

INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL				Vigencia: 28 de septiembre de 2026	
CARACTERIZACIÓN PROCESO GESTIÓN DE SISTEMAS DE INFORMACIÓN Y TECNOLOGÍA				Versión: 6 Código: GST-CAR-001	
OBJETIVO	Gestionar integral y estratégicamente las tecnologías de la información y las comunicaciones del Instituto Distrital de Patrimonio Cultural, mediante la planeación, implementación, operación, seguimiento y mejora de las capacidades tecnológicas, los sistemas de información y la información institucional, garantizando su seguridad y disponibilidad, con el fin de soportar la gestión institucional y contribuir al cumplimiento de los objetivos estratégicos de la Entidad.			LÍDER DEL PROCESO	Subdirector(a) de Gestión Corporativa
ALCANCE	Inicia con la planeación estratégica de las tecnologías de la información y las comunicaciones y la definición de lineamientos para su gobierno, seguridad y operación; comprende la gestión de la información, el desarrollo, integración y mantenimiento de los sistemas de información, la administración de la infraestructura y los servicios tecnológicos, así como la implementación de medidas de seguridad y privacidad de la información; y finaliza con el seguimiento, evaluación y mejora de las capacidades, servicios y controles tecnológicos del Instituto.			DEPENDENCIA:	Subdirección de Gestión Corporativa
TIPO DE PROCESO	Apoyo	INSTRUMENTOS ASOCIADOS AL PROCESO:	Matriz de indicadores, Matriz de riesgos, Plan Operativo Anual del proceso, Planes Institucionales, Normograma, Plan de Mejoramiento (interno/externo), Listado Maestro de Documentos		
CADENA DE VALOR					
GRUPOS DE VALOR/PROVEEDORES	ENTRADAS (Insumos)	CICLO PHVA	ACTIVIDADES	SALIDAS (Productos y Servicios)	GRUPO DE VALOR/USUARIO (CLIENTE)
Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) Alta Consejería Distrital de TI Alta Dirección del IDPC Todos los procesos de la Entidad	Plan Estratégico de Tecnologías de la Información (PETI) Lineamientos y políticas de Gobierno Digital, Seguridad Digital, Arquitectura TI y gestión de información. Necesidades y requerimientos tecnológicos de los procesos y partes interesadas.	P	Identificar y analizar las necesidades y requerimientos tecnológicos de la Entidad, así como los lineamientos aplicables, las tecnologías emergentes y las tendencias del sector para formular o actualizar el Plan Estratégico de Tecnologías de la Información (PETI), articulando las iniciativas, programas y proyectos de TI con la planeación estratégica institucional.	PETI formulado o actualizado. Diagnóstico de necesidades y requerimientos tecnológicos. Iniciativas, programas y proyectos de TI definidos y priorizados. Análisis de tendencias y tecnologías emergentes.	Todos los procesos de la Entidad. Personas servidoras públicas y contratistas. Ciudadanía y personas usuarias.
Alta Dirección del IDPC Todos los procesos de la Entidad	Necesidades y requerimientos de los procesos de la Entidad. Requerimientos funcionales y técnicos. Lineamientos de arquitectura, interoperabilidad y seguridad de la información. Sistemas de información existentes.	P	Identificar y analizar, en articulación con los líderes de los procesos, las necesidades y requerimientos para el desarrollo, evolución e integración de los sistemas de información, considerando su viabilidad técnica, financiera y operativa, así como los requisitos de seguridad, interoperabilidad, usabilidad y experiencia de usuario, con el fin de definir las soluciones tecnológicas requeridas por la Entidad.	Requerimientos funcionales y técnicos definidos. Necesidades de desarrollo, actualización o integración identificadas. Soluciones tecnológicas definidas.	Líderes y responsables de los procesos de la Entidad. Personas usuarias de los sistemas de información. Proceso de Gestión de Sistemas de Información y Tecnología. Alta Dirección y procesos de la Entidad. Proveedores de servicios y soluciones tecnológicas. Equipo técnico y personas responsables del desarrollo de sistemas de información.
Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) Alta Consejería Distrital de TI Alta Dirección del IDPC Todos los procesos de la Entidad	Necesidades y requerimientos de los procesos de la Entidad. Inventario y estado de la infraestructura tecnológica. Requerimientos de disponibilidad, capacidad y continuidad. Resultados del seguimiento a los servicios tecnológicos. Lineamientos de seguridad de la información aplicables.	P	Definir y actualizar los lineamientos e instrumentos para la continuidad y prestación de los servicios tecnológicos, incluyendo el Plan de Contingencia de TI y los Acuerdos de Niveles de Servicio (ANS), de acuerdo con las necesidades institucionales, los requerimientos de disponibilidad y recuperación, y los lineamientos de seguridad de la información aplicables.	Plan de Contingencia de TI formulado o actualizado. Acuerdos de Niveles de Servicio (ANS) definidos o actualizados. Necesidades de capacidad, disponibilidad y continuidad identificadas. Requerimientos de infraestructura y servicios tecnológicos definidos.	Líderes y responsables de los procesos de la Entidad. Proceso de Gestión de Sistemas de Información y Tecnología. Alta Dirección y procesos de la Entidad. Proveedores de servicios tecnológicos. Personas responsables de la gestión de riesgos y de la seguridad de la información. Oficina de Control Interno y organismos de control.

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) Alta Consejería Distrital de TI Alta Dirección del IDPC Todos los procesos de la Entidad	Marco normativo y lineamientos aplicables en seguridad y privacidad de la información. Necesidades y requerimientos de los procesos de la Entidad. Inventario de activos de información. Resultados de la identificación y valoración de riesgos. Resultados de seguimientos, auditorías e incidentes de seguridad.	P	Definir y actualizar las políticas, lineamientos y controles para la gestión de la seguridad y privacidad de la información, incluyendo el Manual de Políticas de Seguridad y Privacidad de la Información, de acuerdo con el marco normativo aplicable, los riesgos identificados, las necesidades institucionales y los estándares adoptados por la Entidad.	Políticas y lineamientos de seguridad y privacidad de la información definidos o actualizados. Manual de Políticas de Seguridad y Privacidad de la Información actualizado. Controles de seguridad definidos o actualizados. Necesidades de tratamiento de riesgos identificadas.	Alta Dirección y procesos de la Entidad. Personas servidoras públicas y contratistas. Personas responsables de los activos de información. Proceso de Gestión de Sistemas de Información y Tecnología. Oficina de Control Interno y organismos de control. Entidades competentes en materia de seguridad y privacidad de la información.
Alta Dirección y procesos de la Entidad. Proceso de Gestión de Sistemas de Información y Tecnología.	PETI vigente y las iniciativas, programas y proyectos de TI aprobados. Requerimientos y necesidades tecnológicas priorizadas. Recursos presupuestales, humanos, tecnológicos y físicos disponibles	H	Ejecutar las iniciativas, programas y proyectos establecidos en el Plan Estratégico de Tecnologías de la Información (PETI), articulando los recursos requeridos para su desarrollo, de acuerdo con la planeación institucional y los lineamientos de Gobierno Digital aplicables.	Iniciativas, programas y proyectos del PETI ejecutados y/o implementados. Soluciones y servicios tecnológicos implementados o fortalecidos. Proyectos de transformación digital ejecutados. Infraestructura y servicios TIC implementados, actualizados o fortalecidos Sistemas de información implementados, integrados, actualizados o mejorados	Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Alta Consejería Distrital de TIC. Todos los procesos de la Entidad. Personas servidoras públicas y contratistas. Ciudadanía y personas usuarias.
Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Alta Consejería Distrital de TIC. Alta Dirección y procesos de la Entidad. Personas servidoras públicas y contratistas.	Necesidades y requerimientos de información de los procesos y partes interesadas. Requerimientos funcionales y técnicos para la captura, procesamiento y validación de información. Sistemas de información y herramientas tecnológicas existentes. Arquitectura tecnológica y lineamientos de interoperabilidad de la Entidad. Inventario y características de las fuentes de información.	H	Implementar y administrar las herramientas tecnológicas requeridas para la captura, procesamiento y validación de la información, de acuerdo con las necesidades institucionales y los lineamientos definidos, garantizando su calidad, integridad y confiabilidad.	Herramientas y soluciones tecnológicas implementadas. Sistemas y aplicaciones configurados, integrados o ajustados. Mecanismos de captura, procesamiento y validación de información implementados. Documentación técnica y evidencias de implementación.	Alta Dirección y procesos de la Entidad. Ciudadanía y personas usuarias externas. Personas servidoras públicas y contratistas. Entidades competentes en materia de Gobierno Digital. Proceso de Gestión de Sistemas de Información y Tecnología. Oficina de Control Interno y organismos de control.
Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Alta Consejería Distrital de TIC. Alta Dirección y procesos de la Entidad. Personas servidoras públicas y contratistas.	Requerimientos funcionales y no funcionales definidos y aprobados. Solución tecnológica seleccionada y aprobada. Diseños funcionales, técnicos y de arquitectura de la solución. Especificaciones técnicas, historias de usuario, casos de uso y criterios de aceptación, cuando aplique. Arquitectura de sistemas, infraestructura tecnológica y ambientes de desarrollo, pruebas y producción. Requisitos de seguridad, privacidad, interoperabilidad, accesibilidad y usabilidad. Planes y cronogramas de desarrollo, integración e implementación. Recursos humanos, tecnológicos y financieros requeridos. Contratos, licencias, servicios tecnológicos y demás recursos necesarios para el desarrollo o adquisición de la solución.	H	Diseñar, desarrollar, integrar, implementar y mantener las soluciones de sistemas de información, de acuerdo con los requerimientos definidos, realizando las pruebas funcionales y técnicas requeridas, la actualización de la documentación asociada y las acciones de capacitación necesarias para facilitar su adecuada implementación y uso.	Sistemas de información desarrollados, actualizados o integrados. Resultados de pruebas funcionales y técnicas. Documentación técnica y funcional actualizada. Materiales o evidencias de orientación a las personas usuarias, cuando corresponda.	Líderes y responsables de los procesos de la Entidad. Personas usuarias de los sistemas de información. Proceso de Gestión de Sistemas de Información y Tecnología. Alta Dirección y procesos de la Entidad. Proveedores de servicios y soluciones tecnológicas. Equipo técnico y personas responsables del desarrollo de sistemas de información.

Alta Dirección de la Entidad. Personas servidoras públicas y contratistas. Proceso de Gestión de Sistemas de Información y Tecnología.	Catálogo de servicios de TI y niveles de servicio (ANS) establecidos. Inventario y caracterización de la infraestructura tecnológica: servidores, almacenamiento, equipos de cómputo, redes, telecomunicaciones y periféricos. Inventario y licenciamiento de software base y herramientas tecnológicas. Arquitectura tecnológica y diseños de infraestructura definidos por la Entidad. Procedimientos de operación, mantenimiento, gestión de cambios, configuraciones, incidentes y problemas. Planes y cronogramas de mantenimiento preventivo y correctivo.	H	Administrar la infraestructura tecnológica y los servicios de TI, incluyendo hardware, software base, redes y telecomunicaciones, mediante la operación y mantenimiento de los recursos tecnológicos, la gestión de cambios y configuraciones, la atención de incidentes y problemas, y la ejecución de las acciones requeridas para la continuidad de los servicios, de acuerdo con los niveles de servicio establecidos.	Infraestructura tecnológica administrada y mantenida. Servicios tecnológicos prestados. Incidentes y problemas atendidos. Cambios y configuraciones implementados. Registros de operación y mantenimiento.	Líderes y responsables de los procesos de la Entidad. Proceso de Gestión de Sistemas de Información y Tecnología. Alta Dirección y procesos de la Entidad. Proveedores de servicios tecnológicos. Personas responsables de la gestión de riesgos y de la seguridad de la información. Oficina de Control Interno y organismos de control.
Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Alta Consejería Distrital de TIC. Alta Dirección. Oficina de Control Interno y organismos de control. Proceso de Gestión de Sistemas de Información y Tecnología.	Política de Seguridad y Privacidad de la Información vigente. Manual, procedimientos, instructivos y demás instrumentos del SGSI. Matriz de riesgos de seguridad de la información y seguridad digital. Planes de tratamiento de riesgos y acciones de mitigación definidas. Controles de seguridad establecidos y criterios para su implementación. Resultados de la identificación, análisis y valoración de riesgos. Inventario y clasificación de activos de información.	H	Implementar las políticas, lineamientos, controles y medidas definidas en el marco del SGSI, incluyendo las acciones para el tratamiento de los riesgos de seguridad de la información y seguridad digital, de acuerdo con los instrumentos y lineamientos establecidos.	Políticas y lineamientos implementados. Controles y medidas de seguridad implementados. Acciones de tratamiento de riesgos ejecutadas. Evidencias de implementación de controles. Riesgos de seguridad de la información tratados.	Alta Dirección y procesos de la Entidad. Personas servidoras públicas y contratistas. Personas responsables de los activos de información. Proceso de Gestión de Sistemas de Información y Tecnología. Oficina de Control Interno y organismos de control. Entidades competentes en materia de seguridad y privacidad de la información.
Alta Dirección. Oficina de Control Interno y organismos de control. Proceso de Gestión de Sistemas de Información y Tecnología.	Resultados y evidencias de ejecución de los proyectos e iniciativas de TI. Información presupuestal y ejecución de recursos asociados a las iniciativas Reportes de incidentes, eventos y situaciones que puedan afectar el cumplimiento del PETI. Resultados de auditorías, seguimientos, evaluaciones y ejercicios de control interno.	V	Realizar seguimiento al cumplimiento de las actividades del Plan Estratégico de Tecnologías de la Información (PETI), mediante el análisis de su avance, resultados e indicadores, así como el monitoreo de los riesgos y la efectividad de los controles asociados, con el fin de identificar desviaciones y oportunidades de mejora que apoyen la toma de decisiones.	Informes de seguimiento al cumplimiento del PETI. Reportes de avance de actividades, metas e indicadores. Resultados del seguimiento a los riesgos y controles asociados. Desviaciones y oportunidades de mejora identificadas.	Todos los procesos de la Entidad. Personas servidoras públicas y contratistas. Ciudadanía y personas usuarias.

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Alta Consejería Distrital de TIC. Proceso de Gestión de Sistemas de Información y Tecnología.	Políticas y procedimientos de control de acceso y seguridad de la información. Matriz de roles, perfiles y permisos de acceso a los sistemas de información. Registros (logs) de autenticación, acceso y actividades realizadas en servidores, bases de datos y aplicaciones. Registros de eventos de seguridad y alertas generadas por las herramientas de monitoreo. Inventario de usuarios, cuentas privilegiadas y cuentas de servicio. Configuraciones y parámetros de seguridad de servidores, bases de datos y aplicaciones. Lineamientos y requisitos de Seguridad Digital, Gobierno Digital y SGSI aplicables. Resultados de auditorías y revisiones anteriores sobre controles de acceso.	V	Monitorear de manera periódica los mecanismos de control de acceso a la información, mediante el análisis de registros (logs) de servidores, bases de datos y aplicaciones, con el fin de detectar eventos anómalos, garantizar la trazabilidad de las operaciones y fortalecer la seguridad de la información.	Informes o reportes de monitoreo y revisión de registros (logs). Eventos anómalos identificados y reportados. Resultados de la verificación de los controles de acceso. Alertas o incidentes de seguridad identificados y gestionados. Recomendaciones y acciones de mejora en materia de seguridad de la información.	Alta Dirección y procesos de la Entidad. Ciudadanía y personas usuarias externas. Personas servidoras públicas y contratistas. Entidades competentes en materia de Gobierno Digital. Proceso de Gestión de Sistemas de Información y Tecnología. Oficina de Control Interno y organismos de control.
Alta Dirección y procesos de la Entidad. Personas servidoras públicas y contratistas. Proceso de Gestión de Sistemas de Información y Tecnología.	Sistemas de información desarrollados o actualizados. Requerimientos funcionales y técnicos definidos. Resultados de pruebas. Criterios de aceptación y estándares aplicables.	V	Verificar que los sistemas de información desarrollados o actualizados cumplan con los requerimientos, criterios de aceptación y estándares definidos, mediante la validación de los resultados de las pruebas y de la documentación técnica, funcional y de usuario, como condición para su aprobación y puesta en producción.	Resultados de la verificación de requerimientos y criterios de aceptación. Observaciones o inconsistencias identificadas. Aprobación para puesta en producción, cuando corresponda.	Líderes y responsables de los procesos de la Entidad. Personas usuarias de los sistemas de información. Proceso de Gestión de Sistemas de Información y Tecnología. Alta Dirección y procesos de la Entidad. Proveedores de servicios y soluciones tecnológicas. Equipo técnico y personas responsables del desarrollo de sistemas de información.
Alta Dirección y procesos de la Entidad. Proceso de Gestión de Sistemas de Información y Tecnología.	Registros de disponibilidad, continuidad, capacidad y rendimiento de los servicios. Reportes y métricas de monitoreo de infraestructura, redes, servidores, aplicaciones y demás componentes tecnológicos. Reportes de incidentes, problemas, solicitudes y requerimientos de servicio. Registros de tiempos de respuesta y solución frente a los ANS. Indicadores de gestión y desempeño de los servicios de TI.	V	Realizar seguimiento y evaluar el desempeño de la infraestructura y los servicios de TI, mediante el análisis de la disponibilidad y continuidad de los servicios, el cumplimiento de los Acuerdos de Niveles de Servicio (ANS), la atención de incidentes y problemas, los indicadores establecidos y la satisfacción de los usuarios, con el fin de identificar desviaciones y oportunidades de mejora.	Informes y reportes de seguimiento al desempeño de la infraestructura y los servicios de TI. Resultados de disponibilidad y continuidad de los servicios tecnológicos. Reportes de cumplimiento de los ANS. Resultados del análisis de incidentes y problemas. Resultados de los indicadores de desempeño de TI. Resultados de medición de la satisfacción de los usuarios. Recomendaciones y acciones de mejora propuestas.	Líderes y responsables de los procesos de la Entidad. Proceso de Gestión de Sistemas de Información y Tecnología. Alta Dirección y procesos de la Entidad. Proveedores de servicios tecnológicos. Personas responsables de la gestión de riesgos y de la seguridad de la información. Oficina de Control Interno y organismos de control.
Proceso de Gestión de Sistemas de Información y Tecnología.	Matriz de riesgos de seguridad de la información y seguridad digital. Plan de tratamiento de riesgos y acciones definidas. Controles de seguridad implementados y criterios de evaluación. Resultados del monitoreo de riesgos y controles. Indicadores de desempeño del SGSI y metas establecidas. Registros de incidentes, eventos y vulnerabilidades de seguridad.	V	Realizar seguimiento a los riesgos de seguridad de la información y seguridad digital, evaluar la efectividad de los controles implementados y el desempeño del SGSI, mediante actividades de monitoreo, evaluación y auditoría, con el fin de identificar desviaciones y oportunidades de mejora.	Informes de seguimiento y evaluación del SGSI. Resultados del monitoreo de riesgos y controles. Evaluación de la efectividad de los controles. Resultados de auditorías y verificaciones. Recomendaciones y acciones de mejora.	Alta Dirección y procesos de la Entidad. Personas servidoras públicas y contratistas. Personas responsables de los activos de información. Proceso de Gestión de Sistemas de Información y Tecnología. Oficina de Control Interno y organismos de control. Entidades competentes en materia de seguridad y privacidad de la información.

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Alta Consejería Distrital de TIC. Proceso de Gestión de Sistemas de Información y Tecnología.	Resultados del seguimiento y evaluación de la gestión estratégica de TI. Informes de avance y cumplimiento de las iniciativas, programas y proyectos del PETI. Indicadores de gestión de TI y resultados frente a las metas establecidas. Identificación de desviaciones, retrasos, incumplimientos y oportunidades de mejora.	A	Implementar los ajustes y acciones de mejora derivados del seguimiento a la gestión estratégica de TI, incluyendo la actualización de la programación del PETI, así como la ejecución de las acciones requeridas frente a los riesgos identificados o materializados, de acuerdo con las necesidades identificadas y los cambios en las prioridades institucionales.	Acciones de mejora implementadas. PETI actualizado o reprogramado, cuando corresponda. Acciones de tratamiento de riesgos implementadas.	Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Alta Consejería Distrital de TIC. Todos los procesos de la Entidad. Personas servidoras públicas y contratistas. Ciudadanía y personas usuarias.
Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Alta Consejería Distrital de TIC. Proceso de Gestión de Sistemas de Información y Tecnología.	Política de Seguridad y Privacidad de la Información y demás políticas de seguridad de la Entidad. Modelo y metodología institucional para la gestión de riesgos. Inventario y clasificación de los activos de información. Identificación y valoración de riesgos de seguridad de la información. Matriz de riesgos y controles asociados. Lineamientos de Gobierno Digital, Seguridad Digital, MSPI, SGSI e ISO/IEC 27001 que resulten aplicables.	A	Definir, implementar y actualizar los controles necesarios para la prevención, mitigación y tratamiento de los riesgos asociados a los activos de información, en concordancia con las políticas de seguridad de la información y los lineamientos del modelo de gestión de riesgos, garantizando la protección de la confidencialidad, integridad y disponibilidad de la información.	Controles de seguridad de la información implementados y mantenidos. Medidas de tratamiento y mitigación de riesgos implementadas. Controles asociados a los activos de información actualizados. Evidencias de implementación y operación de los controles. Reportes sobre la implementación y estado de los controles de seguridad.	Alta Dirección y procesos de la Entidad. Ciudadanía y personas usuarias externas. Personas servidoras públicas y contratistas. Entidades competentes en materia de Gobierno Digital. Proceso de Gestión de Sistemas de Información y Tecnología. Oficina de Control Interno y organismos de control.
Alta Dirección y procesos de la Entidad. Personas servidoras públicas y contratistas. Proceso de Gestión de Sistemas de Información y Tecnología.	Resultados de las verificaciones y pruebas. Observaciones e inconsistencias identificadas. Reportes derivados de la operación. Necesidades reportadas por las personas usuarias.	A	Implementar las acciones correctivas y de mejora identificadas a partir de los resultados de las pruebas, validaciones, seguimiento a la operación y necesidades reportadas por los usuarios, realizando los ajustes requeridos en los sistemas de información para fortalecer su funcionamiento y responder a las necesidades institucionales.	Acciones correctivas y de mejora implementadas. Sistemas de información ajustados o mejorados. Registro de los ajustes realizados.	Líderes y responsables de los procesos de la Entidad. Personas usuarias de los sistemas de información. Proceso de Gestión de Sistemas de Información y Tecnología. Alta Dirección y procesos de la Entidad. Proveedores de servicios y soluciones tecnológicas. Equipo técnico y personas responsables del desarrollo de sistemas de información.
Proceso de Gestión de Sistemas de Información y Tecnología.	Resultados del seguimiento al desempeño. Desviaciones identificadas. Incumplimientos de ANS, cuando se presenten. Resultados del análisis de incidentes y problemas. Oportunidades de mejora identificadas.	A	Implementar las acciones correctivas y de mejora derivadas de los resultados del seguimiento al desempeño de la infraestructura y los servicios de TI, orientadas a fortalecer su disponibilidad, continuidad, capacidad y calidad, así como el cumplimiento de los niveles de servicio establecidos.	Acciones correctivas y de mejora implementadas. Infraestructura tecnológica y servicios de TI ajustados y fortalecidos. Mejoras implementadas en disponibilidad, continuidad y capacidad de los servicios. Evidencias de implementación y cierre de las acciones de mejora. Resultados de verificación de la efectividad de las acciones implementadas	Líderes y responsables de los procesos de la Entidad. Proceso de Gestión de Sistemas de Información y Tecnología. Alta Dirección y procesos de la Entidad. Proveedores de servicios tecnológicos. Personas responsables de la gestión de riesgos y de la seguridad de la información. Oficina de Control Interno y organismos de control.

Proceso de Gestión de Sistemas de Información y Tecnología. Oficina de Control Interno y organismos de control.	Resultados del seguimiento y monitoreo de los riesgos de seguridad de la información y seguridad digital.	A	Implementar las acciones correctivas y de mejora derivadas del seguimiento a los riesgos, la evaluación de los controles, las auditorías, los incidentes de seguridad y demás resultados de la evaluación del SGSI, orientadas a fortalecer su eficacia y mejora continua.	Acciones correctivas y de mejora implementadas.	Alta Dirección y procesos de la Entidad. Personas servidoras públicas y contratistas. Personas responsables de los activos de información. Proceso de Gestión de Sistemas de Información y Tecnología. Oficina de Control Interno y organismos de control. Entidades competentes en materia de seguridad y privacidad de la información.
	Resultados de revisiones y evaluaciones del SGSI.			Riesgos y controles ajustados o fortalecidos.	
	Reportes y análisis de incidentes y eventos de seguridad de la información.			Hallazgos y desviaciones atendidos.	
	Indicadores de desempeño del SGSI y resultados frente a las metas establecidas.			Acciones derivadas de incidentes de seguridad implementadas.	
	Planes de tratamiento de riesgos y acciones pendientes de ejecución.			Planes de mejoramiento y acciones de tratamiento actualizados.	
	Análisis de causas de las desviaciones, incidentes y no conformidades identificadas.			Evidencias de implementación y cierre de acciones. Mejoras implementadas en el SGSI.	
	Recomendaciones de organismos de control, auditoría y demás partes interesadas.				
	Lineamientos aplicables de Gobierno Digital, Seguridad Digital, MSPi y SGSI.				

CONTROL DE CAMBIOS					
FECHA	VERSION	CAMBIOS INTRODUCIDOS		TIPO DE CAMBIO	ORIGEN
12/06/2015	1	Creación del documento		Mejora	
21/12/2018	2	Ajuste del documneto de política y actividades del proceso		Mejora	
30/05/2019	3	Actualización de formato de caracterización y contenido		Mejora	
30/06/2021	4	Actualización de las actividades de PHVA del proceso		Mejora	
25/04/2023	5	Actualización de formato, ajuste del objetivo del proceso, inclusión de actividades en la etapa actuar del dominio de Servicios de T.I, ajuste en los nombres de los proveedores de los procesos		Mejora	Análisis de las necesidades y prioridades en la prestación del servicio
19/09/2026	6	Actualización integral del proceso de Gestion de Sistemas de Información y Tecnología, incorporando enfoque estratégico, seguridad de la información, gestión de servicios, riesgos y mejora continua, alineado con lineamientos normativos y necesidades institucionales.		Mejora	Resultado de revisión y autocontrol

CRÉDITOS		
Elaboró:	Revisó:	Aprobó:
Nombre: MARY ELIZABETH ROJAS MUÑOZ	Nombre: Nadia Camila Cruz Cañas	Nombre: Sandra Carolina Fíórez Gutiérrez
Cargo o Rol: Contratista Subdirección de Gestión Corporativa	Cargo o Rol: Contratista Subdirección de Gestión Corporativa	Cargo o Rol: Subdirector Subdirección de Gestión Corporativa

Documento de aprobación: Memorando interno con N° radicado 20265000176923 del 19-09-2026