



VERSIÓN 1.0
ENERO 2019

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Política de Seguridad y Privacidad de la Información es la declaración general del instituto de turismo del Meta (ITM) con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

El ITM para asegurar el direccionamiento estratégico de la entidad, establece la compatibilidad de la política y de los objetivos de seguridad de la información, estos últimos correspondientes a:

- a) Mitigar los riesgos de la entidad.
- b) Cumplir con los principios de seguridad de la información.
- c) Cumplir con los principios de la función administrativa.
- d) Mantener la confianza de los funcionarios, contratistas y terceros.
- e) Apoyar la innovación tecnológica.
- f) Implementar el sistema de gestión de seguridad de la información.
- g) Proteger los activos de información.
- h) Establecer las políticas, procedimientos e instructivos en materia de
- i) seguridad de la información.
- j) Fortalecer la cultura de seguridad de la información en los funcionarios y clientes externos del ITM.
- k) Garantizar la continuidad del servicio frente a incidentes.

1.1 Alcance

Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros del instituto de turismo del Meta y la ciudadanía en general.

1.2 Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento a esta política.

A continuación, se establecen las políticas que soportan el plan de seguridad y privacidad del ITM.

- a) El instituto ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, amparado en lineamientos claros alineados a las necesidades de la entidad, y a los requerimientos regulatorios que le aplican a su naturaleza.
- b) Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
- c) El ITM protege la información generada, procesada o resguardada por los procesos de la entidad y activos de información que hacen parte de estos.
- d) La entidad protege la información creada, procesada, transmitida o resguardada por sus procesos de la entidad, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- e) El instituto protege las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- f) El ITM controla la operación de sus procesos de la entidad garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- g) El ITM implementa controles de acceso a la información, sistemas y recursos de red.
- h) La entidad garantiza a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

2. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

2.1 Justificación

El instituto de turismo del Meta con el propósito de salvaguardar la información de la entidad en todos sus aspectos, garantizando la seguridad de los datos y el cumplimiento de las normas legales, ha establecido realizar un Plan de Seguridad y Privacidad de la información con el ánimo de que no se presenten pérdidas, robos, accesos no autorizados y duplicación de la misma, igualmente promueve una política de seguridad de la información física y digital de acuerdo a la caracterización de los usuarios tanto internos como externos.

La seguridad de la información se entiende como la preservación de las siguientes características:

- a) Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- b) Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- c) Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, debe considerarse los conceptos de:

- a. Auditabilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
- b. Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
- c. No repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- d. Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.
- e. Confiabilidad de la Información: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

A los efectos de una correcta interpretación del presente plan, se realizan las siguientes definiciones:

- a. Información: se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
- b. Sistema de Información: se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.
- c. Tecnología de la Información: se refiere al hardware y software operados la entidad o por un tercero que procese información en su nombre, para llevar a cabo una función propia del organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

2.2 Objetivo

Definir los mecanismos y todas las medidas necesarias por parte del instituto de turismo del Meta, tanto técnica, lógica, física, legal y ambiental para la protección de los activos de información, los recursos y la tecnología de la entidad, con el propósito de evitar accesos no autorizados, divulgación, duplicación, interrupción de sistemas, modificación, destrucción, pérdida, robo, o mal uso, que se pueda producir de forma intencional o accidental, frente a amenazas internas o externas, asegurando el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

2.3 Alcance

Este Plan de Seguridad y Privacidad de la Información y su política, son aplicables a todos los funcionarios de la entidad, a sus recursos, procesos y procedimientos tanto internos como externos, así mismo al personal vinculado a la entidad y terceras partes, que usen activos de información que sean propiedad de la entidad.

2.4 Roles y Responsabilidades

Es responsabilidad del Comité de Seguridad de la Información, la implementación, aplicación, seguimiento y autorizaciones de la política del plan de seguridad y privacidad de la información en las diferentes áreas y procesos de la entidad, además garantiza el apoyo y el uso de la política de Seguridad de la Información como parte de su herramienta de gestión, la cual debe ser aplicada de forma obligatoria por todos los funcionarios para el cumplimiento de los objetivos.

El Comité de Seguridad de la Información cuya composición y funciones serán reglamentadas por una mesa de trabajo compuesta por:

- ✓ Subdirector general
- ✓ Profesional universitario de planeación
- ✓ Apoyo de sistemas
- ✓ Almacenista

Este comité deberá revisar y actualizar esta política anualmente presentando las propuestas a la alta dirección para su aprobación.

2.5 Cumplimiento

El cumplimiento de la Política de Seguridad y Privacidad de la Información es obligatorio. Si los funcionarios de la entidad o terceros violan este plan, la entidad se reserva el derecho de tomar las medidas correspondientes.

2.6 Comunicación

Mediante socialización a todos los funcionarios de la entidad se dará a conocer el contenido del documento de las políticas de seguridad, así mismo se deberá informar a los contratistas y/o terceros en el momento que se requiera con el propósito de realizar los ajustes y la retroalimentación necesaria para dar cumplimiento efectivo al plan.

Todos los funcionarios, contratistas y/o terceros de la entidad deben conocer la existencia de las políticas, la obligatoriedad de su cumplimiento, la ubicación física del documento

estará a cargo del Sistema de Gestión Integrado para que sean consultados en el momento que se requieran, igualmente estarán alojados en la página de la entidad.

2.7 Monitoreo

Se crearán los mecanismos y los indicadores correspondientes a la política de seguridad con el fin de determinar el cumplimiento de estas para establecer qué modificaciones o adiciones deben hacerse, este monitoreo debe realizarse como mínimo una vez al año o cuando sea necesario.

3. DESCRIPCIÓN DE LAS POLÍTICAS

Generalidades

El instituto de turismo del Meta en todas sus áreas y procesos cuenta con información, reservada, relevante, privilegiada e importante, es decir que esta información es el principal activo de la entidad para el desarrollo de todas sus actividades por lo que se hace necesario y se debe proteger conforme a los criterios y principios de los sistemas de información, como son integridad, disponibilidad y confidencialidad de la información.

3.1 Gestión de activos

3.1.1 Política para la identificación, clasificación y control de activos de información

La entidad a través del Comité de Seguridad de la Información realizará la supervisión de cada proceso, el cual debe aprobar el inventario de los activos de información que procesa y produce la entidad, estas características del inventario deben establecer la clasificación, valoración, ubicación y acceso de la información, correspondiendo a Gestión de TIC y al área de almacén que permitan la administración del inventario por cada área, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen.

El almacenista con apoyo de sistemas tiene la responsabilidad de mantener el inventario completo y actualizado de los recursos de hardware y software de la entidad.

3.2 Control de Acceso

3.2.1 Política de acceso a redes y recursos de red

El apoyo de sistemas de la entidad, como responsable de las redes de datos y los recursos de red de la entidad, debe propender porque dichas redes sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico.

3.2.2 Política de administración de acceso de usuarios

El ITM establecerá privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información de la Entidad. Así mismo, velará porque los funcionarios y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y porque la asignación.

3.2.3 Política de control de acceso a sistemas de información y aplicativos

El instituto de turismo del Meta como propietario de los sistemas de información y aplicativos que apoyan los procesos y áreas que lideran, velarán por la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada. El proceso Gestión de TIC, como responsable de la administración de dichos sistemas de información y aplicativos, propende para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico.

3.2.4 Políticas de seguridad física

El ITM provee la implantación y vela por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus áreas. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se considera áreas de acceso restringido. Se debe tener acceso controlado y restringido a donde se encuentra los servidores y el cuarto de comunicaciones.

3.2.5 Política de uso adecuado de internet

El instituto de turismo del Meta consciente de la importancia del servicio de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la entidad.

Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.

No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento.

4. RESPALDOS O COPIAS DE SEGURIDAD

Toda información que pertenezca a la matriz de activos de información institucional o que sea de interés para un proceso operativo o de misión crítica debe ser respaldada por copias de seguridad tomadas de acuerdo a los procedimientos documentados por el Comité de Seguridad de la Información. Dicho procedimiento debe incluir las actividades de almacenamiento de las copias en sitios seguros.

Las copias de seguridad de archivos personales es responsabilidad exclusiva de los usuarios dueños de la información.