Elaborado por:	**Aprobado por:**	**Registrado SIG:**
ORIGINAL FIRMADO	**ORIGINAL FIRMADO**	**ORIGINAL FIRMADO**
Tirso Sánchez Mejía Profesional CPS	**Jhoana Norelly Guevara** Subdirectora General	**Jhoana Norelly Guevara** Subdirectora General

1. OBJETIVO

Definir los lineamientos y acciones para la gestión integral de los riesgos de seguridad y privacidad de la información, sobre los activos críticos del ITM, mediante su identificación, análisis, valoración y tratamiento, con el fin de proteger y preservar la confidencialidad, disponibilidad e integridad de la información, prevenir su materialización y/o reducir los impactosnegativos en la gestión institucional.

2. ALCANCE Y RESPONSABLES

Aplica para todos los procesos del Instituto de Turismo del Meta, funcionarios y contratistas propietarios, custodios y usuarios de la información.

3. DEFINICIONES

Acción correctiva: Acción para eliminar la causa de una no conformidad y prevenir su repetición. Va más allá de la simple corrección.

Acción preventiva: Medida de tipo pro-activo orientada a prevenir potenciales no conformidades. Es un concepto de ISO 27001:2005. En ISO 27001:2013, ya no se emplea; ha quedado englobada en Riesgos y Oportunidades.

Aceptación del riesgo: Decisión informada de asumir un riesgo concreto [Fuente: Guía ISO 73: 2009].

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.

La aceptación del riesgo puede ocurrir sin tratamiento de riesgo o durante el proceso de tratamiento de riesgo. Los riesgos aceptados están sujetos a monitoreo y revisión.

Amenaza Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis de riesgos: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. [Fuente: Guía ISO 73: 2009]

El análisis de riesgos proporciona la base para la estimación de riesgos y las decisiones sobre el tratamiento de riesgos. El análisis de riesgos incluye la estimación de riesgos.

Análisis de riesgos cualitativo: Análisis de riesgos enel que se usa algún tipo de escalas de valoración para situar la gravedad del impacto y laprobabilidad de ocurrencia.

Análisis de riesgos cuantitativo: Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.

Ataque: Intento de destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo.

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas objetivamente para determinar el grado en elque se cumplen los criterios de auditoría.

Autenticidad: Propiedad de que una entidad es lo que afirma ser.

Continuidad de la seguridad de la información Procesos y procedimientos para garantizar una operativa continuada de la seguridad de la información.

Control: Medida por la que se modifica el riesgo.

Los controles incluyen procesos, políticas, dispositivos, prácticas, entre otras acciones que modifican el riesgo. Es posible que los controles no siempre ejerzan el efecto de modificación previsto o supuesto. El término salvaguardao contramedida son utilizados frecuentemente como sinónimos de control.

Control correctivo: Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas relevantes. Supone que la amenaza ya se ha materializado pero que se corrige.

Control de acceso: Significa garantizar que el acceso a los activos esté autorizado y restringido según los requisitos comerciales y de seguridad.

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Evaluación de riesgos: Proceso global de identificación, análisis y estimación de riesgos.

Evento de seguridad de la información: Ocurrenciaidentificada del estado de un sistema, servicio o red de comunicaciones que indica una posible violación de la política de seguridad de la información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.

Identificación de riesgos: Proceso de encontrar, reconocer y describir riesgos [Fuente: Guía ISO 73:2009]. La identificación de riesgos implica la identificación de las fuentes del riesgo, eventos, suscausas y sus posibles consecuencias. La identificación de riesgos puede involucrar datoshistóricos, análisis teóricos, opiniones informadas y de expertos, y las necesidades de laspartes interesadas.

Impacto: El coste para la empresa de un incidente -de la escala que sea, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc-.

Indicador: Medida que proporciona una estimación o evaluación.

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Plan de tratamiento de riesgos: Documento que define lasacciones para gestionar los riesgos de seguridad de la información inaceptables eimplantar los controles necesarios para proteger la misma.

Sistema de Gestión de la Seguridad de la Información: 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 del riesgo y de mejora continua.

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

4. MARCO NORMATIVO

La actualización del plan estratégico de seguridad y privacidad de la información se define teniendo en cuenta el siguiente marco normativo:

CONPES 3995 de 2020, "POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL".

Ley 1581 de 2012(Habeas data), "Se dictan disposiciones generales para la protección de datos. Esta ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como recolección, almacenamiento, uso, circulación o supresión por parte de entidades de naturaleza pública y privada, sin embargo, a los datos financieros se les continúa aplicando la ley 1266 de 2008, excepto los principios."

Ley 1712 de 2014 (Acceso a la información pública y Uso de las TIC), "Regula el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantías del derecho y las excepciones a la publicidad de la información. Toda persona puede conocer sobre la existencia y acceder a la información pública en posesión o bajo control de los sujetos obligados. El acceso a la información solamente podrá ser restringido excepcionalmente."

Decreto 1078 de 2015, "Decreto Único Reglamentario del sector TIC. En particular las normas referentes a la Estrategia de Gobierno en Línea."

Decreto 415 de 2016 (Lineamientos fortalecimiento institucional en TIC), Se adiciona el decreto único reglamentario del sector de la función pública, decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones; Arts. 2.2.35.5; 2.2.35.6

Decreto Presidencial 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 1008 de 2018, "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"

Decreto Presidencial 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 Ministerial 00500 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"

Norma técnica colombiana NTC - ISO/IEC 27001, "Estándar para la seguridad de la información, describe cómo gestionar la seguridad de la información en una empresa"

5. DESARROLLO

5.1. POLÍTICA DE GESTIÓN DEL RIESGO

El Instituto de Turismo del Meta ha establecido la Política de Gestión del Riesgo, mediante el documento DPE-PO-09 – POLÍTICA DE ADMINISTRACIÓN DEL RIESGO, que tiene como objetivo "Establecer el marco de referencia para la identificación, gestión y control de riesgos paragarantizar un nivel aceptable de riesgos residuales en todos los procesos, para garantizar el logrode los objetivos y metas institucionales del Instituto de Turismo del Meta", en la cual se establecenentre otras los lineamientos institucionales para la gestión

de riesgos de seguridad y privacidad de la información, y así mismo, se definen los criterios para calificación de probabilidad y el impacto de los riesgos en cinco niveles, los criterios para la valoración de la criticidad de los riesgos en cuatro niveles y se establecen los niveles de aceptación.

METODOLOGÍA

El Instituto de Turismo del Meta ha adoptado la metodología de Gestión de Riesgos establecida por el Departamento Administrativo de la Función Publica DAFP, y adaptada por la Gobernación del Meta, alineado al contexto organizacional en el formato "MAPA DE RIESGOS INSTITUCIONAL", el cual cuenta con un instructivo dentro del mismo formato, que detalla cada uno de los campos y el paso a paso parautilización del mismo.

Riesgos de Seguridad y privacidad de la Información

En el contexto de los sistemas de gestión de seguridad de la información, los riesgos de seguridadde la información pueden expresarse como un efecto de incertidumbre sobre los objetivos de seguridad de la información.

El riesgo de seguridad de la información está asociado con el potencial de que las **amenazas** exploten las **vulnerabilidades** de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización.

Frente a la gestión del riesgo se debe considerar el siguiente marco general para la definición de actividades o acciones propias de cada línea así:

Línea Estratégica (Alta Dirección) se debe definir y aprobar la Política de Administración del Riesgo, acorde con la cual, atendiendo la periodicidad para el seguimiento a riesgos críticos debe aplicar el monitoreo correspondiente haciendo uso de la información suministrada por las instancias de 2ª línea identificadas, con base en lo cual toma las acciones necesarias para intervenir situaciones detectadas como incumplimientos, retrasos e incluso posibles actuaciones irregulares, evitando consecuencias más graves para la entidad.

Primera línea de defensa todos los servidores tienen una responsabilidad frente a la aplicación efectiva de los controles, por lo que se trata de un seguimiento permanente, esto incluye la aplicación de controles de gerencia operativa que corresponde a aquellos que son aplicados por servidores con personal a cargo (jefes, coordinadores u otro cargo).

Segunda línea de defensa. El Jefe de planeación o quien haga sus veces debe periódicamente hacer un seguimiento a todos los riesgos, permitiendo que se generen recomendaciones y posibles ajustes a los mapas de riesgos, de manera tal que las

instancias de 1ª línea pueden establecer mejoras a los riesgos y controles, así mismo garantizar su aplicación efectiva, lo que implica que se deben incorporar ejercicios de asesoría y acompañamiento a los líderes de los procesos y sus equipos para la mejora de este tema.

Tercera línea de defensa La Oficina de Control Interno o quien hace sus veces, a través de sus procesos de seguimiento y evaluación, 26 especialmente a través de la auditoría interna deben establecer la efectividad de los controles para evitar la materialización de riesgos. De igual forma, en el marco de su Plan Anual de Auditoría puede proponer esquemas de asesoría y acompañamiento a la entidad, actividades que puede coordinar con la Oficina de Planeación o quien haga sus veces.

En este orden de ideas, la metodología para la identificación, calificación, valoración y tratamientode los Riesgos de Seguridad y Privacidad de la Información del Instituto de Turismo del Meta (ITM), establece los siguientes pasos:

Identificación de los activos críticos de seguridad y privacidad de la información

Como primer paso para la identificación de los riesgos de seguridad y privacidad de la información, es necesario la identificación de los activos críticos de Información, para esto el Instituto de Turismo del Meta, ha definido el "GTI-M-01 MANUAL DE GESTIÓN DE ACTIVOS DEINFORMACIÓN", el cual establece toda la metodología para la gestión de activos, incluidos los criterios de calificación de acuerdo a la confidencialidad, disponibilidad e integridad, y los criteriosde valoración, conforme a los resultados de las calificaciones, para establecer la criticidad de losmismos.

La herramienta "GTI-MT-01 MATRIZ GESTION ACTIVOS DE INFORMACIÓN" registra la identificación, calificación y valoración de los activos de información, esta debe estar debidamente identificada y actualizada con el fin de identificar los riesgos de acuerdo con el inventario de la entidad.

Identificación de los Riesgos Inherentes

Es importante tener en cuenta que, para la identificación de los riesgos de seguridad y privacidadde la información, su **causa inmediata** se limita a:

- **Pérdida de la Disponibilidad**
- **Pérdida de la Integridad**
- **Pérdida de la Confidencialidad**
- **Combinación de las anteriores**

Para cada riesgo se debe asociar un activo o un grupo de activos, conforme a su tipología, y conjuntamente analizar las posibles **amenazas** y **vulnerabilidades** que podrían causar su materialización. Esta metodología está alineada con el "ANEXO 4 LINEAMIENTOS

PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL EN ENTIDADES PÚBLICAS" definido por el
Ministerio de las TIC para entidades públicas.

Las anteriores tablas son un marco de referencia, pero el responsable de cada proceso debe poder identificar las vulnerabilidades de los activos de información a su cargo y las posibles amenazas que pudiesen llegar a explotar estas vulnerabilidades, para así expresarlo en el campo"**CAUSA RAIZ**" del formato de Mapa de Riesgos Institucional.

Nota: La sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño,es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

Valoración del Riesgo Inherente

Para esta etapa se tendrán en cuenta los criterios de Calificación de la probabilidad y el impactodefinidos en la política de administración del riesgo, antes mencionada, esto arrojará el nivel de criticidad del riesgo inherente.

Identificación y valoración de los controles existentes

En esta etapa, los dueños de los procesos deben identificar cuáles son los controles existentes que actualmente se están aplicando para combatir los riesgos inherentes de seguridad yprivacidad de la información identificados y valorados en el paso anterior, para así proceder a suvaloración. Para esta valoración, es importante establecer la descripción y atributos del control, definiendo si corresponde a un control preventivo, correctivo, y así determinar su calificación de acuerdo a su peso, la afectación o desplazamiento en la matriz (en cuanto a probabilidad e impacto del riesgo), su implementación automática o manual, y si está documentado o no, y así la herramienta "MAPA DE RIESGO INSTITUCIONAL" calculará automáticamente su valoración total.

Las entidades públicas podrán mitigar/tratar los riesgos de seguridad de la información teniendoen cuenta los controles definidos en el Anexo A de la ISO/IEC 27001:2022.

Valoración de los riesgos residuales

Con la evaluación de los controles existentes se debe verificar su incidencia en los riesgos inherentes, mediante el desplazamiento en la probabilidad y/o impacto del mismo, y así

poder establecer el nivel de criticidad residual. La herramienta "MAPA DE RIESGOS INSTITUCIONAL" calculará automáticamente esta valoración del riesgo residual de seguridad y privacidad de la información.

Acciones de tratamiento de los riesgos de seguridad y privacidad de la información

Luego de establecer el nivel de criticidad de los riesgos residuales de seguridad y privacidad de la información, se debe evaluar si el riesgo requiere o no tratamiento, conforme a los criterios deaceptación del riesgo definidos en la Política de Administración del Riesgo del ITM, y si es así definir el tipo de tratamiento a seguir y la descripción de las acciones basadas en el análisis de causas, así como los responsables de llevarlas a cabo, las fechas de ejecución y realizar el seguimiento y control a las mismas, y de esta forma definir los planes de tratamiento de los riesgos de seguridad y privacidad de la información.

Las estrategias en el tratamiento de riesgos consisten en minimizar la probabilidad de materialización del riesgo. Para ello, se puede evidenciar cuatro opciones:

- **Transferir**: Son procedimientos que permiten eliminar el riesgo por medio de la transferencia.
- **Mitigar**: Permite reducir la probabilidad de ocurrencia del riesgo o reducir sus consecuencias. La probabilidad de ocurrencia de un riesgo puede reducirse a través de controles de gestión, políticas y procedimientos encaminados a reducir la materialización del riesgo.
- **Evitar**: Puede evitarse el riesgo no procediendo con la actividad que incorporaría el riesgo, o escoger medios alternativos para la actividad que logren el mismo resultado y no incorporen el riesgo detectado.
- **Aceptar**: consiste en hacer frente a un riesgo (positivo o negativo) o porque no se ha identificado ninguna otra estrategia de respuesta adecuada.

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

Teniendo en cuenta la política, manuales y formatos definidos por el Instituto de Turismo del Meta,se establece el siguiente plan para el Tratamiento de los Riesgos de Seguridad y Privacidad de la Información, conforme a la norma ISO 27001 y alineado con el modelo de privacidad y seguridad de la información del Mintic, dando cumplimiento al MIPG en cuanto al habilitador transversal de seguridad de la información para la política de Gobierno Digital.

Este plan se enfocará en fortalecer la implementación de acciones para el tratamiento de riesgos de seguridad y privacidad de la información de acuerdo a los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones y el departamento administrativo de la función pública, enfocados a la seguridad de los activos de información de la entidad.

Las actividades que realizará la entidad en torno al Tratamiento de Riesgos de Seguridad y Privacidad de la Información institucional, serán las que a continuación se presentan teniendo en cuenta las capacidades y recursos disponibles.

A continuación, se describen las actividades más relevantes orientadas al tratamiento de riesgos de Seguridad y Privacidad de la Información

ITEM	ACTIVIDAD	REPSONSABLE	PREIODICIDAD	EVIDENCIA
CAPACITACIÓN EN RIESGOS	Solicitar Capacitación de la Guía para la Administración del Riesgo y diseño de controles.	Profesional SGSI	ENERO JUNIO	Registro de asistencia, informe de capacitación.
ACTIVOS DE INFORMACIÓN	Revisar, actualizar, publicar la Matriz de activos de información	Profesional SGSI	Como lo establezca el Plan de Seguridad y Privacidad de la Información.	Matriz de activos de información
GESTIÓN DE RIESGOS	Identificar, actualizar y publicar mapa de riesgos de Seguridad y Privacidad de la Información	Profesional SGSI	FEBRERO Y CUANDO SE REQUIERA	Mapa de riesgos registrado ante SIG y publicado en pagina WEB
	Socialización del mapa de riesgos de Seguridad y Privacidad de la Información	Profesional SGSI	SEMESTRAL	Registro de Asistencia
POLÍTICA DE GESTION DEL RIESGO	Revisión, actualización y publicación de POLITICA DE GESTIÓN DE RIESGO	Profesional SGSI	FEBRERO	Documento registrado ante SIG y publicado en la página web
	Socializar política de gestión de riesgo	Profesional SGSI	SEMESTRAL	Registro de asistencia
ACCIONES DE MEJORA	Identificar y Documental acciones correctivas y de mejora	Profesional SGSI	CUANDO SE REQUIERA	SIG-F-05 Acciones Correctivas y de Mejora
	Realizar seguimiento a las acciones correctivas y de mejora.	Profesional SGSI	MENSUAL Y CUANDO SE REQUIERA	Reportes de seguimiento y actas de cierre.

Las actividades antes descritas antes propuestas se programarán antes del 28 de febrero, de cada vigencia en la herramienta de seguimiento SIG-MT-06 Matriz de Seguimiento institucional, la cual deberá ser puesta en conocimiento de la subdirección general.

6. FORMATOS

CÓDIGO	NOMBRE DE FORMATO	RESPONSABLE
DPE-PO-03	Política de seguridad de la información	Profesional SGSI Líder del proceso
DPE-MT-01	Mapa De Riesgos Institucional	Líder del proceso
GTI-MT-01	Matriz De Gestión De Activos De Información	Líder de proceso
SIG-MT-06	Matriz de programación y seguimiento institucional	Líder del proceso

7. CONTROL DE DOCUMENTOS

VERSIÓN No.	FECHA	DESCRIPCION MODIFICACIONES
01	23/05/2022	Primera versión nueva codificación
02	20/12/2023	Se realiza ajuste del numeral 3. Definiciones, numeral 4. Marco normativo, numeral 5. Desarrollo del plan, numeral 6 se actualiza el listado de formatos que soportan el desarrollo del plan

8. ANEXOS

No aplica