2024

# MSPI

## MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ESSMAR E.S.P.
EMPRESA DE SERVICIOS PÚBLICOS
DEL DISTRITO DE SANTA MARTA

Oficina Asesora de Planeación Estratégica y Gestión Regulatoria

# RELATO

## ORGANIZACIONAL

"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".

# ELABORÓ Y REVISÓ

**CARLOS SANABRIA**
Profesional Especializado Grupo TIC
Subgerencia Corporativa

**RAFAEL PINEDA**
Profesional Universitario Grupo TIC
Subgerencia Corporativa

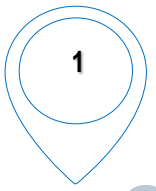
**GERMAN IGUARÁN**
Técnico Administrativo Grupo TIC
Subgerencia Corporativa

**LUIS LOZANO SANTANA**
Profesional Universitario - Adscrito a la Oficina Asesora de Planeación Estratégica y Gestión
Grupo SIG

**PEDRO DIAZ DACONTE**
Profesional Especializado Adscrito a la Oficina Asesora de Planeación Estratégica y Gestión Regulación

**JORGE LÓPEZ ECHEVERRY**
Agente Especial ESSMAR E.S.P.

# TABLA DE CONTENIDO




# INTRODUCCIÓN

Con la institución del Modelo de Seguridad y Privacidad de la Información – MSPI, la ESSMAR ESP busca contribuir a la transparencia del estado, garantizando el aprovechamiento de las herramientas de soporte tecnológico y el uso seguro de la transferencia de datos e información entre los colaboradores internos y partes interesadas.

Este Modelo o MSPI, permite crear un escenario de confiabilidad, fiabilidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos en los procesos de la organización.

El desarrollo del siguiente modelo se materializa a través de un conjunto de acciones e indicadores que permitirán generar logros y resultados en materia de seguridad y privacidad de la información.

## 2 ALCANCE

El Modelo de Seguridad y Privacidad de la Información MSPI, son aplicables para todos los aspectos administrativos y de control a ser cumplidos por los funcionarios, 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 OBJETIVOS

## 3.1 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 todos los funcionarios, contratistas, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con la empresa deberán acatar y cumplir.

## 3.2 Estratégicos

- Planear con base al modelo de Arquitectura TI, el diseño e implementación del proceso Gestión Tecnológica y Comunicaciones de la Entidad.

- Mejorar continua del modelo de Seguridad y Privacidad de la Información con la implementación de la política digital.

# 4 MARCO LEGAL

Son las disposiciones normativas y regulatorias que le dan fundamento al contenido teórico del documento, a continuación, resaltamos las normas más relevantes.

- 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 GENERALIDADES

## 5.1 DIAGNOSTICO

Actualmente en los procesos de mejora continua de seguridad de la información de la empresa, en conjunto con un proveedor de servicios tecnológico con fecha de julio del año 2023 nos entregaron un informe diagnóstico donde evalúan el estado de los procesos de seguridad. Como resultado se desarrollaron documentos para actualizar y optimizar los procesos relacionados a la seguridad de información.

Existen varios procesos por mejorar o incorporar en materia a seguridad de la información de la empresa, a finales de agosto del año 2021 nos entregaron un informe diagnóstico por parte de unos ingenieros asesores que desarrollaron en conjunto una evaluación a la seguridad de la información actual en la empresa. El cual arrojo como resultado una relación de los procesos que habría que mejorar o incorporar para garantizar una seguridad un poco más robusta a la información.

### 5.2.1 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.

### 5.2.2 Modelo sugerido de seguridad de la información

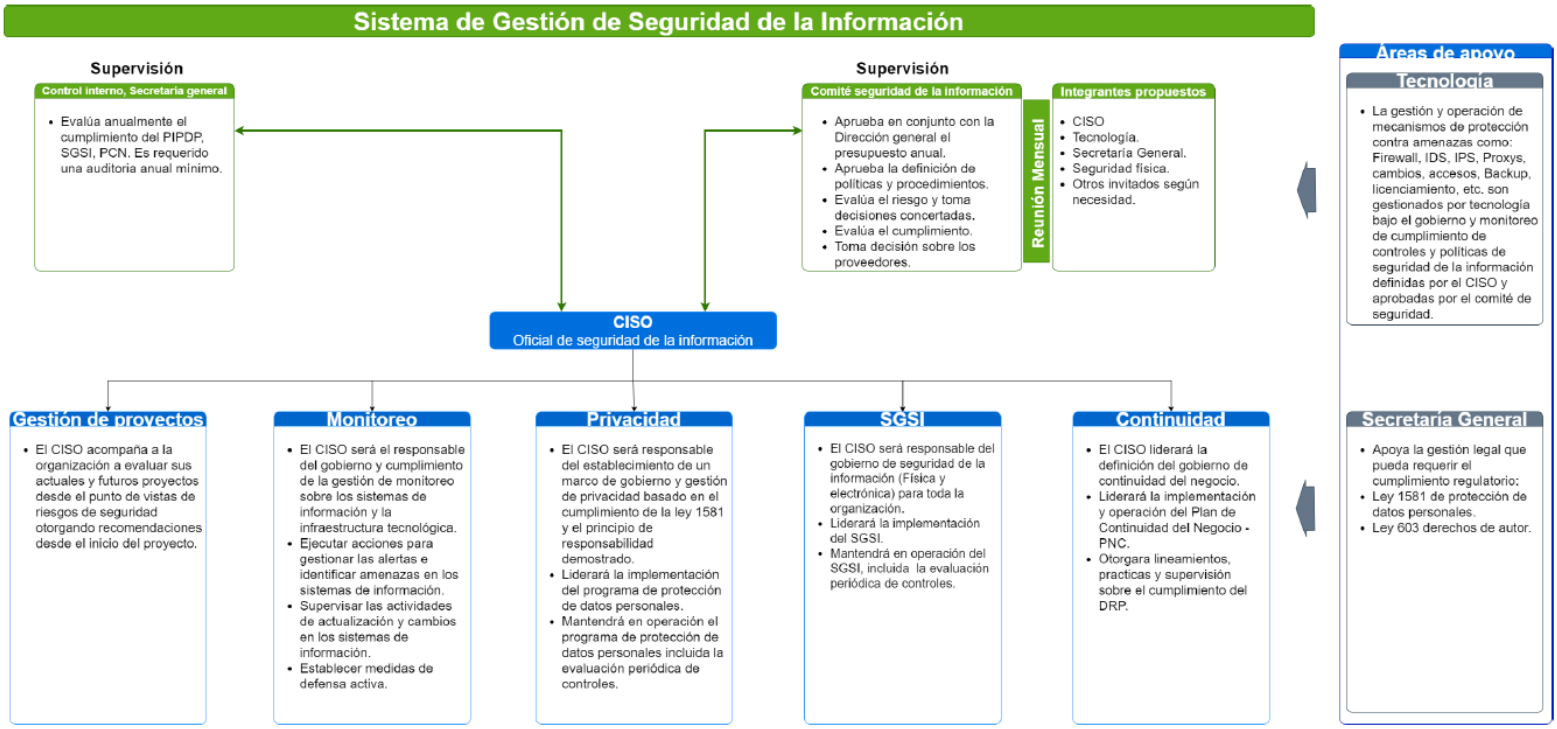
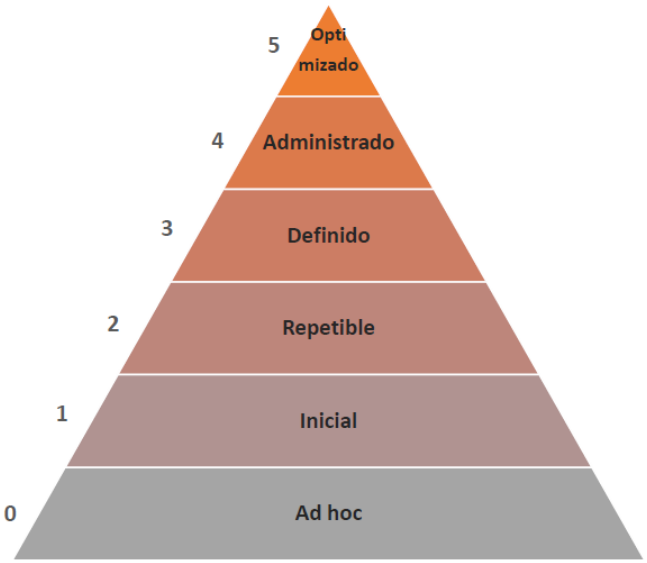



*Imagen tomada del informe final de diagnóstico de seguridad de la información de ESSMAR S.A. E.S.P.*

### 5.2.3 Escalas para la definición del nivel de madurez de la seguridad de la información en ESSMAR



### 5.2.4 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)
- **Inicial.** Existen iniciativas al interior de la entidad para desarrollar los componentes del elemento evaluado
- **Ad Hoc**. No Existe

### 5.2.5 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.

***A5. Políticas de seguridad.***

- No contar o mantener actualizada una política de seguridad de la información formalmente estructurada y divulgada internamente en la empresa y proveedores, la cual debe tener lineamientos clara sobre la gestión de la información teniendo en cuenta los estándares de la norma ISO 27001 o Modelo de seguridad y privacidad de la información (MSPI).

- Pocas capacitaciones de manera periódica orientadas al conocimiento de las políticas de seguridad de la información.

***A6. Organización de la información.***

- Documentar un modelo de gobierno de manera formal definiendo roles y responsabilidad para la gestión de seguridad de la información y protección de datos personales. No existe un orden en las responsabilidades, al no contar con un comité de seguridad de la información donde se planteen estrategias para la empresa. No hay roles específicos para el tema y las funciones en relación están dispersas o no son claras.

- No hay concreto una evaluación de riesgos de seguridad sobre los procesos y gestión de información en la empresa. Faltan lineamientos o configuraciones para la práctica de

teletrabajo. No hay restricción de acceso a correos electrónicos ajenos a los institucionales como Gmail, Hotmail o Yahoo.

### *A7. Seguridad de los recursos humanos.*

- No se cuenta con adecuado cronograma para capacitaciones y sensibilización sobre los temas de seguridad de la información. Poca comunicación para notificaciones de los cambios solicitados para la administración de los sistemas de información. No contar con documento válida para la confidencialidad y seguridad de la información por parte del personal, contratista y proveedores

### *A8. Gestión de activos.*

- No cuenta con un inventario idóneo para la administración de activos o recursos. No cuenta con un documento formal para el procedimiento de ciclo de vida de los activos de la empresa. No existe mecanismos claros de cifrado, bloqueos automáticos y uso de medios de almacenamientos dentro de la empresa, con ello generando posibles riesgos de fuga de información sensible que pueden comprometer la estabilidad del negocio en la empresa.

### *A9. Control de acceso.*

- No se cuenta con un procedimiento formal para los lineamientos de creación, modificación, retiro y revisión de usuarios y privilegios en los sistemas de información. No hay trazabilidad en el proceso de gestión de accesos por las diferentes áreas, falta un control de solicitud de usuarios a proveedores por parte del área de tecnología de la empresa. No hay unanimidad en la asignación de contraseñas para una mayor gestión del uso de las plataformas o recursos.

### *A10. Criptografía.*

- No cuenta con procedimientos, lineamientos o procesos en relación

### *A11. Seguridad física y ambiental.*

- No cuenta con los documentos formales de gestión de cambios y nuevos desarrollos en los sistemas de información, de capacidad, accesos, backups, licenciamientos, entre otros que sean necesarios. No existen claridad o documentación de los ambientes de pruebas por parte de proveedores o la propia empresa.

### *A12. Seguridad en las operaciones.*

- No existe seguimiento en la administración del antivirus, no hay control de filtros de contenido o formalidad del proceso. No se realizan pruebas de vulnerabilidad para detección de fallas o fugas. No existe documentación de procedimiento de control de instalación o eliminación de programas no autorizados.

### *A13. Seguridad de las comunicaciones.*

- No se cuenta con un control formal para la transferencia de información confidencial hacia entes o destinarios externos. Definir lineamientos para la disponibilidad de dispositivos en la red que permitan alarmas tempranas. No tener una adecuada segmentación para los diferentes dispositivos o equipos que se conectan a la red.

### *A15. Relación con proveedores.*

- No hay clausulas claras para el cumplimiento de confidencialidad. No hay documentación clara sobre el manejo o manipulación ejercida por los proveedores a la información de la empresa.

### *A16. Gestión de los incidentes de seguridad.*

- No hay documento del procedimiento de manera formal de la gestión y monitoreo de eventos o incidentes sobre la seguridad de la información donde se contemple roles y responsabilidades claras.

### *A17. Continuidad del negocio.*

- No hay documentado un plan de continuidad del negocio formal, donde se contemplen todos los procesos necesarios para continuidad del negocio en caso de existir contingencias. Faltan lineamientos adecuado para la recuperación de las TICs frente a escenarios adversos de contingencia. No existen un datacenter de respaldo en caso de emergencia.

### *A18. Cumplimiento con los requerimientos legales y contractuales.*

- No hay un control o una clara evaluación al tratamiento de datos personales tanto internos como de usuarios de la empresa. No existe formalidad con los tiempos de retención de la información en custodia en archivo central.

### 5.2.6 Documentación entregada diagnósticos

- 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.

### 5.2.7 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, 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.

### 5.2.8 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.

### 5.2.9 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.

### 5.2.10 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).

### 5.2.11 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).

### 5.2.12 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).

### 5.2.13 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).

### 5.2.14 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).

### 5.2.15 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).

## 5.3 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.

## 5.4 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.

## 5.5 ESTRATEGIAS TIC'S

### 5.5.1 Actividades

| ACTIVIDAD | OBJETIVOS | TIEMPO (ejecución) | SEGUIMIENTO | CONTROL |
|---|---|---|---|---|
| Copias de seguridad de la información de los funcionarios de la ESSMAR E.S.P. | ➢ Programar y realizar copias de seguridad de la información creada y almacenada por los funcionarios de las distintas sedes y áreas de la empresa. | Largo plazo | Trimestral | Grupo TIC |
| Revisar y evaluar el tipo de información de los funcionarios de la ESSMAR E.S.P. | ➢ Revisar la información recibida durante el proceso de copias de seguridad, que los datos sea correctos y funcionales. | Largo plazo | Trimestral | Grupo TIC |
| Actualizar los procedimientos relacionados a la seguridad de la información | ➢ Actualizar los procedimientos revisados y aprobados para la gestión de los procesos de seguridad de la información.<br>➢ Diseñar procedimientos necesarios o faltantes para el desarrollo de los procesos. | Mediano Plazo | Trimestral | Grupo TIC |

| ACTIVIDAD | OBJETIVOS | TIEMPO (ejecución) | SEGUIMIENTO | CONTROL |
|---|---|---|---|---|
| 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 |

### 5.5.2 Indiciadores

| ACTIVIDAD | INDICADORES | PRIORIDAD | META |
|---|---|---|---|
| Copias de seguridad de la información de los funcionarios de la ESSMAR E.S.P. | (N° de copias de seguridad de información realizadas / N° de copias de seguridad de información programadas) *100% | ELEVADO | 820 copias de seguridad |
| Revisar y evaluar el tipo de información de los funcionarios de la ESSMAR E.S.P. | (N° de equipos de cómputo revisados / N° de equipos de cómputo programados) *100% | ELEVADO | 820 equipos |
| Actualizar los procedimientos relacionados a la seguridad de la información | (N° de procedimientos actualizados/ N° de procedimientos programados) *100% | MEDIO | 3 procedimientos |
| Capacitaciones de seguridad informática y seguridad de la información | (N° de capacitaciones realizadas / N° de capacitaciones programadas) *100% | MEDIO | 2 capacitaciones |

## 5.6 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.

# 6 CONTROL DE CAMBIOS

## 6.1 CONTROL DE CAMBIOS HISTÓRICO

| Ítem que cambió | Descripción del cambio | Año de modificación |
|---|---|---|
| Alcance | Se modifica la descripción. | 2022 |
| Generalidades | Se realizó cambios en el marco de las generalidades | 2022 |
| Elaboró y Revisó | Cambiarón los miembros que participaron en el ajuste del documento | 2023 |
| Generalidades | Se realizó cambios en el marco de las generalidades | 2023 |

## 6.2 CONTROL DE CAMBIO DEL PERIODO

| Ítem que cambió | Descripción del cambio | Mes en que se generó |
|---|---|---|
| N/A | N/A | N/A |
| N/A | N/A | N/A |
| N/A | N/A | N/A |
| N/A | N/A | N/A |

# 7 GLOSARIO

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, GoogleDrive, 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.

8

# REFERENCIA BIBLIOGRÁFICAS

MINTIC. (2016). Modelo de Seguridad y Privacidad de la Información. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Obtenido del siguiente enlace: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

MINTIC. (2016). Procedimientos De Seguridad De La Información. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Obtenido del siguiente enlace: https://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf

MINTIC. (2016). Controles de Seguridad y Privacidad de la Información. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Obtenido del siguiente enlace: https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

MINTIC. (2016). Guía de indicadores de gestión para la seguridad de la información. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Obtenido del siguiente enlace: https://www.mintic.gov.co/gestionti/615/articles-5482_G9_Indicadores_Gestion_Seguridad.pdf