SAN GIL

Instituto de **Cultura y Turismo**

PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - PESI

Contenido

1. INTRODUCCIÓN

El Instituto de Cultura y Turismo del Municipio de San Gil, en cumplimiento de su compromiso con la mejora continua, la gestión eficiente de los riesgos tecnológicos y la protección de los derechos de los ciudadanos, presenta el Plan Estratégico de Seguridad y Privacidad de la Información (PESI). Este documento define las directrices y acciones prioritarias para proteger los activos de información, garantizar la continuidad institucional y fortalecer la confianza de los usuarios en los servicios ofrecidos.

El PESI se formula en concordancia con la Política de Gobierno Digital, los lineamientos del Modelo de Seguridad y Privacidad de la Información – MSPI, la Ley 1581 de 2012 sobre protección de datos personales, la Ley 1712 de 2014 de transparencia y acceso a la información pública, y la Resolución 500 de 2021 del MinTIC. Asimismo, adopta las buenas prácticas internacionales establecidas por la norma ISO/IEC 27001 sobre sistemas de gestión de seguridad de la información.

La seguridad y la privacidad de la información constituyen pilares fundamentales para el desarrollo de los procesos misionales, administrativos y tecnológicos del Instituto. Por tanto, este plan orienta la implementación de controles, mecanismos de gestión de riesgos y acciones formativas que permitan garantizar la confidencialidad, integridad, disponibilidad y trazabilidad de la información, así como la protección efectiva de los datos personales.

El Instituto promoverá una cultura organizacional enfocada en la seguridad digital, involucrando a todo su personal en la aplicación de este plan, y asegurando su integración con otros instrumentos de planeación institucional como el Plan Estratégico de Tecnologías de la Información (PETI) y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

2. OBJETIVO GENERAL

Diseñar e implementar una estrategia institucional de seguridad y privacidad de la información que garantice la protección de los activos digitales y físicos del Instituto de Cultura y Turismo del Municipio de San Gil, mediante la gestión integral de riesgos, el cumplimiento normativo y el fortalecimiento de la confianza en los servicios culturales y administrativos ofrecidos.

3. OBJETIVOS ESPECÍFICOS

- Identificar los activos de información del Instituto y los riesgos asociados a su seguridad y privacidad.
- Establecer políticas, procedimientos y controles que aseguren la confidencialidad, integridad, disponibilidad y trazabilidad de la información institucional.
- Fomentar una cultura organizacional de seguridad de la información mediante acciones de formación, sensibilización y comunicación interna.
- Cumplir con los lineamientos establecidos en la Política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información (MSPI) y la normativa vigente en protección de datos personales.
- Integrar el PESI con otros planes institucionales como el PETI, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y el Plan de Trabajo del Sistema de Gestión de Seguridad y Salud en el Trabajo.
- Establecer mecanismos de seguimiento, auditoría y mejora continua que permitan evaluar la efectividad de las acciones implementadas y ajustar el plan de acuerdo con la evolución de los riesgos y necesidades tecnológicas.

4. PRINCIPIOS RECTORES Y MARCO NORMATIVO

Principios Rectores

El Instituto de Cultura y Turismo del Municipio de San Gil adopta los siguientes principios como base para la formulación, implementación y seguimiento del Plan Estratégico de Seguridad y Privacidad de la Información:

- **Confidencialidad**: Garantizar que la información institucional sea accesible solo para quienes estén autorizados a conocerla, protegiendo la privacidad de los datos personales y sensibles.
- **Integridad**: Asegurar la exactitud, consistencia y fiabilidad de los datos a lo largo de su ciclo de vida, previniendo modificaciones no autorizadas.
- **Disponibilidad**: Velar porque la información y los sistemas estén accesibles y operativos cuando sean requeridos por los procesos institucionales o los ciudadanos.
- **Legalidad**: Cumplir con la normativa nacional e internacional sobre protección de datos personales, transparencia, acceso a la información y seguridad digital.
- **Prevención**: Anticipar y mitigar riesgos mediante controles adecuados y buenas prácticas en la gestión de la información.
- **Responsabilidad compartida**: Promover la corresponsabilidad institucional en la gestión segura de la información, involucrando activamente a todos los servidores públicos.
- **Mejora continua**: Evaluar periódicamente los resultados del plan y sus acciones, con el fin de realizar los ajustes necesarios en función de los cambios tecnológicos, normativos y organizacionales.

Marco Normativo de Referencia

El PESI se encuentra alineado con el marco normativo nacional vigente en materia de seguridad digital, privacidad de la información y protección de datos, entre los cuales se destacan:

- **Ley 1581 de 2012** – Protección de datos personales.
- **Ley 1712 de 2014** – Transparencia y acceso a la información pública.
- **Decreto 1377 de 2013** – Régimen para la autorización del tratamiento de datos personales.
- **Ley 1273 de 2009** – Delitos informáticos y protección de la información.
- **Resolución 500 de 2021** – Adopción del Modelo de Seguridad y Privacidad de la Información – MSPI.
- **ISO/IEC 27001 y 27002** – Normas internacionales de sistemas de gestión de seguridad de la información.
- **Modelo Integrado de Planeación y Gestión – MIPG**.
- **Política de Gobierno Digital – CONPES 3920 de 2018**.

5. ALCANCE

El Plan Estratégico de Seguridad y Privacidad de la Información – PESI aplica a todos los procesos, áreas, sistemas de información, servicios digitales, infraestructura tecnológica, datos personales y activos documentales del Instituto de Cultura y Turismo del Municipio de San Gil.

Este plan incluye tanto la información en medios digitales como físicos, e involucra a todos los servidores públicos, contratistas, personal administrativo y operativo que intervienen directa o indirectamente en el manejo, tratamiento, almacenamiento o protección de datos institucionales y personales.

El alcance del PESI comprende:

- La protección de los activos de información institucional (documentos, bases de datos, aplicaciones, redes, servidores, dispositivos, entre otros).
- La gestión del riesgo asociado a la seguridad de la información en todos los niveles de la organización.
- El cumplimiento de la normativa legal vigente en materia de protección de datos personales, transparencia y delitos informáticos.
- La integración del PESI con otros instrumentos institucionales como el Plan Estratégico de Tecnologías de la Información (PETI), el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, el Plan Institucional de Capacitación, el Sistema de Gestión Documental y el Sistema de Gestión de Seguridad y Salud en el Trabajo (en aspectos relacionados con el riesgo digital).

Este plan será aplicable durante el periodo 2025–2027, con posibilidad de ajustes anuales de acuerdo con los cambios tecnológicos, organizacionales o normativos que afecten el ecosistema de información del Instituto.

6. LÍNEAS ESTRATÉGICAS

Estas líneas constituyen los ejes orientadores para la ejecución de las acciones institucionales en materia de seguridad y privacidad de la información durante el periodo 2025–2027:

6.1. Liderazgo institucional en seguridad y privacidad

Objetivo: Fortalecer el compromiso de la Alta Dirección y las áreas estratégicas con la seguridad digital y la protección de la información como parte esencial de la gestión pública.

Acciones clave:

- Definir roles y responsabilidades en el SGSI.
- Incluir la seguridad de la información en el direccionamiento estratégico institucional.
- Establecer canales para la toma de decisiones oportunas en eventos de riesgo o vulnerabilidad.

6.2. Gestión de riesgos de seguridad de la información

Objetivo: Identificar, analizar, evaluar y tratar los riesgos que puedan comprometer los activos de información del Instituto.

Acciones clave:

- Aplicar el instrumento de diagnóstico del MSPI.
- Actualizar anualmente la matriz de riesgos.
- Implementar controles adecuados según la criticidad del riesgo.

6.3. Implementación de controles y medidas de seguridad

Objetivo: Establecer políticas, procedimientos y herramientas que garanticen la protección efectiva de la información institucional.

Acciones clave:

- Definir y aplicar políticas de acceso, respaldo y uso aceptable de los sistemas de información.
- Establecer mecanismos de autenticación, cifrado y auditoría.
- Fortalecer la infraestructura tecnológica en aspectos de seguridad.

6.4. Gestión de incidentes y recuperación

Objetivo: Implementar un sistema efectivo de notificación, atención y recuperación ante incidentes que afecten la seguridad o privacidad de la información.

Acciones clave:

- Diseñar e implementar un protocolo de gestión de incidentes.
- Realizar simulacros periódicos de contingencia digital.
- Documentar y analizar los eventos ocurridos para evitar su repetición.

6.5. Cultura organizacional de seguridad y protección de datos

Objetivo: Fomentar una cultura institucional basada en el uso responsable, ético y seguro de la información, con especial énfasis en la protección de datos personales.

Acciones clave:

- Diseñar e implementar un plan de formación y sensibilización en seguridad y privacidad de la información.
- Capacitar anualmente a todo el personal en normativa y buenas prácticas.
- Incluir contenidos sobre ciberseguridad en los procesos de inducción.

7. PLAN DE ACCIÓN

Línea Estratégica	Actividad Clave	Responsable	Periodo	Indicador
1. Liderazgo institucional	Designar oficialmente al responsable de Seguridad de la Información (RSI)	Dirección / Talento Humano	Primer trimestre 2025	RSI designado y funciones definidas
	Incluir la seguridad de la información en el Plan Estratégico Institucional	Planeación	2025	Plan actualizado con componente de seguridad
	Integrar al RSI en los comités institucionales relevantes	Dirección	2025–2027	N° de comités en los que participa el RSI
2. Gestión de riesgos	Aplicar el diagnóstico del MSPI	Responsable TIC / Planeación	Anualmente	Nivel de madurez evaluado
	Actualizar la matriz de riesgos de seguridad y privacidad de la información	Responsable TIC / Archivo / Jurídica	Anualmente	Matriz revisada y validada
	Integrar la matriz de riesgos al MIPG	Planeación	2025	Matriz incluida en los informes institucionales
3. Controles y medidas de seguridad	Definir políticas internas de acceso, respaldo, contraseñas y uso de la información	Responsable TIC	2025	Manuales y políticas publicadas
	Implementar un sistema de respaldo automático de información crítica	Área TIC	2025	% de información crítica con respaldo activo
	Actualizar antivirus y controles de acceso físicos y digitales	Área TIC	2025–2027	% de estaciones con protección activa
4. Gestión de incidentes	Diseñar e implementar el	TIC / Control Interno	2025	Protocolo aprobado

	protocolo de gestión de incidentes			
	Realizar simulacros anuales de contingencia digital	TIC / Talento Humano	2026–2027	N° de simulacros realizados
	Documentar y analizar incidentes reportados	TIC / Archivo	Trimestral	Informes de incidentes generados
5. Cultura organizacional y protección de datos personales	Diseñar e implementar plan de formación y sensibilización	Talento Humano / Juridica / TIC	Desde 2025	Plan publicado y cronograma ejecutado
	Capacitar a todos los funcionarios sobre Ley 1581 y manejo de datos	Juridica / Talento Humano	Anualmente	% de personal capacitado
	Incluir temas de seguridad en procesos de inducción	Talento Humano	Permanente	Check list de inducción actualizado

8. SEGUIMIENTO Y EVALUACIÓN

El seguimiento y evaluación del PESI garantizarán la trazabilidad de los avances, la toma de decisiones informadas y la mejora progresiva del nivel de madurez del Instituto de Cultura y Turismo del Municipio de San Gil en materia de seguridad y privacidad de la información.

Este proceso será liderado por la **Alta Dirección**, con el acompañamiento del **Responsable de Seguridad de la Información (RSI)**, el área de **Tecnologías de la Información**, **Jurídica**, **Planeación**, y, cuando aplique, **Control Interno**.

Mecanismos de seguimiento

- **Informes trimestrales de avance** por parte del RSI y el área TIC, con consolidado de acciones ejecutadas por línea estratégica.
- **Evaluación semestral del nivel de cumplimiento** del plan, basado en indicadores definidos y análisis de brechas persistentes.
- **Revisión anual del PESI**, incorporando resultados del diagnóstico MSPI, auditorías internas o externas, e incidentes ocurridos.
- **Actualización de políticas, protocolos y planes complementarios**, en articulación con el PETI, el Plan de Tratamiento de Riesgos y el SGSI.

Indicadores sugeridos

Indicador	Frecuencia	Meta esperada
% de cumplimiento de acciones del plan	Trimestral	≥ 80 % al cierre del año
Nivel de madurez MSPI (modelo MINTIC)	Anual	Nivel 3 o superior
% de personal capacitado en seguridad y privacidad	Anual	100 % del personal institucional
N° de incidentes reportados y atendidos	Trimestral	100 % de los incidentes gestionados
% de actualizaciones de políticas y protocolos realizadas	Anual	100 % de los instrumentos priorizados

Mejora continua

El PESI será objeto de actualización cuando:

- Se presenten **cambios sustanciales en el entorno tecnológico o normativo**.

- El diagnóstico MSPI indique **regresividad o estancamiento** en alguno de los pilares evaluados.
- Se deriven **recomendaciones de auditorías internas o externas** que afecten su diseño o implementación.
- Exista una **reorganización institucional** o cambio en las funciones de los responsables del plan.

Este enfoque de mejora continua permitirá que el Instituto consolide un sistema de gestión de seguridad de la información robusto, resiliente y acorde con su misión cultural y social.