



RESOLUCIÓN DE GERENCIA No. 016

22 OCT 2025

POR LA CUAL SE ACTUALIZAN, SE ADOPTAN MANUALES, POLITICAS, CODIGOS Y PLANES PARA LA IMPLEMENTACION DEL MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN "MIPG" EN LA PLANTA DE TRATAMIENTO VILLASANTANA SOCIEDAD LIMITADA.

La Gerente (e) de la Planta De Tratamiento Villasantana Sociedad Limitada Empresa Industrial y Comercial del Estado (EICE) constituida por escritura pública número 6 del 04 de enero de 2005 otorgada por asamblea de constitución de Dosquebradas, registrado en esta cámara de comercio bajo el número 1004150 del libro ix del registro mercantil el 13 de enero de 2005, se inscribe: la constitución de persona jurídica denominada Planta De Tratamiento Villasantana S.A E.S.P.

Que por escritura pública número 1505 del 31 de mayo de 2010 otorgada por asamblea general de Dosquebradas, registrado en esta cámara de comercio bajo el número 1016804 del libro IX del registro mercantil el 28 de julio de 2010, la persona jurídica cambio su nombre de Planta De Tratamiento Villasantana S.A. E.S.P por Planta De Tratamiento Villasantana Sociedad Limitada.

Que por escritura pública número 2021 del 26 de julio de 2010 de la notaría única de Dosquebradas, inscrita en esta entidad el 28 de julio de 2010, en el libro IX bajo el número 1016805, se aclara la escritura número 1505 del 31 de mayo de 2010 de la transformación cuyo objeto social de la Planta de Tratamiento Villasantana es el arrendamiento de infraestructura para la producción y venta de agua tratada en bloque; así mismo podrá prestar servicios de análisis de laboratorio para medición de potabilización de agua y servicios complementarios de asesoría en procesos de potabilización de agua y en ejercicio de sus facultades constitucionales y legales.

CONSIDERANDO:

1. Que el Decreto 1083 de 2015 reglamenta todo lo relacionado con el Sistema de Gestión y actualiza el Modelo Integrado de Planeación y Gestión, de tal manera que permita el fortalecimiento de los mecanismos, métodos y procedimientos de gestión y control al interior de los organismos y entidades del Estado; y el artículo 2.2.22.3.1 del mismo Decreto adopta la versión actualizada del Modelo Integrado de Planeación y Gestión – MIPG con el fin de lograr el funcionamiento del Sistema de Gestión y su articulación con el Sistema de Control Interno.

018 22 OCT 2025

2. Que mediante el Decreto 1499 de 2017 se implementó el Modelo Integrado de planeación y Gestión MIPG, el cual integra los sistemas que se hayan adoptado en las entidades públicas, el cual busca dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades públicas.
3. Que dentro de la estructura de la operación MIPG se encuentra con 7 dimensiones, las cuales incluye: Talento Humano, Direccionamiento Estratégico y de Planeación, Gestión con Valor para el Resultado, Evaluación de Resultados, Información y Comunicación, Gestión del Conocimiento y la Innovación y Control Interno que busca dar cumplimiento a las metas institucionales de las entidades públicas con la elaboración y adopción de manuales, programas, políticas, planes, código, matrices, formatos para la implementación del Modelo Integrado de Planeación y Gestión en la Planta de Tratamiento Villasantana Sociedad Limitada.
4. Que mediante la Resolución 0000025 del 27 diciembre de 2023 "Por la cual se reglamenta el modelo integrado de planeación y gestión y se definen lineamientos para su operación en la organización y se integra el comité institucional de gestión y desempeño" de la Planta de Tratamiento de Villasantana Sociedad Limitada.
5. Por medio de la resolución No. 006 de 2021 se adoptó el código de integridad del servicio público del servicio público del Departamento Administrativo de la Función Pública en la Planta de Tratamiento Villasantana Sociedad Limitada.

Con fundamento en las anteriores consideraciones,

RESUELVE:

Artículo 1. Actualizar el Código de integridad de la Planta de Tratamiento Villasantana Sociedad Limitada.

Artículo 2. Adoptar el Manual de evaluación, seguimiento y auditoría interna de gestión de la Planta de Tratamiento Villasantana Sociedad Limitada.

Artículo 3. Adoptar la Política de Gobierno Digital para la Planta de Tratamiento Villasantana Sociedad Limitada y el Procedimiento de PQRS.

Artículo 4. Adoptar los siguientes planes y procedimientos de la Planta de Tratamiento Villasantana Sociedad Limitada.; así:

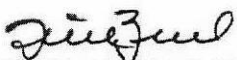
1. Plan anticorrupción y de atención al ciudadano
2. Plan de bienestar social e incentivos
3. Plan estratégico de talento humano (PETH)

4. Plan institucional de gestión ambiental
5. Plan Institucional de capacitación
6. Plan de participación ciudadana
7. Plan estratégico de tecnología de la información y las comunicaciones (PETIC)
8. Plan estratégico de riesgo de seguridad y privacidad de la información
9. Plan de seguridad y privacidad de la información
10. Plan de vacantes y previsión de talento humano
11. PINAR

Artículo 5: La presente resolución rige a partir de la fecha de la expedición.

COMUNÍQUESE Y CÚMPLASE

Dada en Pereira, a los 22 OCT 2025


MARTHA LUCIA SARRIA COLON
Gerente (E)


Reviso: Olga Cecilia Arenas Forestiery
Asesora Jurídica


Reviso: Paula Andrea Benjumea Ramirez
Apoyo Control Interno


Elaboró: Cesar Echeverri Álvarez.
Contratista MIPG

	PLANTA DE TRATAMIENTO VILLASANTANA SOCIEDAD LIMITADA		Fecha de emisión 04-08-2025
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		Versión: 1
			Página: 1 de 18

Tabla de Contenido

Contenido

1. Introducción	2
2. Objetivos.....	2
3. Principios y valores.....	3
4. Alcance	4
5. Política	4
6. Marco Normativo y metodológico	4
7. Estrategias de la Implementación.....	5
8. Glosario	6
9. Conceptos básicos	10
10. Lineamientos del plan.....	11
12. Implementación del Plan.....	14
13. Responsable y actualización del Plan	16
14. Seguimiento.....	16
15. Indicadores	16
16. Comité de seguridad digital	16
17. Bibliografía.....	17



1. Introducción

El Plan de Seguridad y Privacidad de la Información cuyo objetivo es darle cumplimiento al Modelo de Seguridad y Privacidad de la Información (MSPI) definida por el Ministerio de Tecnologías de la Información y Comunicaciones en adelante MINTIC, el cual orienta a las entidades a la preservación de la confidencialidad, integridad y disponibilidad de la información, además permite fijar los criterios para proteger la privacidad de la información y los datos.

2. Objetivos

Objetivo General

Establecer acciones y las actividades contempladas en el Modelo de Seguridad y Privacidad de la Información – MSPI de MinTIC, buscando fortalecer la integridad, confidencialidad y disponibilidad de los activos de la información de la entidad.

Objetivos Específicos:

- Establecer acciones encaminadas a la implementación del Plan de Seguridad y Privacidad de la Información.
- Concientizar a los servidores públicos y contratistas de la entidad de la importancia de cumplir los lineamientos establecidos en el plan de seguridad y privacidad de la información.
- Facilitar la gestión de los riesgos de seguridad y privacidad de la información y de seguridad digital.
- Mitigar el impacto de los incidentes de seguridad y privacidad de la información y de seguridad digital, de forma efectiva, eficaz y eficiente.
- Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, autenticidad, privacidad de la información.

Aut

	PLANTA DE TRATAMIENTO VILLASANTANA SOCIEDAD LIMITADA		Fecha de emisión 04-08-2025
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		Versión: 1
			Página: 3 de 18

- Definir los lineamientos necesarios para el manejo de la información, tanto física como digital, en el marco de una gestión documental basada en seguridad y privacidad de la información.

3. Principios y valores

Principios:

- **Transparencia y acceso a la información:** Garantizar que la información relevante sea pública, accesible y en formatos abiertos.
- **Eficiencia y optimización:** Implementar herramientas digitales que mejoren los procesos internos y la prestación de servicios.
- **Seguridad digital:** Asegurar la protección de los datos y la infraestructura tecnológica.
- **Innovación y mejora continua:** Fomentar el uso de nuevas tecnologías para optimizar la gestión y los servicios.
- **Participación y colaboración:** Promover la interacción con la ciudadanía y otros actores mediante canales digitales (Página web, redes sociales, etc.).

Valores:

- **Honestidad:** Actúo siempre con fundamento en la verdad, cumpliendo mis deberes con transparencia y rectitud, y siempre favoreciendo el interés general.
- **Respeto:** Reconozco, valoro y trato de manera digna a todas las personas, con sus virtudes y defectos, sin importar su labor, su procedencia, títulos o cualquier otra condición.
- **Compromiso:** Soy consciente de la importancia de mi rol como servidor público y estoy en disposición permanente para comprender y resolver las necesidades de las personas con las que me relaciono en mis labores cotidianas, buscando siempre mejorar su bienestar.
- **Diligencia:** Cumpro con los deberes, funciones y responsabilidades asignadas a mi cargo de la mejor manera posible, con atención, prontitud, destreza y eficiencia, para así optimizar el uso de los recursos.
- **Justicia:** Actúo con imparcialidad garantizando los derechos de las personas, con equidad, igualdad y sin discriminación.

Aut

	PLANTA DE TRATAMIENTO VILLASANTANA SOCIEDAD LIMITADA		Fecha de emisión 04-08-2025
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		Versión: 1
			Página: 4 de 18

- **Trabajo en equipo:** Trabajo en conjunto con mis compañeros, cada uno hace parte, pero todos tenemos un objetivo en común.
- **Profesionalidad:** Desempeño mi trabajo con pericia, aplicación, seriedad, honradez y eficacia.

4. Alcance

Este plan aplica a todos los procesos de la Planta de Tratamiento Villasantana Sociedad Limitada, funcionarios y contratistas que compartan, utilicen, recolecten, procesen, intercambien o consulten información de la entidad.

El presente el Plan de Seguridad y Privacidad esta alineado con los objetivos, metas, procesos, procedimientos y estructura organizacional, de tal forma que se asegure la confidencialidad, integridad y disponibilidad de la información.

5. Política

La Planta de Tratamiento Villasantana Sociedad Limitada mediante la adopción e implementación del Plan de Seguridad y Privacidad de la Información, protege, preserva y administra la confidencialidad, integridad, disponibilidad, autenticidad, privacidad de la información, mediante una gestión de los riesgos y la implementación de controles físicos y digitales para prevenir incidentes.

6. Marco Normativo y metodológico

- Ley 527/99 Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos.
- Ley 594/00 Por medio de la cual se dicta la Ley General de Archivo 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.
- Ley 527/99 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.
- Ley 1581/12 Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales.
- Ley 1712/14 Ley de transparencia y del derecho de acceso a la Información pública nacional”.

ms

	PLANTA DE TRATAMIENTO VILLASANTANA SOCIEDAD LIMITADA		Fecha de emisión 04-08-2025
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		Versión: 1
			Página: 5 de 18

- Ley 1581/12 Ley de protección de datos personales.
- Ley 1273/09 Ley de delitos informáticos y la protección de la información y de los datos.
- Decreto 1377/13 Ley de protección de datos personales.
- Decreto 2573/14 Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
- Decreto 1377/13 Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 2609/12 Por el cual se reglamenta el Título V de la Ley 594 de 2000 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado".
- Decreto 2693/12 Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones
- Decreto 1078/15 Por medio del cual se expide el "Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones", se define el componente de seguridad y privacidad de la información, como parte integral de la estrategia GEL.
- Decreto 1008/2018 Por el cual se establecen los lineamientos generales de la política Gobierno Digital.
- Decreto 612/18 Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- Resolución 001519/20 del Ministerio De Tecnologías De La Información Y Las Comunicaciones Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos"
- ISO 27001 Tecnología De La Información.

7. Estrategias de la Implementación

Para la aplicación, la entidad desarrollará las siguientes estrategias:

- **Seguridad de la información:** Adopción de procedimientos para la protección de datos y ciberseguridad.
- **Capacitación:** Formación del personal en el uso de herramientas digitales y buenas prácticas en seguridad de la información.

La entidad con la aplicación del plan de la privacidad y Seguridad de la información busca que todos sus procesos, trámites, servicios, sistemas de

mf



información, datos e infraestructura se garantice la confidencialidad, disponibilidad de la información y privacidad de los datos personales.

Adicionalmente la entidad cuenta con el formato de autorización para el tratamiento de datos personales.

8. Glosario

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

Ant

	PLANTA DE TRATAMIENTO VILLASANTANA SOCIEDAD LIMITADA		Fecha de emisión 04-08-2025
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		Versión: 1
			Página: 7 de 18

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)

Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

amb

	PLANTA DE TRATAMIENTO VILLASANTANA SOCIEDAD LIMITADA		Fecha de emisión 04-08-2025
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		Versión: 1
			Página: 8 de 18

Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad

amf



de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

Ley de Habeas Data: Se refiere a la Ley Estatutaria 1266 de 2008.

Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Responsable del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Amf

	PLANTA DE TRATAMIENTO VILLASANTANA SOCIEDAD LIMITADA		Fecha de emisión 04-08-2025
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		Versión: 1
			Página: 10 de 18

Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

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

9. Conceptos básicos

La seguridad informática se refiere a la protección de la información y los sistemas informáticos contra amenazas y vulnerabilidades. Esto incluye la protección de la confidencialidad, integridad y disponibilidad de la información.

Existen varios tipos de amenazas que pueden afectar la seguridad informática, incluyendo:

- **Malware:** software malicioso que puede dañar o robar información.
- **Phishing:** ataques que intentan engañar a los usuarios para que revelen información confidencial.
- **Ataques de denegación de servicio (DDoS):** ataques que intentan sobrecargar un sistema para que no pueda funcionar correctamente.
- **Ataques de inyección de código:** ataques que intentan inyectar código malicioso en un sistema.

Importancia de la confidencialidad, integridad y disponibilidad:

- **Confidencialidad:** la protección de la información contra acceso no autorizado.
- **Integridad:** la protección de la información contra modificaciones no autorizadas.
- **Disponibilidad:** la protección de la información y los sistemas para asegurar que estén disponibles cuando se necesiten.

Amenazas:

- **Virus:** software que se replica a sí mismo y puede dañar o robar información.
- **Gusanos:** software que se replica a sí mismo y puede dañar o robar información, pero no necesita de un archivo huésped.
- **Troyanos:** software que se disfraza como software legítimo, pero en realidad es malware.
- El phishing es un ataque que intenta engañar a los usuarios para que revelen información confidencial.
- El spear phishing es un tipo de phishing que se dirige a un objetivo específico.

	PLANTA DE TRATAMIENTO VILLASANTANA SOCIEDAD LIMITADA		Fecha de emisión 04-08-2025
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		Versión: 1
			Página: 11 de 18

- Un ataque de denegación de servicio (DDoS) es un ataque que intenta sobrecargar un sistema para que no pueda funcionar correctamente.
- Un ataque de inyección de código es un ataque que intenta inyectar código malicioso en un sistema.

Medidas De Seguridad: Autenticación y autorización:

- La autenticación y autorización son procesos que verifican la identidad de un usuario y determinan si tiene permiso para acceder a un sistema o recurso.
- El cifrado de datos es el proceso de convertir la información en un formato que no pueda ser leído sin la clave de descifrado correspondiente.
- Los firewalls y sistemas de detección de intrusos son herramientas que ayudan a proteger un sistema contra ataques y vulnerabilidades.
- Las actualizaciones y parches de seguridad son importantes para mantener un sistema seguro y protegido contra vulnerabilidades.
- Las copias de seguridad y la recuperación de datos son importantes para proteger la información y asegurar que esté disponible en caso de una emergencia.

Mejores Prácticas:

- El uso de contraseñas seguras es importante para proteger la información y los sistemas.
- La actualización de software y sistemas operativos es importante para mantener un sistema seguro y protegido contra vulnerabilidades.
- El uso de antivirus y software de seguridad es importante para proteger un sistema contra malware y otras amenazas.
- Evitar abrir correos electrónicos sospechosos.
- Evitar abrir correos electrónicos sospechosos es importante para proteger la información y los sistemas contra phishing y otros ataques.
- Utilizar redes seguras y VPNs es importante para proteger la información y los sistemas cuando se accede a Internet desde una red pública.

10. Lineamientos del plan

El Sistema de Gestión de Seguridad de la Información (SGSI) proporciona un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la protección de los activos de información para lograr objetivos de la entidad.

La seguridad de la información como elemento de la política de Gobierno Digital, permite alinearse con sus componentes denominados: TIC para el Estado: Tiene

amb

	PLANTA DE TRATAMIENTO VILLASANTANA SOCIEDAD LIMITADA		Fecha de emisión 04-08-2025
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		Versión: 1
			Página: 12 de 18

como objetivo mejorar el funcionamiento de las entidades públicas y su relación con otras entidades públicas, a través del uso de las Tecnologías de la Información y las Comunicaciones, TIC para la Sociedad: Tiene como objetivo fortalecer interacción con la comunidad, los arrendatarios y otras entidades a través de plataformas digitales, promoviendo la transparencia y el acceso a la información pública; y TIC para la Gestión Interna con la formulación e implementación del modelo de seguridad, el cual se enfoca en garantizar y preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión de la entidad.

Adicionalmente, el plan tiene como objetivo mejorar la eficiencia de los procesos administrativos y operativos mediante el uso de tecnologías digitales, garantizando el cumplimiento del objeto social de la entidad y la privacidad de la información.

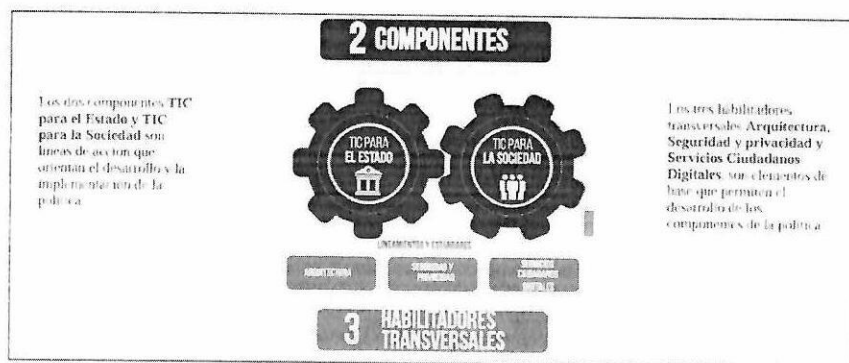


Ilustración 1 Componentes

Arquitectura: Busca que las entidades públicas apliquen en su gestión, un enfoque de Arquitectura Empresarial para el fortalecimiento de sus capacidades institucionales y de gestión de TI, aplicando los lineamientos, estándares y mejores prácticas contenidos en el Marco de Referencia de Arquitectura Empresarial del Estado.

Seguridad y Privacidad: Busca que las entidades públicas incorporen la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información de las entidades del Estado, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos. Este habilitador se desarrolla a través del Modelo de Seguridad y Privacidad de la Información, que orienta la gestión e implementación de la seguridad de la información en el Estado.

Handwritten signature



Servicios Ciudadanos Digitales: Busca que los servicios ciudadanos digitales sean integrados a los procesos, servicios digitales, trámites digitales, sistemas de información y demás que lo requieran, buscando racionalizar recursos, estandarizar y armonizar la administración pública en pro de mejorar los servicios del Estado.

11. Infraestructura tecnológica con la que cuenta la entidad y las medidas de seguridad

El objetivo es garantizar el buen y continuo funcionamiento de la infraestructura tecnológica de la entidad, en el entendido que por infraestructura tecnológica nos referimos a hardware, software, conectividad, datos y servicios con las que cuenta la Planta de Tratamiento Villasantana.

- **Colombia Hosting:** Plataforma de alojamiento web donde se encuentra registrada y alojada la página institucional. Desde allí se gestiona el dominio, el almacenamiento de archivos y se garantiza la disponibilidad del sitio web; y se cuenta con contraseña y usuarios autorizado.
- **Correos electrónicos corporativos:** Cuentas institucionales destinadas a la comunicación interna y externa de la empresa. Cuento con las credenciales necesarias para la configuración, recuperación de contraseñas, gestión de redireccionamientos y soporte técnico básico; y se cuenta con contraseña y usuarios autorizado.
- **cPanel:** Panel de control del hosting que permite la administración técnica del sitio, incluyendo la gestión de archivos del servidor, bases de datos, cuentas FTP, copias de seguridad y la creación y mantenimiento de los correos electrónicos corporativos; y se cuenta con contraseña y usuarios autorizado.
- **Go Daddy:** Plataforma donde compramos el dominio; y se cuenta con contraseña y usuarios autorizado.
- **WordPress:** Sistema de gestión de contenidos (CMS) mediante el cual se realiza la edición, actualización y publicación de contenidos en la página web institucional, incluyendo noticias, informes, documentos de interés público y secciones informativas requeridas por ley, y se cuenta con contraseña y usuarios autorizado.

	PLANTA DE TRATAMIENTO VILLASANTANA SOCIEDAD LIMITADA		Fecha de emisión 04-08-2025
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		Versión: 1
			Página: 14 de 18

- **Programa del sistema de inventarios:** Herramienta que permite el registro, seguimiento y control de los bienes e insumos de la entidad, el uso garantiza la trazabilidad, control y actualización permanente del inventario.
- **Software de Contabilidad y Presupuesto:** Herramienta especializada fundamental para la gestión financiera y contable de la entidad.
- **Servidor:** Este servidor es el entorno donde se encuentra instalado y en funcionamiento el Programa de Contabilidad y Presupuesto.

ITEM	ACTIVIDADES	RESPONSABLE	RECURSOS
1	INTRANET Administración técnica, operativa y actualización de contenido	Personal de apoyo TIC	Tecnológicos y de la Información
2	PORTAL WEB Administración técnica, operativa y actualización de contenido	Personal de apoyo TIC	Tecnológicos y de la Información
3	INFORMACION DE EQUIPOS Y USUARIOS Copias de respaldo	Personal de apoyo TIC	Tecnológicos y de la Información
4	EQUIPOS TECNOLOGICOS Soporte técnico, mantenimiento preventivo y correctivo computadoras, impresoras, escáner, etc	Personal de apoyo TIC	Tecnológicos y de la Información
5	SERVIDOR Soporte técnico, copias de seguridad, mantenimiento preventivo y correctivo	Personal de apoyo TIC	Tecnológicos y de la Información

Tabla 1 Infraestructura

12. Implementación del Plan

De acuerdo con el modelo de seguridad y privacidad de la información emanado por el ministerio de las TIC dentro del marco de la política de Gobierno Digital contempla un ciclo de operación que consta de varias etapas, las cuales permitirán que la Entidad pueda implementar adecuadamente la seguridad y privacidad de la información.

A. DIAGNÓSTICO

En esta etapa se pretende analizar mediante un diagnóstico, el estado actual de la entidad con respecto a los requerimientos del MSPI y determinar el estado actual de la gestión de seguridad y privacidad de la información en la entidad e

Handwritten signature

	PLANTA DE TRATAMIENTO VILLASANTANA SOCIEDAD LIMITADA												Fecha de emisión 04-08-2025
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION												Versión: 1
													Página: 15 de 18

identificar las vulnerabilidades técnicas y administrativas con el objetivo de generar planes de mejoramiento para subsanar dichas vulnerabilidades.

B. PLANIFICACIÓN

En esta etapa se pretende desarrollar y formalizar los procedimientos que permitan gestionar la seguridad de la información, fortalecer los procesos que hacen referencia a la implementación de la seguridad y privacidad de la información y realizar el inventario de los activos de información con las que cuenta la entidad, sus propietarios, custodios y usuarios autorizados.

Adicionalmente la identificación de los riesgos y controles de Seguridad con el fin de implementar procesos para el manejo y respuesta a incidentes asociados a Seguridad y Privacidad de la Información y establecer controles.

C. IMPLEMENTACIÓN

En esta etapa se llevará a cabo la implementación de los documentos señalados en la etapa de planificación.

D. SEGUIMIENTO

En esta fase se deberá contemplar dentro del proceso de auditorías, el seguimiento a la planificación e implementación del MSPI de acuerdo con el siguiente cronograma.

VIGENCIA 2026														
N°	Actividad para la implementación	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sept	Oct	Nov	Dic	Responsable
1	Diagnóstico			x										Gerencia y encargados del proceso de medios tecnológicos
2	Realización del inventario activos de información			X										Gerencia y encargados del proceso de medios

Handwritten signature

VIGENCIA 2026														
N°	Actividad para la implementación	Ene	Fe	Mar	Abr	May	Jun	Jul	Ago	Sept	Oct	Nov	Dic	Responsable
														tecnológicos
3	Elaboración de Planes de contingencia para garantizar la seguridad de la información						X							Gerencia y encargados del proceso de medios tecnológicos

Tabla 2 Cronograma

13. Responsable y actualización del Plan

El plan será revisado anualmente y actualizado conforme a cambios normativos, directrices institucionales y avances tecnológicos, la revisión será liderada por el equipo de Tecnologías de la Información en conjunto con la Gerencia.

14. Seguimiento

El seguimiento a la implementación del plan será realizado de acuerdo con el manual de auditoría de la entidad.

15. Indicadores

Para dar cumplimiento al Plan, se realizará seguimiento mediante al siguiente indicador; así:

- Número de documentos implementados * el número de documentos solicitados x 100

16. Comité de seguridad digital

De acuerdo con la Resolución No. 004 del 02 de enero de 2023 "Por la cual se actualiza el Manual de funciones, requisitos y competencias laborales de los empleos públicos de la Planta de Tratamiento Villasantana Sociedad Limitada y se dictan otras Disposiciones donde en su estructura cuenta con dos (2) funcionarios: un GERENTE, código 039, grado 1 y un PROFESIONAL

ant

	PLANTA DE TRATAMIENTO VILLASANTANA SOCIEDAD LIMITADA		Fecha de emisión 04-08-2025
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		Versión: 1
			Página: 17 de 18

UNIVERSITARIO, código 001, grado 01, el comité de seguridad digital será el mismo comité institucional de gestión y desempeño adoptado mediante Resolución 0000025 del 27 diciembre de 2023 "Por la cual se reglamenta el modelo integrado de planeación y gestión y se definen lineamientos para su operación en la organización y se integra el comité institucional de gestión y desempeño".

17. Bibliografía

- Plan De Seguridad Y Privacidad De La información de EDOS
<https://www.edos.gov.co/index.php/normativa/planeacion-gestion-y-control/category/555-2025>.
- Plan De Seguridad Y Privacidad De La información de Min TIC chrome-extension://efaidnbmninnibpcajpcglclefindmkaj/https://mintic.gov.co/portal/715/articles-135830_plan_seguridad_privacidad_informacion_v1_20230124.pdf.

ELABORADO POR:	REVISADO POR:	APROBADO POR:
-----------------------	----------------------	----------------------

Ans



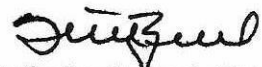
PLANTA DE TRATAMIENTO VILLASANTANA SOCIEDAD
LIMITADA

Fecha de emisión
04-08-2025

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA
INFORMACION

Versión: 1

Página: 18 de 18

Nombre y Cargo:	Nombre y Cargo:	Nombre y Cargo:
 Cesar Augusto Álvarez Profesional MIPG	 Jhon Stiven Sampedro Profesional en sistemas	 Martha Lucia Sarria Colon Gerente (E)
	 Kristhian Robayo Profesional en sistemas	
	 Daniel Martinez Profesional en sistemas	