SAN GIL Instituto de Cultura y Turismo

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Contenido

1. INTRODUCCIÓN

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Instituto de Cultura y Turismo del Municipio de San Gil tiene como propósito establecer un marco de gestión que permita identificar, analizar, evaluar y mitigar los riesgos asociados al uso, tratamiento y protección de los activos de información institucional.

Este plan se enmarca en los principios del Sistema de Gestión de Seguridad de la Información – SGSI, en articulación con el Plan Estratégico de Tecnologías de la Información – PETI, la Política de Seguridad Digital, la Política de Tratamiento de Datos Personales, así como los lineamientos del Modelo Integrado de Planeación y Gestión – MIPG.

La creciente dependencia de las tecnologías de la información, así como la responsabilidad institucional frente al manejo de datos personales, estratégicos y operativos, hacen indispensable una gestión sistemática del riesgo que permita garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información, en todos los niveles y procesos de la entidad.

Este documento constituye un insumo fundamental para la toma de decisiones en materia de seguridad de la información, en cumplimiento de la Ley 1581 de 2012 (protección de datos personales), la Ley 1712 de 2014 (transparencia y acceso a la información pública), el Decreto 1377 de 2013, y las buenas prácticas internacionales como las establecidas en la Norma ISO/IEC 27001.

2. OBJETIVO GENERAL

Establecer un conjunto de medidas y procedimientos para la identificación, análisis, evaluación y tratamiento de los riesgos que puedan afectar la seguridad y privacidad de la información institucional, garantizando su confidencialidad, integridad y disponibilidad, y promoviendo la protección de los datos personales gestionados por el Instituto de Cultura y Turismo del Municipio de San Gil.

3. OBJETIVOS ESPECÍFICOS

- Identificar los activos de información institucional y los riesgos asociados a su uso, tratamiento, almacenamiento o transmisión.
- Evaluar la probabilidad e impacto de los riesgos de seguridad digital y privacidad, con base en criterios técnicos, normativos y estratégicos.
- Establecer medidas de control y tratamiento adecuadas que permitan mitigar los riesgos identificados, conforme a su nivel de criticidad.
- Cumplir con las disposiciones legales en materia de seguridad de la información y protección de datos personales, especialmente las establecidas en la Ley 1581 de 2012, la Ley 1712 de 2014 y sus normas reglamentarias.
- Fomentar una cultura organizacional orientada a la prevención, sensibilización y actuación frente a eventos que puedan vulnerar los activos de información institucional.
- Garantizar el seguimiento y mejora continua del plan a través de indicadores, responsables definidos y revisiones periódicas del nivel de riesgo.

4. POLÍTICA DE SEGURIDAD Y TRATAMIENTO DE RIESGOS

El Instituto de Cultura y Turismo del Municipio de San Gil adopta la presente política con el objetivo de proteger de manera integral la información que custodia y administra, así como los sistemas y medios mediante los cuales es procesada. Esta política responde al compromiso institucional con la seguridad digital, la protección de datos personales y la garantía del derecho a la información en condiciones de disponibilidad, integridad, confidencialidad y trazabilidad.

La política se fundamenta en los siguientes principios:

- Responsabilidad institucional: Toda persona que accede, manipula o administra información dentro del Instituto debe actuar bajo criterios de legalidad, transparencia, ética y corresponsabilidad.
- Prevención y gestión del riesgo: Se fomentan acciones sistemáticas de identificación, análisis, evaluación y tratamiento de los riesgos que puedan comprometer los activos de información.
- Protección de datos personales: El Instituto garantizará el cumplimiento de la Ley 1581 de 2012 y demás normas aplicables, protegiendo los derechos de los titulares frente al tratamiento de su información.
- Cumplimiento normativo y técnico: Esta política está alineada con las directrices del Modelo Integrado de Planeación y Gestión – MIPG, el marco de Seguridad Digital del Estado colombiano y las mejores prácticas internacionales (ISO/IEC 27001 y 27005).
- Mejora continua: Las medidas adoptadas serán evaluadas de forma periódica, permitiendo la actualización del plan y la adopción de nuevas prácticas conforme evolucione el entorno tecnológico y regulatorio.

La Alta Dirección promoverá el fortalecimiento de una cultura organizacional basada en la seguridad de la información, destinando recursos técnicos, humanos y presupuestales para la implementación, monitoreo y evaluación permanente de esta política.

5. CRITERIOS DE ANÁLISIS Y EVALUACIÓN DE RIESGOS

Para realizar una adecuada gestión de los riesgos que puedan afectar la seguridad y privacidad de la información en el Instituto de Cultura y Turismo del Municipio de San Gil, se adoptan los siguientes criterios para su identificación, análisis, evaluación y clasificación:

1. Valoración del impacto del riesgo

El impacto se evalúa en función de las posibles consecuencias que tendría la materialización de un evento de riesgo, considerando los siguientes dominios:

Dominio	Descripción
Confidencialidad	Acceso no autorizado a información sensible o clasificada.
Integridad	Alteración, manipulación o corrupción de los datos.
Disponibilidad	Interrupción del acceso o pérdida de disponibilidad del servicio o sistema.
Legal	Incumplimiento de normativas legales o contractuales (ej. Habeas Data).
Imagen institucional	Deterioro de la percepción pública o reputación del Instituto.

2. Valoración de la probabilidad

Estima la frecuencia con la que podría ocurrir el evento de riesgo, considerando la naturaleza del activo, el entorno y el historial de incidentes:

Nivel	Descripción
Alta	El evento puede ocurrir con frecuencia o es inminente.
Media	El evento puede ocurrir ocasionalmente.
Baja	El evento es poco probable o raro.

3. Clasificación del nivel de riesgo

La clasificación final se obtiene de la combinación entre la probabilidad y el impacto:

Nivel de riesgo	Interpretación	Tratamiento sugerido
Alto	Aceptación del riesgo es inaceptable	Se deben aplicar medidas inmediatas.
Medio	Requiere mitigación y seguimiento continuo	Se aplican controles razonables.
Bajo	Riesgo aceptable o residual	Se puede monitorear periódicamente.

Estos criterios permiten construir la matriz de riesgos y priorizar las acciones de tratamiento, de acuerdo con los activos afectados, el tipo de amenaza y los mecanismos de control existentes o por implementar.

6. MATRIZ DE RIESGOS Y MEDIDAS DE TRATAMIENTO

A continuación, se presentan algunos ejemplos representativos que pueden ser adaptados y complementados según el contexto del Instituto de Cultura y Turismo del Municipio de San Gil:

Proceso / Activo	Riesgo Identificado	Probabilidad	Impacto	Nivel de Riesgo	Medidas de Tratamiento	Responsable
Plataforma web institucional	Acceso no autorizado a información personal	Alta	Alto	Alto	Implementar autenticación reforzada, auditorías de acceso, actualización de contraseñas	Área TIC / Proveedor tecnológico
Base de datos de usuarios (correo / PQRS)	Pérdida de datos por fallo de respaldo	Media	Alto	Alto	Establecer política de backup automático semanal y verificación mensual	Responsable de archivo / TIC
Información financiera	Divulgación no autorizada o alteración de datos contables	Baja	Alto	Medio	Control de accesos por rol, monitoreo de logs, cifrado de archivos	Coordinador financiero / TIC
Servidores locales	Daño físico por humedad o fluctuaciones eléctricas	Media	Medio	Medio	Instalar UPS, mejorar ventilación, revisar puntos de humedad	Coordinador locativo / TIC
Documentación física (contratos / actas)	Extravío o daño por mal almacenamiento	Baja	Medio	Bajo	Inventario, organización por series documentales, foliación y archivo en condiciones adecuadas	Auxiliar administrativo / Archivo
Equipos de cómputo institucionales	Uso no autorizado de software o instalación de malware	Alta	Medio	Alto	Política de uso aceptable, capacitación en ciberseguridad, antivirus actualizado	Área TIC

7. SEGUIMIENTO Y EVALUACIÓN

El seguimiento y evaluación del presente plan son fundamentales para asegurar la efectividad de las acciones implementadas y su alineación permanente con las prioridades institucionales, los avances tecnológicos y las disposiciones legales vigentes.

Mecanismos de Seguimiento

- **Revisión semestral del plan** por parte del equipo responsable de tecnologías de la información, con participación del área de planeación y control interno.
- **Registro de incidentes de seguridad** y análisis de causas para retroalimentar el análisis de riesgos.
- **Actualización de la matriz de riesgos** cada vez que se incorporen nuevos activos, procesos o tecnologías, o cuando se presenten eventos relevantes.
- **Informes de cumplimiento y monitoreo**, que deberán ser socializados con la Alta Dirección y el Comité Institucional de Archivos o Seguridad de la Información, si existe.

Indicadores sugeridos

Indicador	Frecuencia	Fuente
% de medidas de tratamiento implementadas	Trimestral	Matriz de seguimiento
Número de incidentes de seguridad reportados y gestionados	Trimestral	Registro de incidentes TI
% de servidores capacitados en privacidad y seguridad	Semestral	Registro de capacitaciones / Talento Humano
Nivel de actualización del inventario de activos de información	Anual	Informe TIC / Área de archivo

Mejora continua

El plan será objeto de revisión anual o cuando ocurra alguno de los siguientes eventos:

- Cambios significativos en la infraestructura tecnológica o en los activos de información.
- Recomendaciones de auditoría interna o externa.
- Actualización del PETI o la Política de Seguridad de la Información.
- Cambios normativos o jurisprudenciales relacionados con la privacidad o protección de datos personales.

Estas revisiones permitirán ajustar las medidas de control y tratamiento de riesgos, y asegurar que el plan siga siendo una herramienta eficaz y actualizada para la protección de los activos institucionales.