TI-Q01 (v1) 2022

POLITICA

SEGURIDAD DIGITAL

Empresa de Servicios Públicos del Distrito de Santa Marta ESSMAR E.S.P.

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

ELABORÓ Y REVISÓ

CARLOS SANABRIA CABRA
Profesional Especializado – Adscrito a Secretaría General
Grupo TICs

RAFAEL PINEDA GARCÍA
Profesional Universitario - Adscrito a Secretaría General
Grupo TICs

JANGEL DAVILA STAND
Profesional Universitario - Adscrito a Secretaría General
Grupo MIPG

YAHAIRA INDIRA DE JESÚS DIAZ QUESADA
Agente Especial ESSMAR E.S.P.

TABLA DE CONTENIDO

1 INTRODUCCION

El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, es la entidad promotora de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones, tiene como finalidad afianzar el máximo aprovechamiento de las tecnologías de la información para ayudar a un estado más participativo, más eficiente y transparente.

Mediante el decreto 1499 de 2017 se diseñó el Modelo Integrado de Planeación y Gestión - MIPG, en el cual resalta la importancia de la implementación de la Política de Seguridad Digital, el propósito de esta política es la protección de amenazas informáticas que pueden impactar negativamente los procesos y la seguridad digital de la entidad.

Para dar cumplimiento a este decreto se realiza la política de seguridad digital, la cual procura dar fortalecimiento, protección y privacidad de la información de los servidores de la Empresa de Servicios Publico del Distrito de Santa marta ESSMAR E.S.P, dando cumplimiento a la normativa legal vigente. Esta política es implementada para garantizar la confidencialidad, integridad y disponibilidad de información y dar confianza a las partes interesadas.

2 ALCANCE

La política de Seguridad digital aplica a todos los procesos de la entidad, así mismo para todos los servidores, contratistas y terceros.

3 POLITICA DE SEGURIDAD DIGITAL

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 comprometida con la protección de 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 digital descritas en el presente documento.

3.1 Objetivos estratégicos

- Establecer directrices generales para la adecuada gestión de la seguridad de la información en la ESSMAR E.S.P.

- Diseñar y ejecutar procedimientos con las acciones necesarias para minimizar la ocurrencia de riesgos, eventos e incidentes asociados a la seguridad de la información en la ESSMAR E.S.P.

- Generar conciencia colectiva sobre la importancia de clasificar, valorar y proteger los activos de información en la ESSMAR E.S.P.

- Garantizar la integridad, confidencialidad y disponibilidad de la información y la protección de las tecnologías de la información y las comunicaciones de la ESSMAR E.S.P.

- Garantizar la implementación de la Política de Seguridad Digital a partir de la definición de roles y responsabilidades.

- Definir los Lineamientos, directrices y prohibiciones que debe llevar la Política de Seguridad Digital

4 LINEAMIENTOS PARA LA IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD DIGITAL

La presente Política de transparencia se realiza con el propósito de dar cumplimiento al Decreto 1499 de 2017 del Modelo Integrado de Planeación y Gestión - MIPG, en la cual dictamina que se debe elaborar e implementar la política de seguridad digital. Estos van de la mano con el CONPES 3854 de 2016 reúne la Política Nacional de Seguridad Digital coordinada por la Presidencia de la República. Esta política es implementada para garantizar la confidencialidad, integridad y disponibilidad de información, que permita brindar confianza a las partes interesadas.

4.1 Compromiso de la alta dirección

La alta dirección de la ESSMAR E.S.P se compromete a apropiar y apoyar activamente la seguridad de la información dentro de la entidad, asignando los recursos necesarios para su desarrollo, generando las herramienta necesarias, que permitan establecer controles

encaminados a prevenir y administrar los riesgos que puedan afectar la seguridad de la información de la entidad.

4.2 Controles de la política de seguridad digital

la ESSMAR E.S.P. cuenta con el sistema de gestión SIGES, donde el área de TIC's tiene documentado procedimientos, manuales y formatos necesarios para minimizar la ocurrencia de riesgos, controles de seguridad de equipos y sistemas de información, eventos e incidentes asociados a la seguridad de la información en la entidad.

A continuación, se relacionan los procedimientos y formatos por medio del cual se operativizan los controles y seguimientos establecidos por el área de TIC para la preservación y confidencialidad de la información de la entidad.

- ✓ TI-P01 Procedimiento Administración Copias de Respaldo.
- ✓ TI-P02 Procedimiento Administración y Mantenimiento de Sistemas de Información.
- ✓ TI-P03 Salidas de recursos tecnológicos.
- ✓ TI-P04 Entradas y retornos de Recursos Tecnológicos.
- ✓ TI-P05 Procedimiento Administración Copias Base de datos.
- ✓ TI-P06 Procedimiento de adquisición de hardware y software
- ✓ TI-P07 Mantenimiento preventivo y correctivo de hardware
- ✓ TI-P08 Gestión de la actualización de políticas
- ✓ TI-F03 Entrega de equipos de cómputo.
- ✓ TI-F04 Entrega de dispositivos.
- ✓ TI-F05 Prestamos de equipos.
- ✓ TI-F06 Verificación de estados de equipos tecnológicos.
- ✓ TI-F07 Entrega correo corporativo.
- ✓ TI-F08 Entrega usuario impresora.
- ✓ TI-F09 Entrega usuario red WIFI.
- ✓ TI-F10 Solicitud de recursos tecnológicos
- ✓ TI-F11 Registro de mantenimientos oficina TIC
- ✓ TI-F12 Registro de soportes TIC
- ✓ TI-C01 caracterización del proceso Gestión TICs.

4.3 Roles y responsabilidades de la política de seguridad digital

ESSMAR E.S.P. define los siguientes roles y responsabilidades para la implementación del MSPI y el cumplimiento de los lineamientos de seguridad descritos en esta política:

ROL / DEPENDENCIA	RESPONSABILIDADES
Alta Dirección	• Garantizar los recursos necesarios (económicos y capital humano) para la implementación y mantenimiento del sistema de gestión de seguridad de la información.
Comité de Gestión y Desempeño	• Aprobar los recursos necesarios para la implementación y mantenimiento del sistema de gestión de seguridad de la información.
Grupo TIC	• Implementar los controles descritos en el plan de seguridad y privacidad de la información que permiten mitigar los riesgos de seguridad de la información.
Capital Humano	• Apoyar que los empleados, contratistas y demás vinculados en la empresa a tomar conciencia sobre sus responsabilidades en la seguridad de la información y estas sean cumplidas.
Control Interno	• Supervisar que la seguridad de la información este incluida dentro de los planes de auditoría institucionales. • Evaluar los riesgos de proceso y de corrupción. • Apoyar en los procesos de posibles violaciones a las políticas de seguridad de la información.
Comunicación Interna	• Comunicar sobre la sensibilización en la seguridad de la información, mediante difusión en los medios dispuestos por la alta dirección.
Grupo Contratación	• Verificar y proteger con el cumplimiento de las medidas de seguridad de la información los activos (procesos, contratos) de información en la gestión con los proveedores y contratistas.
Líderes de Proceso	• Implementar las políticas y procedimientos de seguridad de la información que se definidos como parte del SGSI.
Todos los funcionarios y contratistas	• Apoyar a los líderes de proceso en el desarrollo de tareas garantizando la gestión de activos y gestión de riesgos. • Cumplir idóneamente con las políticas y procedimientos de seguridad de la información definidos y aprobados.

4.4 Implementación de estrategias

A continuación, se describen las estrategias que se implementarán para alcanzar la política de seguridad digital:

- Implementar iniciativas apropiadas para prevenir, coordinar, atender, controlar, generar recomendaciones y regular los incidentes o emergencias digitales para afrontar las amenazas y los riesgos que atentan contra la seguridad digital.

- Brindar capacitación en seguridad de la información y seguridad digital a todos los funcionarios de la entidad.

- Definir, implementar, operar y mejorar de forma continua el Plan institucional de Seguridad y privacidad de la información, soportado en lineamientos claros alineados a las necesidades, a la normatividad y a los requerimientos regulatorios.

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los usuarios, o terceros.

- Aplicar controles de acuerdo con la clasificación de la información salvaguardada y en custodia por cada uno de los funcionarios, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta.

- Realizar ejercicios de auditoría y monitoreo de la operación de sus procesos que involucren la plataforma tecnológica para minimizar los riesgos asociados al manejo de los recursos tecnológicos y las redes de datos.

- Implementar controles de acceso a la información, sistemas y recursos de red.

- Adoptar una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información e implementar estrategias de mejoramiento continuo.

- Elaborar procedimientos de acuerdo con la normatividad que permitan minimizar los riesgos que puedan generar los eventos.

4.5 Generalidades de cumplimiento

En cumplimiento a la ley de delitos informáticos en Colombia (Ley 1273 de 2009) o afectaciones a los activos de información de la ESSMAR E.S.P. y dentro de las estrategias de seguridad de la información, está establecido un proceso disciplinario formal para los

funcionarios que hayan cometido alguna violación de la Política Seguridad Digital de la Información. El proceso disciplinario también se debería utilizar como disuasión para evitar que los funcionarios, contratistas y demás 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 establecidos por la dependencia de TIC. Las investigaciones disciplinarias corresponden a actividades pertenecientes al proceso de gestión disciplinaria adscrito a la Secretaria General de la entidad.

4.6 Prohibiciones y restricciones

A continuación, se describen las 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, estas se encuentran descritas en el plan de seguridad y privacidad de la 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.

- 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.

- Destruir, alterar, eliminar, dañar o suprimir datos informáticos o un sistema de tratamiento de información crítica de la entidad.

- Entregar, enseñar y divulgar información institucional, calificada como información pública reservada y clasificada a personas o entidades no autorizadas.

  COPIAS DE SEGURIDAD – trimestralmente se realiza el proceso de copias de seguridad de la información, según lo establecido en el TI-P01 Procedimiento Administración

Copias de Respaldo, debe garantizarse la entrega de información de uso exclusivo de la entidad. De igual forma mensualmente se realizan copias a los correos institucionales cuando cubre su cuota de almacenamiento. Toda información de la entidad almacenada en dispositivos, equipos o drives en la nube personales deben realizarse sus respectivos respaldos garantizando su disponibilidad de esta. Al momento de desvinculación el funcionario debe entregar la información de la entidad con acta de copia debidamente diligenciada, en caso de que aplique.

- MANEJO DE CORREOS ELECTRONICOS Y DRIVE PERSONALES – restringir uso de correos electrónicos personales o drives para responder, recibir, reenviar o almacenar información de la ESSMAR E.S.P. La programación de reuniones o compartir información debe ser autorizadas y utilizadas por correos institucionales.

- La información debe pertenecer 100% a la entidad, en caso de tener proveedores externos con manejo de información, estos deberán firmar una cláusula de confidencialidad en los contratos sobre el manejo de la información.

5 SEGUIMIENTO, MEDICION Y EVALUACION

El seguimiento y cumplimiento a la presente política estará programado en revisiones periódicas cada vez que sea requerido por la alta dirección. Dichas revisiones se fundamentan en los siguientes aspectos:

- Revisión de indicadores definidos en el plan de acción 2022.

- Revisión de avance en la implementación del Modelo de Seguridad y Privacidad de la Información del Ministerio TIC.

- Revisión de avance de la Política de Seguridad digital de acuerdo con lo solicitado por FURAG o la herramienta autodiagnóstico definida para tal fin.

- Resultados de la medición de desempeño institucional (MDI).

- Matriz de riesgo de proceso y corrupción.

6 COMUNICACIÓN

La divulgación de la Política debe ser transmitida e implementada a través de las diferentes dependencias que conforman la estructura organizacional y jerarquía de la empresa de servicios publico ESSMAR E.S.P., se cargará en la plataforma de la entidad en el módulo MIPG, será visible para todos los funcionarios.

7 MARCO LEGAL Y/O REQUISITOS TECNICOS

- Decreto 1499 de 2017 se crea el nuevo Modelo Integrado de Planeación y Gestión.

- Decreto 2693 de 2012: Lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia que lidera el Ministerio de las Tecnologías de Información y las Comunicaciones, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.

- Decreto 2609 de 2012: Por medio del cual se reglamenta el Título V de la Ley General de Archivo del año 2000. Incluye aspectos que se deben considerar para la adecuada gestión de los documentos electrónicos.

- Ley 1273 DE 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado “de la protección de la información y los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

- Ley 1341 DE 2009: Por medio de la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y comunicaciones - TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.

- NTC 27001:2006: Sistema de Gestión de Seguridad de la Información (SGSI).

- ISO 27002:2005: Esta norma proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar e implantar o mantener sistemas de gestión de la seguridad de la información.

- ISO/IEC 27001:2005: Es la evolución certificable del código de buenas prácticas ISO 17799. Define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información.

8 DOCUMENTOS DE REFERENCIA

- 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