



SANTA MARTA

El cambio es **imparable**

SETP

Sistema Estratégico de Transporte Público

Santa Marta

PLAN DE TRATAMIENTO DE RIESGOS 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



SANTA MARTA

El cambio es **imparable**

SETP

Sistema Estratégico de Transporte Público

Santa Marta

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

En convenio con



**Universidad Cooperativa
de Colombia**

Presentado por el practicante de ingeniería electrónica

ANDRES MAURICIO MEDINA LUNA

Programa de Ingeniería Electrónica.

Campus Ucc Santa Marta.

Vigencia de practicas septiembre 2021 a febrero 2022.

Revisado por

ING. SERGIO MARTINEZ – UCC

ING. CARLOS DEHORTA – SETP



2021.



Contenido

1. INTRODUCCIÓN	5
2. JUSTIFICACIÓN.....	6
3. OBJETIVOS	7
3.1. Objetivo general	7
3.2. Objetivos específicos.....	7
4. ALCANCE.....	8
5. NIVEL DE CUMPLIMIENTO.....	9
6. LINEAMIENTOS.....	11
7. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.....	12
8. MARCO NORMATIVO	13
9. SISTEMA ESTRATÉGICO DE TRANSPORTE PUBLICO DE SANTA MARTA S.A.S.	15
9.1. MISIÓN	15
9.2. VISIÓN.....	15
9.3. POLÍTICA DE CALIDAD.....	15
9.4. ESTRUCTURA ORGANIZACIONAL.....	16
10. AVANCES DE LA ENTIDAD EN EL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.....	17
11. METODOLOGÍA.....	19
11.1. Sensibilización institucional sobre política de seguridad de la información.....	20
11.2. Actualizar el inventario de activos de información.....	20
11.3. Elaborar procedimientos de seguridad de la información.....	20
11.4. Definir metodología para la gestión de los riesgos de seguridad y privacidad de la información	20
11.5. Definir herramienta del análisis de Riesgo de seguridad de la Información para la implementación del riesgo.....	20
12. Ejecutar Plan de riesgos de seguridad y privacidad de la información.....	21
12.1. Establecer estrategia.....	21
12.2. Establecer equipo de trabajo	21
12.3. Identificación de Riesgos.....	21
12.4. Análisis de Riesgos.....	22
12.5. Valoración de Riesgos.....	22



12.6. Evaluación de Controles	22
12.7. Socialización y Comunicación Políticas de Riesgos	22
12.8. Monitoreo y Revisión al Tratamiento de los Riesgos.....	22
13. Terminologías	23



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 plan de tratamiento de riesgos de seguridad y privacidad de la información, 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 plan pertenece al habilitador transversal de Seguridad y Privacidad de la Política de Gobierno Digital.

El Modelo de Seguridad y Privacidad de la Información toma como sustento el estándar NTC ISO 27001:2013 o Sistema de Gestión de Seguridad de la Información y los principios legales de la Ley 1712 de 2014; resaltando que tanto el estándar en mención, como el modelo, conciben obligatorio la identificación, valoración, tratamiento y gestión de los riesgos de seguridad, coincidiendo con los objetivos específicos de la política de Seguridad Digital, en cuanto al establecimiento de un marco institucional para la seguridad digital, consistente con un enfoque de gestión de riesgos, enfatizando en la implementación por parte del gobierno nacional a un modelo de gestión de riesgos de seguridad digital.

El plan de tratamiento de riesgos de seguridad y privacidad de la información 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 plan de tratamiento de riesgos de seguridad y privacidad de la información, 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 plan de tratamiento de riesgos 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 plan de tratamiento de riesgos 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, entendiéndose como premisa que la responsabilidad por la seguridad de la información es de todos y cada uno.



2. JUSTIFICACIÓN

En el marco del proceso de seguridad de la información es importante contar con políticas de seguridad ya que son ellas quienes guiarán 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.



3. OBJETIVOS

3.1. Objetivo general

Documentar, establecer, definir e implementar el plan de tratamiento de riesgos de seguridad y privacidad de la información, de acuerdo con lo establecido en el Modelo de Privacidad y Seguridad de la Información – MSPI, la Guía No. 7 – Guía de Gestión de Riesgos y la Guía No. 8 – Controles de Seguridad y Privacidad de la Información, para el Sistema Estratégico de Transporte Público de Santa Marta S.A.S.

3.2. Objetivos específicos

Establecer e implementar las políticas de seguridad de la información y conocer, asumir, gestionar y tratar los riesgos 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.



4. ALCANCE

Los requisitos, lineamientos y acciones establecidas en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información son aplicables de forma anualizada a los procesos estratégicos, misionales, de apoyo y de evaluación, por lo cual deberán ser conocidos y cumplidos por todos los funcionarios, contratistas, recursos de infraestructura tecnológica para el tratamiento de la información y terceras partes vinculadas a la Entidad que accedan a los activos de información, sistemas de información e instalaciones físicas del Instituto.

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.



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 para la implementación en el plan de tratamiento de riesgos de seguridad y privacidad de la información del Sistema Estratégico de Transporte público de Santa Marta SETP:

- El Sistema Estratégico de Transporte público 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 público 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 público 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 público de Santa Marta SETP protegerá su información de las amenazas originadas por parte del personal.
- El Sistema Estratégico de Transporte público de Santa Marta SETP protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- El Sistema Estratégico de Transporte público 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 público de Santa Marta SETP implementará control de acceso a la información, sistemas y recursos de red.
- El Sistema Estratégico de Transporte público 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 público 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.
- El Sistema Estratégico de Transporte público 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 público 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 Plan 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.



6. LINEAMIENTOS

El Sistema Estratégico de Transporte público 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



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 artículo 2º, 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 artículo 2.2.9.1.1.1. 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 público 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.

**8. 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 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.



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

9.1. 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.

9.2. 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.

9.3. 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.



9.4. ESTRUCTURA ORGANIZACIONAL



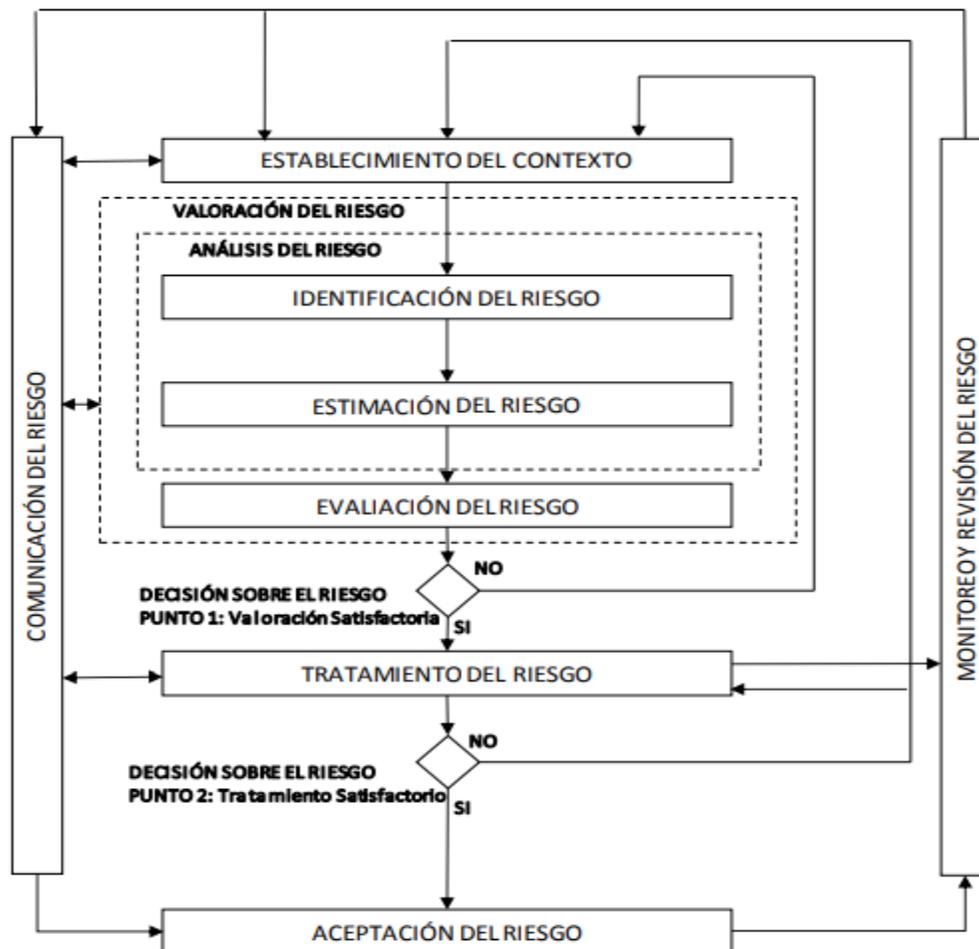


10. AVANCES DE LA ENTIDAD EN EL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

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.

El proceso de gestión de riesgo en la seguridad de la información consta de la definición del enfoque organizacional para la valoración del riesgo y su posterior tratamiento.



Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf



SANTA MARTA

El cambio es **imparable**

SETP

Sistema Estratégico de Transporte Público

Santa Marta

El proceso de gestión del riesgo en la seguridad de la información puede ser iterativo para las actividades de valoración del riesgo y/o el tratamiento de este. Un enfoque iterativo para realizar la valoración del riesgo puede incrementar la profundidad y el detalle de la valoración en cada iteración.

El contexto se establece como primera medida, luego se realiza la valoración del riesgo y si esta suministra información suficiente para determinar de manera eficaz las acciones que se necesitan para modificar los riesgos a un nivel aceptable entonces la labor está terminada y sigue el tratamiento del riesgo. Si la información no es suficiente, se llevará a cabo otra iteración de la valoración del riesgo con un contexto revisado.



11. METODOLOGÍA

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016):

GESTIÓN	ACTIVIDAD	FECHA DE INICIO	FECHA DE FIN
FASES PARA LA GESTIÓN DE RIESGOS	Sensibilización institucional sobre política de seguridad de la información		
	Actualización el inventario de activos de información		
	Elaboración de procedimiento gestión de Riesgos de seguridad de la información		
	Definir metodología para la gestión de los riesgos de seguridad y privacidad de la información		
	Definir herramienta del análisis de Riesgo de seguridad de la Información para la implementación del riesgo.		
	Ejecución Plan de riesgos de seguridad y privacidad de la información		



11.1. Sensibilización institucional sobre política de seguridad de la información

Realizar la divulgación de manera apropiada de las reglas de comportamiento adecuadas para el uso de los sistemas y la información, que generalmente están plasmadas en las políticas y procedimientos de seguridad de la información que la Entidad, requiere que sean cumplidos por parte de todos los usuarios del sistema. Cualquier incumplimiento a las políticas, debe llevar a la imposición de una sanción, siempre y cuando el usuario haya sido adecuadamente capacitado e informado sobre todo el contenido de seguridad correspondiente a su rol y responsabilidades dentro de la Entidad.

11.2. Actualizar el inventario de activos de información

El SETP SANTA MARTA S.A.S, desarrollará una metodología para la identificación, clasificación, mantenimiento y actualización del inventario de activos de información, entendiéndose que hace parte de la debida diligencia que a nivel estratégico se ha definido en el Modelo de Seguridad y Privacidad de la Información. En concordancia, el inventario de activos de la información se registra en la matriz definida por la Entidad incluyendo la información pertinente respecto a los propietarios, custodios y usuarios de los activos de información identificados en cada vigencia.

11.3. Elaborar procedimientos de seguridad de la información

Se realizará la revisión de los actuales procedimientos, con el objeto de identificar las necesidades de documentación y/o actualización de procedimientos en el marco de la implementación del Modelo de Seguridad y Privacidad de la información. El propósito de esta actividad se fundamenta en desarrollar y formalizar procedimientos que permitan gestionar la seguridad y privacidad de la información en todos los procesos de la Entidad.

11.4. Definir metodología para la gestión de los riesgos de seguridad y privacidad de la información

El SETP SANTA MARTA S.A.S debe definir una metodología de gestión del riesgo enfocada a procesos, que le permita identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que estén expuestos los activos, así, como la declaración de aplicabilidad. Para conseguir una integración adecuada entre el MSPI y la guía de gestión del riesgo emitida por el DAFP respecto a este procedimiento, se recomienda emplear los criterios de evaluación (impacto y probabilidad) y niveles de riesgo emitidos por esta entidad.

11.5. Definir herramienta del análisis de Riesgo de seguridad de la Información para la implementación del riesgo

El SETP SANTA MARTA S.A.S, debe definir la herramienta de gestión del riesgo enfocada a procesos, que le permite localizar y visualizar los recursos de la entidad que se encuentran más en peligro de sufrir daño por algún impacto negativo, para posteriormente ser capaz de tomar decisiones y medidas adecuadas para la reducción de amenazas.

**12. Ejecutar Plan de riesgos de seguridad y privacidad de la información**

FASE	ACTIVIDAD PRINCIPAL	FECHA DE INICIO	FECHA DE FIN
1	Estrategia		
2	Establecer el equipo de trabajo		
3	Análisis de riesgos		
4	Valoración de riesgos		
5	Evaluación de controles		
6	Socialización y comunicación de las políticas de riesgo		
7	Monitoreo y revisión al tratamiento de riesgos		

12.1. Establecer estrategia

Definir el contexto estratégico contribuye al control de la entidad frente a la exposición al riesgo, ya que permite conocer las situaciones generadoras de riesgos, impidiendo con ello que la entidad actúe en dirección contraria a sus propósitos institucionales.

Para la definición del contexto estratégico, es fundamental tener claridad de la misión institucional, sus objetivos y tener una visión sistémica de la gestión, de manera que se perciba la administración del riesgo como una herramienta gerencial y no como algo aislado del accionar administrativo. Por lo tanto, el diseño de esta primera etapa se fundamenta en la identificación de los factores internos (debilidades) y externos (amenazas) que puedan generar riesgos que afecten el cumplimiento de los objetivos institucionales.

Esta etapa es orientadora, se centra en determinar las amenazas y debilidades de la entidad; es la base para la identificación del riesgo, dado que de su análisis suministrará la información sobre las CAUSAS del riesgo.

12.2. Establecer equipo de trabajo

Tomando como referente lo anterior, se debe atender y seguir las siguientes orientaciones:

- Cada responsable de proceso del EI SETP SANTA MARTA S.A.S, deberá identificar a los funcionarios que por su competencia pueden ser considerados claves dentro de cada una de las dependencias que participan 9 en el proceso, serán factores de selección de estos, el conocimiento y nivel de toma de decisiones sobre el proceso.
- Los funcionarios seleccionados deberán ser convocados a una reunión inicial, en donde se presentará el propósito de esta actividad.

12.3. Identificación de Riesgos

Es la etapa que permite conocer los eventos potenciales, estén o no bajo el control del SETP SANTA MARTA S.A.S, que ponen en riesgo el logro de su misión, estableciendo las causas y consecuencias de la ocurrencia del riesgo.



12.4. Análisis de Riesgos

El análisis del riesgo busca establecer la probabilidad de ocurrencia de este y sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo.

Se han establecido dos aspectos para tener en cuenta en el análisis de los riesgos identificados, probabilidad e impacto. Por la primera se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de Frecuencia, si se ha materializado, o de Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado. Por Impacto se entiende las consecuencias que puede ocasionar a la Entidad la materialización del riesgo.

12.5. Valoración de Riesgos

Es el producto de confrontar la evaluación del riesgo y los controles (preventivos o correctivos) de los procesos.

La valoración del riesgo se realiza en tres momentos: primero, identificando los controles (preventivos o correctivos) que pueden disminuir la probabilidad de ocurrencia o el impacto del riesgo; luego, se deben evaluar los controles, y finalmente, con base en los resultados de la evaluación de los controles, determinar la evaluación del riesgo residual y definir la opción de manejo del riesgo.

Lo anterior de acuerdo con los formatos Identificación y evaluación de controles y Valoración del riesgo.

12.6. Evaluación de Controles

Permite determinar en qué medida los controles identificados están aportando para disminuir los niveles de probabilidad e impacto del riesgo. Se evalúan verificando su documentación, aplicación y efectividad.

12.7. Socialización y Comunicación Políticas de Riesgos

Actividad mediante el cual se da conocer a funcionarios, Contratistas y terceros de la Entidad las políticas de tratamiento de riesgos de Seguridad y Privacidad de la Información, mediante charlas y el uso de las herramientas de comunicaciones disponibles en la Entidad.

12.8. Monitoreo y Revisión al Tratamiento de los Riesgos

El monitoreo y revisión debe asegurar que las acciones establecidas en los mapas de riesgo se están llevando a cabo y evaluar la eficacia en su implementación, adelantando revisiones sobre la marcha para evidenciar todas aquellas situaciones o factores que pueden influir en la aplicación de acciones preventivas.



13. Terminologías

Los siguientes términos son utilizados en el contexto de la gestión de la seguridad de la información y aplican para todas sus fases y momentos, incluyendo la gestión de riesgos.

Administración del riesgo: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado. Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27001)

Amenaza: Es la causa potencial de una situación de incidente y no deseada por la organización

Causa: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

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

Consecuencia: Resultado de un evento que afecta los objetivos.

Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.

Control: Medida que modifica el riesgo. 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.

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.



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

Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

Estimación del riesgo. Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

Evitación del riesgo. Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

Identificación del riesgo. Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

Integridad: Propiedad de la información relativa a su exactitud y completitud. Impacto. Cambio adverso en el nivel de los objetivos del negocio logrados.

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

Matriz de riesgos: Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

Monitoreo: Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de control o las diferentes auditorías de los sistemas integrados de gestión.



Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos inaceptables en el marco de la seguridad de la información e implantar los controles necesarios para proteger la misma.

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.

Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

Proceso: Conjunto de actividades interrelacionadas que apuntan a un objetivo o que interactúan para transformar una entrada en salida.

Riesgo en la seguridad de la información: 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.

Riesgo Inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

Reducción del riesgo. Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

Retención del riesgo: Aceptación de la pérdida o ganancia proveniente de un riesgo particular.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

Seguimiento: Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación de los controles de seguridad de la información sobre cada uno de los procesos.

Tratamiento del Riesgo: Proceso para modificar el riesgo (Icontec Internacional, 2011).

Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

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



SANTA MARTA

El cambio es **imparable**

SETP

Sistema Estratégico de Transporte Público

Santa Marta

DIEGO ARMANDO LOPEZ ORTEGA

GERENTE

	Nombre	Cargo	Firma
Proyectó:	Andrés Medina Luna	Practicante Área Tic	
Revisó:	Carlos DeHorta Fernández	Profesional Área Tic	
Revisó:	Xaira Mahecha Ceballos	Coordinador(a) Área administrativa	
Revisó:	Rafael Del Toro Guzmán	Jefe de 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.