



CARACTERIZACIÓN DEL PROCESO
GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

Código: GTI-C026
Versión: 01
Fecha: 08/10/2025

INFORMACIÓN DEL PROCESO										
TIPO DE PROCESO	OBJETIVO			ALCANCE						
Apoyo	Gestionar de manera eficaz y segura los recursos tecnológicos de Empresas Públicas de Cundinamarca S.A. E.S.P., garantizando la confidencialidad, integridad, disponibilidad y privacidad de la información, en cumplimiento de la normatividad vigente.			Inicia con la identificación de necesidades tecnológicas y la planeación de soluciones, continua con el soporte, gestión de incidentes, control riesgos TI, continuidad de los procesos y finaliza con la verificación de resultados y la ejecución de acciones de mejora, aplica a todos los funcionarios, contratistas y terceros que utilizan recursos tecnológicos institucionales.						
RESPONSABLE										
DIEGO ERNESTO GUEVARA FORERO										
ELEMENTOS DE ENTRADA		ACTIVIDADES			SALIDAS					
INSUMOS	PROVEEDORES	PLANEAR	HACER	CLIENTES	PRODUCTOS					
Requerimientos tecnológicos de los diferentes Procesos identificadas a través del Plan Estratégico Institucional, PETI, PESI y MSPI.	Procesos Estratégicos, Misionales y de Apoyo.	Identificar y priorizar necesidades tecnológicas de la entidad, estructurar proyectos estratégicos de TI y se plantean las soluciones a través del PETI, asegurando su alineación con el PEI, el MIPG y los lineamientos nacionales, incluyendo planeación del tratamiento de riesgos tecnológicos y la definición de controles asociados.	Comprender la ejecución de proyectos tecnológicos priorizados, administración de la infraestructura y sistemas de información, atención de incidentes y solicitudes de soporte, implementación de controles de seguridad digital y realiza la supervisión técnica de los contratos tecnológicos y la gestión de proveedores.	Procesos Estratégicos, Misionales y de Apoyo del SIG.	Servicios tecnológicos estables y disponibles. Informes de avance y gestión (incluyendo PETI, PESI y MSPI).					
Resultados de auditorías internas y externas.	Equipo de Tecnologías de la Información.									
Diagnósticos de brechas tecnológicas. Registros de incidentes y solicitudes de soporte técnico.	Proveedores externos de telecomunicaciones, servicios en la nube y consultores especializados en seguridad digital.	Medición y seguimiento del proceso mediante indicadores de desempeño, verificación del cumplimiento de SLA, revisión de los riesgos identificados y la evaluación de los resultados de las auditorías, garantizando la trazabilidad y la rendición de cuentas en materia tecnológica.	Ejecutar acciones de mejora derivadas de las verificaciones anteriores, ajustando planes estratégicos y operativos, corrigiendo desviaciones y fortaleciendo las capacidades técnicas y de seguridad digital, asegurando el ciclo de mejora continua.	Funcionarios y contratistas Ciudadanía Entes de control Proveedores estratégicos que dependen de la interoperabilidad y	Indicadores de desempeño Evidencias de continuidad operativa. Planes de tratamiento de riesgos. Reportes de incidentes atendidos. Documentos de supervisión de contratos tecnológicos.					
Inventory y clasificación de activos de información.	MinTIC, Entes de control, ICONTEC.									
Resultados de autodiagnósticos del MSPI y reportes FURAG.										
REQUISITOS Y RECURSOS DOCUMENTALES										
REQUISITOS LEGALES Y REGLAMENTARIOS		MIPG	ISO 9001	DOCUMENTOS INTERNOS						
Ley 1581 de 2012; Ley 1712 de 2014; Ley 1273 de 2009; Ley 594 de 2000; Decreto 338 de 2022 que reglamenta la Política de Gobierno Digital.		Como marco obligatorio de gestión pública que garantiza articulación entre planeación, gestión del talento humano, control interno y mejora continua.	Como estándar de referencia para el enfoque en la calidad, la orientación a procesos y la satisfacción de los usuarios internos y externos.	Normograma GJ-F209, Política General de Seguridad de la Información, PESI, MSPI, Mapa de Riesgos de TI, Inventario de Activos de Información, procedimientos de soporte e incidentes, matrices de partes interesadas y contexto estratégico.						
El Modelo Integrado de Planeación y Gestión - MIPG			ISO 45001							
Norma Internacional ISO 9001:2015; 45001:2018; 27001; 27005, 27017 y 27018 para seguridad y privacidad de la información.			Como lineamiento en seguridad y salud en el trabajo, aplicable a las operaciones de TI en lo que respecta al ambiente laboral, ergonomía y prevención de riesgos asociados a la operación de equipos.							
SEGUIMIENTO Y MEDICIÓN										
RIESGOS			INDICADORES							
Indisponibilidad de servicios críticos, vulnerabilidades de seguridad de la información, fallas en la interoperabilidad, incumplimientos contractuales de proveedores, brechas en la capacitación de usuarios.			Disponibilidad de sistemas críticos, incidentes atendidos en tiempos establecidos, cumplimiento del cronograma PETI, porcentaje de proveedores con SLA cumplido, cobertura de formación en seguridad digital. Estos indicadores se revisan de forma trimestral y alimentan informes al Comité de Gestión y Desempeño Institucional.							
RECURSOS										
FÍSICOS: TÉCNICOS, TECNOLÓGICOS E INFRAESTRUCTURA			TALENTO HUMANO							
Incluyen servidores, equipos de red, firewalls, consolas de monitoreo, sistemas de información corporativos, aplicaciones en la nube, equipos de usuario final y demás herramientas necesarias para garantizar la continuidad de los procesos.			Funcionarios, contratistas y directamente el equipo de Tecnologías de la Información.							
CONTROL DE CAMBIOS										
VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO			RESPONSABLE					
0	08/10/2025	El formato fue actualizado para integrar un enfoque más descriptivo y técnico, alineado al MIPG, normas ISO y documentos internos de la entidad, consolidando riesgos, indicadores y recursos bajo el esquema PHVA.			Héctor Gil					
					Coordinador TI					