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

INSTITUTO DE CULTURA Y TURISMO DEL MUNICIPIO DE SAN GIL – ICT

SAN GIL

Instituto de **Cultura y Turismo**

SAN GIL – 2024

Tabla de contenido

INTRODUCCIÓN

El presente plan se elabora con el fin de dar a conocer cómo se realizará la implementación y socialización del componente de Gobierno en línea del **INSTITUTO DE CULTURA Y TURISMO DEL MUNICIPIO DE SAN GIL** en el Eje Temática de la Estrategia en seguridad y privacidad de la información, el cual busca guardar los datos de los ciudadanos como un tesoro, garantizando la seguridad de la información.

El proceso de administración de riesgos es un método lógico y sistemático para establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso de tal forma que permita al Instituto minimizar pérdidas de información y maximizar oportunidades.

Todos los servidores públicos, en cumplimiento de sus funciones, están sometidos a riesgos que pueden hacer fracasar su gestión; por lo tanto, es necesario tomar las medidas, para identificar las causas y consecuencias de la materialización de dichos riesgos.

OBJETIVOS

Objetivo General:

- Controlar y minimizar los riesgos asociados a los procesos tecnológicos existentes, en el **INSTITUTO DE CULTURA Y TURISMO DEL MUNICIPIO DE SAN GIL**, el manejo de medios, control de acceso y gestión de usuarios.

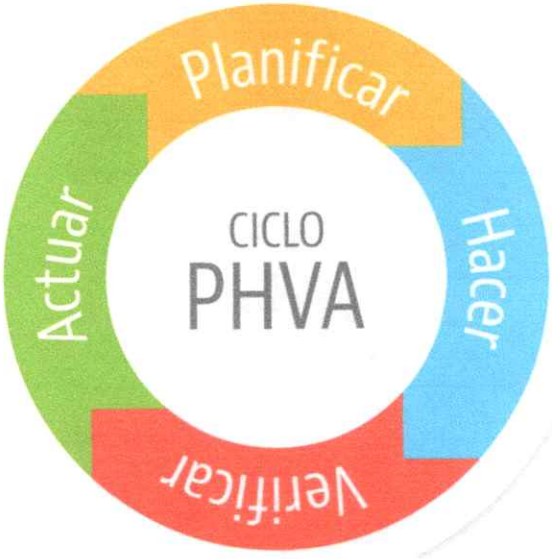
Objetivo Específicos:

- Concientizar a todos los funcionarios, contratistas y terceros en general sobre la necesidad e importancia de gestionar de manera adecuada, los riesgos inherentes a la gestión.
- Realizar el plan de trabajo específico validando los recursos con los que se cuentan actualmente el **INSTITUTO DE CULTURA Y TURISMO DEL MUNICIPIO DE SAN GIL** para tener un plan de tratamiento de riesgo de seguridad y privacidad de la información.
- Establecer, mediante una adecuada administración del riesgo, una base confiable para la toma de decisiones y la planificación institucional

ALCANCE DEL DOCUMENTO

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información del **INSTITUTO DE CULTURA Y TURISMO DEL MUNICIPIO DE SAN GIL**, se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC,

a través de los decretos emitidos. De acuerdo con esto, se definen las siguientes fases de implementación del MSPI:



DEFINICIONES:

Para la administración del riesgo del **INSTITUTO DE CULTURA Y TURISMO DEL MUNICIPIO DE SAN GIL**, se tendrán en cuenta los siguientes términos y definiciones:

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).

- **Activo de Información:** En relación con la privacidad de la Información, se refiere a la actividad que contiene información pública que el sujeto obligado genere, obtenga, adquiera transporte o controlar en su calidad de tal.

- **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. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

- **Bases de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

- **Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **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 (Ley 1712 de 2014, art 6).

- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

- **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. (Decreto 1377 de2013, art 3).

- **Datos Personales Mixtos:** Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

- **Datos Personales Sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas pertenencia a sindicatos, organizaciones sociales, de derechos promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).

- **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información - SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

- **Derecho a la Intimidad:** Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

- **Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3).

- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

- **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

- **Información Pública Reservada:** Es aquella información que estando en poder o custodia de su calidad de tal, es exceptuada de acceso a la ciudadanía por el bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 712 de 2014. (Ley 1712 de 2014, art 6).

- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

- **Privacidad:** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

- **Responsabilidad Demostrada:** Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

- **Responsable del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información (ISO/IEC 27000).

- **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. (ISO/IEC 27000).

- **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

- **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. (ISO/IEC 27000).

ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DEL RIESGO

El éxito de la administración del riesgo depende de la decidida participación de los directivos, servidores públicos y contratistas del Instituto; por esto, es preciso identificar los actores que intervienen:

Alta Dirección: Aprueba las directrices para la administración del riesgo en la Entidad. La Alta Dirección es la responsable del fortalecimiento de la política de administración del riesgo.

Proceso Administración del Sistema Integrado de Gestión: Genera la metodología para la administración del riesgo de la Entidad, coordina, lidera, capacita y asesora en su aplicación.

Responsables de los procesos: Identifican, analizan, evalúan y valoran los riesgos de la entidad (por procesos e institucionales) al menos una vez al año. Si bien los Líderes SIG apoyan la ejecución de las etapas de gestión del riesgo a nivel de los procesos, esto no quiere decir que el proceso de administración de riesgos este solo bajo su responsabilidad. Al contrario, cada responsable de proceso se encarga de garantizar que en el proceso a su cargo se definan los riesgos que le competen, se establezcan las estrategias y responsabilidades para tratarlos y, sobre todo, que se llegue a cada funcionario que trabaja en dicho proceso. No se debe olvidar que son las personas que trabajan en cada uno de los procesos los que mejor conocen los riesgos existentes en el desarrollo de sus actividades.

Servidores públicos y contratistas: Ejecutar los controles y acciones definidas para la administración de los riesgos definidos, aportar en la identificación de posibles riesgos que puedan afectar la gestión de los procesos y/o de la entidad.

Control Interno: Debe realizar evaluación y seguimiento a la política, los procedimientos y los controles propios de la administración de riesgos.

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

El **INSTITUTO DE CULTURA Y TURISMO DEL MUNICIPIO DE SAN GIL** adelantará las acciones pertinentes para la implementación y mantenimiento del proceso de Administración del Riesgo, y para ello todos los servidores de la entidad se comprometen a:

1. Conocer y cumplir las normas internas y externas relacionadas con la administración de los riesgos.
2. Fortalecer la cultura de administración de los riesgos para crear conciencia colectiva sobre los beneficios de su aplicación y los efectos nocivos de su conocimiento.
3. Someter los procesos y procedimientos permanentemente al análisis de riesgos con base en la aplicación de las metodologías adoptadas para el efecto.
4. Mantener un control permanente sobre los cambios en la calificación de los riesgos para realizar oportunamente los ajustes pertinentes.

5. Reportar los eventos de riesgo que se materialicen, utilizando los procedimientos e instrumentos establecidos para el efecto.
6. Desarrollar e implementar planes de contingencia para asegurar la continuidad de los procesos, en los eventos de materialización de los riesgos que afecten a los objetivos institucionales previstos y los intereses de los usuarios y partes interesadas.
7. Presentar propuestas de mejora continua que permitan optimizar la forma de realizar y gestionar las actividades de la entidad para así aumentar nuestra eficacia y efectividad.

Para lograr lo anteriormente enunciado la Dirección General asignará los recursos tanto humanos, presupuestales y tecnológicos necesarios que permitan realizar el seguimiento y evaluación a la implementación y efectividad de esta política.

De igual manera, el presente plan forma parte de la política de administración del riesgo, por cuanto detalla las directrices que deben tenerse en cuenta para la gestión del riesgo en la entidad y que tienen como propósito evitar la materialización del riesgo.

EVALUACIÓN DEL RIESGO

El análisis de riesgos informáticos es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

Dentro de estos parámetros, como lo propone la Guía de gestión de riesgos, Seguridad y privacidad de la información de MINTIC.

Para la evaluación de riesgos se cuenta con una matriz de calificación tal cual como se muestra a continuación:

CRITERIOS DE EVALUACIÓN SEGÚN PROBABILIDAD DE OCURRENCIA	CALIFICACIÓN DEL RIESGO	CRITERIOS DE EVALUACIÓN SEGÚN IMPACTO				
		GENERAL	CONFIDENCIALIDAD DE LA INFORMACIÓN	CREDIBILIDAD O IMAGEN	LEGAL	OPERATIVO
Raro: el evento puede ocurrir solo en	1	Insignificante: de presentarse el hecho,	Personal	Grupo de funcionarios	Multas	Ajustes a una actividad concreta

Improbable: El evento puede ocurrir en algún momento. Al menos de 1 vez en los últimos 5	2	Menor: de presentarse el hecho tendria bajo impacto o efecto sobre la entidad	Grupo de trabajo	Todos los funcionarios	Demandas	Cambios en procedimientos
Posible: el evento podrá ocurrir en algún momento .al menos de 1 vez en los últimos 2 años	3	Moderado: de presentarse el hecho, tendria medianas consecuencias o efectos sobre la entidad.	Relativa al proceso	Usuarios de la ciudad	Investigación disciplinarios	Cambios en la interacción de los procesos
Probable: es viable que el evento probablemente ocurra en la mayoria de las	4	Mayor: de presentarse el hecho, tendria altas consecuencias o	Mayor: de presentarse el hecho, tendria altas consecuencias o efectos sobre la	institucional	usuarios de la región	investigación fiscal
Casi seguro: se espera que el evento ocurra en la mayoria de las circunstancias. Más de 1 vez al año,	5	catastrófico: de presentarse el hecho tendria desastrosas consecuencias o efectos sobre la entidad	estratégica	usuarios del país	Intervención sanción	paro total del proceso

ANALISIS DE RIESGOS:

Para el análisis de riesgos se cuenta con las siguientes calificaciones tal cual como se muestra a continuación:

NOMBRE DEL PROCESO:	Gestión de Infraestructura			RESPONSABLE DEL PROCESO:	Dirección General – Técnico Administrativo		
OBJETIVO DEL PROCESO:	Desarrollar, mantener y mejorar la infraestructura física y tecnológica, requeridos para la adecuada prestación del servicio en sus funciones administrativas.						
RIESGO O ASOCIADO AL PROCESO	TIPO DE RIESGO	PROBALIDAD DE OCURRENCIA	IMPACTO	CALIFICACION DEL RIESGO		EVALUACION	
				PROBALIDAD DE OCURRENCIA	IMPACTO	ZONA DE RIESGO	MEDIDAS DE RESPUESTA

Falta de mantenimiento y daños eventuales sobre la infraestructura física y tecnológica	R. Estratégico	Casi Seguro: Se espera que el evento ocurra en la mayoría de las circunstancias. Más de 1 vez al año	Menor. Todos los funcionarios s	5	2	Alta	Reducir, Evitar, Compartir o Transferir el riesgo
Infraestructura física, tecnológica.	R. Estratégico	Probable: es viable que el evento probablemente ocurra en la mayoría de las circunstancias. Al menos de 1 vez en el último año	Mayor. Institucional l	4	4	Extrema	Reducir, Evitar, Compartir o Transferir el riesgo
Vulnerabilidad de los sistemas de información	R. Operativo (misional)	Probable: Es viable que el evento probablemente ocurra en la mayoría de las circunstancias. Al menos de 1 vez en el último año.	Mayor. Instituciona l	4	4	Extrema	Reducir, Evitar, Compartir o Transferir el riesgo
Desastre natural	R. Estratégico	Posible: El evento podrá ocurrir en algún momento. Al menos de 1 vez en los últimos 2 años.	Moderado. Usuarios de la cuidad	3	3	Alta	Evitar, Compartir o Transferir el riesgo
Peculado	R. Corrupción	Improbable: E l evento puede ocurrir en algún momento. Al menos de 1	Menor. Todos los funcionarios	2	2	Baja	Baja
Prevaricato	R. Corrupción	Raro: El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales). No se ha	Menor. Todos los funcionarios s	1	2	Baja	Baja
Vandalismo	R. Corrupción	Casi Seguro: Se espera que el evento ocurra en la mayoría de las circunstancias. Mas de 1 vez al año	Mayor. Institucional l	5	4	Extrema	Reducir, Evitar, Compartir o Transferir el

SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

El **INSTITUTO DE CULTURA Y TURISMO DEL MUNICIPIO DE SAN GIL** evaluará el ejercicio de "tratamiento de riesgos y privacidad de la información", por medio de seguimientos para revisar que las acciones se están llevando a cabo y evaluar la eficiencia en su implementación adelantando verificaciones al menos una vez al año o cuando sea necesario. De esta forma conlleva, dado el caso, a evidenciar todas aquellas situaciones que pueden estar influyendo en la aplicación de las acciones de tratamiento.

Dado en el Municipio de San Gil en el año 2024.

CARMEN YANETH ÁLVAREZ MARTÍNEZ
Directora General del Instituto de Cultura y Turismo del Municipio de San Gil