

MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

Versión 3.0

SETP

Sistema Estratégico de Transporte Público

Santa Marta



**ALCALDÍA DE
SANTA MARTA**
Distrito Turístico,
Cultural e Histórico

2020

Contenido

1.	INTRODUCCIÓN	2
2.	OBJETIVO	2
3.	ALCANCE	2
4.	RESPONSABLE	2
5.	GENERALIDADES	3
	GLOSARIO DE TERMINOS	3
6.	ELEMENTOS INFORMÁTICOS	6
	Claves De Acceso	6
	Derechos de Propiedad	6
	Licencias de Uso	6
	Préstamo de Equipos y Elementos Informáticos	7
	Mantenimientos Preventivos y Correctivos	7
	Seguridad en Red Interna	7
	Configuración e Instalación de los Servidores	8
	Periféricos Y Otros Elementos Informáticos	8
	Inventario de Equipos	8
7.	MARCO LEGAL	8
8.	BITÁCORA DE ACTUALIZACIÓN	9

	SISTEMA DE GESTIÓN INTEGRAL DE LA CALIDAD	Código: AGA-MA-01
	MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA	Versión: 3.0
		Fecha: 30 de Julio 2020
		Página 2 de 10

1. INTRODUCCIÓN

Las Políticas de Seguridad Informática son las directrices de índole técnica y de organización que se llevan adelante respecto de un determinado sistema de computación a fin de proteger y resguardar su funcionamiento y la información en él contenida. El principio y final de toda red es el usuario, esto hace que las políticas de seguridad deban, principalmente, enfocarse a los usuarios, indican a las personas cómo actuar frente a los recursos informáticos de la Entidad.

Actualmente el Sistema Estratégico de Transporte Público de Santa Marta S.A.S. cuenta con una plataforma tecnológica que almacena, procesa y transmite la información institucional, incluye equipos de cómputo de usuario y un servidor que se interconectan por medio de una red de datos, así como servicio de internet y correo electrónico institucional. Siendo la información institucional un activo valioso para la Entidad, se hace necesario no solo la implementación de herramientas de hardware y software de seguridad, sino involucrar al personal para proteger su integridad y confidencialidad.

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

2. OBJETIVO

Garantizar el buen uso de los equipos informáticos, así como adoptar las medidas necesarias para salvaguardar la información, garantizando su confiabilidad, integridad y disponibilidad; y así crear conciencia en los funcionarios y contratistas sobre la necesidad de proteger los equipos, el software e información digital del **Sistema Estratégico de Transporte Público S.A.S SETP**

3. ALCANCE

Las políticas de seguridad informática, están orientadas a toda la información almacenada, procesada y transmitida en medios electrónicos, estas políticas deben ser conocidas y cumplidas tanto por funcionarios de planta como por los contratistas que apoyan la gestión y por los terceros o grupos de interés que utilicen la información generada y custodiada. El contenido del presente manual aplica para todos los elementos informáticos del **Sistema Estratégico de Transporte Público S.A.S SETP**.

4. RESPONSABLE

El responsable del cumplimiento del presente manual es el Coordinador del proceso Administrativo del **Sistema Estratégico de Transporte Público S.A.S SETP**.

	SISTEMA DE GESTIÓN INTEGRAL DE LA CALIDAD	Código: AGA-MA-01
	MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA	Versión: 3.0
		Fecha: 30 de Julio 2020
		Página 3 de 10

5. GENERALIDADES

La seguridad informática, es un proceso donde se deben evaluar y administrar los riesgos apoyados en políticas y directrices para lograr establecer medidas y patrones técnicos de administración y organización con el ánimo de propender por la seguridad que cubran las necesidades del **Sistema Estratégico de Transporte Público S.A.S SETP** en materia de seguridad.

Toda persona que utilice los servicios que ofrece la red, deber conocer y aceptar el reglamento vigente sobre su uso, el desconocimiento del mismo, no exonera de responsabilidad al usuario, ante cualquier eventualidad que involucre la seguridad de la información o de la red institucional.

GLOSARIO DE TERMINOS

- **Acceso físico:** La posibilidad de acceder físicamente a un computador o dispositivos, manipularlo tanto interna como externamente.
- **Acceso lógico:** Ingresar al sistema operativo o aplicaciones de los equipos y operarlos, ya sea directamente, a través de la red de datos interna o de Internet.
- **Activos de Información:** Toda aquella información que la Entidad considera importante o fundamental para sus procesos, puede ser ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, aplicaciones, software del sistema, etc.
- **Aplicaciones o aplicativos:** Son herramientas informáticas que permiten a los usuarios comunicarse, realizar trámites, entretenerse, orientarse, aprender, trabajar, informarse y realizar una serie de tareas de manera práctica y desde distintos tipos de terminales como computadores tabletas o celulares.
- **Cableado estructurado:** Cableado de un edificio o una serie de edificios que permite interconectar equipos activos, de diferentes o igual tecnología permitiendo la integración de los diferentes servicios que dependen del tendido de cables como datos, telefonía, control, etc.
- **Cifrado de datos:** Proceso por el que una información legible se transforma mediante un algoritmo (llamado cifra) en información ilegible, llamada criptograma o secreto. Esta información ilegible se puede enviar a un destinatario con muchos menos riesgos de ser leída por terceras partes.
- **Configuración Lógica:** conjunto de datos que determina el valor de algunas variables de un programa o de un sistema operativo, elegir entre distintas opciones con el fin de obtener un programa o sistema informático personalizado o para poder ejecutar dicho programa correctamente.

	SISTEMA DE GESTIÓN INTEGRAL DE LA CALIDAD MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA	Código: AGA-MA-01
		Versión: 3.0
		Fecha: 30 de Julio 2020
		Página 4 de 10

- **Copia de respaldo o backup:** Operación que consiste en duplicar y asegurar datos e información contenida en un sistema informático. Es una copia de seguridad.
- **Contenido:** Todos los tipos de información o datos que se divulguen a través de los diferentes servicios informáticos, entre los que se encuentran: textos, imágenes, video, diseños, software, animaciones, etc.
- **Contraseñas:** Clave criptográfica utilizada para la autenticación de usuario y que se utiliza para acceder a los recursos informáticos.
- **Correo electrónico institucional:** Servicio que permite el intercambio de mensajes a través de sistemas de comunicación electrónicos, que se encuentra alojado en un hosting de propiedad de la Entidad.
- **Cuenta de acceso:** Colección de información que permite a un usuario identificarse en un sistema informático o servicio, mediante un usuario y una contraseña, para que pueda obtener seguridad, acceso al sistema, administración de recursos, etc.
- **Dispositivos/Periféricos:** Aparatos auxiliares e independientes conectados al computador o la red.
- **Dominio:** Es un conjunto de computadores, conectados en una red, que confían a uno de los equipos de dicha red la administración de los usuarios y los privilegios que cada uno de los usuarios tiene en la red.
- **Espacio en disco duro:** Capacidad de almacenamiento de datos en la unidad de disco duro.
- **Herramientas ofimáticas:** Conjunto de aplicaciones informáticas que se utilizan en funciones de oficina para optimizar, automatizar y mejorar los procedimientos o tareas relacionadas. En la Contraloría Municipal de Tuluá se hace uso de la Herramienta Microsoft Office.
- **Información confidencial:** Se trata de una propiedad de la información que pretende garantizar el acceso sólo a personas autorizadas.
- **Información/Documento electrónico:** Es la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares. Se pueden clasificar por su forma y formato en documentos ofimáticos, cartográficos, correos electrónicos, imágenes, videos, audio, mensajes de datos de redes sociales, formularios electrónicos, bases de datos, entre otros.
- **Integridad:** propiedad de salvaguardar la exactitud y estado completo de los activos.
- **Licencia de uso:** Contrato entre el licenciante (autor/titular de los derechos de explotación/distribuidor) y el licenciario (usuario consumidor/usuario profesional o empresa) del programa informático, para utilizar el software cumpliendo una serie de términos y condiciones establecidas dentro de sus cláusulas, es decir, es un conjunto de permisos que un desarrollador le puede otorgar a un usuario en los que tiene la posibilidad de distribuir, usar y/o modificar el producto bajo una licencia determinada.

	SISTEMA DE GESTIÓN INTEGRAL DE LA CALIDAD	Código: AGA-MA-01
	MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA	Versión: 3.0
		Fecha: 30 de Julio 2020
		Página 5 de 10

- **Mantenimiento lógico preventivo:** Es el trabajo realizado en el disco duro del equipo de cómputo, con la finalidad de mejorar el rendimiento general del sistema operativo.
- **Mantenimiento físico preventivo:** Actividad de limpieza de elementos como polvo, residuos de alimentos y otro tipo de partículas que debe realizarse sobre el equipo de cómputo, con el propósito de posibilitar que su correcto funcionamiento sea más prolongado en el tiempo.
- **Medios de almacenamiento extraíble:** Son aquellos soportes de almacenamiento diseñados para ser extraídos del computador sin tener que apagarlo. Por ejemplo, memorias USB, discos duros externos, discos ópticos (CD, DVD), tarjetas de memoria (SD, CompactFlash, Memory Stick).
- **Plataforma web:** Sistema que permite la ejecución de diversas aplicaciones bajo un mismo entorno, dando a los usuarios la posibilidad de acceder a ellas a través de Internet.
- **Propiedad intelectual:** Se relaciona con las creaciones de la mente como invenciones, obras literarias y artísticas, así como símbolos, nombres e imágenes utilizados en el comercio. Es el conjunto de derechos que corresponden a los autores y a otros titulares.
- **Recurso informático:** Todos aquellos componentes de Hardware y programas (Software) que son necesarios para el buen funcionamiento de un computador o un sistema de gestión de la información. Los recursos informáticos incluyen medios para entrada, procesamiento, producción, comunicación y almacenamiento.
- **Red de datos:** Es un conjunto de ordenadores que están conectados entre sí, y comparten recursos, información, y servicios.
- **Riesgo:** Posibilidad de que se produzca un contratiempo o una desgracia, las vulnerabilidades y amenazas a que se encuentran expuestos los activos de información.
- **Servicio informático:** Conjunto de actividades asociadas al manejo automatizado de la información que satisfacen las necesidades de los usuarios.
- **Servidor:** Se entiende como el software que configura un PC como servidor para facilitar el acceso a la red y sus recursos. Ofrece a los clientes la posibilidad de compartir datos, información y recursos de hardware y software. Los clientes usualmente se conectan al servidor a través de la red pero también pueden acceder a él a través de la computadora donde está funcionando.
- **Sistema de información:** Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.

	SISTEMA DE GESTIÓN INTEGRAL DE LA CALIDAD	Código: AGA-MA-01
	MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA	Versión: 3.0
		Fecha: 30 de Julio 2020
		Página 6 de 10

- **Software antivirus:** Son programas que buscan prevenir, detectar y eliminar virus informáticos. En los últimos años, y debido a la expansión de Internet, los nuevos navegadores y el uso de ingeniería social, los antivirus han evolucionado para detectar varios tipos de software fraudulento, también conocidos como malware.
- **Software de gestión:** Son todos aquellos programas utilizados a nivel empresarial, que por su definición genera acción de emprender algo y por su aplicación persigue fines lucrativo y no lucrativo. También es un software que permite gestionar todos los procesos de un negocio o de una empresa en forma integrada. Por lo general está compuesto por modulo cruzado del proceso del negocio.
- **Software malicioso:** Es aquel que se ha diseñado específicamente para dañar un computador, este tipo de software realiza acciones maliciosas como instalar software sin el consentimiento del usuario o virus.

6. ELEMENTOS INFORMÁTICOS

Claves De Acceso

Todos los equipos deben contar con una contraseña, esta será asignada por el ingeniero de sistemas o en su defecto el coordinador administrativo de la entidad. El manejo de las claves implica responsabilidades sobre su uso, por lo tanto, siempre que ingrese o digite la clave de acceso en el sistema tenga especial cuidado de que no hay sido observada por otras personas.

Derechos de Propiedad

Los programas, aplicaciones y ejecutables desarrollados o adquiridos por el Sistema Estratégico de Transporte Publico SETP Santa Marta S.A.S, incluyendo su documentación, no deben ser reproducidos, publicados, transmitidos o copiados por los usuarios. Todo funcionario o contratista que se retire del SETP Santa Marta S.A.S debe presentar paz y salvo de entrega de equipos y de todas las cuentas (claves) que posea para el ingreso a los diferentes ambientes donde esté autorizado. Esta información debe ser presentada con la liquidación en el caso de los contratistas o en el acta de entrega del puesto en el caso de los funcionarios.

Licencias de Uso

Todos los productos de Software que se utilicen deberán contar con su factura y licencia de uso respectiva; por lo que se promoverá la regularización o eliminación de los productos que no cuenten con el debido licenciamiento. El área de sistemas promoverá y propiciará que la adquisición de software de dominio público provenga de sitios oficiales y seguros.

	SISTEMA DE GESTIÓN INTEGRAL DE LA CALIDAD	Código: AGA-MA-01
	MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA	Versión: 3.0
		Fecha: 30 de Julio 2020
		Página 7 de 10

Préstamo de Equipos y Elementos Informáticos

Las computadoras personales, las computadoras portátiles, video beams y cualquier activo de tecnología de información, podrán ser retirados de las instalaciones del Sistema Estratégico de Transporte Publico SETP Santa Marta S.A.S. únicamente con la autorización de salida del Coordinador Administrativo dejando registro en el **AGA-FO-13 Formato para Préstamo de Elementos**.

Mantenimientos Preventivos y Correctivos

La entidad cuenta con un **AGAL-PD-01 Procedimiento para la Realización de Mantenimiento Preventivos y Correctivos** que tiene por objeto generar el plan de mantenimiento preventivo y actividades necesarias para los mantenimientos correctivos de los equipos de cómputo el Sistema Estratégico de Transporte Publico SETP Santa Marta S.A.S, que garanticen la continuidad de las operaciones de la Entidad.

Para solicitar una revisión por daño o falla al equipo, se solicita mantenimiento correctivo a través del **correo electrónico institucional** describiendo el daño y datos del usuario del mismo, haciendo entrega de este al Ingeniero de Sistemas. O a través de un reporte por la Mesa de ayuda de la entidad la cual se encuentra divulgada a todos los funcionarios y contratistas de la entidad.

Seguridad en Red Interna

Las redes tienen como propósito principal servir en la 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

	SISTEMA DE GESTIÓN INTEGRAL DE LA CALIDAD	Código: AGA-MA-01
	MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA	Versión: 3.0
		Fecha: 30 de Julio 2020
		Página 8 de 10

Configuración e Instalación de los Servidores

El área de sistemas tiene la responsabilidad de verificar la instalación, configuración e implementación de seguridad, en los servidores conectados a la red. Durante la configuración de los servidores se deben genera las normas para el uso de los recursos del sistema y de la red, principalmente la restricción de directorios, permisos y programas a ser ejecutados por los usuarios.

Periféricos Y Otros Elementos Informáticos

Los periféricos y en general, todos los elementos accesorios de los equipos, no deben ser removidos ni intercambiados sin la autorización del coordinador administrativo o en su defecto, el Ing. De Sistemas de la entidad. En caso de mal funcionamiento, debe reportarse al **correo electrónico institucional** del Ing. De Sistemas, para proceder a su verificación y de ser necesario, el reemplazo del elemento averiado.

Inventario de Equipos

El **AGA-FO-10 Formato de Asignación o Retiro de Bienes de Inventario** será diligenciado para la asignación de bienes de inventario (Equipos de Cómputo) a funcionarios y contratistas del **SETP Santa Marta S.A.S.** Para conocer o verificar las asignaciones y No. De equipos disponibles en la entidad, debe verificarse el **AGAL-FO-11 Formato de Control de Activos Fijos**.

7. MARCO LEGAL

Tipo de Norma	Entidad que Emite	No. De Identificación	Fecha de Expedición	Descripción de artículos, capítulos o partes de la Norma que aplican al documento
Decreto	Presidencia de la República	1360	1989	Por el cual se reglamenta la inscripción del soporte lógico (software) en el Registro Nacional del Derecho de Autor
Ley	Congreso de la República de Colombia	87	1993	"Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones".
Ley	Congreso de la República de Colombia	527	1997	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones
Ley	Congreso de la República de Colombia	1273	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

	SISTEMA DE GESTIÓN INTEGRAL DE LA CALIDAD	Código: AGA-MA-01
	MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA	Versión: 3.0
		Fecha: 30 de Julio 2020
		Página 9 de 10

				información y las comunicaciones, entre otras disposiciones.
Ley	Congreso de la República de Colombia	594	2000	Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.
Decreto	Presidencia de la República	2609	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	Presidencia de la República	2573	2014	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.

8. BITÁCORA DE ACTUALIZACIÓN

Versión	Fecha	Ítem Modificado	Descripción
2.0	25/09/2017	5. Elementos Informáticos	En la descripción de los mantenimientos correctivos y preventivos y periféricos se eliminó el registro AGAL-FO-06 Formato Reporte de Daños de Equipos de Cómputo . Ya que las solicitudes se realizan de manera digital por correo electrónico institucional.
3.0	30/07/2020	1. Introducción	Se incorpora Introducción al Manual, donde especifica que las políticas son las directrices que indican a las personas cómo actuar frente a los recursos informáticos de la Entidad, con el fin de proteger su integridad y confidencialidad.
3.0	30/07/2020	2. Alcance	Se amplia y especifica a quien va orientado el Manual de Políticas de Seguridad Informática.
3.0	30/07/2020	Glosario de Términos	Se agregan definiciones con el fin de ampliar el Glosario de Términos como apoyo a éste Manual.

3.0	30/07/2020	7. Marco Legal	Se incluyen Ley 87 de 1993, Ley 527 de 1997, Ley 1273 de 2009, Ley 594 de 2000, Decreto 2609 de 2012 y Decreto 2573 de 2014.
-----	------------	----------------	--

	ELABORADO POR:	REVISADO POR:	APROBADO POR:
Nombre	Shirley Correa Meza	Xaira Mahecha Ceballos	Diego López Ortega
Cargo	Ingeniera De Sistemas	Gestión Administrativa	Gerente
Fecha	27/07/20	30/07/20	31/07/20
Firma			