asegurando la trazabilidad de incidentes, generando acompañamiento técnico y garantizando la disponibilidad de los servicios requeridos por los procesos institucionales.

El quinto eje corresponde al gobierno digital y alineación estratégica, asegurando que las iniciativas tecnológicas se integren con los objetivos definidos en el PETI, el PESI y el Plan Estratégico Institucional, promoviendo el cumplimiento de la Política de Gobierno Digital, la mejora en la madurez digital institucional y el uso eficiente de los recursos asignados.

Finalmente, el sexto eje se enfoca en la gestión documental, transparencia y articulación institucional, garantizando que las acciones del área cuenten con evidencia suficiente, registros oportunos, control documental y alineación con el Sistema Integrado de Gestión, facilitando procesos de auditoría, toma de decisiones y rendición de cuentas.

Estos ejes constituyen la base para la estructuración del plan de acción, permitiendo organizar las actividades de manera coherente, medible y orientada a resultados que fortalecen la operación tecnológica y aportan valor directo a la gestión institucional.

10. Plan de Acción

El conjunto de acciones que se presenta a continuación constituye la hoja de ruta operativa para fortalecer la seguridad digital, asegurar la continuidad de los servicios tecnológicos, optimizar la infraestructura y brindar soporte eficiente a los procesos institucionales, cada acción se alinea con los instrumentos estratégicos y normativos vigentes, garantizando coherencia con el PETI, PESI, MSPI, PCN, DRP y con el Sistema Integrado de Gestión, de acuerdo con los siguientes ejes temáticos.

	Plan de Acción Gestión de Tecnologías de la Información	Código: GTI-PI021
		Versión:00
		Fecha: 16/12/2025

Seguridad y privacidad de la información

Este eje integra las actividades necesarias para proteger los activos institucionales y gestionar adecuadamente los riesgos tecnológicos, se incluye el fortalecimiento de los controles establecidos en el MSPI, la actualización permanente de los análisis de riesgo, la revisión de configuraciones críticas, la gestión de vulnerabilidades y la implementación de mecanismos de autenticación, monitoreo y protección acorde con los estándares nacionales e internacionales, las acciones contemplan la actualización de los activos de información, la revisión del cumplimiento de la Política General de Seguridad, la implementación progresiva de controles priorizados del Anexo A de ISO/IEC 27001, el fortalecimiento de la arquitectura de seguridad y el aseguramiento del ciclo de vida de la información.

Continuidad operativa y recuperación tecnológica

Este eje articula los procedimientos del PCN y el DRP, asegurando que los sistemas y servicios críticos funcionen o puedan restablecerse dentro de los parámetros definidos, incluye actividades de mantenimiento de respaldos, validación de restauración, pruebas de contingencia, ejercicios de simulación y actualización de estrategias de continuidad conforme a los cambios tecnológicos o institucionales, las acciones priorizan el aseguramiento de los RTO y RPO establecidos, la revisión anual del BIA, la actualización de inventarios críticos, la verificación de los mecanismos de respaldo bajo el esquema 3-2-1-1-0, la coordinación con proveedores estratégicos y la ejecución de simulacros de recuperación.

Modernización y optimización de la infraestructura tecnológica

En este eje se consolidan las actividades dirigidas a mantener la infraestructura tecnológica en condiciones adecuadas de rendimiento, seguridad, estabilidad y disponibilidad. Incluye la actualización de servidores, redes, equipos de usuario final, sistemas de almacenamiento, servicios en nube y herramientas de monitoreo, las acciones se orientan a la renovación progresiva de infraestructura prioritaria, la actualización de sistemas operativos y aplicaciones, la mejora de la conectividad, la gestión eficiente de licencias y la adopción de soluciones que permitan ampliar la capacidad de procesamiento, almacenamiento y comunicaciones de forma escalable y sostenible.

Servicios tecnológicos y soporte al usuario

Este eje aborda la operación diaria de la Mesa de Ayuda, la atención de incidentes, la administración de solicitudes, la mejora en los tiempos de respuesta y las acciones de acompañamiento técnico a las áreas institucionales, busca asegurar que el soporte tecnológico sea oportuno, confiable y trazable, las acciones incluyen la

	Plan de Acción Gestión de Tecnologías de la Información	Código: GTI-PI021
		Versión:00
		Fecha: 16/12/2025

gestión del sistema de tickets, el mantenimiento preventivo y correctivo de equipos, la documentación de procedimientos operativos, el control de inventarios tecnológicos, la atención directa al usuario y el registro de evidencias técnicas que respalden la operación del área.

Gobierno digital y alineación estratégica

Este eje se orienta a garantizar que la gestión tecnológica contribuya al cumplimiento de las metas institucionales, fortalezca la madurez digital y asegure la adopción de prácticas de gobierno digital. Incluye la articulación con el PETI y el PESI, la participación en comités estratégicos, el seguimiento a indicadores de madurez y la identificación de oportunidades de mejora para fortalecer la capacidad tecnológica institucional, las acciones implican el seguimiento a los proyectos tecnológicos, la verificación del cumplimiento de lineamientos de Gobierno Digital, la actualización de instrumentos de planeación y la coordinación interinstitucional necesaria para garantizar la alineación con las metas del Plan Estratégico Institucional.

Gestión documental, control y transparencia

Este eje fortalece la trazabilidad de las actividades del área mediante registros, evidencias y documentación técnica, garantiza el cumplimiento de los lineamientos de gestión documental, facilita auditorías internas y externas, y contribuye a la rendición de cuentas y al mejoramiento continuo, las acciones incluyen el mantenimiento de archivos técnicos, la actualización de documentos institucionales, la integración de evidencias en el SIG, la entrega de informes periódicos y la revisión constante de los procedimientos operativos.

11. Indicadores de Seguimiento y Cumplimiento

El seguimiento al desempeño tecnológico requiere indicadores que permitan evaluar la eficacia de las acciones ejecutadas, la disponibilidad de los sistemas, el nivel de cumplimiento de los controles de seguridad y la capacidad de respuesta ante incidentes o contingencias. Estos indicadores facilitan la toma de decisiones, permiten evidenciar avances y constituyen insumos para auditorías internas, revisiones estratégicas y reportes del Sistema Integrado de Gestión.

Los indicadores se estructuran en coherencia con los ejes estratégicos y se orientan a medir la calidad del servicio, la continuidad de la operación, la protección de la información, la eficiencia de la Mesa de Ayuda y el cumplimiento de lineamientos institucionales y normativos.

	Plan de Acción Gestión de Tecnologías de la Información	Código: GTI-PI021
		Versión:00
		Fecha: 16/12/2025

En materia de seguridad digital, los indicadores se enfocan en la verificación de controles implementados, la gestión de vulnerabilidades, la integridad de los respaldos y la capacidad de respuesta ante incidentes de seguridad, estos resultados permiten evaluar el nivel de madurez del sistema y determinar acciones de refuerzo técnico o administrativo.

Para la continuidad operativa, los indicadores se orientan a medir el cumplimiento de los RTO y RPO definidos, la ejecución de pruebas y simulacros, la disponibilidad de infraestructura crítica y la efectividad del modelo de recuperación, su seguimiento permite valorar la resiliencia de los servicios y ajustar estrategias cuando se identifiquen desviaciones o riesgos emergentes.

En cuanto a infraestructura y servicios tecnológicos, los indicadores permiten evaluar la disponibilidad de los sistemas, la estabilidad de las plataformas, el rendimiento de la red, la gestión de actualizaciones y la capacidad general de la infraestructura instalada, identificando oportunidades de mejora o requerimientos de modernización.

Respecto al soporte al usuario, se incluyen métricas relacionadas con los tiempos de atención, la resolución de incidentes, la satisfacción del usuario y la trazabilidad de los casos, garantizando una prestación de servicios oportuna y alineada con las necesidades institucionales.

Finalmente, se contemplan indicadores asociados a la gestión documental, que permiten verificar la existencia de evidencias, la actualización de documentos, el cumplimiento de requisitos del SIG y la disponibilidad de registros necesarios para auditorías o procesos de control.

Estos indicadores conforman un mecanismo de medición integral que permite evaluar el desempeño del área, priorizar acciones y garantizar la alineación con los objetivos estratégicos, fortaleciendo el ciclo de mejora continua y la capacidad operativa de la entidad.

Eje Estratégico	Indicador	Descripción	Método de Cálculo / Fórmula	Meta	Periodicidad	Responsable
Seguridad y privacidad	Cumplimiento de	Mide el porcentaje de	(Controles implementados /	≥ 90%	Trimestral	Área TI

d de la informaci ón	controles del MSPI	controles implementados y validados conforme al MSPI y Anexo A ISO/IEC 27001	Controles aplicables) $\times 100$			
	Validación de respaldos	Evalúa la integridad y recuperabilidad de las copias de seguridad	(Backups validados / Backups ejecutados) $\times 100$	100%	Mensual	Área TI – MDA
	Gestión de vulnerabilidades	Controla la atención oportuna de vulnerabilidades identificadas	(Vulnerabilidades corregidas / Vulnerabilidades detectadas) $\times 100$	$\geq 95\%$	Trimestral	Área TI
	Incidentes de seguridad atendidos dentro del tiempo objetivo	Mide la eficacia en la atención de incidentes de seguridad	(Incidentes atendidos en tiempo / Total incidentes) $\times 100$	$\geq 90\%$	Mensual	Área TI
Continuidad operativa y recuperación	Cumplimiento de RTO	Evalúa si los sistemas críticos se restauran dentro del	(Servicios recuperados dentro de RTO / Total servicios	$\geq 95\%$	Trimestral	Área TI

tecnología		tiempo objetivo definido	críticos) $\times$ 100			
	Cumplimiento de RPO	Verifica que la pérdida de datos se mantenga dentro del límite establecido	(Sistemas recuperados dentro del RPO / Total sistemas críticos) $\times$ 100	$\geq$ 95%	Trimestral	Área TI
	Ejecución de pruebas de restauración	Mide el cumplimiento de pruebas de recuperación y contingencia	(Pruebas ejecutadas / Pruebas programadas) $\times$ 100	100%	Mensual	Área TI
	Simulacros de continuidad realizados	Evalúa el cumplimiento del programa anual de simulacros	(Simulacros realizados / Simulacros programados) $\times$ 100	100%	Anual	Área TI
Modernización y optimización de infraestructura	Disponibilidad de infraestructura crítica	Mide la disponibilidad de servidores, red y servicios esenciales	% Uptime (según herramienta de monitoreo)	$\geq$ 99.5%	Mensual	MDA – Infraestructura
	Avance del plan de modernización	Controla el progreso de la renovación	(Acciones ejecutadas / Acciones programadas) $\times$ 100	$\geq$ 90%	Trimestral	Área TI

		n tecnológica				
	Estado de actualización de plataformas	Verifica la instalación oportuna de parches y actualizaciones	(Plataformas actualizadas / Plataformas totales) × 100	≥ 95%	Mensual	MDA
Servicios tecnológicos y soporte al usuario	Tiempo promedio de atención de incidentes	Mide la eficiencia en la respuesta de la Mesa de Ayuda	Σ Tiempo atención / Total incidentes	≤ 24 horas (promedio general)	Mensual	MDA
	Incidentes resueltos dentro del tiempo objetivo	Evalúa cumplimiento de SLA internos	(Incidentes resueltos en tiempo / Total incidentes) × 100	≥ 90%	Mensual	MDA
	Nivel de satisfacción del usuario	Mide percepción de los usuarios frente al soporte recibido	(Respuestas positivas / Total encuestas) × 100	≥ 85%	Trimestral	Área TI – MDA
	Ciclo de mantenimiento preventivo	Evalúa cumplimiento del programa de mantenimiento	(Equipos intervenidos / Equipos programados) × 100	≥ 95%	Trimestral	MDA
Gobierno digital y alineación	Avance de proyectos del PETI	Mide el progreso del	(Proyectos con avance según	≥ 90%	Trimestral	Área TI – Planeación

n estratégica		portafolio de proyectos tecnológicos	cronograma / Total proyectos) × 100			
	Cumplimiento de lineamientos de Gobierno Digital	Evalúa el nivel de madurez digital institucional	Autoevaluación oficial MinTIC / Matriz GD	Nivel ≥ "Alto"	Semestral	Área TI – Planeación
	Actualización de instrumentos estratégicos	Verifica cumplimiento de actualizaciones reglamentarias	Cumplimiento (Sí/No)	Sí	Anual	Área TI
Gestión documental, control y transparencia	Disponibilidad de evidencias del SIG	Mide la actualización y completitud de registros institucionales	(Evidencias cargadas / Evidencias requeridas) × 100	100%	Mensual	Área TI
	Cumplimiento de auditorías	Evalúa cierre de hallazgos y observaciones	(Hallazgos cerrados / Hallazgos generados) × 100	≥ 95%	Trimestral	Área TI
	Actualización de documentación técnica	Verifica mantenimiento de documentos institucionales	(Documentos actualizados / Documentos requeridos) × 100	≥ 90%	Trimestral	Área TI

	Plan de Acción Gestión de Tecnologías de la Información	Código: GTI-PI021
		Versión:00
		Fecha: 16/12/2025

12. Cronograma General del Plan de Acción

El cronograma establece la programación temporal de las actividades previstas, permitiendo organizar la ejecución de las acciones tecnológicas de manera coordinada y conforme a las prioridades institucionales, su objetivo es asegurar que la planificación anual se desarrolle de forma ordenada, que los recursos se asignen adecuadamente y que los tiempos de ejecución sean consistentes con las necesidades operativas, los riesgos identificados y los lineamientos estratégicos, la programación contempla actividades de carácter permanente y acciones con periodicidad definida, las actividades permanentes incluyen la administración de la infraestructura, la gestión de seguridad digital, la operación de la Mesa de Ayuda, el mantenimiento de sistemas de información, la gestión documental y el monitoreo continuo de servicios, estas actividades deben mantenerse durante todo el ciclo operativo, ya que garantizan la disponibilidad, estabilidad y seguridad de los sistemas.

Las actividades con periodicidad definida se distribuyen en ciclos mensuales, trimestrales, semestrales o anuales, según la naturaleza de cada una, entre ellas se encuentran las pruebas de restauración de respaldos, actualizaciones de inventarios tecnológicos, revisiones de riesgos, ejercicios de continuidad, validación del cumplimiento de controles, análisis de vulnerabilidades, revisión de proveedores críticos, actualización de documentos institucionales y mantenimiento programado de infraestructura.

El cronograma debe ajustarse a las prioridades definidas en los ejes estratégicos y a los tiempos establecidos en el PETI, el PESI, el PCN y el DRP. Su programación se coordina con las áreas involucradas para garantizar la disponibilidad de recursos humanos, técnicos y logísticos, especialmente cuando las acciones requieren interrupciones programadas de los servicios o intervenciones en la infraestructura, como instrumento vivo, el cronograma puede ser ajustado durante el año cuando se presenten cambios tecnológicos, incidentes relevantes, actualizaciones normativas, nuevos requerimientos institucionales o recomendaciones derivadas de auditorías internas o externas, dichos ajustes deben ser documentados y aprobados conforme a los procedimientos establecidos en el Sistema Integrado de Gestión.

El seguimiento al cronograma se realizará a través de revisiones periódicas dentro del área y en los espacios de coordinación institucional, permitiendo verificar el

	Plan de Acción Gestión de Tecnologías de la Información	Código: GTI-PI021
		Versión:00
		Fecha: 16/12/2025

cumplimiento de las metas previstas, identificar retrasos o desviaciones y tomar decisiones oportunas que aseguren la correcta ejecución del plan.

Eje Estratégico	Acción Principal	Periodicidad	Responsable
Seguridad y privacidad de la información	Actualización del inventario de activos de información	Trimestral	Área TI
	Revisión y actualización de la Matrices	Semestral	Área TI – Seguridad Digital
	Validación de controles del MSPI y Anexo A ISO 27001	Trimestral	Área TI
	Ejecución de análisis de vulnerabilidades	Trimestral	Área TI
	Actualización de parches y configuraciones críticas	Mensual	MDA – Infraestructura
	Verificación de cumplimiento de la Política General de Seguridad	Semestral	Área TI
Continuidad operativa y recuperación tecnológica	Ejecución de pruebas de restauración (esquema 3-2-1-1-0)	Mensual	Área TI – MDA
	Actualización del BIA y revisión de procesos críticos	Anual	Área TI – Planeación
	Simulacro interno de recuperación DRP	Anual	Área TI
	Verificación de RTO y RPO establecidos	Trimestral	Área TI
	Actualización de inventario de sistemas críticos	Semestral	Área TI
Modernización y optimización de infraestructura tecnológica	Mantenimiento preventivo de servidores y red	Trimestral	MDA – Infraestructura
	Actualización de sistemas operativos y plataformas	Mensual	MDA
	Revisión de capacidad de almacenamiento y uso de recursos	Trimestral	Área TI

	Seguimiento a contratos de telecomunicaciones	Trimestral	Área TI
	Renovación progresiva de equipos de usuario final	Semestral	Área TI – MDA
Servicios tecnológicos y soporte al usuario	Gestión del sistema de tickets y seguimiento de incidentes	Diario	MDA
	Mantenimiento preventivo de equipos de usuario	Trimestral	MDA
	Atención de incidentes y soporte técnico	Diario	MDA
	Documentación de procedimientos y registros técnicos	Mensual	Área TI
	Revisión del inventario de equipos y licencias	Semestral	Área TI
Gobierno digital y alineación estratégica	Seguimiento a proyectos del PETI	Trimestral	Área TI – Planeación
	Verificación de cumplimiento de lineamientos de Gobierno Digital	Semestral	Área TI
	Actualización de instrumentos estratégicos (PETI, PESI, MSPI)	Anual	Área TI – Planeación
	Participación en comités estratégicos institucionales	Mensual / Según convocatoria	Área TI
Gestión documental, control transparencia y	Actualización de documentos técnicos del área	Trimestral	Área TI
	Registro de evidencias en el SIG	Mensual	Área TI – MDA
	Atención y soporte a auditorías internas y externas	Según programación	Área TI
	Revisión de cumplimiento de procedimientos del SIG	Trimestral	Área TI
	Elaboración de informes de seguimiento y avances	Trimestral	Área TI

13. Recursos Necesarios para la Ejecución del Plan

La correcta ejecución de las acciones previstas requiere la disponibilidad y administración adecuada de recursos técnicos, humanos, financieros y contractuales, estos recursos permiten asegurar que las actividades se desarrollen de manera oportuna, eficiente y conforme a los lineamientos institucionales, normativos y estratégicos.

En primer lugar, se requiere recurso humano especializado, capaz de ejecutar tareas técnicas, operativas y de gestión derivadas de los ejes estratégicos, este recurso incluye al personal del área de TI, la Mesa de Ayuda (MDA), profesionales de seguridad digital, administradores de infraestructura, gestores de continuidad y personal de soporte, la disponibilidad y continuidad de este equipo resulta esencial para garantizar la operación, recuperación y mejora de los servicios tecnológicos.

En segundo lugar, se requieren recursos tecnológicos que soporten la infraestructura institucional y permitan la implementación de controles, actualizaciones, integraciones y mejoras. Entre ellos se encuentran servidores, equipos de red, herramientas de seguridad, plataformas en nube, sistemas de respaldo, dispositivos de usuario final, licenciamientos, servicios de monitoreo, soluciones de colaboración y herramientas de gestión de incidentes. Estos elementos deben contar con soporte técnico vigente y actualizaciones permanentes para asegurar su estabilidad y seguridad.

También son necesarios recursos financieros para la ejecución de inversiones estratégicas en infraestructura, renovación tecnológica, contratación de servicios especializados, adquisición de licencias y fortalecimiento de plataformas críticas, estos recursos deben estar previstos en el presupuesto anual y alineados con el PETI y el Plan Estratégico Institucional, garantizando sostenibilidad y continuidad en los proyectos tecnológicos.

Los recursos contractuales constituyen un componente fundamental, ya que permiten la vinculación de proveedores estratégicos para servicios de soporte, comunicaciones, almacenamiento, mantenimiento, respaldo, seguridad digital, DRaaS, hosting, licenciamiento y consultoría especializada. Los contratos deben incorporar cláusulas de continuidad, seguridad, confidencialidad y cumplimiento normativo.

Se requieren recursos logísticos y documentales que faciliten la ejecución y seguimiento de las actividades, esto incluye la disponibilidad de espacios adecuados,

	Plan de Acción Gestión de Tecnologías de la Información	Código: GTI-PI021
		Versión:00
		Fecha: 16/12/2025

acceso a sedes alternas en caso de contingencia, sistemas de registro de evidencias, procedimientos actualizados, herramientas para reuniones técnicas y sistemas institucionales que garanticen la trazabilidad de las acciones, la disponibilidad, administración y seguimiento de estos recursos permiten asegurar el cumplimiento de las actividades previstas, fortalecer la operación tecnológica y contribuir al logro de los objetivos institucionales.

14. Gestión de Riesgos Asociados al Plan de Acción

Las actividades tecnológicas son un componente esencial para garantizar la efectividad del plan, la alineación con los objetivos institucionales y el cumplimiento de los requisitos del Sistema Integrado de Gestión, estos mecanismos permiten verificar el avance, detectar desviaciones, evaluar el impacto de las acciones y definir ajustes necesarios para garantizar la mejora continua.

El seguimiento se desarrolla a partir de revisiones periódicas dentro del área, mediante la actualización de indicadores, la verificación de evidencias, el análisis de incidentes y la revisión de avances en los ejes estratégicos, estos espacios permiten identificar dificultades operativas, priorizar actividades y asegurar que las acciones se mantengan dentro de los tiempos definidos.

Adicionalmente, se consideran los resultados de auditorías internas y externas, las observaciones de entes de control, los hallazgos derivados de revisiones del SIG y las recomendaciones emanadas de ejercicios de continuidad, restauración o simulacros, estos insumos permiten evaluar el cumplimiento de los lineamientos de seguridad digital, continuidad operativa, gestión del riesgo, gestión documental y operación tecnológica.

La mejora continua se articula con el ciclo institucional de planeación, facilitando la actualización de procedimientos, la revisión de documentos estratégicos, la incorporación de nuevos controles, el fortalecimiento de la infraestructura y la adopción de prácticas emergentes que respondan a la evolución del entorno tecnológico. Asimismo, permite definir nuevas acciones cuando se identifiquen riesgos emergentes, cambios regulatorios, modificaciones en el portafolio de servicios o necesidades adicionales de los procesos misionales.

El área debe documentar de manera permanente las actividades ejecutadas, los ajustes realizados, los resultados de las evaluaciones y el estado de cumplimiento de las acciones previstas, esta documentación constituye evidencia para auditorías,

	Plan de Acción Gestión de Tecnologías de la Información	Código: GTI-PI021
		Versión:00
		Fecha: 16/12/2025

respalda la trazabilidad del proceso y garantiza que las mejoras implementadas queden registradas conforme a los lineamientos del SIG.

El seguimiento y la mejora continua permiten consolidar un modelo tecnológico robusto, adaptable y en capacidad de responder a los retos operativos y regulatorios, fortaleciendo la sostenibilidad y resiliencia de los servicios tecnológicos institucionales.

15. Mecanismos de Seguimiento, Evaluación y Mejora Continua

La actualización del presente documento se realiza conforme a los lineamientos definidos en el Sistema Integrado de Gestión y a las políticas institucionales de información documentada, su propósito es garantizar que el contenido se mantenga vigente, coherente con los cambios tecnológicos y alineado con la normativa aplicable y las necesidades operativas de la entidad.

La revisión debe efectuarse de manera periódica o cuando se presenten modificaciones significativas en la infraestructura tecnológica, en los sistemas de información, en los riesgos asociados, en la normativa nacional o en los instrumentos estratégicos como el PETI, PESI, MSPI, PCN o DRP, cualquier ajuste debe quedar documentado, contar con la aprobación correspondiente y registrarse en el historial de versiones.

Los cambios pueden originarse por resultados de auditorías internas o externas, recomendaciones de entes de control, incidentes de seguridad, activaciones del PCN o del DRP, actualizaciones normativas, avances tecnológicos o necesidades identificadas por las áreas involucradas, cada modificación debe evaluarse para determinar su impacto en las actividades del área, los roles asignados, el cronograma de ejecución y los recursos necesarios.

La versión vigente del documento debe estar publicada en el repositorio institucional autorizado y disponible para consulta de los responsables de su implementación, todas las versiones anteriores deben conservarse en el archivo institucional conforme a las directrices de gestión documental, garantizando trazabilidad y respaldo histórico.

	Plan de Acción Gestión de Tecnologías de la Información	Código: GTI-PI021
		Versión:00
		Fecha: 16/12/2025

CONTROL DE CAMBIOS				
VERSIÓN	FECHA	DESCRIPCION DEL CAMBIO	RESPONSABLE	CARGO
0	16/12/2025	Versión inicial	Diego Ernesto Guevara Forero	Director de Planeación

PROYECTÓ	REVISÓ	APROBÓ
Nombre: Héctor Gil	Nombre: Luis Mendoza	Nombre: Diego Guevara
Cargo: Coordinador TI - Contratista	Cargo: Asesor de Planeación - Contratista	Cargo: Director de Planeación
Dirección: Planeación	Subgerencia y/o Dirección: Planeación	Dirección: Planeación
Fecha: 16/12/2025	Fecha: 16/12/2025	Fecha: 16/12/2025

