MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

SISTEMA ESTRATÉGICO DE TRANSPORTE PUBLICO DE SANTA MARTA

Santa Marta

2021

@setpsantamarta
www.setpsantamarta.gov.co

Calle 24 No. 03 - 99 Ofi. 1202
Edificio Banco de Bogotá
Telefono: (+57) 5 4317777
info@setpsantamarta.gov.co
Nit: 900.342.579-4

Tabla de contenido

1. INTRODUCCIÓN. 3
2. JUSTIFICACIÓN. 4
3. OBJETIVOS. 5
4. ALCANCE: 6
5. NIVEL DE CUMPLIMIENTO. 7
6. LINEAMIENTOS. 9
7. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. 10
7.1 MARCO NORMATIVO 11
8. SISTEMA ESTRATÉGICO DE TRANSPORTE PUBLICO DE SANTA MARTA S.A.S. . 13
8.1. MISIÓN 13
8.2. VISIÓN 13
8.3. POLÍTICA DE CALIDAD 13
9. PROCEDIMIENTOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. 14
9.1. SEGURIDAD DEL RECURSO HUMANO. 14
9.2. GESTIÓN DE ACTIVOS. 15
9.3. CONTROL DE ACCESO. 16
9.4. SEGURIDAD FÍSICA Y DEL ENTORNO 16
9.4.1. PROCEDIMIENTO DE PROTECCIÓN DE ACTIVOS: 16
9.4.2. PROCEDIMIENTO DE RETIRO DE ACTIVOS: 17
9.4.3. PROCEDIMIENTO DE MANTENIMIENTO DE EQUIPOS: 17
9.5 SEGURIDAD DE LAS COMUNICACIONES: 17
9.5.1. PROCEDIMIENTO DE ASEGURAMIENTO DE SERVICIOS EN LA RED: 17
9.5.1.1. Antivirus: 18
9.5.1.2. Infraestructura tecnológica SETP Santa Marta. 18
10. TERMINOLOGÍAS: 19

Calle 24 No. 03 - 99 Ofi. 1202
Edificio Banco de Bogotá
Telefono: (+57) 5 4317777
info@setpsantamarta.gov.co
Nit: 900.342.579-4

1. INTRODUCCIÓN.

El **Sistema Estratégico De Transporte Público de Santa Marta - SETP** a través de su área TIC, dando cumplimiento a sus funciones; publica el Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y La Guía para la Administración del Riesgo y el Diseño Controles en entidades Públicas, este modelo pertenece al habilitador transversal de Seguridad y Privacidad de la Política de Gobierno Digital.

El Modelo de Seguridad y Privacidad para estar acorde con las buenas prácticas de seguridad será actualizado periódicamente; reuniendo los cambios técnicos de la norma ISO/IEC 27001 del 2013, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública.

La implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, en la Entidad está determinado por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de esta, todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.

Mediante la adopción del Modelo de Seguridad y Privacidad de la información por parte del Sistema Estratégico De Transporte Publico de Santa Marta – SETP se busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital.

El siguiente documento tiene la finalidad de dar a conocer el modelo de Seguridad y privacidad de la información, que deben aplicar y acatar los empleados, contratistas y terceros del **Sistema Estratégico de Transporte Publico S.A.S SETP**, entendiendo como premisa que la responsabilidad por la seguridad de la información es de todos y cada uno.

Calle 24 No. 03 - 99 Ofi. 1202
Edificio Banco de Bogotá
Telefono: (+57) 5 4317777
info@setpsantamarta.gov.co
Nit: 900.342.579-4

2. JUSTIFICACIÓN.

En el marco del proceso de seguridad de la información es importante contar con políticas de seguridad ya que son ellas quienes guiaran el comportamiento personal y profesional de los funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada por la entidad, así mismo las políticas permitirán que la entidad trabaje bajo las mejores prácticas de seguridad y cumpla con los requisitos legales a los cuales esté obligada a cumplir; se ha determinado que los activos de información necesitan ser administrados, controlados física y lógicamente para mitigar el impacto y la posibilidad de riesgos cuando ocurren.

Para realizar este plan tomamos como lineamiento los cambios técnicos de la norma ISO 27001 del 2013, el Modelo de seguridad y privacidad de la información propuesto por el ministerio de las tecnologías y las comunicaciones en concordancia con las actividades de la estrategia de gobierno en línea buscando así de esta manera proteger los bienes, activos y servicios tecnológicos de la entidad.

Calle 24 No. 03 - 99 Ofi. 1202
Edificio Banco de Bogotá
Telefono: (+57) 5 4317777
info@setpsantamarta.gov.co
Nit: 900.342.579-4

3. OBJETIVOS.

3.1. Objetivo General.

Documentar, establecer, definir e implementar el Modelo de seguridad y privacidad de la información **MSPI** para el **Sistema Estratégico de Transporte Público de Santa Marta SAS**.

3.2. Objetivos Específicos.

Establecer e implementar las políticas de seguridad de la información y conocer, asumir, gestionar y tratar los riegos de seguridad de la información de una manera sistemática, documentada y eficiente.

Establecer los lineamientos y las responsabilidades de los actores que intervienen en la política de seguridad digital de la entidad para que conozcan sobre su implementación desde una perspectiva basada en riesgos.

Promover el uso de mejores prácticas de seguridad de la información y el manejo seguro de los elementos informáticos con los que cuenta la entidad.

Generar conciencia de los cambios organizacionales requeridos para la apropiación de la Seguridad y Privacidad de la Información como eje transversal de la entidad.

Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la información, seguridad digital y protección de la información personal.

Calle 24 No. 03 - 99 Ofi. 1202
Edificio Banco de Bogotá
Telefono: (+57) 5 4317777
info@setpsantamarta.gov.co
Nit: 900.342.579-4

4. ALCANCE:

El Sistema Estratégico de Transporte publico de Santa Marta SETP entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un Modelo de gestión de seguridad de la información para así establecer un marco de confianza en el ejercicio de sus deberes con el Estado y buscando así aplicarla a todos sus funcionarios, contratistas, terceros, colaboradores y ciudadana en general, así como a todos los activos de información, servicios, procesos, las tecnologías de información incluida el hardware y el software, instalaciones imagen perceptual y demás herramientas utilizadas por la entidad en el ejercicio de sus funciones, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para el SETP Santa Marta 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 esta, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad, sus funcionarios, 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 **Modelo De Seguridad y Privacidad de la Información** estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- 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 funcionarios, terceros, aprendices, practicantes y clientes del SETP.
- Garantizar la continuidad del negocio frente a incidentes.

El Sistema Estratégico de Transporte Publico de Santa Marta SAS SETP 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.

Calle 24 No. 03 - 99 Ofi. 1202
Edificio Banco de Bogotá
Telefono: (+57) 5 4317777
info@setpsantamarta.gov.co
Nit: 900.342.579-4

5. NIVEL DE CUMPLIMIENTO.

Todas las personas cubiertas por el alcance deberán dar cumplimiento un 100% de la política.

A continuación, se establecen las políticas de seguridad que soportan el MSPI del **Sistema Estratégico de Transporte publico de Santa Marta SETP**:

• El Sistema Estratégico de Transporte publico de Santa Marta SETP ha decidido **definir, implementar, operar y mejorar** de forma continua un Modelo de Seguridad y Privacidad de la Información, soportado en lineamientos claros alineados a las necesidades de la entidad, y a los requerimientos regulatorios que le aplican a su naturaleza.

• Las **responsabilidades** frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de **los empleados, contratistas o terceros**.

• El Sistema Estratégico de Transporte publico de Santa Marta SETP **protegerá la información** generada, procesada o resguardada por los procesos y activos de información que hacen parte de estos.

• El Sistema Estratégico de Transporte publico de Santa Marta SETP **protegerá la información** creada, procesada, transmitida o resguardada por sus procesos, 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.

• El Sistema Estratégico de Transporte publico de Santa Marta SETP **protegerá su información** de las amenazas originadas por parte **del personal**.

• El Sistema Estratégico de Transporte publico de Santa Marta SETP **protegerá las instalaciones** de procesamiento y la infraestructura tecnológica **que soporta sus procesos críticos**.

• El Sistema Estratégico de Transporte publico de Santa Marta SETP **controlará la operación** de sus procesos garantizando la seguridad de los recursos tecnológicos y las redes de datos.

• El Sistema Estratégico de Transporte publico de Santa Marta SETP **implementará control de acceso** a la información, sistemas y recursos de red.

• El Sistema Estratégico de Transporte publico de Santa Marta SETP garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

• El Sistema Estratégico de Transporte publico de Santa Marta SETP garantizará 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.

Calle 24 No. 03 - 99 Ofi. 1202
Edificio Banco de Bogotá
Telefono: (+57) 5 4317777
info@setpsantamarta.gov.co
Nit: 900.342.579-4

• El Sistema Estratégico de Transporte publico de Santa Marta SETP **garantizará la disponibilidad** de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.

• El Sistema Estratégico de Transporte publico de Santa Marta SETP |garantizará el cumplimiento de las **obligaciones legales, regulatorias y contractuales establecidas.**

Cabe resaltar que las redes y la infraestructura informática implementadas en las instalaciones de la entidad tienen como propósito principal servir como medio de comunicación y de enlace para el movimiento, transformación e intercambio de información dentro de la entidad, por lo tanto:

• El Área de sistemas **no es responsable por el contenido de datos ni por el tráfico que en ella circule**, la responsabilidad recae directamente sobre el usuario que los genere o solicite.

• **Nadie puede ver, copiar, alterar o destruir la información** que reside en los equipos sin el consentimiento explícito del responsable del equipo.

• No se permite el uso de los servicios de la red cuando no cumplan con las labores propias de la entidad.

• Las cuentas de ingreso a los sistemas y los recursos de cómputo son propiedad de la entidad y se usarán exclusivamente para actividades relacionadas con la labor asignada.

• Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles. Se permite su uso única y exclusivamente durante la vigencia de derechos del usuario.

• **No se permitirá el uso de analizadores para monitorear o censar redes ajenas** a Las Empresas y no se deberán realizar análisis de la Red desde equipos externos a la entidad.

• No deben ser reemplazados ni modificados sin la intervención del Ing. De Sistemas de la Entidad los Firewalls, antivirus y en general, todos los programas o aplicativos destinados a la prevención de intrusos no deseados y de elementos dañinos para los equipos.

El incumplimiento a la política de Seguridad y Privacidad de la Información propuesta en este modelo traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

Calle 24 No. 03 - 99 Ofi. 1202
Edificio Banco de Bogotá
Telefono: (+57) 5 4317777
info@setpsantamarta.gov.co
Nit: 900.342.579-4

6. LINEAMIENTOS.

El Sistema Estratégico de Transporte publico de Santa Marta SETP, mediante la Política de seguridad de información da cumplimiento a los lineamientos de la Planeación Estratégica de la entidad en concordancia con su misión, visión, objetivos y para ello debe tener en cuenta:

a) Gestionar el riesgo de los procesos estratégicos, misionales, de apoyo y de evaluación de la entidad.

b) Cumplir con los principios de seguridad de la información:

• CONFIDENCIALIDAD: la información debe ser accesible solo a aquellas personas autorizadas.

• INTEGRIDAD: la información y sus métodos de procesamiento deben ser completos y exactos.

• DISPONIBILIDAD: la información y los servicios deben estar disponible cuando se requieran.

c) Mantener la confianza de los funcionarios, contratistas y terceros.

d) Mantener y Mejorar constantemente el sistema de gestión de seguridad de la información.

e) Proteger los activos de información.

f) Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.

g) Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices y/o practicantes.

h) Proteger la información y los activos tecnológicos de la entidad.

i) Adquirir un compromiso de concientización para que todos los funcionarios, contratistas aprendices y/o practicantes sobre el uso adecuado de los activos de información puestos a su disposición para la realización de las funciones y actividades)

j) Dar cumplimiento a los lineamientos de la Estrategia de Gobierno Digital respecto a la Seguridad de la Información.

k) Garantizar la continuidad de los servicios frente a incidentes.

L) Realizar campañas de sensibilización

Calle 24 No. 03 - 99 Ofi. 1202
Edificio Banco de Bogotá
Telefono: (+57) 5 4317777
info@setpsantamarta.gov.co
Nit: 900.342.579-4

7. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Mediante la Ley 1341 de 2009 "por la cual se definen principios y conceptos sobre la seguridad de la información y la organización de las tecnologías de la información y las comunicaciones -TIC-se crea la agencia nacional de espectro y se dictan otras disposiciones", señala en su artículo2°, como principios orientadores y aspectos fundamentales para la promoción de la libre competencia y el comercio electrónico, lo siguiente: la protección a los derechos de los usuarios de las TIC, el acceso y uso de las TIC, la garantía de los derechos de los ciudadanos y la masificación del Gobierno Digital.

Que el Decreto 1078 de 2015 en el artículo2.2.9.1.1.1. establece como objeto "Definir los lineamientos, instrumentos y plazos de la estrategia de Gobierno en línea para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el fin de contribuir con la construcción de un Estado abierto, más eficiente, más transparente, más participativo y que preste mejores servicios con la colaboración de toda la sociedad".

Que el Ministerio de Tecnologías de la Información y las Comunicaciones -MinTIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, dando cumplimiento a sus funciones; publicó el Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes.

Con el fin de garantizar la disponibilidad, integridad y confidencialidad de la información, El Sistema Estratégico de Transporte publico de Santa Marta SETP, empleará y distribuirá equipos con los controles criptográficos en toda la organización, conforme se establece en el (AGA-MA-01 Manual de Políticas de Seguridad Informática V3…) implementado en la entidad.

Calle 24 No. 03 - 99 Ofi. 1202
Edificio Banco de Bogotá
Telefono: (+57) 5 4317777
info@setpsantamarta.gov.co
Nit: 900.342.579-4

7.1 MARCO NORMATIVO

CÓDIGO NORMATIVIDAD	DESCRIPCIÓN
Ley 1221 de 2008	**Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.**
Ley 1341 de 2009	**Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones - TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones**
Ley 1266 de 2008:	**Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.**
Ley 1273 de 2009:	**Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.**
Ley 1437 de 2011.	**Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.**
Ley 1581 de 2012:	**Por la cual se dictan disposiciones generales para la protección de datos personales.**
Decreto 3816 de 2003:	**"Por el cual se crea la Comisión Intersectorial de Políticas y de Gestión de la Información para la Administración Pública".**
Decreto 235 DE 2010:	**Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones.**
Decreto 019 de 2012:	**Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.**
Decreto 2609 de 2012:	**Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de**

Calle 24 No. 03 - 99 Ofi. 1202
Edificio Banco de Bogotá
Telefono: (+57) 5 4317777
info@setpsantamarta.gov.co
Nit: 900.342.579-4

	Gestión Documental para todas las Entidades del Estado.
Decreto 1078 de 2015:	**"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"**
Decreto 2094 de 2016:	**Por el cual se modifica la estructura del Departamento Administrativo para la Prosperidad Social - Prosperidad Social.**
Decreto 1499 de 2017:	**Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.**
Documento CONPES No. 3854 de 2016:	**Política Nacional de Seguridad Digital.**
Acuerdo 003 de 2015 del AGN:	**Por el cual se establecen los lineamientos generales para las entidades del Estado en cuanto a la gestión de documentos electrónicos generados como resultado del uso de medios electrónicos de conformidad con lo establecido en el capítulo IV de la Ley 1437 de 2011, se reglamenta el artículo 21 de la Ley 594 de 2000 y el capítulo IV del Decreto 2609 de 2012.**

Calle 24 No. 03 - 99 Ofi. 1202
Edificio Banco de Bogotá
Telefono: (+57) 5 4317777
info@setpsantamarta.gov.co
Nit: 900.342.579-4

8. SISTEMA ESTRATÉGICO DE TRANSPORTE PUBLICO DE SANTA MARTA S.A.S.

8.1. MISIÓN

El SETP de Santa Marta, es una organización descentralizada del orden Municipal, que tiene por objetivo planear, coordinar, gestionar, desarrollar e implementar y Supervisar el SISTEMA ESTRATÉGICO DE TRANSPORTE PÚBLICO DE PASAJEROS PARA LA CIUDAD DE SANTA MARTA, contribuyendo con la construcción de una ciudad moderna e incluyente y al mejoramiento de La Calidad De Vida De Sus Habitantes.

8.2. VISIÓN

En el año 2022 ser líderes y modelo de eficiencia en el desarrollo e implementación del SISTEMA ESTRATÉGICO DE TRANSPORTE PÚBLICO, dentro de la estrategia de SISTEMAS ESTRATÉGICOS, a través de un manejo eficiente de los recursos asignados y a su vez ser reconocidos por la ciudadanía como gestores del desarrollo y movilidad del transporte público en la ciudad de Santa Marta.

8.3. POLÍTICA DE CALIDAD

El SETP SANTA MARTA S.A.S es una entidad que, a través de la articulación con organismos a nivel nacional y local de orden público y privado, tiene por objeto poner en marcha y gestionar el sistema Estratégico de Transporte Público de pasajeros del Distrito Turístico, Cultural e Histórico de Santa Marta. Para ello ha establecido procesos eficaces y efectivos, logrando el cumplimiento de los requerimientos y actividades inherentes a la misión del Ente, mediante la mejores continua de los mismos.

Calle 24 No. 03 - 99 Ofi. 1202
Edificio Banco de Bogotá
Telefono: (+57) 5 4317777
info@setpsantamarta.gov.co
Nit: 900.342.579-4

9. PROCEDIMIENTOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El Modelo de Seguridad y Privacidad de la Información constituye una base sólida para que El Sistema Estratégico de Transporte Publico de Santa Marta S.A.S. SETP genere sus documentaciones propias dependiendo de sus características particulares, sus activos de información, sus procesos y los servicios de información que pueda prestar.

Con el objetivo de hacer una implementación transversal de Seguridad de la Información en la Entidad, se tomaron en cuenta los numerales de control de seguridad de la información definidas en la norma ISO/IEC 27001, para definir los procedimientos de seguridad necesarios.

9.1. SEGURIDAD DEL RECURSO HUMANO.

- **Procedimiento de capacitación y sensibilización del personal:** Mediante este procedimiento se establecen los lineamientos y cronogramas definidos para atender las etapas de capacitación de los funcionarios y/o contratistas del Sistema Estratégico de Transporte Publico de Santa Marta S.A.S. SETP, mediante este modelo se implementará el proceso de sensibilización y capacitación de la siguiente manera.

    1. Socialización de las medidas y procesos implementados en el nuevo modelo de seguridad y privacidad de la información, por medio del cual se instruirá a los funcionarios y/o contratistas sobre como operarán las medidas

propuestas y su relación comprendida en el punto **(4. Alcance)** del presente documento.

2. Compartir con los usuarios por medio físico o digital la información relacionada con las diferentes amenazas que diariamente pueden atentar contra la seguridad de la información en la entidad.
3. Socializar y enseñar el manejo de carpetas individuales para copias de seguridad, donde cada usuario recopilará y guardará en una carpeta designada la información de importancia con la cual trabaja; esta información será resguardada por el equipo del Área Tic de la entidad mediante el proceso de copia de seguridad tomando como lineamiento el punto **(5. Nivel de cumplimiento)** del presente documento.
4. Socializar e instruir sobre la importancia de la confidencialidad, disponibilidad y manejo de la información; todo esto comprendido y documentado según el punto **(6. Lineamientos)** del presente documento.

9.2. GESTIÓN DE ACTIVOS.

- En este dominio relacionado con la identificación y clasificación de activos de acuerdo con su criticidad y nivel de confidencialidad se pueden definir los siguientes procedimientos:

    1. **Procedimiento de identificación y clasificación de activos:** Mediante este procedimiento se realiza la identificación y correctamente inventariados en la entidad, además de cómo son clasificados según su nivel de confidencialidad o criticidad, además de como se hace la debida disposición de dichos activos cuando ya no se requieran o su vida útil haya llegado a su fin.

- Tomando en cuenta lo anterior se dispone en el Sistema Estratégico de Transporte Publico de Santa Marta S.A.S. SETP unos módulos debidamente diligenciados, publicados y puestos en marcha para el proceso de identificación, documentación, clasificación y debida integración al inventario general de activos de la entidad, tomando como referencia estos parámetros, los nombres e identificación de dichos modelos es puesta a continuación.

    1. **AGA-FO-11 Control de Activos Fijos v3.**
    2. **AGA-FO-11 Control de Activos Fijos V4.**
    3. **AGA-FO-03 Hoja de Vida de Equipos De Cómputo V2.0.**
    4. **AGA-IN-01 Instructivo Para la Realización de Copias de Seguridad (Backup) V2.0.**
    5. **AGA-PD-04 Procedimiento para la Gestión de Activos Fijos.**
    6. **AGA-FO-22 Control de Backups y revisión de Servidores V1.0.**

Calle 24 No. 03 - 99 Ofi. 1202
Edificio Banco de Bogotá
Telefono: (+57) 5 4317777
info@setpsantamarta.gov.co
Nit: 900.342.579-4

9.3. CONTROL DE ACCESO.

- En relación con el acceso a la información, a las instalaciones de procesamiento de datos y las diferentes plataformas de acceso, manejo, publicación y control de la información de la entidad se tienen planteados los siguientes procedimientos.

- **Procedimiento para ingreso seguro a los sistemas de información:** para el correcto ingreso a los sistemas de información, El Sistema Estratégico de Transporte Publico de Santa Marta S.A.S. SETP, tiene habilitado protocolos a través del servidor principal, mediante el cual son asignados los usuarios que se requieran y sus respectivas contraseñas, cada usuario cumple con los siguientes requisitos.

    1. Cada usuario es asignado según el área o dependencia que lo requiera.
    2. Cada usuario solo tiene acceso a la información de los procesos del área a la que pertenece o a la información que sea requerida con antelación y aprobada por el/la Ingeniero (a) a cargo del Área Tic de la entidad.
    3. El/la Ingeniero(a) encargado del Área Tic es quien tiene la completa autoridad para crear, modifica y/o eliminar los usuarios y/o contraseñas de acceso a los diferentes servicios de información de la entidad.

9.4. SEGURIDAD FÍSICA Y DEL ENTORNO.

- En relación con la prevención del acceso a áreas no autorizadas, el daño a la infraestructura, las instalaciones o de la información, el Sistema Estratégico de Transporte Publico de Santa Marta S.A.S. SETP mediante su área administrativa y su área Tic supervisa, protege, mantiene y vigila todos sus recursos; en estas actividades encaminadas al soporte de los procesos misionales de la institución, así como actividades encaminadas al cumplimiento de los objetivos estratégicos de la entidad:

    1. Se implementaron jornadas de capacitación en herramientas de ofimática a los empleados.
    2. Realizó jornadas de sensibilización de la política de Seguridad de la Información.

    9.4.1. PROCEDIMIENTO DE PROTECCIÓN DE ACTIVOS: mediante el área administrativa que es el área encargada de velar por la seguridad de los activos, el ingreso a áreas no autorizadas y la vigilancia en las instalaciones de la entidad, además es responsable de los mantenimientos y reemplazo de los elementos que componen la infraestructura de esta, para esto:

        1. Se realizaron con las dependencias de esta entidad capacitaciones buscando así la protección de la integridad de estos, promoviendo mediante campañas de sensibilización y concientización para que los contratistas que prestan sus servicios en la entidad cuiden y mantengan

Calle 24 No. 03 - 99 Ofi. 1202
Edificio Banco de Bogotá
Telefono: (+57) 5 4317777
info@setpsantamarta.gov.co
Nit: 900.342.579-4

en buen estado todas las áreas y todos los recursos que son dispuestos para el desarrollo de las actividades que aquí se realizan.

2. Mediante procesos documentados, aprobados y puestos en marcha el Sistema Estratégico de Transporte Publico de Santa Marta S.A.S. SETP, dispone de instrucciones y directrices para garantizar la integridad y la salvedad de cada uno de sus activos; estos procesos toman lista de cada activo, recurso o elemento que es entregado a los contratistas al momento de asignar cada puesto de trabajo.

    - **AGA-FO-20 Acta de Entrega de Puesto de Trabajo**
    - **AGA-FO-21 Acta de Paz y Salvo entrega de Puesto**

9.4.2. PROCEDIMIENTO DE RETIRO DE ACTIVOS: para el correcto retiro de los activos el Sistema Estratégico de Transporte Publico de Santa Marta S.A.S. SETP dispone de los siguientes procesos documentado aprobado e implementados donde se especifica y se indica el correcto proceso a realizar al momento de dar de baja y/o retirar un activo de la entidad.

1. **AGA-PD-04 Procedimiento para la Gestión de Activos Fijos.**
2. **AGA-FO-10 Asignación o Retiro de Activo Fijo V3.0.**
3. **AGA-FO-11 Control de Activos Fijos V4**

9.4.3. PROCEDIMIENTO DE MANTENIMIENTO DE EQUIPOS: el Sistema Estratégico de Transporte Publico de Santa Marta S.A.S. SETP dispone de procesos documentados, aprobados y puestos en marcha donde se especifican y se indican las directrices y procesos a realizar al momento de hacer mantenimiento preventivo y/o correctivo a los equipos informáticos, impresoras y activos que así lo requieran.

1. **AGA-FO-04 Programa de Mantenimiento V2.0**
2. **AGA-FO-05 Mantenimiento Preventivo y Correctivo V3.0**

9.5 SEGURIDAD DE LAS COMUNICACIONES: con el fin de garantizar la seguridad privacidad y correcto tráfico de la información que por medios digitales transita por la infraestructura tecnológica de la entidad, el Sistema Estratégico de Transporte Publico de Santa Marta S.A.S. SETP dispone de procesos puntuales que buscan el aseguramiento y la protección de la información a través de los diferentes servicios de comunicaciones de la organización.

9.5.1. PROCEDIMIENTO DE ASEGURAMIENTO DE SERVICIOS EN LA RED: mediante las políticas propias del servidor principal de la entidad se implementan las directrices y procedimientos para asegurar el trafico seguro y la protección de todos los servicios en la red interna de la entidad; el uso de antivirus representa un

Calle 24 No. 03 - 99 Ofi. 1202
Edificio Banco de Bogotá
Telefono: (+57) 5 4317777
info@setpsantamarta.gov.co
Nit: 900.342.579-4

plus al momento de asegurar la protección de los archivos, procesos y protocolos internos de la entidad con esto se activa la prevención y se evita el acceso de información de procedencia dudosa así mismo de amenazas de tipo informática tanto internas como externas, como adware, aplicaciones engañosas, ataques web entre otras.

9.5.1.1. Antivirus: Microsoft Defender para punto de conexión es una solución de seguridad de puntos de conexión integral y proporcionada en la nube que incluye administración y evaluación de vulnerabilidades basadas en riesgos, reducción de la superficie expuesta a ataques, protección de nueva generación basada en comportamientos con tecnología de la nube, detección y respuesta de puntos de conexión (EDR), investigación y corrección automáticas, servicios de búsqueda de amenazas administrados, API enriquecidas y administración de seguridad unificada.

9.5.1.2. Infraestructura tecnológica SETP Santa Marta.

INFRAESTRUCTURA TECNOLÓGICA SETP		
SETP SANTA MARTA	Rack de comunicaciones con 1 MIKROTIK 10/100/1000	Habilitado
	Servicios de red LAN 72 puntos de red	Habilitado
	Servicio de internet con canal dedicado de 200mb	Habilitado
	sistema de impresión por área o proceso.	Habilitado
	Servicio WIFI - Access Point de alta disponibilidad	Habilitado

Calle 24 No. 03 - 99 Ofi. 1202
Edificio Banco de Bogotá
Telefono: (+57) 5 4317777
info@setpsantamarta.gov.co
Nit: 900.342.579-4

10. TERMINOLOGÍAS:

Activo: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

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).

Adware: es un software, generalmente no deseado, que facilita el envío de contenido publicitario a un equipo.

Advertencia: Mensaje que comunica al usuario que una acción puede ocasionar u ocasionara la pérdida de datos del sistema del usuario.

Alerta: Notificación automática de un suceso o un error.

Amenaza: Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio.

Amenaza Externa: Amenaza que se origina fuera de una organización.

Amenaza Interna: Amenaza que se origina en una organización.

Antivirus: Antivirus es una categoría de software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Aplicaciones engañosas: Las aplicaciones engañosas son programas que intentan engañar a los usuarios informáticos para que emprendan nuevas acciones que normalmente están encaminadas a causar la descarga de malware adicional o para que los usuarios divulguen información personal confidencial. Un ejemplo es el software de seguridad fraudulento, que también se denomina scareware.

Arquitectura de Seguridad: Conjunto de principios que describe los servicios de seguridad que debe proporcionar un sistema para ajustarse a las necesidades de sus usuarios, los elementos de sistema necesarios para implementar tales servicios y los niveles de rendimiento que se necesitan en los elementos para hacer frente a las posibles amenazas.

Ataques multi-etapas: Un ataque en múltiples etapas es una infección que normalmente implica un ataque inicial, seguido por la instalación de una parte adicional de códigos maliciosos. Un ejemplo es un troyano que descarga e instala adware.

Calle 24 No. 03 - 99 Ofi. 1202
Edificio Banco de Bogotá
Telefono: (+57) 5 4317777
info@setpsantamarta.gov.co
Nit: 900.342.579-4

Ataques Web: Un ataque Web es un ataque que se comete contra una aplicación cliente y se origina desde un lugar en la Web, ya sea desde sitios legítimos atacados o sitios maliciosos que han sido creados para atacar intencionalmente a los usuarios de ésta.

Autenticación: Garantía de que una parte de una transacción informática no es falsa. La autenticación normalmente lleva consigo el uso de una contraseña, un certificado, un número de identificación personal u otra información que se pueda utilizar para validar la identidad en una red de equipos.

FIRMADO EN ORIGINAL

DIEGO ARMANDO LOPEZ ORTEGA

GERENTE

	Nombre	**Cargo**	**Firma**
Proyectó:	Carlos DeHorta Fernandez	Profesional Área Tic	
Revisó:	Shirley Correa Meza	Líder Área Tic	
Revisó:	Rafael del Toro Guzmán	Jefe control interno	
Los arriba firmantes declaramos que hemos revisado el presente documento y lo encontramos ajustado a las normas y demás disposiciones jurídicas y/o técnicas vigentes.			

Calle 24 No. 03 - 99 Ofi. 1202
Edificio Banco de Bogotá
Telefono: (+57) 5 4317777
info@setpsantamarta.gov.co
Nit: 900.342.579-4