PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ASOCIACIÓN DE MUNICIPIOS DEL META

ASMETA

2024

Teléfonos 320 301 5193 - 320 301 5206
E-mail: direccionasmeta@gmail.com - secretariaasmeta@gmail.com
Calle 18 No. 41Bis - 23 Barrio Villa María
Villavicencio - Meta

JUSTIFICACIÓN

La Asociación de Municipios del Meta - ASMETA, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información, integrándola de manera activa en la cultura organizacional, y promoviendo la responsabilidad corporativa en tres componentes esenciales, como lo son la confidencialidad, integridad y disponibilidad de la información. Para soportar esto, el Estado Colombiano, ha desarrollado un completo marco legal y normativo, que permite a entidades como La Asociación de Municipios del Meta - ASMETA, desarrollar planes y políticas robustas, orientadas a garantizar la seguridad de la información. Entre otras normas podemos encontrar:

Para La Asociación de Municipios del Meta - ASMETA, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados. De acuerdo con lo anterior, esta política aplica a la entidad según como se defina en el alcance, sus colaboradores, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en cada uno de los procesos.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los clientes internos y externos de La Asociación de Municipios del Meta - ASMETA
- Garantizar la continuidad del negocio frente a incidentes.
- La Asociación de Municipios del Meta – ASMETA, ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

MARCO LEGAL

- Ley 1581 de 2012 Protección de datos personales, Artículo 4,literal g Principio de seguridad: *"La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento."*
- Ley 1581 de 2012, Artículo 17, literal d: *"Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento"*
- Ley 1712 de 2014 Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional, artículo 7: "Disponibilidad de la información"

"En virtud de los principios señalados, deberá estar a disposición del público la información a la que hace referencia la presente ley, a través de medios físicos, remotos o locales de comunicación electrónica. Los sujetos obligados deberán tener a disposición de las personas interesadas dicha información en la web, a fin de que estas puedan obtener la información, de manera directa o mediante impresiones. Así mismo, estos deberán proporcionar apoyo a los usuarios que lo requieran y proveer todo tipo de asistencia respecto de los trámites y servicios que presten."

- Decreto 2573 de 2014 Estrategia Gobierno en Línea (Gobierno Digital): "Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones".
- Decreto 2573 de 2014 Estrategia Gobierno en Línea (Gobierno Digital), Artículo 5 numeral 4: *"Seguridad y privacidad de la Información. Comprende acciones transversales a demás componentes enunciados, a proteger la información y sistemas de información, del acceso, divulgación, interrupción o destrucción no autorizada.".*
- Decreto 1413 de 2017, artículo 2.2.17.6.6, Seguridad de la información.

"Los actores que traten información, en el marco del presente título, deberán adoptar medidas apropiadas, efectivas y verificables de seguridad que le permitan demostrar el correcto cumplimiento de las buenas prácticas consignadas en el modelo de seguridad y privacidad de la información emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones, o un sistema de gestión de seguridad de la información certificable. Esto con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información."

- Decreto 1413 de 2007, artículo 2.2.17.6.1, Responsable y encargado del tratamiento:

"Los operadores de servicios ciudadanos digitales serán responsables del tratamiento de los datos personales que los ciudadanos le suministren directamente y encargados del tratamiento respecto de los datos que otras entidades le proporcionen."

- Decreto 1413 de 2007, artículo 2.2.17.6.5, Privacidad por diseño y por defecto:

"Los operadores de servicios ciudadanos digitales deberán atender las buenas prácticas y principios desarrollados en el ámbito internacional en relación con la protección y tratamiento de datos personales que son adicionales a la Accountability, y que se refieren al Privacy by design (PbD) y Privacy Impact Assessment (PIA), cuyo objetivo se dirige a que la protección de la privacidad y de los datos no puede ser asegurada únicamente a través del cumplimiento de la normativa, sino que debe ser un 'modo de operar de las organizaciones, y aplicarlo a los sistemas de información, modelos, prácticas de negocio, diseño físico, infraestructura e interoperabilidad, que permita garantizar la privacidad al ciudadano y a las empresas en relación con la recolección, uso, almacenamiento, divulgación y disposición de los mensajes de datos para los servicios ciudadanos digitales gestionados por el operador"

- Decreto 1499 de 2017, por medio del cual se modifica el Sistema de gestión y se da forma al Modelo Integrado de Planeación y Gestión, Manual Operativo, Capítulo 3.2.1.3, Seguridad de la Información:

"Una constante en la gestión de las entidades públicas debe ser implantar en todos los procesos de la entidad, políticas, controles y procedimientos con el fin de aumentar los niveles de protección y adecuada salvaguarda de la información, preservando su confidencialidad, integridad y disponibilidad, mediante la aplicación de un proceso de gestión del riesgo de tal manera que se brinde confianza a las partes interesadas."

- Resolución 2710 de 2017 (IPV6): *"Por la cual se establecen los lineamientos para la adopción del protocolo IPv6".*

GLOSARIO

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).

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 auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

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: Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701, Tomado de la Academia de la lengua Española).

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.

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).

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).

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).

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).

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).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

Parte interesada (Stakeholder): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

OBJETIVO

3.1 Objetivo General

Establecer el Sistema de seguridad de la información dentro del marco conceptual, sobre el cual se soporta el plan de seguridad, brindando los conceptos requeridos para realizar el aseguramiento de la información en la Asociación de Municipios del Meta - ASMETA.

3.2 Objetivos Específicos

- Fortalecer el Sistema de Gestión de Seguridad de la Información y facilitar su inclusión en el Sistema Integrado de Gestión de La Asociación de Municipios del Meta - ASMETA.
- Impulsar la conciencia en las partes interesadas, respecto a la importancia que tiene la seguridad de la información, para garantizar la continuidad del servicio.
- Construir una plataforma, conformada por planes de acción y políticas generales y específicas, que brinden las herramientas necesarias para fomentar las mejores prácticas en La Asociación de Municipios del Meta - ASMETA, en cuanto a la seguridad de la información.
- Socializar y difundir el Sistema de Seguridad de la Información de La Asociación de Municipios del Meta - ASMETA.

ALCANCE

El Plan de Seguridad y privacidad de la información, y la Política de Seguridad de la Información se establecen en cumplimiento de las disposiciones legales vigentes, que permitan la gestión adecuadamente de la seguridad de la información, los sistemas informáticos y el ambiente tecnológico de la Asociación de Municipios del Meta – ASMETA.

La Asociación de Municipios del Meta – ASMETA., en su búsqueda de fortalecer la seguridad de la información generada en el desarrollo de los procesos de la institución, con el fin de preservar la **INTEGRIDAD, CONFIDENCIALIDAD, DISPONIBILIDAD Y PRIVACIDAD DE LOS ACTIVOS DE INFORMACIÓN** mediante el Modelo de Seguridad y Privacidad de la Información **(MSPI)** paralelo con el Sistema de Gestión de Seguridad de la Información **(SGSI)**, para mejorar la prestación de los servicios.

La Política de Seguridad de la Información es de obligatorio cumplimiento y aplica a todos los funcionarios, contratistas y demás partes interesadas en la Asociación de Municipios del Meta – ASMETA., que en ejercicio de sus funciones o en el cumplimiento de sus obligaciones contractuales, según el caso, tengan acceso a los activos de información de la entidad.

ROLES Y RESPONSABILIDADES

Todos los funcionarios, contratistas y demás partes son responsables de la seguridad de la información; adicionalmente, se establecen los siguientes roles y responsabilidades:

El Comité Institucional de Gestión y Desempeño, tiene la responsabilidad de impulsar la implementación del Modelo de Seguridad de la Información alineado al Sistema de Gestión de Seguridad de la Información SGSI., además de realizar el seguimiento y /o verificación de la implementación del mismo.

La Oficina **GESTION DE LA INFORMACION** o quien haga sus veces, será el responsable del funcionamiento del Modelo de Seguridad y Privacidad de la Información y tendrá la responsabilidad de coordinar la implementación y cumplimiento del Modelo de Seguridad y Privacidad de la Información MSPI

Los **Propietarios de la Información** son responsables de clasificarla de acuerdo con el grado de sensibilidad de la misma, de documentar y mantener actualizada la clasificación efectuada, y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia.

El **responsable del Área de Recursos Humanos** o quién desempeñe esas funciones, cumplirá la función de notificar a todo el personal que ingresa, de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan.

El **Usuario de la Información**, es el funcionario, contratista y/o tercero autorizado para utilizar la información en el ejercicio de sus funciones o en el cumplimiento de sus obligaciones contractuales o vigencia del respectivo contrato y es el responsable del buen uso de los activos de información durante el cumplimiento de sus labores o compromisos, según de quien se trate.

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, ASMETA. se reserva el derecho de tomar las medidas correspondientes.

COMUNICACIÓN

Mediante socialización a todos los funcionarios de ASMETA. 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 para que sean consultados en el momento que se requieran, igualmente estarán alojados en la página de la entidad https://asmeta.gov.co/

MONITOREO

Se crearán los mecanismos y los indicadores correspondientes a la política de seguridad con el fin de determinar el cumplimiento de las mismas para establecer

qué modificaciones o adiciones deben hacerse, este monitoreo debe realizarse como mínimo una vez al año o cuando sea necesario.

PLAN DE ACCIÓN 2024

- **Actualización y Fortalecimiento de Políticas de Seguridad de la Información**

La Dirección TIC, lidera un proceso en el cual, busca que para el año 2024, se continúe con unas políticas de seguridad de la información robusta y específica.

Estas políticas se basan en tres elementos esenciales:

1. Lineamientos de Gobierno en Línea, en lo que respecta al eje temático de Seguridad y Privacidad de la información, incluyendo las plantillas que ofrece Mintic para la construcción de políticas.
2. Políticas y Objetivos de la Norma NTC-ISO/IEC 27001
3. Análisis del contexto de La Asociación de Municipios del Meta - ASMETA, entre lo que se incluyen:
    - 3.1 Inventario de Activos de la Información Actualizado
    - 3.2 Diagnóstico de Infraestructura TI
    - 3.3 Matriz de Riesgos en Seguridad de la Información, orientado para esta vigencia, en el Proceso de Dirección Comercial

- **Plan de Divulgación de Políticas de Seguridad de la Información**

Para el año 2024, la Dirección TIC, inicia un proceso de divulgación y difusión de las nuevas políticas, para lo cual, se realizará un trabajo conjunto con la Dirección de Comunicaciones, de modo que se construyan mensajes asertivos y que lleguen a la audiencia definida de forma clara y directa.

- **Actualización de Activos de Información**

A partir del año 2024, la Dirección TIC, realizara un trabajo exhaustivo, inventariando los activos de información, detallando y registrando adecuadamente, cada elemento que hace parte del inventario, para que de este modo se puedan identificar, vulnerabilidades, amenazas, riesgos y controles a aplicar en el caso que uno de estos activos se vea afectado por un fallo en el Sistema de Seguridad de la Información.

- **Construcción del Mapa de Riesgos de Seguridad de la Información**

Una vez identificado y documentado el inventario de activos, se ha construido el mapa de riesgos.

- **Fortalecimiento de Infraestructura TI**

Se ejecutarán proyectos para la actualización de la infraestructura, llegando a cambiar más puntos de datos antes del mes de diciembre del 2024.

- **Plan de Auditorías internas ISO 27000**

Teniendo en cuenta que se realiza el alistamiento del proceso de Dirección Comercial, en lo que respecta a ISO 27000, se plantea un plan de auditorías internas a partir del mes de noviembre de la presente vigencia, con el fin de evaluar lo siguiente:

1. Entendimiento y conocimiento general del Sistema de Gestión de Seguridad de la Información
2. Conocimiento de las políticas de seguridad que aplican al puesto de trabajo
3. Identificación y aplicación de controles, según la matriz de riesgos identificado
4. Conciencia de la Seguridad y Privacidad de la Información.