“Somos un equipo comprometido con nuestro hogar. Trabajamos con pasión por servir, estamos avanzando y tenemos la esperanza de ser cada vez mejores por el bienestar de nuestra comunidad y la convicción de sumar voluntades para un desarrollo ambiental, social y económico.”

Plan Estratégico de Seguridad de la Información

ESSMAR 2026 - 2027

Subgerencia Corporativa

GERMAN IGUARÁN ROMERO
Técnico Administrativo Grupo TIC
Subgerencia Corporativa

EDWIN ANTONIO PARADA CABRERA
Agente Especial ESSMAR E.S.P.

Tabla de contenido

1. Introducción

El Plan Estratégico de Seguridad de la Información –PESI– constituye el instrumento rector para la consolidación de las capacidades institucionales en materia de seguridad digital en ESSMAR E.S.P. Su propósito es orientar de manera sistemática y sostenible el fortalecimiento de los controles, políticas y procesos que permiten proteger la información crítica, garantizar la continuidad de los servicios y mitigar riesgos asociados al uso de tecnologías de la información.

Este documento se desarrolla en cumplimiento de la Guía para la Formulación del PESI del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), y se articula con el Modelo de Seguridad y Privacidad de la Información –MSPI–, el Marco de Gobierno Digital, el Modelo Integrado de Planeación y Gestión –MIPG– y los lineamientos estratégicos institucionales.

La aplicación efectiva de este plan no solo dependerá de la tecnología implementada, sino también de la cultura organizacional, por lo que el PESI 2026–2027 se proyecta como una hoja de ruta que permitirá a la Empresa avanzar desde su estado actual, caracterizado por prácticas incipientes en algunos componentes claves, hacia un nivel de madurez que asegure la protección de los activos de información, la resiliencia operacional y el cumplimiento de la normatividad vigente.

1.1 Propósito

El PESI tiene como propósito definir el marco estratégico, programático y operativo que orientará las acciones necesarias para implementar, fortalecer y mantener las capacidades de seguridad de la información en ESSMAR E.S.P., garantizando la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información institucional.

2.Alcance

El PESI es aplicable para todos los procesos misionales, estratégicos y de apoyo de la empresa de servicios públicos del distrito de Santas Marta ESSMAR E.S.P., incluyendo;

- La infraestructura tecnológica y de comunicaciones
- Los sistemas de información corporativos y aplicativos de terceros.
- Los datos personales, corporativos, técnicos y operativos administrados por la entidad.
- Los funcionarios, contratistas, proveedores tecnológicos y aliados estratégicos que acceden a información.
- Los servicios prestados mediante outsourcing, arrendamiento o modelos SaaS.

3.Objetivos

3.1. Objetivo general

Garantizar la protección, confidencialidad, integridad y disponibilidad de la información institucional, mediante la implementación de lineamientos, controles, buenas prácticas y mecanismos de gestión del riesgo de seguridad de la información, que fortalezcan la continuidad de los servicios, la confianza de los grupos de interés y el cumplimiento de los requisitos legales, regulatorios y organizacionales.

3.2. Objetivos específicos

1- Fortalecer la gobernanza y el marco institucional de seguridad de la información, mediante políticas, procedimientos, roles y responsabilidades claramente definidos.
2- Proteger los activos de información a través de controles de seguridad integrales y sistemáticos.
3- Implementar un esquema formal de gestión del riesgo, alineado con el MSPI y la norma ISO 27005.
4- Asegurar la continuidad operativa, garantizando capacidades de respaldo, recuperación y redundancia.

5- Promover la cultura organizacional en seguridad digital, favoreciendo el uso seguro de los recursos tecnológicos.
6- Garantizar el cumplimiento normativo, especialmente en materia de protección de datos personales.
7- Reducir vulnerabilidades tecnológicas mediante mantenimiento, actualización y controles preventivos.

4. Marco Normativo

Las Políticas de Seguridad de la Información son aplicables para todos los

Norma	Descripción
Constitución Política de Colombia 1991. Artículo 15	Reconoce como Derecho Fundamental el Habeas Data.
Artículo 20	Libertad de Información.
Ley 23 de 1982	Propiedad Intelectual - Derechos de Autor.
Ley 594 de 2000	Ley General de Archivos.
Ley 527 de 1999	Por 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 1032 de 2006	Por el cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
Ley 1266 de 2007	Por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
Ley 1273 de 2009	"Delitos Informáticos" protección de la información y los datos.
Ley 1437 de 2011	"Código de procedimiento administrativo y de lo contencioso administrativo".
Ley 1581 de 2012	"Protección de Datos personales".
Ley 1712 de 2014	“De transparencia y del derecho de acceso a la información pública nacional”.
Ley 1150 de 2007	“Seguridad de la información electrónica en contratación en línea”
Ley 1341 de 2009	“Tecnologías de la Información y aplicación de seguridad”.

Norma	Descripción
Decreto 1377 de 2013	“Establece los principios que deben guiar el tratamiento de los datos personales en Colombia”.
Decreto 1078 de 2015	“Establece la Política Nacional de Seguridad Digital”.
Decreto 612 de 2018	MIPG
Decreto 620 de 2019	“Establece disposiciones específicas sobre la protección de la información y los sistemas de información en el ámbito de las entidades públicas”.
Decreto 338 de 2022	“Establece los lineamientos para fortalecer la seguridad digital en Colombia”.
Resolución 500 de 2021 (MinTic)	Modelo de Seguridad y Privacidad de la Información
CONPES 3701 de 2011	Lineamientos de Política para Ciberseguridad y Ciberdefensa.
CONPES 3854 de 2016	Política Nacional de Seguridad digital.
CONPES 3995 de 2020	Política Nacional de Confianza y Seguridad digital.
Norma técnica colombiana NTC - ISO/IEC 27001	Estándar para la seguridad de la información, describe cómo gestionar la seguridad de la información en una empresa

5.Generalidades

5.1. Misión PESI

Consolidar un sistema de seguridad de la información articulado, eficiente y sostenible que responda a las necesidades tecnológicas de ESSMAR E.S.P., garantice la protección de los activos de información y soporte la continuidad de los servicios públicos esenciales prestados por la Empresa.

5.2. Visión PESI

Para el año 2027, ESSMAR E.S.P. contará con un sistema de seguridad de la información con mayor nivel de madurez y alineado con las mejores prácticas del MSPI y la norma ISO 27001, soportado por políticas robustas, procesos estandarizados, infraestructura confiable y una cultura organizacional comprometida con la seguridad digital.

5.3. Marco Estratégico

5.3.1. Principios rectores de seguridad de la información

ESSMAR E.S.P. adopta los siguientes principios como lineamientos fundamentales de su estrategia de seguridad;

- Confidencialidad: La información será accesible únicamente por personal autorizado.
- Integridad: La información se mantendrá completa, precisa y protegida contra modificaciones no autorizadas.
- Disponibilidad: Los sistemas, servicios y datos estarán disponibles cuando se requieran.
- Trazabilidad: Todas las acciones relevantes sobre los sistemas estarán registradas y auditables.
- Autenticidad: Se garantizará la legitimidad de los usuarios, dispositivos y sistemas que acceden a la información.
- No repudio: Ningún actor podrá negar acciones previamente ejecutadas sobre los sistemas.

5.3.2. Partes Interesadas

Entre las partes interesadas que intervienen en el ecosistema de seguridad de ESSMAR E.S.P. se encuentran:

- Alta dirección
- Grupo de trabajo TIC – Subgerencia Corporativa
- Áreas misionales, estratégicas y de apoyo de la ESSMAR
- Funcionarios y contratistas
- Proveedores de bienes y servicios tecnológicos
- Aliados estratégicos
- Entes de Control
- Superintendencia de Servicios Públicos
- Comunidad de usuarios y ciudadanía en general

5.3.3. Roles y Responsabilidades

En aras de garantizar la correcta gestión de la seguridad de la información, se deberán definir responsables para los siguientes roles:

- Líder de Seguridad de la Información (LSI): Responsable de direccionar la implementación del PESI.
- Administrador de Infraestructura TI: Responsable técnico de los componentes de hardware, software y redes.
- Responsables de activos: Encargados del ciclo de vida, clasificación y control de los activos bajo su custodia.
- Usuarios: Deben cumplir las políticas y procedimientos definidos por la Empresa.
- Comité TIC: Instancia de seguimiento estratégico del PESI.
- Equipo de seguimiento de Seguridad de la Información: Instancia de toma de decisiones y validación del SGSI.

5.3.4. Riesgos estratégicos de seguridad

En El análisis preliminar identifica los siguientes riesgos críticos:

- Accesos no autorizados a información sensible o infraestructura crítica.
- Indisponibilidad de sistemas corporativos clave.
- Fallas o ausencia de mecanismos de respaldo y recuperación.
- Vulnerabilidades persistentes por desactualización tecnológica.
- Dependencia elevada de proveedores externos.
- Incidentes de ciberseguridad que afecten la operación misional.

5.4. Diagnóstico del Estado Actual

Para En materia de seguridad de la información, la Empresa presenta diversos procesos que requieren fortalecimiento, actualización o formalización para alcanzar un nivel de madurez adecuado.

En agosto de 2021, asesores externos realizaron una evaluación integral de la seguridad de la información en ESSMAR E.S.P., cuyo informe diagnóstico identificó brechas relevantes y una serie de procesos que debían mejorarse o incorporarse para consolidar un esquema de protección más robusto de los activos de información.

Posteriormente, en julio de 2023, y en el marco de las acciones de mejora continua, la Empresa adelantó un nuevo diagnóstico en conjunto con un proveedor tecnológico especializado. Este ejercicio permitió evaluar nuevamente el estado de los procesos de seguridad, y como resultado se elaboraron y actualizaron diversos documentos orientados a optimizar prácticas internas relacionadas con la gestión de la seguridad de la información.

Durante la vigencia 2024, se formularon planes de mejora orientados a la formalización y fortalecimiento de los procesos de seguridad informática. Dentro de estas proyecciones se incluyó la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), así como la adopción y alineación a la política de Gobierno Digital. Adicionalmente, se priorizó la actualización del documento TI-Q01 – Política de Seguridad Digital, con el fin de garantizar su pertinencia frente a los estándares actuales y los requisitos del Modelo de Seguridad y Privacidad de la Información.

.

5.4.1. Estado actual con respecto al MSPI

El Modelo de Seguridad y Privacidad de la Información (MSPI) es el marco de referencia definido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), cuyo propósito es orientar a las entidades públicas en la gestión integral de la seguridad y la privacidad de la información.

Este modelo establece lineamientos, controles, responsabilidades, estructuras de gobierno y prácticas mínimas que las entidades deben adoptar para garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información que administran, constituyendo un componente obligatorio dentro del enfoque de Gobierno Digital y se encuentra reglamentado mediante la Resolución

500 de 2021, la cual actualiza su estructura e incorpora el Anexo 1, que detalla los requisitos para la implementación progresiva del modelo.

El modelo está compuesto por elementos como: Gobierno de seguridad y privacidad de la información, Gestión de riesgos en seguridad de la información, Gestión de incidentes de seguridad digital, Gestión de controles, Gestión de usuarios, Gestión de activos de información, Cultura y formación en seguridad de la información, entre otros.

La adopción del MSPI permite a ESSMAR E.S.P. evaluar su nivel de madurez, identificar brechas, planear intervenciones y ejecutar acciones para alcanzar un nivel óptimo de gestión de la seguridad, en coherencia con las normativas nacionales y las necesidades operativas de la empresa.

Con base en los insumos existentes con relación a las TIC's en la ESSMAR, se identifican las siguientes condiciones:

- El inventario de activos existe, pero no está completo ni estandarizado.
- Los mecanismos de respaldo son funcionales, pero no formalizados en procedimientos.
- Parte significativa de la infraestructura tecnológica presenta obsolescencia.
- La gestión de accesos carece de controles robustos de privilegios y segregación.
- No existe un SGSI formalmente implementado bajo ISO 27001.
- Los procesos de monitoreo y telemetría requieren fortalecimiento.
- Se requiere actualizar el acto administrativo de mipg incluir temas de privacidad y seguridad de la información
- Establecer procedimiento para control de información para las distintas situaciones administrativas asociadas a la gestión del talento humano.
- Establecer procedimiento de autorización de punto de conexión para los casos de reubicación de personal

5.4.2. Nivel de madurez – Escalas definidas

Gobierno: Ausencia de un gobierno de seguridad de la información formalmente definido y reconocido por la entidad.

Ausencia de roles y funciones:

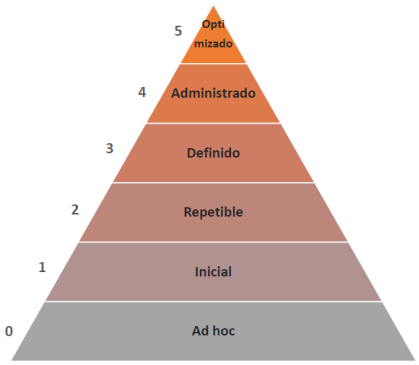
- No se evidencia una clara asignación de roles y responsabilidades para la gestión de seguridad de la información.
- No se han definido formalmente controles de seguridad para protección de los activos de información, ni responsables asignados.

Visibilidad: Poca visibilidad y empoderamiento en las funciones de seguridad de la información al interior de la empresa.

Responsabilidades: Dispersión de las responsabilidades sobre la gestión y control de la seguridad y privacidad de la información.

5.4.3. Escalas para la definición del nivel de madurez de la seguridad de la información en ESSMAR

El diagnóstico se realizará con base en los siguientes niveles:



Gráfica 1 (Elaboración propia)

5. Optimizado. Los componentes del elemento evaluado cuentan con esquemas de sostenibilidad.

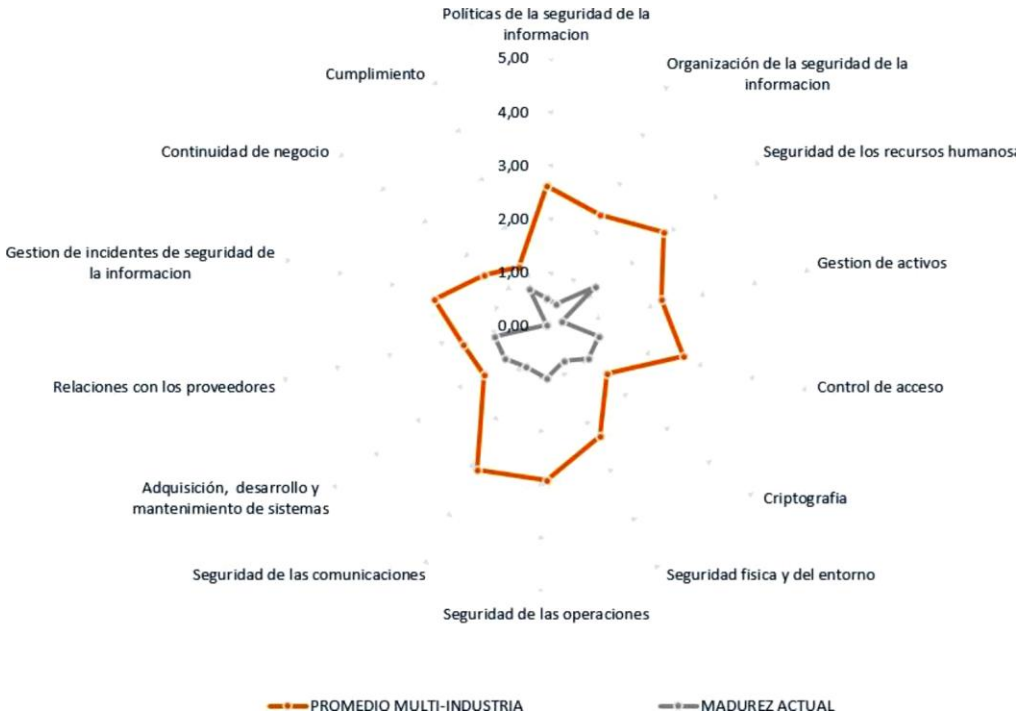
4. Administrado. Los componentes del elemento evaluado cuentan con esquemas de monitoreo para determinar su gestión.

3. Definido. Los componentes del elemento evaluado se encuentran documentados, formalizados, divulgados y operando.

2. Repetible. Los componentes del elemento evaluado no cuentan con todas las variables establecidas (formalizado, divulgado y operando).

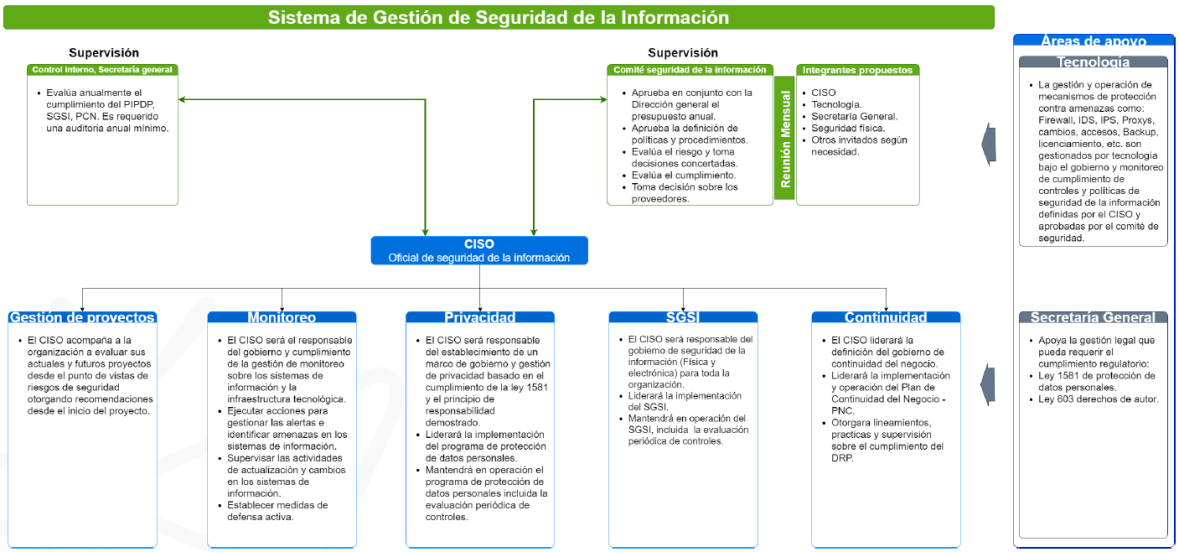
1. Inicial. Existen iniciativas al interior de la entidad para desarrollar los componentes del elemento evaluado.

0. Ad Hoc. No Existe



Gráfica 2 (Elaboración propia)

5.4.4. Modelo sugerido de seguridad de la información



Gráfica 3 (Elaboración propia)

5.4.5. Análisis de brechas – Evaluación de controles de seguridad de la información según ISO 27001

Con base en la revisión de diagnósticos de las vigencias 2021, 2023 y 2024, se consolidó un análisis del nivel de implementación de los controles de la norma ISO/IEC 27001 y del Modelo de Seguridad y Privacidad de la Información (MSPI). A partir de estos insumos, se identificaron controles existentes, controles por mejorar y controles que deben ser incorporados.

A continuación, se presenta la descripción estructurada por dominios.

Políticas de seguridad.

El diagnóstico evidenció que la empresa no cuenta con una Política de Seguridad de la Información actualizada, formalizada y divulgada entre funcionarios, contratistas y proveedores. Actualmente no se han establecido lineamientos explícitos alineados con ISO 27001 o MSPI, ni existe un mecanismo de capacitación periódica para su socialización.

Tampoco se solicita la lectura, conocimiento y aceptación formal de dicha política a los actores involucrados, lo que genera debilidad en el marco normativo interno y en la cultura organizacional de seguridad.

Organización de la información.

Se identificó la ausencia de un modelo formal de gobierno que defina roles, responsabilidades y niveles de autoridad sobre la seguridad de la información.

Las funciones se encuentran distribuidas entre la Dirección TIC, diferentes áreas operativas y la Oficina de Planeación Estratégica, sin lineamientos unificados ni claridad sobre la toma de decisiones.

Entre los principales hallazgos se destacan:

- Inexistencia de un Comité de Seguridad de la Información que oriente la estrategia institucional.
- No se ha designado formalmente un Oficial de Seguridad de la Información.

- No existen prácticas sistemáticas de evaluación de riesgos sobre los procesos críticos.
- No se han definido lineamientos de teletrabajo ni configuraciones de seguridad asociadas.
- Acceso sin restricciones a correos y nubes externas no corporativas.

La dispersión de responsabilidades impide una gestión integral y consistente del riesgo.

Seguridad de los recursos humanos.

No existe un proceso formal que exija la aceptación de la Política de Seguridad por parte de funcionarios y proveedores, ni un programa de capacitación continua que fortalezca el conocimiento sobre riesgos, manejo de activos, buenas prácticas y obligaciones asociadas.

Adicionalmente, el área de Recursos Humanos no cuenta con un procedimiento estructurado para notificar cambios de cargo que requieran ajustes en los privilegios de acceso a los sistemas de información.

En la relación con proveedores, no se evidencian cláusulas contractuales de confidencialidad o de cumplimiento de controles mínimos de seguridad, tampoco auditorías periódicas o exigencias de estándares como SOC2 o ISAE3402.

Gestión de activos.

La empresa no cuenta con un inventario consolidado de activos de información que incluya clasificación por niveles de confidencialidad, integridad y disponibilidad, ni procedimientos para su gestión durante el ciclo de vida.

Asimismo, se identificaron brechas en cuanto a:

- Ausencia de mecanismos de cifrado en dispositivos autorizados.
- Falta de lineamientos para la gestión de dispositivos móviles y medios removibles.
- No existen controles que limiten el uso de correo o almacenamiento en la nube no corporativos.
- No se implementan mecanismos automáticos de prevención de fuga de información (DLP).

Control de acceso.

El proceso de gestión de accesos no está formalizado ni centralizado. Las solicitudes de creación, modificación y retiro de usuarios son realizadas directamente al proveedor por diferentes áreas, sin trazabilidad ni gobierno desde la Dirección TIC.

Se observaron principalmente:

- Ausencia de una política de contraseñas y configuraciones adecuadas en los sistemas.
- Inexistencia de un Directorio Activo que permita una administración centralizada de equipos y usuarios.
- Falta de controles para revisión periódica de privilegios.

Estas brechas incrementan el riesgo de accesos no autorizados y manipulación indebida de información crítica.

Criptografía.

Actualmente no existe un inventario de activos que identifique información que requiera cifrado ni políticas que regulen el uso de controles criptográficos y la gestión del ciclo de vida de las claves.
Asimismo, algunos sistemas críticos no cuentan con certificados digitales vigentes que garanticen autenticidad y comunicación segura.

Seguridad física y ambiental.

Se identificaron debilidades en los mecanismos de control de acceso físico y en las condiciones ambientales de protección:

- El centro de cómputo no cuenta con cerraduras seguras ni mecanismos biométricos.
- Áreas de archivo físico sin sistemas de control de acceso, CCTV o mecanismos de prevención de incendios.
- No existe un programa de mantenimiento preventivo sobre equipos y servidores.
- No se han configurado bloqueos automáticos en las estaciones de trabajo ni medidas para prevenir el robo de equipos.

Seguridad en las operaciones.

No se dispone de procedimientos formalizados para gestionar la operación tecnológica (gestión de cambios, incidentes, capacidad, respaldo, licenciamiento, etc.).

También se evidenció que:

- No existe separación adecuada entre ambientes de producción, pruebas y desarrollo.
- No se cuenta con políticas claras de backup ni se ejecutan respaldos periódicos.
- Solo el 41% de los equipos cuenta con antivirus.
- No hay mecanismos de filtro de contenido ni monitoreo de administradores.
- No se realizan escaneos de vulnerabilidades ni pruebas de Ethical Hacking.
- No existe un procedimiento para controlar la instalación de software en los equipos.

Estas falencias aumentan significativamente la exposición a amenazas cibernéticas.

Seguridad de las comunicaciones.

No existen lineamientos para el intercambio seguro de información con terceros.

Además, se evidenció:

- Ausencia de certificados digitales para intercambio seguro.
- No existen lineamientos para el monitoreo de la red ni segmentación por VLAN.
- La red inalámbrica permite que funcionarios, contratistas y visitantes se conecten al mismo segmento.

Adquisición de sistemas, desarrollo y mantenimiento.

No existe un proceso formalizado de gestión de cambios ni gobierno sobre los cambios ejecutados por proveedores en los sistemas core.

Tampoco se han establecido lineamientos de desarrollo seguro, ni criterios de seguridad que proveedores deben cumplir.

Relación con proveedores.

En los procesos contractuales vigentes no se incluyen requisitos relacionados con seguridad de la información, tratamiento de datos personales o auditorías.

Tampoco se exige a los proveedores la aceptación de la Política de Seguridad ni se han definido mecanismos de supervisión y control sobre los activos que administran.

Gestión de los incidentes de seguridad.

No cuenta con un procedimiento para la gestión de incidentes ni herramientas como un SIEM para monitoreo centralizado.

La organización tampoco mantiene relación con los grupos especializados del ecosistema nacional de ciberseguridad (colCERT, CSIRT Gobierno, CCOC, entre otros).

Continuidad del negocio.

Se identificaron falencias en materia de:

- Plan de Continuidad del Negocio (BCP).
- Plan de Recuperación ante Desastres (DRP).
- Data center de respaldo para soportar la operación en contingencia.

Cumplimiento con los requerimientos legales y contractuales.

Se identificaron falencias en el cumplimiento de la Ley 1581 de protección de datos personales y la Ley 603 de propiedad intelectual.

Entre los principales hallazgos se encuentran:

- No existen bases de datos personales identificadas y documentadas.
- No se han asignado roles claros para la gestión de datos personales.
- No existe gestión de riesgos específica para datos personales.
- No se cuenta con procedimientos internos para peticiones y reclamos en materia de protección de datos.
- No hay capacitación continua en protección de datos.
- No se realizan auditorías independientes de cumplimiento.

Se deberá propender por una revisión y atención inmediata con relación a las regulaciones y cumplimiento de normativas asociadas a la implantación de controles para la gestión de seguridad de la información y del programa de protección de datos personales (buscando para este último el cumplimiento del principio de responsabilidad demostrado solicitado por la SIC).

5.4.6. Documentación entregada en diagnósticos realizados.

- Informe del diagnóstico de seguridad ESSMAR (Proyecto de condonación MinTic Icetex)
- Informe del diagnóstico de seguridad ESSMAR ISO VF (Proveedor EXTREME).
- Informe del diagnóstico de seguridad ESSMAR (Grupo TIC)

5.4.7. Política general de seguridad de la información.

La empresa de servicios públicos del distrito de Santa Marta ESSMAR E.S.P., como entidad prestadora de servicios públicos de acueducto, alcantarillado e interventoría a la empresa prestadora del servicio de aseo, establece que, la información es vital para el desarrollo de los procesos y de las actividades misionales e institucional, motivo por el cual, el grupo TIC está comprometido a proteger los activos de información de la entidad (Empleados, información y entorno laboral), orientando sus esfuerzos a la preservación de la confidencialidad, integridad, disponibilidad, a la continuidad de las operaciones de gobernabilidad, la administración y/o gestión de riesgos, la creación de cultura y conciencia de seguridad de la información en los funcionarios, contratistas, proveedores y personas que hagan uso de los activos de información de la empresa, tomando como base que la efectividad de esta política depende finalmente del comportamiento de las personas y los controles establecidos en las políticas de seguridad descritas en el presente documento.

El grupo TIC diseño y estructuró un documento de política seguridad digital (TI-Q01 política seguridad digital (V1)), los requerimientos de las actualizaciones en la política son debidamente revisados y aprobados por el comité MIPG.

5.4.8. Oportunidades de mejora

Los procedimientos que soportan la política de seguridad de la información describen de forma más detallada las actividades a desarrollar de los procesos, en él, se especifica las actividades, los recursos, la metodología y el objetivo que se pretende lograr o el valor agregado que genera y caracteriza el proceso.

5.4.9. Procedimiento de control de documentos

Garantiza que la empresa cuente con los documentos estrictamente necesarios en cada momento y maneja la dinámica del mejoramiento, mostrando la realidad que atraviesa, incorpora la eficacia de las diferentes acciones, a través de la revisión documental y del cumplimiento de los requisitos en los diferentes modelos de gestión, sobre el control de documentos. Así mismo, busca garantizar que los documentos en uso sean confiables y se mantengan actualizados, una vez sea evidenciado la eficacia de las acciones correctivas, preventivas y de mejora de los procesos. Soportado en el documento (TI-P10 Procedimiento Gestión de Seguridad de la Información).

5.4.10. Procedimiento de control de registros

Está definido para evidenciar las acciones realizadas y los resultados obtenidos en la ejecución de las actividades, con el fin de analizar los datos, y lo que es más importante, para la toma de decisiones, de tal forma que el registro que no aporta valor de mejora o de acción, no se deba tener en cuenta en el sistema. Soportado en el documento (TI-P11 Procedimiento Gestión del Cambio).

5.4.11. Procedimiento de auditoría interna

La auditoría interna es una herramienta para la alta dirección, en el momento de determinar la eficacia y la eficiencia del sistema de gestión, a través de la identificación de las fortalezas y debilidades. Por ello se desarrollan auditorias para evaluar la conformidad con las políticas de la organización, para evaluar el nivel de implementación del sistema de gestión, para evaluar el estado de mantenimiento y la capacidad de mejoramiento del sistema de gestión. Soportado en el documento (TI-P13 Procedimiento Formulación y Actualización de Políticas TI).

5.4.12. Procedimiento de acción correctiva

El objetivo de este procedimiento es definir los lineamientos para eliminar la causa de no conformidades dichos lineamientos son identificar, registrar, controlar, desarrollar, implantar y dar seguimiento a las acciones correctivas necesarias para evitar que se repita la no conformidad. Soportado en el documento (TI-P02 Procedimiento Administración y Mantenimiento de Sistemas de Información - TI-P07 Procedimiento Mantenimiento Preventivo y Correctivo Hardware).

5.4.13. Procedimiento de acción preventiva

El objetivo de este procedimiento es definir los lineamientos para identificar, registrar, controlar, desarrollar, implantar y dar seguimiento a las acciones preventivas generadas por la detección de una no conformidad real o potencial en el sistema de gestión de seguridad de la información y eliminar sus causas. Soportado en el documento (TI-P02 Procedimiento Administración y Mantenimiento de Sistemas de Información - TI-P07 Procedimiento Mantenimiento Preventivo y Correctivo Hardware).

5.4.14. Procedimiento de revisión del manual de política de seguridad de la información

El objetivo de este procedimiento es revisar, por parte de la dirección o jefes, en el Manual de la Política de Seguridad de la Información de la empresa de servicios públicos del distrito de Santas Marta ESSMAR E.S.P se encuentre planificado, para asegurar su conveniencia, eficiencia y eficacia continua. Soportado en el documento (TI-P08 Procedimiento Gestión de Políticas de Seguridad de la Información).

5.5. Proceso disciplinario

Dentro de la estrategia de seguridad de la información, está establecido un proceso disciplinario formal para los funcionarios que hayan cometido alguna violación a la Política de Seguridad de la Información. El proceso disciplinario también se debería utilizar como disuasión para evitar que los funcionarios, trabajadores, contratistas y demás colaboradores de la empresa de servicios públicos del distrito de Santas Marta ESSMAR E.S.P, violen los procedimientos de seguridad de la información. Las investigaciones disciplinarias corresponden a actividades pertenecientes al proceso de gestión de secretaria general y capital humano.

Actuaciones que conllevan a la violación de la seguridad de la información establecidas por la empresa de servicios públicos del distrito de Santas Marta ESSMAR E.S.P:

- Ingresar a la información de otros procesos, unidades, grupos o áreas, sin autorización del funcionario.
- No firmar los acuerdos de confidencialidad o de entrega de información o de activos de información.
- No reportar incidentes de seguridad o violaciones a la política de seguridad, cuando se tenga conocimiento de ello.
- Clasificar y registrar de manera inadecuada la información, desconociendo los estándares establecidos para este fin.
- No guardar de forma segura la información cuando se ausenta de su puesto de trabajo o al terminar la jornada laboral.
- Dejar información pública reservada, en carpetas compartidas o en lugares distintos al servidor de archivos, obviando las medidas de seguridad.
- Dejar equipos de cómputo encendidos en horas no laborables estando ausente.
- Permitir que personas ajenas, deambulen sin acompañamiento, al interior de las instalaciones, en áreas no destinadas al público.
- Utilización de software no relacionados con la actividad laboral y que pueda degradar el desempeño de las plataformas tecnológicas institucionales.
- Recibir o enviar información institucional a través de correos electrónicos personales, diferentes a los asignados por la institución, o en caso no esté autorizado por jefe inmediato o por el grupo TIC.
- Usar dispositivos de almacenamiento externo en los computadores, cuya autorización no haya sido otorgada por quien corresponda.
- Permitir el acceso de funcionarios a la red corporativa, sin la autorización o firmar ingreso por el grupo TIC.
- No cumplir con las actividades designadas para la protección de los activos de información.
- Descuidar documentación con información pública reservada o clasificada de la entidad, sin las medidas apropiadas de seguridad que garanticen su protección.
- Archivar información pública reservada o clasificada, sin claves de seguridad o cifrado de datos.

- Destruir, alterar, eliminar, dañar o suprimir datos informáticos o un sistema de tratamiento de información crítica de la entidad.
- Permitir el acceso u otorgar privilegios de acceso a las redes de datos de la ESSMAR E.S.P a personas no autorizadas.
- Entregar, enseñar y divulgar información institucional, calificada como información pública reservada y clasificada a personas o entidades no autorizadas.
- Instalar programas o software no autorizados en los equipos de cómputo o equipos portátiles institucionales, cuyo uso no esté autorizado por el grupo TIC.
- Copiar sin autorización los programas de la empresa de servicios públicos del distrito de Santas Marta ESSMAR E.S.P, o violar los derechos de autor o acuerdos de licenciamiento.

5.6. CUMPLIMIENTO

Los diferentes aspectos contemplados en este documento son de obligatorio cumplimiento para todos los funcionarios, contratistas y otros colaboradores de la empresa de servicios públicos del distrito de Santas Marta ESSMAR E.S.P. En caso de que se violen las políticas de seguridad ya sea de forma intencional o por negligencia, la empresa tomará las acciones disciplinarias y legales correspondientes. Estas Políticas de Seguridad de la Información deben prevenir el incumplimiento de las leyes, estatutos, regulaciones u obligaciones contractuales que se relacionen con los controles de seguridad informática.

5.7. ESTRATEGIAS TIC'S

Dimensión de TI	Actividad	Entregable o Producto	Meta o Indicador	Fecha Inicio	Fecha Fin
Gestión administrativa, de alineamiento, organización y planeación de TI	Matriz de controles de seguridad de la información (ISO 27001)	Matriz de controles de seguridad de la información.	≥ 90% controles críticos implementados.	1/02/2026	31/12/2026

Administración de los datos	Plan de copias de seguridad	Plan de copias de seguridad.	2 informes del proceso de copias de seguridad realizados. (	05/07/2026	05/01/2027
Administración de la seguridad y privacidad de la información	Diagnóstico seguridad de la información	Documentar informe diagnóstico del estado actual de seguridad de la información teniendo en cuenta la norma ISO 27001.	1 informe diagnóstico de seguridad de la información. aprobado.	1/03/2026	30/06/2026
	Política de seguridad digital	Procedimientos y formatos relacionados a la seguridad y privacidad de la información.	100% de documentos actualizados y aprobados.	1/02/2026	31/12/2026

Tabla 1 (Elaboración propia)

5.8. SEGUIMIENTO Y CONTROL

La oficina Asesora de planeación Estratégica y Gestión Regulatoria, realizara un seguimiento trimestral de las acciones establecidas dentro del plan acción institucional del proceso de TIC.

6. Control de cambios

Ítem que cambió	Descripción del cambio	Año de modificación
Elaboró y Revisó	Se hizo cambio de los responsables	2022
Alcance	Se modifica la descripción.	2022
Elaboró y Revisó	Se hizo cambio de los responsables	2023
Generalidades	Se hizo ajustes en el contenido	2023

Ítem que cambió	Descripción del cambio	Año de modificación
Generalidades	Se hizo ajustes en el contenido	2024
Introducción	Se hizo ajustes en el contenido	2024
Definiciones	Se hizo ajustes en el contenido	2024
Generalidades	Se hizo ajustes en el contenido	2025
Introducción	Se hizo ajustes en el contenido	2025
Definiciones	Se hizo ajustes en el contenido	2025
Elaboró y Revisó	Se hizo cambio de los responsables	2026
Generalidades	Se hizo ajustes en el contenido	2026
Introducción	Se hizo ajustes en el contenido	2026
Definiciones	Se hizo ajustes en el contenido	2026
Estrategias	Se hizo ajustes en el contenido	2026

7. Anexos

TI-Q01 política seguridad digital (V1)