“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 de Seguridad y Privacidad de la Información

ESSMAR 2025

ELABORÓ Y REVISÓ

ISMAEL ANTONIO MOLINA GIRALDO
Subgerente Corporativa

CRISTIAN PAUL SILVA USAQUEN
Profesional Especializado Grupo TIC
Subgerencia Corporativa

RAFAEL MAURICIO PINEDA GARCIA
Profesional Universitario Grupo TIC
Subgerencia Corporativa

GERMAN IGUARÁN ROMERO
Técnico Administrativo Grupo TIC
Subgerencia Corporativa

ERNEY VELÁSQUEZ TORRES
Agente Especial ESSMAR E.S.P.

Tabla de contenido

1. Introducción 5
2. Alcance 5
3. Objetivo 6
   3.1. Objetivo General 6
   3.2. Objetivos Especifico 6
4. Marco legal 7
5. Definiciones 8
6. Generalidades 9
   6.1. Diagnóstico 9
   6.2.1. Procedimiento de control de documentos 25
   6.2.3. Procedimiento de auditoría interna 25
   6.2.5. Procedimiento de acción preventiva 26
   6.2.6. Procedimiento de revisión del manual de política de seguridad de la información 26
   6.3. Proceso disciplinario 26
   6.5. ESTRATEGIAS TIC'S 28
   6.5.1. Actividades 28
   6.5.2. Indiciadores 30
7. Control de cambios 31
8. Anexos 32

1. Introducción

En un entorno cada vez más digitalizado, la seguridad y privacidad de la información se han convertido en pilares fundamentales para garantizar la protección de los datos personales, empresariales y cualquier tipo de información sensible. Este Plan de Seguridad y Privacidad de la Información tiene como objetivo establecer un marco de políticas, procedimientos y medidas técnicas que permitan a la organización proteger los datos frente a amenazas internas y externas, asegurando su confidencialidad, integridad y disponibilidad.

La protección de la información no solo es un requisito legal y normativo, sino que también es un compromiso con nuestros clientes, colaboradores y otras partes interesadas. Un manejo adecuado de la seguridad y privacidad de los datos fortalece la confianza, mitiga riesgos operativos y previene posibles consecuencias legales y reputacionales.

La aplicación efectiva de este plan no solo dependerá de la tecnología implementada, sino también de la cultura organizacional, por lo que se fomentará la capacitación continua del personal y la sensibilización sobre la importancia de la seguridad y privacidad en todas las actividades de la empresa.

Este documento establece las bases necesarias para garantizar un entorno seguro y transparente, en el que tanto la organización como sus usuarios puedan confiar plenamente.

2.Alcance

Las Políticas de Seguridad de la Información son aplicables para todos los aspectos administrativos y de control a ser cumplidos por funcionarios, visitantes, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con a la empresa de servicios públicos del distrito de Santas Marta ESSMAR E.S.P.

3. Objetivo

3.1. Objetivo General

Establecer las políticas que regulen la seguridad de la información de la empresa de servicios públicos del distrito de Santas Marta ESSMAR E.S.P, de forma clara y coherente, las cuales todo funcionario, contratista, visitante y tercero que presten sus servicios o tengan algún tipo de relación con la empresa deberán acatar y cumplir.

3.2. Objetivos Especifico

- Garantizar la seguridad de los datos y la información de todos los empleados de la empresa.
- Proteger la memoria institucional frente a los riesgos de fuga de información, mal uso o deterioro de las bases de datos.
- Asegurar que la información solo sea accesible a las personas o entidades autorizadas, evitando filtraciones o accesos no autorizados.
- Garantizar que la información se mantenga completa, precisa y sin alteraciones no deseadas, tanto durante el almacenamiento como la transmisión.
- Asegurar que la información esté disponible cuando sea necesaria, garantizando el acceso de usuarios autorizados sin interrupciones indebidas.
- Confirmar la identidad de los usuarios o sistemas para asegurarse de que solo los autorizados accedan a los recursos o datos.
- Implementar mecanismos de control de acceso a la información, como contraseñas, tokens, cifrado o biometría, para prevenir accesos no deseados.

4. Marco legal

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data.
- Artículo 20. Libertad de Información.
- Decreto 1599 de 2005, por el cual se adopta el Modelo Estándar de Control Interno MECI para el Estado Colombiano.
- Ley 734 de 2002, del Congreso de la República de Colombia, Código Disciplinario Único.
- Ley 23 de 1982 de 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”.
- CONPES 3701 de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016 Política Nacional de Seguridad digital.

5.Definiciones

Para facilitar la compresión del presente documento, se definen los siguientes términos.

Antivirus: herramientas de seguridad para la información cuyo objetivo es proteger la computadora de amenazas cibernéticas.

Virus: programas informáticos tipo malicioso, buscan alterar el normal funcionamiento de la red, de los sistemas o computador personal, por lo general su acción es transparente al usuario y puede tardar tiempo en descubrir su infección.

Almacenamiento en la Nube: es un modelo de almacenamiento de datos basado en redes de computadoras que consiste en guardar archivos en un lugar de Internet. Ejemplo: Gmail, Hotmail, OneDrive, Google Drive, etc.

Amenaza: Según [ISO/IEC 13335-1:2004): causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización de este.

Computo forense: también llamado informática forense, son técnicas científicas y analíticas especializadas a infraestructuras tecnológicas que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

Confidencialidad: acceso a la información únicamente quienes estén autorizados, Según [ISO/IEC 13335-1:2004]: propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

Ingeniería Social: es la manipulación por parte de individuos para lograr debilitar la seguridad de la red por medio de mecanismos que facilitan obtener información con clasificación confidencial. Ej: acercamiento a la víctima con preguntas especificas o contacto por redes sociales.

IPS: Sistema de prevención de intrusos. Es un dispositivo que permite dar control de acceso en una red para proteger los sistemas computacionales de ataques o vulnerabilidades.

VPN (Virtual Private Network): es una tecnología de red que permite una extensión segura de la red privada de área local (LAN) sobre una red pública.

Ransomware: software malicioso para secuestrar información, el atacante encripta los datos de la víctima y exige un pago por la clave de descifrado.

Firewall: es un dispositivo de seguridad de la red que monitorea el tráfico de red (entrante y saliente) y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.

6. Generalidades

6.1. Diagnóstico

Existen varios procesos por mejorar o incorporar en materia a seguridad de la información de la empresa.

Para fecha de agosto del año 2021 se proyectó un informe diagnóstico generado por unos asesores externos que desarrollaron una evaluación a la seguridad de la información a la empresa durante ese año, arrojando un resultado con una relación de los procesos que debían mejorarse o incorporar para garantizar una seguridad un poco más robusta a la información.

Para fecha de julio del año 2023 dentro de los procesos de mejora continua en materia de seguridad de la información de la empresa, en conjunto con un proveedor de servicios tecnológico se proyectó un informe diagnóstico donde evalúan el estado de los procesos de seguridad. Como resultado del ejercicio se desarrollaron documentos para actualizar logrando optimizar algunos procesos relacionados a la seguridad de información.

Para vigencia 2024, se proyectaron planes de mejoras para formalizar adecuadamente los procesos relacionados a la seguridad informática. Entre las proyecciones se encuentra por implementar SGSI (Sistema de Gestión de Seguridad de la Información) y la política de gobierno digital. Además, actualización del documento de TI Q01 politica seguridad digital

6.1.1. Situación actual identificada

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

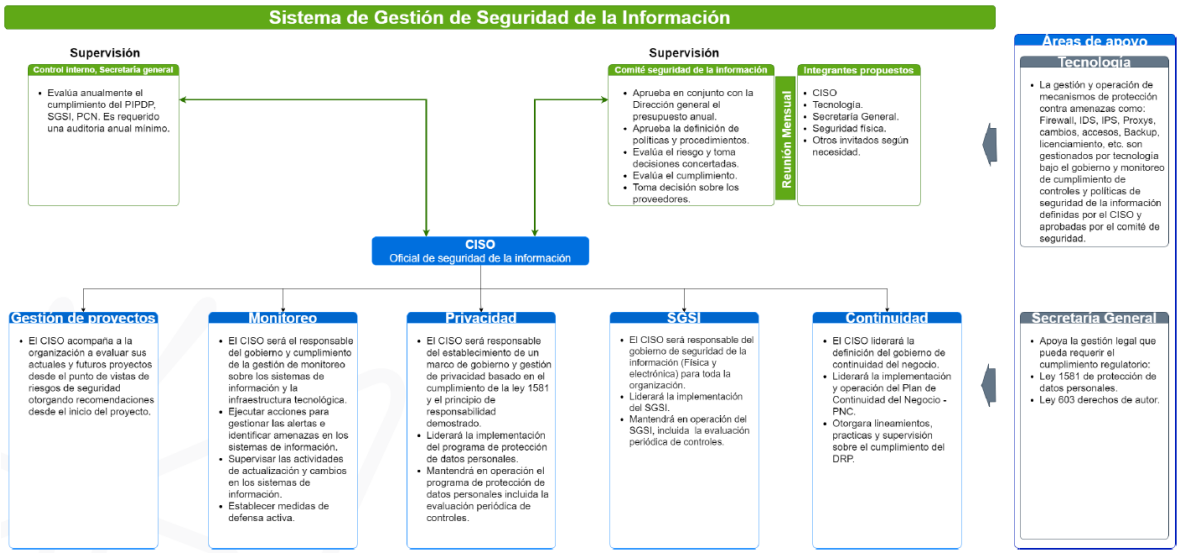
Ausencia de roles y funciones:

- 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.

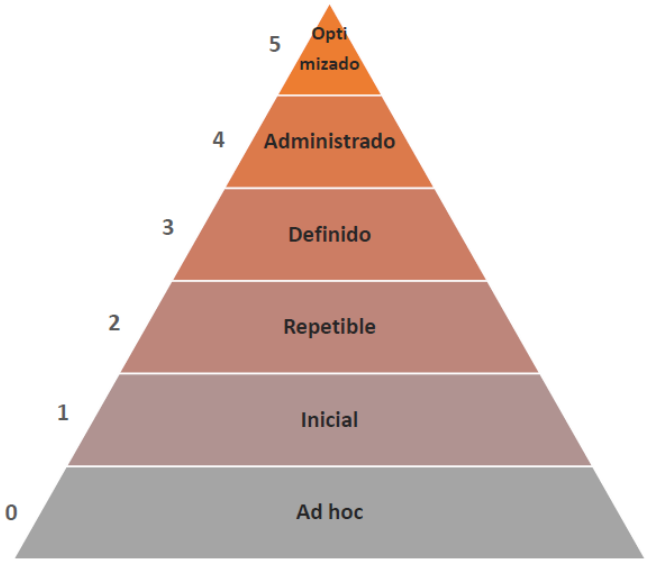
Responsabilidades: Dispersión de las responsabilidades sobre la gestión y control de la seguridad.

6.1.2. Modelo sugerido de seguridad de la información



Gráfica 1 (Elaboración propia)

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



Gráfica 2 (Elaboración propia)

CRITERIOS

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

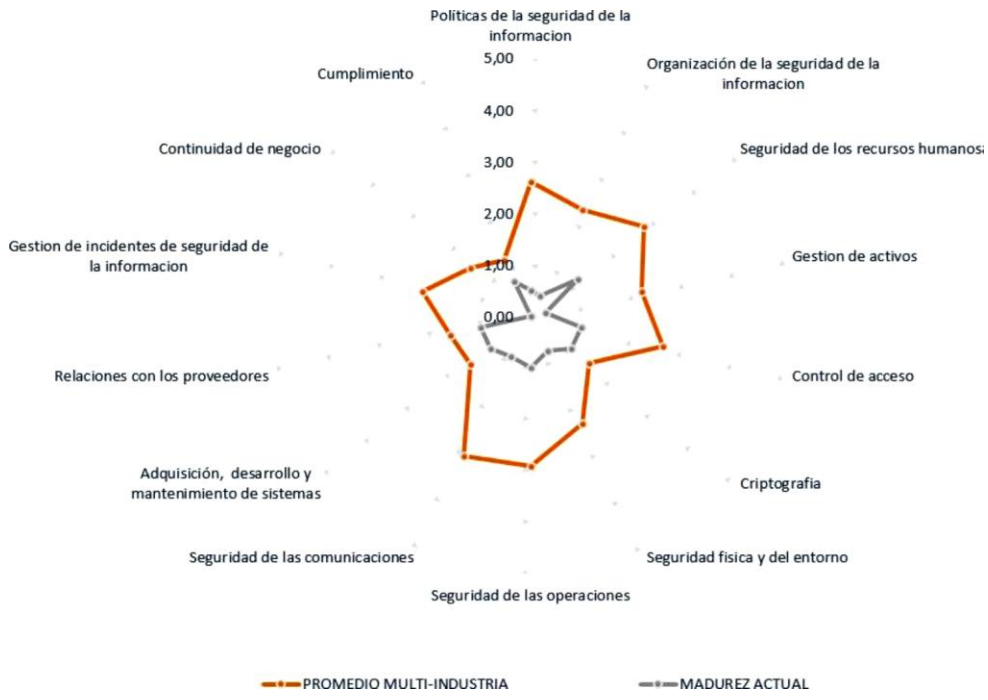
4. Administrado. Los componentes del elemento evaluado cuentan con esquemas de monitoreo para determinar su gestión.

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 3 (Elaboración propia)

6.1.4. Resumen informe diagnóstico realizado

A continuación, una breve descripción de cada aspecto a mejorar o para incorporar controles. Aclarando que es el resultado de los diagnósticos realizados y con ello se ha estado trabajando en las mejoras en cada punto.

Políticas de seguridad.

- La empresa no cuenta con una Política de Seguridad de la Información formalmente definida, documentada y divulgada entre sus funcionarios y proveedores, que contemple lineamientos relacionados con la gestión de seguridad de la información según estándares o marcos de referencia como la norma ISO 27001 y/o el modelo de seguridad y privacidad de la información (MSPI), según las recomendaciones descritas en el diagnóstico detallado.

- No se imparten capacitaciones periódicas orientadas al conocimiento de las políticas de seguridad de la información y su contenido.

- No se solicita confirmación de conocimiento, lectura y aceptación de la política de seguridad de la información a empleados, contratistas y proveedores.

Organización de la información.

- No ha definido un modelo de gobierno formal que detalle los roles y las responsabilidades de gestión de seguridad de la información y la protección de datos personales.

- En la actualidad existen responsabilidades dispersas y ausentes sobre la seguridad de la información, lo cual impide su adecuada gestión:

    - No se encuentra constituido y operando un comité de seguridad de la información que dicte la estrategia de seguridad de la empresa.

    - No se ha asignado de manera formal el rol de Oficial de Seguridad de la Información

    - Las funciones de seguridad y privacidad se encuentran dispersas en diferentes áreas de la organización: Dirección de TIC (gestión de tecnología y seguridad informática); la gestión de accesos y gestión de cambios en los sistemas de información son administrados por diferentes áreas de ESSMAR (sin lineamientos, procesos o administración clara), mientras que las funciones asociadas a la protección de datos personales se encuentran a cargo del área de planeación estratégica.

- Ausencia de una evaluación de riesgos de seguridad sobre los procesos core y sobre la gestión misma de la seguridad de la información.

- Ausencia lineamientos formales asociados a la práctica de teletrabajo y las configuraciones de seguridad que ésta requiere.

- No se restringe el acceso a correo electrónico diferentes al corporativo, por ejemplo, Hotmail y Gmail. Las cuentas de correo personales de los funcionarios son comúnmente usadas para comunicaciones corporativas.

Seguridad de los recursos humanos.

- No se solicita confirmación de conocimiento, lectura y aceptación de la política de seguridad de la información a empleados y proveedores.

- No se tiene definido un plan formal de capacitación y sensibilización constante en aspectos de seguridad de la información.

- No se evidencia un proceso de notificación de cambios de cargos por parte del área de Recursos Humanos a las áreas encargadas de la administración de los sistemas de información.

- En los contratos con proveedores no se identificaron clausulas asociadas a la confidencialidad y seguridad de la información, que restrinja la divulgación de información de la empresa o datos personales por parte del proveedor.

- No se realizan auditorias sobre controles de seguridad implementados por los proveedores para proteger la información de la empresa que custodian o gestionan, tampoco se solicitan reportes de control interno (tipo ISAE3402 /SSAE18/ SOC2).

Gestión de activos.

- No cuenta con un inventario de activos de información críticos para la operación de los procesos de negocio que contenga la clasificación de cada uno según los principios de confidencialidad, integridad y disponibilidad tipo de activo, procesos a los que pertenecen, ubicación, propietarios y usuarios que los utilizan, entre otros.

Adicionalmente, la empresa no cuenta con los siguientes controles o buenas prácticas para la protección de sus activos de información:

- Un procedimiento formal que dicte lineamientos para la gestión y ciclo de vida de los activos de información (desde su levantamiento hasta su evaluación de riesgos).

- No se cuenta con mecanismos de cifrado de datos en los dispositivos de almacenamiento autorizados por la Dirección de TI para su utilización en procesos de negocio.

- No existen lineamientos o controles para la gestión, configuración, cifrado o restricción de dispositivos móviles y medios de almacenamiento removibles como puertos USB, discos duros portables, unidades CD/DVD RW que eviten la posible fuga de información.

- No se implementan mecanismos automáticos para bloquear la salida de archivos con información confidencial mediante correo electrónico.

- No de identifican controles que restrinjan el uso de cuentas de correos públicas (Hotmail, Gmail, Outlook, Yahoo, entre otros), desde los equipos de funcionarios y contratistas de la empresa. Así mismo, no se restringe el acceso a servicios de almacenamiento en nube (como OneDrive, Google Drive, Dropbox, Mega, entre otros).

Las anteriores situaciones podrían facilitar la fuga de información sensible del negocio o datos personales de clientes, proveedores, empleados, entre otros; lo cual podría a su vez causar la aplicación de sanciones por parte de entes de control.

Control de acceso.

- No cuenta con un procedimiento o política de gestión de accesos formal que contemple lineamientos relacionados con la creación, modificación, retiro y revisión periódica de usuarios y privilegios en los sistemas de información.

- El proceso de gestión de accesos se encuentra desagregado en diferentes áreas de la empresa y no se involucra ni es administrado por la dirección de tecnología. Al no encontrarse centralizado, se evidenció la falta de trazabilidad en las evidencias del proceso, dado que las solicitudes de creación de usuarios son realizadas directamente al proveedor por parte de diferentes áreas o lideres encargados.

- No cuenta con una política de contraseña formalmente definida. Así mismo, se identificó una inadecuada configuración de parámetros de contraseñas en los sistemas de información y/o plataformas tecnológicas.

- La Dirección de TICS, no ejerce un gobierno claro sobre el proceso de gestión de accesos (creación, modificación y retiro de usuarios), ni emite lineamientos para la ejecución de estas actividades por parte de los proveedores.

- CONTROLADOR DE DOMINIO:
  No se ha configurado en la red corporativa un directorio activo para la administración de sus computadores y recursos, por lo tanto, no existe una administración centralizada que permita gestionar los recursos en los equipos conectados a la red. Las brechas identificadas aumentan el riesgo de acceso no autorizado, fuga o robo de información crítica de la compañía y/o datos personales de usuarios, proveedores, entre otros.

Criptografía.

- Ausencia de un inventario de activos de información que permita identificar aquellos que requieran procedimientos de encriptación o cifrado.

- No cuenta con políticas divulgadas e implementadas sobre el uso de controles criptográficos para la protección de la información, así como políticas o procedimientos específicos sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.

- Algunos aplicativos críticos de la entidad no cuentan con certificados digitales que permitan garantizar su autenticidad e intercambio seguro de información.

Seguridad física y ambiental.

- No se identificaron controles automáticos de acceso a la empresa y las áreas que procesan información crítica, cómo lectores de proximidad, lectores biométricos, entre otros.

- El centro de cómputo no cuenta con un sistema de control de acceso mediante puertas aseguradas con cerraduras, lector biométrico o de tarjetas de proximidad. Así mismo, no se cuenta con controles ambientales adecuados.

- El área de almacenamiento de archivo físico no cuenta con dispositivos automáticos de control de acceso seguros ni mecanismos para garantizar la integridad de los archivos almacenados (CCTV, sistema de detección y prevención de incendios, entre otros).

- No se realizan mantenimiento preventivos periódicos sobre los equipos y servidores de la empresa.

- No se encuentra configurado el bloqueo automático de sesiones en los equipos, ni se usan guayas de seguridad, lo cual facilita el robo de equipos y/o información almacenada en estos.

Seguridad en las operaciones.

- Se identificó que no existe documentación (procedimientos o guías operacionales) asociada a procesos que soporten la operación del servicio, tales como: gestión de cambios y nuevos desarrollos en los sistemas, gestión de capacidad, gestión de accesos, gestión de backups (definiendo una periodicidad diaria, semanales, mensuales y anuales), gestión de incidentes, gestión de licenciamiento, gestión de cambios organizacionales, entre otros.

- No tiene control y/o gobierno sobre la separación de ambientes de producción, desarrollo y pruebas de los sistemas, y la restricción de acceso de desarrolladores a producción.

- Para las aplicaciones se identificó que solo se cuentan con ambientes de producción y no existen ambientes de pruebas y/o desarrollo.

- Se identificó una ausencia de lineamientos formales para la realización periódica de copias de seguridad (diarias, mensuales, anuales, etc) en los sistemas de información. Así mismo, se identificó que no se realiza respaldo de la información de los servidores.

Por otra parte, se identificaron las siguientes falencias con relación a controles o mecanismos de protección contra amenazas cibernéticas:

- Únicamente el 41% de los equipos de la empresa está protegido por las licencias de antivirus actualmente adquiridas. No se realizan escaneos masivos de ciberamenazas.

- En la actualidad no se están aplicando controles de filtro de contenido para la navegación de usuarios internos y/o externos.

- No cuenta con herramientas para el monitoreo de actividades de los administradores sobre los sistemas Kagua y Treassury y su infraestructura tecnológica.

- No se cuenta con un base de aseguramiento mínimo de configuración estándar de la infraestructura tecnológica (Hardening) propia o administrada por proveedores.

- La entidad no realiza de manera periódica escaneos de vulnerabilidades técnicas o pruebas de Ethical Hacking sobre la infraestructura tecnológica que soporta sus sistemas core.

- No se cuenta con un procedimiento formal para controlar la instalación de aplicaciones en los equipos de la entidad. No se identificaron controles para la ejecución de programas ejecutables portables, lo cual aumenta el riesgo de introducción de código malicioso.

Seguridad de las comunicaciones.

- No cuenta lineamientos formales o controles de seguridad para transferencia de información confidencial hacia entes o destinatarios externos a la red corporativa.

- No cuentan con certificados digitales que permitan garantizar su autenticidad, e intercambio seguro de datos.

- La entidad no ha definido lineamientos formales para el monitoreo proactivo y reactivo de desempeño y disponibilidad de dispositivos de red, que incluya la definición de umbrales y configuración de alarmas requeridas.

- La red no está segmentada en VLANs que permitan restringir el acceso lógico a los servidores de producción y otros recursos o activos de información.

- Para la red inalámbrica, se observó que los equipos conectados de funcionarios, contratistas y visitantes pertenecen al mismo segmentó de red. Esta configuración no restringe el acceso de externos a recursos críticos de la empresa.

Adquisición de sistemas, desarrollo y mantenimiento.

- No cuenta con un procedimiento de gestión de cambios formalmente definido, documentado y divulgado que contemple los lineamientos, actividades y aprobaciones necesarias para controlar los cambios que son implementados sobre los sistemas de información. La empresa, y en particular la Dirección de TICS, no ejerce un gobierno claro sobre la de gestión de cambios implementados por terceros/proveedores sobe los sistemas core.

- Se identificó que la gestión de cambios actual se encuentra desagregada en diferentes áreas de la empresa, quienes solicitan cambios directamente al proveedor sin involucrar a la Dirección de TICS, y dificultando la trazabilidad y evidencias de los mismos.

- Se identificaron cambios desarrollados y/o ejecutados en ambiente de producción del sistema, sin la realización de pruebas previas (en un ambiente de pruebas o QA) por parte de los usuarios solicitantes.

- No cuenta con una política o procedimiento asociado al desarrollo seguro, que establezca lineamientos para el análisis y especificación de requisitos de seguridad de la información en el software a desarrollar.

- No ha definido lineamientos de seguridad mínimos para el software desarrollado por terceros/proveedores.

- No se han realizado auditorías o cuestionarios relacionado con el cumplimiento de controles de seguridad de la información por parte de proveedores de software e infraestructura.

- Dado que la empresa no ejerce un gobierno y control sobre el proceso de gestión de cambios en los sistemas, no se tiene claridad sobre los datos que son usados por los proveedores para la realización de pruebas de cambios, ni de los controles de seguridad empleados para la protección de esta información.

Relación con proveedores.

- En los contratos celebrados con los proveedores no se evidenciaron cláusulas relacionadas con el cumplimiento de políticas de seguridad de la información propuestas por la empresa, avisos de privacidad que expongan las finalidades de la recolección y tratamiento de datos personales, acuerdos para la realización de auditorías relacionadas con el cumplimiento de controles de seguridad por parte de la empresa, entre otras.

- No ha definido los requisitos de seguridad de la información exigidos a proveedores para mitigar los riesgos asociados con sus accesos a los activos de información.

- Al no contar con una política de seguridad formalmente definida, no se solicita explícitamente la confirmación de conocimiento, lectura, aceptación y cumplimiento de la política de Seguridad de la Información de la compañía por parte de proveedores.

- No se contempla de manera contractual la supervisión y seguimiento sobre las actividades ejecutadas por los proveedores sobre los activos de información de la compañía, auditorías y/o realización de cuestionarios de cumplimiento de controles de seguridad de la información.

Gestión de los incidentes de seguridad.

- No cuenta con un procedimiento formalmente definido, documentado y divulgado para la gestión y monitoreo de eventos e incidentes de seguridad de la información, que defina las responsabilidades, actividades y canales disponibles para el reporte, clasificación y gestión de incidentes de seguridad.

- No cuenta con un sistema de gestión de eventos de seguridad de la información (SIEM), que permita monitorear las distintas

plataformas y detectar amenazas de forma centralizada, con el fin de responder de forma oportuna ante la ocurrencia de incidentes.

- La entidad no se relaciona con grupos especializados en seguridad de la información cómo: El grupo de respuesta a emergencias cibernéticas (colCERT), CSIRT de gobierno, Comando Conjunto Cibernético (CCOC), armada nacional, entre otros.

Continuidad del negocio.

- No cuenta con un plan de continuidad del negocio (BCP) formal, que cubra los procesos indispensables para continuar la operación en escenarios de contingencia, así como aspectos de continuidad de la seguridad de la información.

- No cuenta con planes de recuperación ante desastres (DRP) que dicten lineamientos para la recuperación de las TIC en escenarios de contingencia.

- No cuenta con un data center de respaldo en el que se pueda apoyar la operación del negocio en caso de desastres. La Dirección de TICS no tiene conocimiento acerca de los planes, controles o infraestructura de contingencia de los proveedores de los sistemas de información core para la continuidad del servicio.

Cumplimiento con los requerimientos legales y contractuales.

- Al evaluar la actual gestión realizada por la empresa frente al cumplimiento de la ley 1581 de protección de datos personales, se observaron las siguientes falencias:

    - Fallas sobre la debida diligencia demostrable realizada por parte de la alta dirección para asignar recursos humanos y financieros para la implantación del programa de protección de datos personales (PIPDP).

    - La entidad no tiene una identificación formal de las bases de datos personales que recolecta y custodia (usuarios, empleados, proveedores, entre otros), por tanto, en la actualidad no existe

una evaluación del ciclo de vida de los datos para cada una de estas, que permita identificar las finalidades particulares de la recolección, los responsables internos, los flujos transaccionales, las autorizaciones para el acceso a la información personal, el almacenamiento de los distintos flujos de datos, los riesgos asociados y los controles requeridos.

- No existe una adecuada estructura de roles y asignación de responsabilidades para la gestión del tratamiento de datos personales al interior de la empresa.

- No se evidenció una gestión de riesgos específica para la protección de datos personales y que se relacione con las bases de datos identificadas por la entidad.

- No se evidenció un procedimiento interno para otorgar trámite a las peticiones y reclamos relacionados con protección de datos personales

- No se evidenció un programa de capacitación y formación en materia de protección de datos personales.

- No se observa un modelo de evaluación sobre la gestión de protección de datos personales al interior de la Entidad y la alienación que debe existir con el modelo de seguridad de la información.

➢ Se identificó que no existen suficientes controles preventivos para asegurar el cumplimiento de los requisitos propuestos por la ley 603 de 2000 (relacionada con derechos de propiedad intelectual y el uso de productos de software patentados). La empresa no cuenta con controles de escaneo, monitoreo, identificación y desinstalación de software no licenciado o no autorizado en los equipos de los funcionarios.

- No se han definido de manera formal los tiempos de retención para los diferentes documentos que son custodiados en el archivo central.

- No se realizan evaluaciones periódicas independientes sobre la gestión de seguridad de la información y el tratamiento de datos personales, que permitan fortalecer el ambiente de control.

Se sugiere 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).

6.1.5. 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).
- Manual políticas de seguridad ESSMAR E.S.P.
- Modelo procedimiento copias de respaldo.
- Modelo procedimiento de contraseñas.

6.1.6. 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, alumbrado público 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 área de 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 Área de TIC diseño y estructuró el 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.

6.1.7. Directrices

- Verificar que se definan, implementen, revisen y actualicen las políticas de seguridad de la información en la ESSMAR E.S.P.
- Todos los usuarios que hagan uso de los sistemas de información y telecomunicaciones de la empresa tienen la responsabilidad y obligación de cumplir con las políticas, normas, procedimientos y buenas prácticas de seguridad de la información establecidas en el presente plan.
- Diseñar, programar y realizar los programas de auditoría del sistema de gestión de seguridad de la información – SGSI.
- Los jefes de área o dependencia deben asegurarse de que todos los procedimientos de seguridad de la información dentro de su área de responsabilidad se realicen correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información.

6.2. Procedimientos que apoyan la política de seguridad

Los procedimientos que soportan las políticas de seguridad de la información describen de forma más detallada las actividades a

desarrollar de un proceso, en él, se especifica cómo cuales son las actividades, los recursos, la metodología y el objetivo que se pretende lograr o el valor agregado que genera y caracteriza el proceso.

6.2.1. 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).

6.2.2. 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 el sistema, ya que lo único que haría es desgastar a la empresa generando residuos sólidos como papel mal utilizado. Soportado en el documento (TI-P11 Procedimiento Gestión del Cambio).

6.2.3. 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).

6.2.4. 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).

6.2.5. 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).

6.2.6. 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, el Manual de la Políticas de Seguridad de la Información de la empresa de servicios públicos del distrito de Santas Marta ESSMAR E.S.P planificados, para asegurar su conveniencia, eficiencia y eficacia continua. Soportado en el documento (TI-P08 Procedimiento Gestión de Políticas de Seguridad de la Información).

6.3. 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 de la Política de Seguridad de la Información. El proceso disciplinario también se debería utilizar como disuasión para evitar que los funcionarios, contratistas y los otros colaboradores de la empresa de servicios públicos del distrito de Santas Marta ESSMAR E.S.P, violen las políticas y los procedimientos de seguridad de la información. Las investigaciones disciplinarias corresponden a actividades pertenecientes al proceso de gestión de 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:

- No firmar los acuerdos de confidencialidad o de entrega de información o de activos de información.
- Ingresar a carpetas de otros procesos, unidades, grupos o áreas, sin autorización del funcionario.
- No reportar los incidentes de seguridad o las violaciones a las políticas 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 área de las 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 área 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 área 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.

6.4. 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.

6.5. ESTRATEGIAS TIC'S

6.5.1. Actividades

ACTIVIDAD	OBJETIVOS	TIEMPO (ejecución)	SEGUIMIENTO	CONTROL	PRIORIDAD
Copias de seguridad de la información de los funcionarios de la ESSMAR E.S.P.	Programación proceso copias de seguridad de la información creada y almacenada	Largo plazo	Trimestral	Grupo TIC	ELEVADO

ACTIVIDAD	OBJETIVOS	TIEMPO (ejecución)	SEGUIMIENTO	CONTROL	PRIORIDAD
	por los funcionarios de las distintas sedes y áreas de la empresa.				
Revisar y evaluar el tipo de información de los funcionarios de la ESSMAR E.S.P.	Revisar que la información recibida durante el proceso de copias de seguridad, que los datos sea correctos y funcionales.	Largo plazo	Trimestral	Grupo TIC	ELEVADO
Actualizar los procedimientos relacionados a la seguridad de la información	Actualizar los procedimientos existentes aprobados de la gestión de procesos de seguridad de la información. Diseñar procedimientos necesarios o faltantes para el desarrollo de los procesos.	Mediano Plazo	Trimestral	Grupo TIC Oficina de planeación y regulación	MEDIO
Capacitaciones de seguridad informática y seguridad de la información	Desarrollar jornadas de capacitaciones de los temas de seguridad informática y seguridad de la información.	Mediano Plazo	Semestral	Grupo TIC Dirección de Capital Humano	MEDIO

Tabla 1 (Elaboración propia)

6.5.2. Indiciadores

ACTIVIDAD	TAREAS	INDICADORES	META
Copias de seguridad de la información de los funcionarios de la ESSMAR E.S.P.	Realizar un seguimiento al proceso automatizado con la herramienta SharePoint de Office365. Diligenciamiento de actas copias de seguridad de la información en los casos de desvinculaciones, traslados o devolución de equipos.	(N° de copias de seguridad de información realizadas / N° de copias de seguridad de información programadas/solicitadas) *100%	100 %
Revisar y evaluar el tipo de información de los funcionarios de la ESSMAR E.S.P.	Desarrollo de informe relacionando el tipo de información que es almacenada por los funcionarios de la empresa.	(N° de copias de seguridad revisadas / N° de copias de seguridad de información realizadas) *100%	100 %
Actualizar procedimientos relacionados a la seguridad de la información	Revisar los documentos de los procedimientos aprobados para actualizar la información descriptiva de los mismo. Aprobación y publicación de las actualizaciones realizadas en los procedimientos. Crear nuevos procedimientos necesarios para continuar en las	(N° de procedimientos actualizados/ N° de procedimientos documentados) *100%	100 %

	mejoras en los temas relacionados a la seguridad de la información.		
Capacitaciones de seguridad informática y seguridad de la información	Programación de capacitaciones socializando los temas relacionados a la seguridad informática para evaluar el impacto que genera la conciencia sobre la información vital de la entidad. Fechas estimada programación de capacitaciones. Primera jornada abril 2025 y segunda jornada septiembre 2025.	(N° de capacitaciones realizadas / N° de capacitaciones programadas) *100%	2 capacitaciones

Tabla 2 (Elaboración propia)

6.6. 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.

7. 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
Generalidades	Se hizo ajustes en el contenido	2024
Introducción	Se hizo ajustes en el contenido	2024
Definiciones	Se hizo ajustes en el contenido	2024

Ítem que cambió	Descripción del cambio	Año de modificación
Generalidades	Se hizo ajustes en el contenido	2025
Introducción	Se hizo ajustes en el contenido	2025
Definiciones	Se hizo ajustes en el contenido	2025

8. Anexos

N.A.