Tabla de Contenido

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

Establecer la hoja de ruta para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) del Instituto de Turismo del Meta (ITM), alineada con el Sistema Integrado de Gestión (SIG) de la organización, la NTC-ISO 27001, y el modelo de seguridad y privacidad de la información (MSPI) del MINTIC, dando cumplimiento al habilitador de seguridad de la información de la política de Gobierno Digital del Modelo Integrado de Planeación y Gestión (MIPG), con el fin de proteger y preservar la integridad, disponibilidad y confidencialidad de la información.

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 riesgosen

función de las pérdidas financieras que causaría el impacto.

Ataque: Intento de destruir, exponer, alterar, deshabilitar, robar u obteneracceso 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.

Confidencialidad: Propiedad de la información de no ponerse adisposición o ser revelada a individuos, entidades o procesos no autorizados.

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.

[Fuente: ISO Guide 73:2009] 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 queinterrumpe 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. [Fuente: ISO Guide 73:2009]

Evento de seguridad de la información: Ocurrencia identificada 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 continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.

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 defineteniendo en cuenta el siguiente marco normativo:

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

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

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."

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"

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."

5. DESARROLLO

5.1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El Instituto de Turismo del Meta ha establecido la Política de Seguridad de la Información DPE-PO-03 – POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN, que tiene como objetivo

"Establecer los lineamientos necesarios, con el objetivo de fortalecer la Gestión de Seguridad y Privacidad de la Información del Instituto de Turismo del Meta, enmarcados en la implementación de un Sistema de Gestión de Seguridad de la Información, basado en la identificación y valoración de los riesgos asociados a ella, propendiendo por la protección de su confidencialidad, integridad, disponibilidad y privacidad de los activos de Información"

La seguridad de la información es el conjunto de medidas técnicas, operativas, organizativas, y legales que permiten a las organizaciones resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

La seguridad de la información se encarga de garantizar la integridad, confidencialidad, disponibilidad de nuestra información.

- Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos de información.

- Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.
- Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos entidades o procesos no autorizados.

Uno de los objetivos del sistema de seguridad y privacidad de la Información es el de garantizar un adecuado manejo de la información de la entidad, la cual es uno de los activos más valiosos de la entidad para la toma de decisiones, es por ello que la entidad estableció una política de seguridad de la información con el fin de garantizar información integra, disponible y autentica.

Para ello a través del Plan de seguridad y privacidad de la información se establecen las actividades de implementación del sistema con un enfoque de privacidad ya que para la ejecución de actividades contractuales y funciones propias de los cargos se requiere otorgar acceso a la información de la entidad.

Para que los servidores públicos entiendan mejor los conceptos de seguridad y privacidad de la información se deben realizar sensibilizaciones y capacitaciones, así como documentar procesos relacionados con el uso de información susceptible.

SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información es una cultura que se debe promover en la entidad involucrando a todos los colaboradores, tanto servidores públicos, usuarios y contratistas para que contribuyan a crear un clima de seguridad tanto al interior como al exterior de la entidad.

La organización de seguridad debe estar distribuida por toda la entidad en diferentes funciones con responsabilidades relacionadas con la seguridad de la información, a través de roles para la realización de las actividades en las diferentes actividades, por ellos es indispensable contar con profesionales encargados de coordinar todo el modelo de seguridad, este debería estar dedicado a temas de seguridad y debe velar por el mejoramiento continuo del modelo de seguridad.

Con relación a la seguridad de los recursos humanos se debe tener en cuenta el ciclo de vida del recurso humano, esto es, antes, durante y después de su contratación.

GESTIÓN DE ACTIVOS

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 DE INFORMACIÓN”, 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 criterios

de valoración, conforme a los resultados de las calificaciones, para establecer la criticidad de los mismos.

La herramienta "GTI-MT-01 MATRIZ GESTION ACTIVOS DE INFORMACIÓN" registra la identificación, calificación y valoración de los activos de información

• Realizar un inventario de todos los activos de información, para este fin normalmente se realiza una búsqueda de los activos de información en los procesos y procedimientos, buscando el flujo de información en los mismos.
• Incluir en el inventario, el tipo de activo (físico o digital), ubicación, activos de soporte, redes, medios, servidores o servicios en las que se encuentra, proceso al que pertenece, entre otros.

Se considera a los activos de información como cualquier otro activo, con un valor financiero y estratégico.

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

Los activos críticos de Información se agrupan en tipologías de la siguiente forma:

TIPIFICACIÓN DEL ACTIVO	DESCRIPCIÓN	COMPONENTES
Información	Corresponden a este tipo datos e información almacenada o procesada electrónicamente tales como: bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros.	Archivos físicos de gestión, archivo físico general, bases de datos, documentos digitales, cuentas de correo.
Hardware	Se consideran los medios materiales físicos destinados a soportar directa o indirectamente los servicios que presta la Entidad.	Servidores, routers, Computadores (portátiles, escritorio), impresoras, Celulares Tablet, Teléfonos IP
Software	Se refiere a los programas, aplicativos, sistemas de información que soportan las actividades de la Entidad y la prestación de los servicios.	Software de aplicación, correo electrónico, sistema operativo, etc.
Servicios	Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e Intranet.	Servicio de internet, carpetas compartidas, servicios de almacenamiento en la nube.

RecursoHumano	Aquellas personas que, por su conocimiento, experiencia y criticidad para el proceso, son consideradas activos de información	Contratistas, funcionarios, proveedores.
Instalaciones	Los lugares donde se almacenan o resguardan los sistemas de información y comunicaciones.	Centros de cómputo, Centro deableado, Datacenter

ACTIVIDADES PARA LA IMPLEMENTACION DEL PLAN

Para el desarrollo de las actividades, la entidad deberá contar con un equipo humano dispuesto para adelantar actividades de sensibilización, capacitación y atención de inquietudes a todas las áreas del Instituto de Turismo del Meta a través de cronogramas definidos.

En este plan se establecen unos tiempos en los cuales se brindará y apoyará el seguimiento al desarrollo de los planes de seguridad y privacidad de la información, los responsables adelantaran las actividades concernientes con el propósito de aportar al fortalecimiento del Modelo de Seguridad y Privacidad de la Información institucional.

A continuación, se relacionan las actividades a desarrollar para la implementación del Plan.

ITEM	ACTIVIDAD	REPSONSABLE	PERIODICIDAD	EVIDENCIA
ACTIVOS DE INFORMACIÓN	Revisar, actualizar y publicar la GTI-MT-01 Matriz de activos de información	Profesional SGSI	FEBRERO Y CUANDO SE REQUIERA	Documento registrado ante SIG y publicado en pagina WEB
	Socialización de GTI-MT-01 Matriz de activos de Información	Profesional SGSI	SEMESTRAL	Registro de asistencia
GESTIÓN DE RIESGOS	Identificar, actualizar y publicar DPE-MT-01 mapa de riesgos de Seguridad y Privacidad de la Información.	Profesional SGSI	Como lo establezca el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Mapa de Riesgos publicada y seguimientos respectivos.
GESTIÓN DE INCIDENTES DE SEGURIDAD Y DE LA INFORMACIÓN	Crear, actualizar y publicar procedimiento de incidentes de seguridad de la información	Profesional SGSI	ANUAL Y CUANDO SE REQUIERA	Revisión anual una vez creado el documento
	Socialización procedimiento de incidentes de seguridad de la información	Profesional SGSI	SEMESTRAL Y CUANDO SE REQUIERA	Registro de asistencia
	Seguimiento a los incidentes de seguridad de la información de acuerdo al procedimiento	Profesional SGSI	MENSUAL	Registro de eventos
ESTRATEGIA DE COMUNICACIÓN SGSI	Documentar, actualizar y publicar estrategia y socialización del SGSI	Profesional SGSI	ANUAL Y CUANDO SE REQUIERA	Documento registrado ante SIG y publicación en pagina web.
	Seguimiento a la implementación de la estrategia	Profesional SGSI	TRIMESTRAL	Cronograma de actividad y registros de asistencia
MATRIZ DE REQUISITOS	Revisión, actualización y publicación de SIG-MT-	Profesional SGSI	ANUAL Y CUANDO SE REQUIERA	Documento registrado ante SIG y publicado en la

ITEM	ACTIVIDAD	REPSONSABLE	PERIODICIDAD	EVIDENCIA
LEGALES	01 matriz de requisitos legales GTIC			pagina web
	Socialización de SIG-MT-01 Matriz de requisitos legales del proceso GTIC	Profesional SGSI	SEMESTRAL Y CUANDO SE REQUIERA	Registro de asistencia
PLAN DE CONTINUIDAD DEL NEGOCIO	Elaborar, actualizar y publicar un plan de continuidad del negocio	Profesional SGSI	ANUAL Y CUANDO SE REQUIERA	Documento registrado ante SIG y publicado en la página web
	Socializar plan de continuidad de negocio y sus estrategias de implementación	Profesional SGSI	CUATRIMESTRAL	Registro de asistencia
POLÍTICA SGSI	Revisión, actualización y publicación de POLÍTICA SGSI	Profesional SGSI	FEBRERO	Documento registrado ante SIG y publicado en la pagina web
	Socializar políticas SGSI con el personal de la entidad.	Profesional SGSI	SEMESTRAL	Registro de asistencia
AUDITORIAS INTERNAS	Planificar, aplicar y documentar auditorías internas articulando con el Sistema Integrado de Gestión.	Profesional SGSI	ANUAL	Documentación requerida de acuerdo con el GCI-P-01 Procedimiento para la gestión de auditorias internas
	Realizar seguimiento a las acciones correctivas y de mejora.	Profesional SGSI	MENSUAL Y CUANDO SE REQUIERA	Reportes de seguimiento y actas de cierre (SIG-P-02 Procedimiento para la gestión de acciones correctivas y de mejora)
INDICADORES DE GESTIÓN	Revisión y actualización de indicadores de gestión del proceso	Profesional SGSI	ANUAL Y CUANDO SE REQUIERA	SIG-F-24 Ficha de indicador, indicador registrado ante el SIG
	Reporte y seguimiento indicadores de gestión	Profesional SGSI	TRIMESTRAL	SIG-F-24 Ficha de indicador reportada ante el SIG, evidencias de mejoras.
JORNADAS DE INDUCCION, REINDUCCIÓN Y CAPACITACIÓN	Realizar Capacitaciones e inducciones del Plan de Tratamiento de Seguridad y Privacidad de la Información	Profesional SIG	Con las jornadas de inducción y reinducción Generales y especificas al personal de planta	Registro de Asistencia e informe de la capacitación
REVISIÓN POR LA DIRECCIÓN	Realizar seguimiento, evaluación, presentación y reporte del SGSI de la vigencia	Profesional SGSI	ANUAL	DPE-F-02 Revisión por la Dirección

Las actividades antes propuestas se deben programar antes del 28 de febrero de cada vigencia en en la herramienta de seguimiento SIG-MT-06 Matriz de programación y seguimiento institucional, la cual deberá ser enviada y socializada con 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	Profesional SGSI Líder del proceso
GTI-MT-01	Matriz De Gestión De Activos De Información	Profesional SGSI
SIG-F-24	Ficha de Indicadores	Líder del proceso
SIG-MT-01	Matriz de requisitos legales	Profesional SGSI Líder del proceso
SIG-MT-06	Matriz de programación y seguimiento institucional	Profesional SGSI 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