Plan de Seguridad y Privacidad de la Información

Secretaría TIC, Innovación y Gobierno Abierto
Gobernación de Nariño

2026 | Versión 1

Tabla de contenido

Introducción

La información es considerada el activo más importante y valioso para todas las organizaciones, y un recurso indispensable para el desarrollo y cumplimiento de sus objetivos misionales, esta puede llegar a ser vulnerable, sensible o crítica y por lo tanto requiere de una evaluación para determinar su nivel de protección necesario para mitigar o evitar posibles situaciones de riesgo e impacto asociado a la pérdida de su disponibilidad, integridad o confidencialidad.

Para la Gobernación de Nariño es indispensable establecer un modelo de gestión de seguridad y privacidad de la información, para salvaguardar de posibles afectaciones a la información que soportan los procesos y la gestión diaria de la entidad en el desempeño de sus funciones y en todos sus aspectos, garantizando la seguridad de los datos, el cumplimiento de las normas legales, las políticas de seguridad digital y continuidad del servicio de MinTIC, la norma NTC/IEC ISO 27001:2022, el Modelo de Seguridad y Privacidad de Información MSPI de MinTIC y el Modelo Integrado de Planeación y Gestión MIPG de la entidad.

El Sistema de Seguridad y Privacidad de la información está determinado por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la Entidad, todo con el objetivo de preservar la confidencialidad, disponibilidad e integridad de los activos de la información, garantizando su buen uso y la privacidad de los datos, todo esto enmarcado en el ciclo PHVA (Planear, Hacer, Verificar y Actuar), para crear condiciones de uso confiable en el entorno digital y físico de la información, mediante un enfoque basado en la gestión de riesgos e implementación de un conjunto de actividades, estrategias, herramientas y controles de seguridad de la información.

1. Objetivo

Establecer acciones que apoye el establecimiento, operación, mejora continua y sostenibilidad del Sistema de Gestión de Seguridad y Privacidad de la Información de la Gobernación de Nariño, acorde con los requerimientos de la entidad y en cumplimiento a las disposiciones legales vigentes emitidas por el Gobierno Nacional.

2. Alcance

El alcance del Plan de Seguridad y Privacidad de la Información abarca el diagnóstico, la planificación, implementación, evaluación y mejora continua el sistema, aplicado a todas las áreas, procesos y procedimientos de la entidad respaldados por la infraestructura tecnológica clasificada y administrada por la Secretaría TIC, Innovación y Gobierno Abierto, y que conforman el Modelo Integrado de Planeación y Gestión – MIPG de la Gobernación de Nariño.

3. Marcos

3.1. Marco conceptual

Activo de información: toda la información, elementos, servicios o personas, relacionados con la producción o tratamiento de información, que tengan valor para la entidad, y por lo tanto se deben administrar y proteger.

Amenaza: es una circunstancia que tiene el potencial de causar un daño o una pérdida.

Anexo SL: nuevo esquema definido por International Organization for Standarization - ISO para todos los Sistemas de Gestión acorde al nuevo formato llamado “Anexo SL”, que proporciona una estructura uniforme como el marco de un sistema de gestión genérico.

Análisis de riesgos: utilización sistemática de la información disponible, para identificar amenazas y vulnerabilidades sobre activos de información.

Archivo: conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia.

Autorización: consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.

Bases de datos personales: conjunto organizado de datos personales que sea objeto de Tratamiento.

Ciberseguridad: es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de una entidad.

Confidencialidad: propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

Control: medida, política o procedimiento implementado para proteger sistemas, redes, programas y datos digitales contra amenazas, accesos no autorizados y daños, asegurando su confidencialidad, integridad y disponibilidad, mediante herramientas como controles de acceso para prevenir ataques y garantizar la continuidad de las operaciones en línea.

Datos abiertos: son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

Datos biométricos: parámetros físicos únicos de cada persona que comprueban su identidad y se evidencian cuando la persona o una parte de ella interacciona con el sistema.

Datos personales: cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Datos personales públicos: es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

Datos personales privados: es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

Disponibilidad: propiedad de ser accesible y utilizable por los usuarios autorizados de la entidad autorizados.

Estándar: regla que especifica una acción o respuesta que se debe seguir a una situación dada. Son orientaciones obligatorias que buscan hacer cumplir las políticas.

Gestión del riesgo: proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Impacto: resultado o consecuencia de la materialización de un incidente de seguridad digital para una entidad.

Incidente de seguridad de la información: resultado de intentos intencionales o accidentales de romper las medidas de seguridad de la información impactando en la confidencialidad, integridad o disponibilidad de la información.

Información pública: es aquella información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.

Información: es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno. Indicación o evento llevado al conocimiento de una persona o de un grupo.

Integridad: propiedad de exactitud y completitud de la información.

Mejora continua: Evaluación y fortalecimiento permanente de los controles de seguridad.

Privacidad: derecho de los individuos a controlar la recopilación, uso y divulgación de sus datos personales, decidiendo quién puede acceder a ellos y con qué propósito, protegiéndolos de accesos no autorizados y mal uso, y asegurando el respeto a la autonomía personal en el entorno digital.

Responsabilidad: compromiso institucional con la seguridad y privacidad de la información.

Riesgo: es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o de los procesos. Se expresa en términos de probabilidad y consecuencias.

Riesgo de seguridad y privacidad: potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización. Se mide en términos de probabilidad y consecuencias.

Seguridad de la información: preservación de la confidencialidad, integridad y disponibilidad de la información.

Sistema de Gestión de Seguridad de la Información - SGSI: conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua.

Sistema de información: se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales

Trazabilidad: cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

Usuarios: personas que, directa o indirectamente, tengan algún tipo de relación con

la Entidad y/o que tengan acceso a los recursos tecnológicos de la Entidad

Vulnerabilidad: debilidad de un activo o control que puede ser explotada por una o más amenazas.

3.2. Marco normativo

En esta sección se incluye la normatividad vigente y aplicable que está directamente relacionada con el plan institucional.

Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1083 de 2015	Por medio del cual se expide el Decreto único Reglamentario del Sector de Función Pública, el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de Gobierno Digital, antes Gobierno en Línea y Seguridad Digital.
Decreto 612 de 2018	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
Decreto 767 de 2022	Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Resolución 500 de 2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital
Resolución 1519 de 2020.	Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
Resolución 746 de 2022	Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la

	Resolución No. 500 de 2021.
CONPES 3701 de 2011	Lineamientos de Política para Ciberseguridad y Ciberdefensa.
CONPES 3854 de 2017	Política Nacional de Seguridad digital.
CONPES 3995 de 2020	Confianza y Seguridad Digital
CONPES 4069 de 2022	Política Nacional de Ciencia, tecnología e innovación 2022 – 2031.
Modelo de Seguridad y Privacidad de la información MSPI V5 de 2025 MinTIC	Documento Maestro del Modelo de Seguridad y Privacidad de la Información dirigida a las entidades del Estado
ISO/IEC 27001:2022	Estándar internacional que establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información.

4. Descripción del desarrollo del Plan

4.1. Diagnóstico

El estado actual de la Gestión de Seguridad y Privacidad de la Información en la Gobernación de Nariño, de acuerdo al autodiagnóstico realizado a través del Instrumento de identificación de la línea base de seguridad de MinTIC, es INICIAL.

Este diagnóstico se basa en métricas cuantitativas del instrumento MinTIC, y se actualizará anualmente para rastrear avances hacia nivel efectivo, gestionado y optimizado.

Evaluación de efectividad de controles - ISO 27001:2022 Anexo A

No.	Evaluación de Efectividad de controles	
	DOMINIO	Nivel de Madurez
A.5	CONTROLES ORGANIZACIONALES	INICIAL
A.6	CONTROLES DE PERSONAS	INICIAL
A.7	CONTROLES FÍSICOS	INICIAL
A.8	CONTROLES TECNOLÓGICOS	INICIAL
PROMEDIO EVALUACIÓN DE CONTROLES		INICIAL

Avance cláusulas del Modelo de operación (PHVA)

AÑO	COMPONENTE (PHVA)	CLAUSULAS	% de Avance Actual	% Avance Esperado
2025	Planificación	Contexto de la organización	6%	14%
		Liderazgo	9%	14%
		Planificación	7%	14%
		Soporte	3%	14%
	Implementación	Operación	6%	16%
	Evaluación de Desempeño	Evaluación del desempeño	3%	14%
	Mejora Continua	Mejora	1%	14%
TOTAL			35%	100%

4.2. Política general de Seguridad y Privacidad de la Información

La Gobernación de Nariño, comprometida con sus usuarios, proveedores, clientes y de más partes interesadas, establece la necesidad de implementar un Sistema de Gestión de Seguridad y Privacidad de la información encaminado a proteger los activos de la información a través de la implementación de Política general de seguridad y privacidad de la información y Políticas específicas, procedimientos, lineamientos, como apoyo en la implementación de herramientas tecnológicas de prevención y forjar una cultura de concientización de seguridad de la información en todos los funcionarios y contratistas de la entidad.

Todo esto con el objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de los activos de información, garantizando la continuidad del servicio y minimizar el impacto causado por los riesgos identificados, logrando así mantener la confianza y responder frente a las necesidades de sus diferentes grupos de interés.

4.3. Roles y responsabilidades

La Gobernación de Nariño define los roles y responsabilidades para la implementación del MSPI y el cumplimiento de los lineamientos de seguridad descritos en la Política de seguridad y privacidad de la información y los demás documentos derivados.

Rol	Responsabilidades
Comité institucional de Gestión y Desempeño	● Aprobación y seguimiento de políticas, planes, programas, proyectos, estrategias y herramientas necesarias para la implementación y mejora continua del SGSI en la Gobernación de Nariño. ● Promover activamente una cultura de seguridad y privacidad de la información basada en riesgos, para la entidad. ● Aprobar los roles y responsabilidades relacionados con la seguridad de la información en todos los niveles de la entidad. ● Aprobar y adoptar decisiones que permitan la gestión y minimización de riesgos críticos de seguridad de la información. ● Las demás que tengan competencia en relación con el estudio, análisis y recomendaciones en materia de seguridad y privacidad de la información.
Responsable de Seguridad de la Información	● Liderar la planificación, implementación, despliegue y sostenibilidad del SGSI en la entidad. ● Proyectar y actualizar, promover y mantener la Política de Seguridad y Privacidad de la Información. ● Proyectar y actualizar periódicamente, la Política de Seguridad y

Rol	Responsabilidades
	Privacidad de la Información y Tratamiento de datos personales, y presentar para aprobación del comité de gestión y desempeño institucional. ● Socializar y promover el cumplimiento de las Políticas de Seguridad y Privacidad de la Información y Tratamiento de datos personales. ● Definir, elaborar e implementar las políticas específicas, planes, procedimientos, estándares y demás documentos relacionados con el SGSI. ● Realizar seguimiento a la implementación del SGSI y cronograma de ejecución, para gestionar la mejora continua del mismo. ● Liderar la gestión de Riesgos de seguridad de la información, implementación de controles, y seguimiento al plan de tratamiento de riesgos. ● Liderar la formulación del plan de comunicaciones y sensibilización de seguridad y privacidad de la información, y su implementación en todas las dependencias de la entidad, usuarios externos y demás partes interesadas. ● Gestionar los recursos físicos, humanos y financieros, necesarios para la implementación y mejora continua del SGSI en la entidad. ● Definir, socializar e implementar los procedimientos de Gestión de Incidentes de seguridad de la información en la entidad. ● Seguimiento permanente a los incidentes de seguridad, y poner en conocimiento de las dependencias con competencia funcional cuando se detecten irregularidades o prácticas que atenten contra la seguridad y privacidad de la información de acuerdo con la normatividad vigente. ● Liderar el comité de seguridad de la información, para asegurar el liderazgo y cumplimiento de los roles y responsabilidades definidos en el SGSI. ● Atender las auditorías internas y externas en materia de seguridad de la información, y gestionar los planes de mejora producto de las mismas. ● Definir Indicadores de la Seguridad y Privacidad de la Información, y medición de cumplimiento periódico.
Equipo estratégico de Seguridad y Privacidad de la Información	● Apoyar la implementación del SGSI en la Gobernación de Nariño, según el Modelo de Seguridad y privacidad de la Información de MinTIC y las normas vigentes relacionadas. ● Revisar los diagnósticos del estado de la seguridad de la información en la entidad. ● Acompañar e impulsar el desarrollo de proyectos de seguridad. ● Coordinar y dirigir acciones específicas que ayuden a proveer un

Rol	Responsabilidades
	ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de la entidad. ● Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información. ● Aprobar el uso de metodologías y procesos específicos para la seguridad de la información. ● Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos. ● Realizar seguimiento periódico del SGSI (por lo menos una vez al año), y aplicar acciones pertinentes según los resultados obtenidos y la medición de indicadores de eficiencia y eficacia. ● Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad. ● Poner en conocimiento de la entidad, los documentos generados al interior del equipo de seguridad de la información que impacten de manera transversal a la misma. ● Las demás funciones inherentes a la naturaleza del equipo.
Equipo operativo del proyecto	● Apoyar al responsable del SGSI, en la proyección e implementación de las políticas, planes, proyectos y procedimientos de seguridad de la información y tratamiento de datos personales, según las actividades y responsabilidades asignadas. ● Apoyar en la adquisición de infraestructura (bienes y servicios) tecnológica para fortalecer la seguridad informática en la entidad. ● Implementar controles de seguridad de acuerdo al plan de tratamiento de riesgos y declaración de aplicabilidad. ● Operar la infraestructura de red, dispositivos de seguridad informática y sistemas de información, con las reglas y mecanismos necesarios para garantizar la confidencialidad, integridad y disponibilidad de los activos de información de la entidad. ● Gestionar los incidentes de seguridad y documentarlos para la construcción de la base de conocimientos, control y trazabilidad permanente. ● Participar en las reuniones y auditorías a las que sea designado por el responsable del SGSI, y gestionar la información y/o actividades que le sean asignadas. ● Oficiar como consultores de primer nivel en cuanto a las dudas técnicas y de procedimiento que se puedan suscitar en el desarrollo del proyecto. ● Garantizar y poder informar oportunamente el ejercicio de los derechos de los dueños de los datos personales identificados. ● Debe tramitar continuamente las consultas, solicitudes o reclamos, esto se define actualmente como atención de los PQR

Rol	Responsabilidades
	alineados a los datos personales. ● Tener el compromiso de utilizar únicamente los datos personales que hayan sido obtenidos con autorización. ● Siempre respetar y controlar las condiciones de privacidad y seguridad de la información del titular que interactúa con la Gobernación de Nariño. ● Responder por el cumplimiento de las instrucciones y requerimientos impartidos por la autoridad legal o administrativa correspondiente.
Usuarios	● Conocer, aplicar y respetar las normas, procedimientos, manuales y buenas prácticas, definidos en las políticas de seguridad de la información y tratamiento de datos personales de la entidad del SGSI. ● Mantener la confidencialidad, integridad y disponibilidad de la información, según las directrices impartidas por la Secretaría TIC y las restricciones de seguridad informática aplicadas en los activos de información. ● Hacer buen uso de los activos de información de la entidad, para fines institucionales y según los permisos de acceso autorizados. ● Participar activamente en la ejecución del plan de capacitación y sensibilización en seguridad de la información, adquirir los conocimientos y competencias necesarias para la protección, buen uso de los activos de información y minimizar la materialización de los riesgos. ● Cumplir la legislación y regulación vigente en materia de Seguridad y Privacidad de la Información. ● Notificar al responsable de seguridad y Soporte Técnico (Secretaría TIC) las anomalías o incidentes de seguridad, así como las situaciones sospechosas.

4.4. Procedimientos de seguridad de la información

Para la gestión de la seguridad en la entidad se crearon procedimientos alineados al Modelo de seguridad y privacidad de la información de MinTIC, los cuales serán implementados en la Secretaría TIC de la Gobernación de Nariño durante la vigencia 2026 y en adelante con su correspondiente mejoramiento continuo:

- Control de acceso
- Gestión del Cambio
- Gestión de Copias de seguridad
- Gestión de incidentes de seguridad digital
- Análisis de Vulnerabilidades

4.5. Metodología de gestión de activos de información

Teniendo en cuenta la metodología del inventario de activos de la información en el cual se dan las pautas para la construcción de la matriz de identificación de los activos de la información por cada proceso, se identificó y actualizó el inventario de activos de la información de la infraestructura tecnológica de la entidad correspondiente al Proceso Gestión de Tecnología, sobre el cual se realizó la valoración de criticidad de cada activo según los principios de confidencialidad, disponibilidad e integridad, el cual fue aprobado por el Comité Institucional de Gestión y Desempeño en la vigencia 2025.

Matriz de inventario de activos de información

GOBERNACIÓN DE NARIÑO	INVENTARIO DE ACTIVOS DE INFORMACIÓN DE LA GOBERNACIÓN DE NARIÑO	CÓDIGO: GTC-F-10 VERSIÓN: 02 FECHA DE VERSIÓN: 19/11/2025 PÁGINA:

COLOMBIA POTENCIA DE LA VIDA		TIC
ENTIDAD	GOBERNACIÓN DE NARIÑO	

IDENTIFICACIÓN DEL ACTIVO DE INFORMACIÓN (LEY 594 DE 2000 - LEY 1712 DE 2014- DECRETO 103 DE 2015 - DECRETO 1080 DE 2015 - ISO 27001)														CLASIFICACIÓN DEL ACTIVO DE INFORMACIÓN (ISO 27001)				
Macroproceso	Proceso	Identificador	Tipo	Oficina	Serie documental	Subserie documental	Nombre	Nombre del responsable de la producción de la información (Propietario del activo)	Nombre del responsable de la información (Custodio del activo)	Fecha de ingreso del activo al archivo	Soporte de registro	Medio de conservación	Idioma	Confidencialidad	Integridad	Disponibilidad	Criticidad del activo	Es Infraestructura Crítica Cibernética
APOYO	Gestión de Tecnología	GTC	Hardware	SECRETARÍA TIC, INNOVACIÓN Y GOBIERNO ABIERTO	ND	ND	CENTROS DE CABLEADO	Grupo interno de trabajo Secretaría TIC	Grupo interno de trabajo Secretaría TIC	ND	Físico	DATACENTER Secretaría TIC Centros de cableado segundo y tercer piso del edificio central, NA	Español	INFORMACIÓN PÚBLICA CLASIFICADA	ALTO	ALTO	ALTO	SI
APOYO	Gestión de Tecnología	GTC	Hardware	SECRETARÍA TIC, INNOVACIÓN Y GOBIERNO ABIERTO	ND	ND	SWITCHES	Grupo interno de trabajo Secretaría TIC	Grupo interno de trabajo Secretaría TIC	ND	Físico	DATACENTER Secretaría TIC, NA	Español	INFORMACIÓN PÚBLICA CLASIFICADA	ALTO	ALTO	ALTO	SI

4.6. Identificación de riesgos de seguridad de la información

Sobre el inventario de activos de información actualizado se realizará la identificación y valoración de riesgos de seguridad y privacidad de la información utilizando la matriz actualizada de MinTIC, en la cual se definen los Criterios de probabilidad e impacto y el nivel de criticidad del riesgo identificado, teniendo en cuenta el Modelo nacional de gestión de riesgos de seguridad de la información en entidades públicas del MinTIC.

Matriz de Identificación, valoración y tratamiento de riesgos

COLOMBIA POTENCIA DE LA VIDA

MATRIZ RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

TIC

ENTIDAD

Nombre de la Entidad: Gobernación de Nariño

Proceso	Referencia	Activo de Información	Tipo de activo	Amenazas (Causa Inmediata)	Vulnerabilidades (Causa raiz)	Tipo de riesgo	Descripción del Riesgo	Clasificación riesgo	Frecuencia	% Probabilidad inherente	Probabilidad inherente	% Impacto inherente	Impacto inherente	No Control	Control Anexo A
Gestión de Tecnologia	1	Correo electrónico	Servicio	Falla del proveedor del servicio Falla en la oportunidad de contratación del servicio Falla en la red de comunicaciones de la entidad	Ausencia de acuerdos de nivel de servicio y penalización por incumplimientos. Procedimientos inadecuados de planificación y contratación. Cableado o equipos de red deficientes y sin	Pérdida de disponibilidad Perdida de Integridad	Probalidad de afectacion económica y legal por no acceso a la información y medios de comunicación debido la indisponibilidad del correo electrónico corporativo	Fraude externo Fraude interno Ejecución y administración de procesos	8688	100%	Muy alta	100%	Catastrófico		
Gestión de Tecnologia	2	Internet	Servicio	Falla del provedor del servicio Falla en la oportunidad de contratación del servicio Falla en la red de comunicaciones de la entidad Personal Técnico no idóneo o	Ausencia de acuerdos de nivel de servicio y penalización por incumplimientos. Procedimientos inadecuados de planificación y contratación. Cableado o equipos de red deficientes y sin monitoreo.	Pérdida de disponibilidad	Probalidad de afectacion económica, legal y de la imagen institucional, por la no prestación oportuna del servicio debido a fallos en las comunicaciones	Ejecución y administración de procesos Fallas tecnológicas	8688	100%	Muy alta	100%	Catastrófico		

5. Matriz operativa del plan institucional

La matriz operativa del presente plan institucional contiene varias actividades de gestión que permitirán cumplir con el objetivo general planteado anteriormente. Con el propósito de medir estas actividades se incluye los respectivos productos y las metas que se programaron para la presente vigencia. Cada actividad tiene definida la fecha límite para su ejecución y la evidencia que soporta el cumplimiento de cada una. Finalmente, se relaciona el responsable quien liderará la articulación institucional que sea necesaria para lograr la ejecución satisfactoria de este plan.

Actividad de gestión	Producto	Meta	Fecha límite mm/año	Soporte o evidencia	Responsable
Socialización de la Política de seguridad y privacidad de la información a los funcionarios y contratistas de la entidad.	Una Política de seguridad y privacidad de la información socializada al personal de la entidad por dependencias.	1	12/2026	Correos electrónicos Publicaciones en página web e Intranet institucional	Secretaría TIC, Innovación y Gobierno Abierto
Ejecución parcial del Plan de implementación de la Política de Tratamiento de datos personales.	Un Plan de implementación de la Política de tratamiento de datos personales ejecutado parcialmente en 50%.	1	12/2026	Acciones de implementación	Secretaría TIC, Innovación y Gobierno Abierto
Implementación parcial de la Política de seguridad de la información en la relación con proveedores.	Una Política de seguridad en la relación con proveedores aprobada por comité institucional, socializada al personal e implementada parcialmente en 50%.	1	12/2026	Política aprobada, socializada e implementada parcialmente Acciones de implementación	Secretaría TIC, Innovación y Gobierno Abierto
Implementación del procedimiento de gestión de incidentes de seguridad digital (reporte a COLCERT de MinTIC).	Uno o más Incidentes de seguridad reportados y gestionados (la cantidad que se presente)	1	12/2026	Base de datos de incidentes de seguridad gestionados	Secretaría TIC, Innovación y Gobierno Abierto
Socializar e Implementar procedimiento de pantalla y escritorio limpio, mediante la aplicación de buenas prácticas en el uso de los equipos de cómputo.	Un Procedimiento de pantalla y escritorio limpio socializado e implementado a los funcionarios y contratista de la entidad.	1	12/2026	Soporte de socialización e implementación del procedimiento Sensibilización y publicidad sobre buenas prácticas	Secretaría TIC, Innovación y Gobierno Abierto

Actividad de gestión	Producto	Meta	Fecha límite mm/año	Soporte o evidencia	Responsable
Actualización del inventario de activos de información para tres procesos de la entidad: Gestión de tecnología (Secretaría TIC), Gestión Financiera (Secretaría de Hacienda) y Gestión de Contratación (Departamento de Contratación), y presentar para aprobación al comité institucional.	Tres procesos actualizados en la Matriz de inventario de activos de información: Gestión de tecnología, Gestión Financiera y Gestión de Contratación.	3	11/2026	Inventario de activos de información actualizado, aprobado y publicado.	Secretaría TIC, Innovación y Gobierno Abierto
Implementación del Plan de Capacitación y sensibilización en Seguridad Digital, mediante socialización y difusión de materia publicitario sobre Políticas, procedimientos y buenas prácticas en seguridad digital.	Un plan de capacitación y sensibilización en seguridad digital ejecutado.	1	12/2026	Correos electrónicos Publicaciones en intranet. Publicidad física. Registro de asistencia a socialización	Secretaría TIC, Innovación y Gobierno Abierto
Gestionar el sistema antivirus licenciado e Implementado en los equipos de cómputo de la entidad, mediante el seguimiento y monitoreo permanente.	Dos reportes de monitoreo sistema antivirus.	2	12/2026	Dos reportes de monitoreo sistema antivirus	Secretaría TIC, Innovación y Gobierno Abierto
Gestionar y monitorear de manera permanente los dispositivos firewall de seguridad interna y perimetral implementados en la Secretaría TIC.	Dos reportes de monitoreo dispositivos firewall.	2	12/2026	Reportes de actualización y monitoreo de equipos firewall	Secretaría TIC, Innovación y Gobierno Abierto
Elaboración del Plan de Recuperación de Desastres de Infraestructura Tecnológica.	Un plan de recuperación de desastres de infraestructura tecnológica elaborado y socializado en Secretaría TIC.	1	12/2026	Plan de recuperación de desastres documentado y socializado en Secretaría TIC	Secretaría TIC, Innovación y Gobierno Abierto

6. Monitoreo y seguimiento.

El responsable de este plan es el Secretaría TIC, Innovación y Gobierno Abierto y su equipo de trabajo, quien deberá liderar la ejecución del mismo y articular esfuerzos con las demás dependencias para lograr el cumplimiento de las actividades aquí planteadas. Así mismo, de manera periódica realizará ejercicios de autocontrol con su equipo de trabajo para verificar el avance de las mismas, identificar alertas tempranas y garantizar la ejecución de las actividades de gestión.

Por su parte, la Secretaría de Planeación realizará monitoreo permanente al cumplimiento del presente plan para determinar el avance del mismo y socializar los resultados en el Comité Institucional de Gestión y Desempeño (CIGD). Cuando se requiera, brindará acompañamiento a la dependencia responsable del presente plan para que realice los ajustes que sean necesarios y se sometan a consideración del CIGD para su respectiva aprobación.

El seguimiento lo realizarán conjuntamente la Secretaría de Planeación y la Oficina de Control Interno de Gestión de manera semestral o en el momento en que se requiera.

7. Revisión, aprobación y verificación.

Revisión:	Aprobación:	Verificación:
Jonnathan Huertas Salas	**Jonnathan Huertas Salas**	**Armando Rosero García**
Secretario TIC, Innovación y Gobierno Abierto	Secretario TIC, Innovación y Gobierno Abierto	Secretario de Planeación