2022

PLAN

SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

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

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

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

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

LUIS LOZANO SANTANA
Profesional Universitario - adscrito a Secretaría General
Grupo SIG

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

TABLA DE CONTENIDO

1 OBJETIVO 2
2 ALCANCE 2
3 RESPONSABILIDAD 2
4 GLOSARIO 2
5 DIAGNÓSTICO DE SEGURIDAD DE LA INFORMACIÓN 3
5.1 Situación actual identificada 3
5.2 Modelo sugerido de seguridad de la información 4
5.3 Escalas para la definición del nivel de madurez de la seguridad de la información en ESSMAR 4
5.4 Resumen informe diagnóstico realizado 5
6 POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN. 8
6.1 Directrices 9
7 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 9
7.1 Política de estructura organizacional de seguridad de la información 9
7.2 Política de seguridad para los recursos humanos 9
7.3 Política de gestión de activos de Información 10
7.4 Política de uso de los activos 10
7.5 Política de uso de Internet 10
7.6 Política de manejo disposición de información, medios y equipos 10
7.7 Política de control de acceso 11
7.8 Política de establecimiento, uso y protección de claves de acceso 11
7.9 Política de uso de puntos de red de datos (red de área local – LAN). 11
7.10 Política de respaldo y restauración de información. 11
7.11 Política de gestión de vulnerabilidades 11
7.12 Política para la Transferencia de Información. 12
7.13 Política de uso de correo electrónico. 12
7.14 Políticas específicas para WEBMASTER. 12
7.15 Políticas específicas para funcionarios y contratistas del área TIC 12
7.16 Política de gestión de los incidentes de la seguridad de la información 12
7.17 Política de revisiones de seguridad de la información 12
7.18 Política de uso de mensajería instantánea y redes sociales. 13
8 PROCEDIMIENTOS QUE APOYAN LA POLÍTICA DE SEGURIDAD 13
8.1 Procedimiento de control de documentos 13
8.2 Procedimiento de control de registros 13
8.3 Procedimiento de auditoría interna 14
8.4 Procedimiento de acción correctiva 14
8.5 Procedimiento de acción preventiva 14
8.6 Procedimiento de revisión del manual de política de seguridad de la información 14
9 PROCESO DISCIPLINARIO 15
10 CUMPLIMIENTO 17
11 CONTROLES 17
12 MARCO LEGAL 17
13 REQUISITOS TÉCNICOS 18
14 REFERENCIA 19

1 OBJETIVO

Establecer de forma clara y coherente las políticas que regulen la seguridad y privacidad de la información de la Empresa de Servicios Públicos del Distrito de Santa Marta ESSMAR E.S.P. y que deberán acatadas y cumplidas por todos los funcionarios, contratistas, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con la Empresa.

2 ALCANCE

Las Políticas de Seguridad de la Información son aplicables en la vigencia 2022 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 la Empresa de Servicios Públicos del Distrito de Santa Marta ESSMAR E.S.P.

3 RESPONSABILIDAD

El personal del área TIC es encargado de socializar y hacer cumplir dichas políticas en cada dependencia y por parte de cada funcionario o contratista sea interno o externo que tenga algún tipo de vinculación con la Organización.

4 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, 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.

5 DIAGNÓSTICO DE SEGURIDAD DE LA INFORMACIÓN

En agosto de 2021 se recibió un informe diagnóstico elaborado por ingenieros asesores sobre el estado actual de la Empresa en materia de seguridad de la información y en el mismo, se establecen una serie de procesos que se requiere mejorar o incorporar para favorecer este tema.

5.1 Situación actual identificada

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

- Ausencia de roles y funciones:

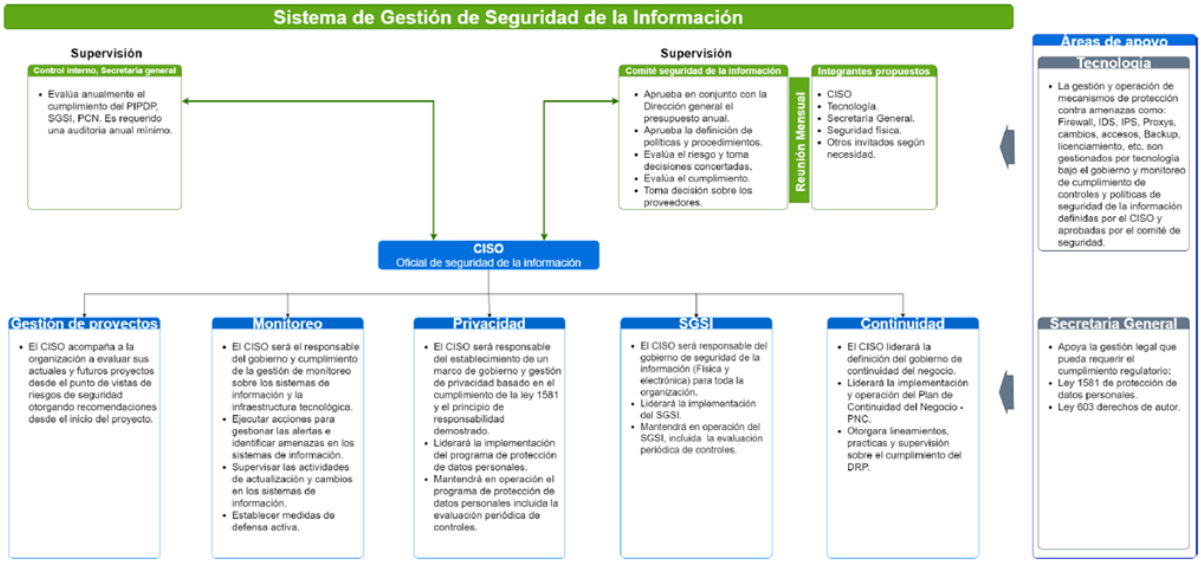
    - No se evidencia una clara asignación de roles y responsabilidades para la gestión de seguridad de la información.
    - No se han definido formalmente controles de seguridad para protección de los activos de información, ni responsables asignados.

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

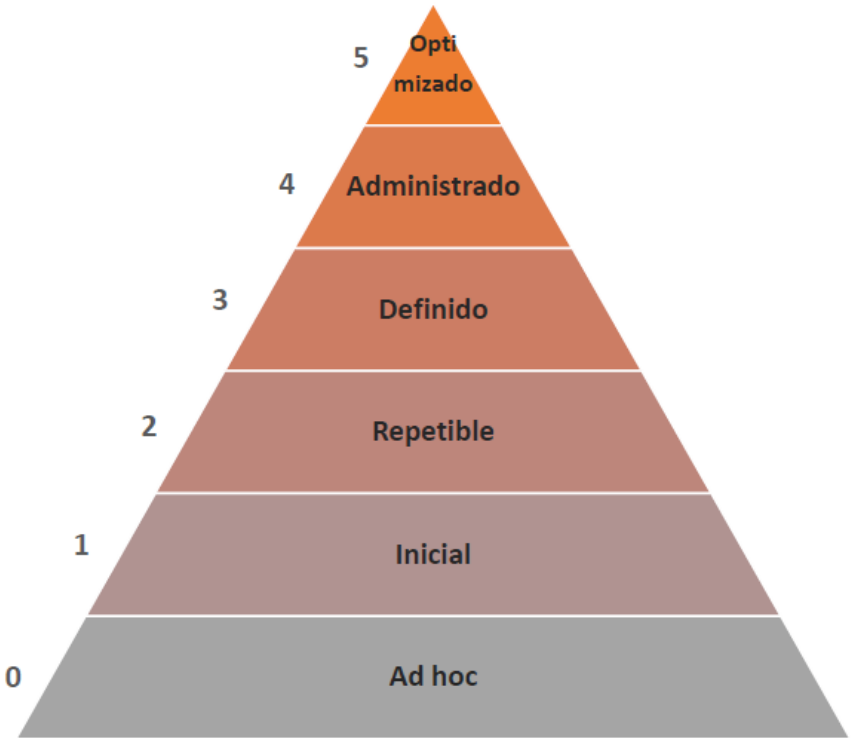
- Responsabilidades: Dispersión de las responsabilidades sobre la gestión y control de la seguridad.

5.2 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.



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



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 de los elementos evaluados 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

5.4 Resumen informe diagnóstico realizado

A continuación, una breve descripción de cada aspecto a mejorar o para incorporar controles. Aclarando que fue el resultado en su momento y se han estado trabajando en la mejora de muchos puntos.

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 válido 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.

A14. Adquisición de sistemas, desarrollo y mantenimiento.

- No existe procedimiento formal para el adecuado manejo al proceso de adquisición.

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.

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 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 descritas en el presente documento.

6.1 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.

7 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

7.1 Política de estructura organizacional de seguridad de la información

El Área TIC debe establecer los roles, funciones y responsabilidades de operación y administración de los sistemas de información de la empresa a los funcionarios, estos roles, funciones y responsabilidades, deberán estar debidamente documentadas, autorizadas y revisadas.

7.2 Política de seguridad para los recursos humanos

El Área TIC implementa acciones para asegurar que los funcionarios, contratistas y demás colaboradores de la empresa, entiendan sus responsabilidades, como usuarios y responsabilidad de los roles asignados, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información y de las instalaciones de software.

El funcionario o contratista debe entregar los activos de información de acuerdo con el procedimiento de terminación de contrato laboral firmando el formato GT-FT004 Seguimiento A Equipos Informáticos seleccionando devolución del equipo, el cual deberá ser verificado por el supervisor del contrato o por el jefe de área que corresponda.

7.3 Política de gestión de activos de Información

El Área TIC es administrador de los activos de información y los responsables de estos activos son los funcionarios, contratistas o demás colaboradores que estén autorizados y manipulen información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware o infraestructura de Tecnología y Sistemas de Información (TIC). Para ello se utilizan formatos de entrega de equipos, información digital o usuarios a plataformas facilitando el monitoreo y control sobre los responsables.

7.4 Política de uso de los activos

La empresa implementa las directrices para lograr y mantener la protección adecuada y uso de los activos de información mediante la asignación a los usuarios finales que deban administrarlos de acuerdo con sus roles y funciones. Los usuarios no deben mantener almacenados en los discos duros de los equipos de cómputo, archivos de vídeo, música, y fotos y cualquier tipo de archivo que no sean de carácter institucional.

7.5 Política de uso de Internet

La empresa permite el acceso a servicio de internet, estableciendo lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los usuarios finales, evitando errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones WEB. Por ello tiene implementado un portal cautivo para garantizar la conectividad a la red wifi de forma independiente a trabajadores y a visitantes.

7.6 Política de manejo disposición de información, medios y equipos

La empresa establece actividades para evitar la divulgación, la modificación, el retiro o la destrucción no autorizada de información almacenada en los medios proporcionados por el área de TIC, velando por la disponibilidad y confidencialidad de la información. Los medios y equipos donde se almacenen procesan o comunica la información, deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento, para ello se debe realizar los mantenimientos preventivos y correctivos que se requieran. Soportado en los planes de copias de seguridad y mantenimientos a los equipos.

7.7 Política de control de acceso

La empresa define las reglas para asegurar un acceso controlado, físico o lógico, a la información y plataforma informática, considerándolas como importantes para el SGSI. La conexión remota a la red de área local debe realizarse a través de una conexión VPN segura suministrada por la entidad, la cual debe ser aprobada, registrada y auditada, por el área TIC.

7.8 Política de establecimiento, uso y protección de claves de acceso

Ningún usuario deberá acceder a la red o a los servicios TIC de la empresa, utilizando una cuenta de usuario o clave de otro usuario. El área TIC suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible. La entrega de usuarios y claves se realizan mediante los formatos respectivos de acuerdo a los requerimientos por líderes de proceso sea para correos corporativos, impresoras, red wifi, plataformas entre otros.

7.9 Política de uso de puntos de red de datos (red de área local – LAN).

Asegurar la operación correcta y segura de los puntos de red supervisado por el área de TIC. Esta actividad se realiza cada cierto tiempo cuando es requerido solucionar inconvenientes por los puntos de conexión o daños en los cables. O cuando se requiere montaje de punto nuevos.

7.10 Política de respaldo y restauración de información.

Proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y software, se pueda recuperar después de una falla, garantizando que la información y la infraestructura de software crítica de la empresa, sean respaldadas y puedan ser restauradas en caso de una falla y/o desastre. La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información y solicitadas a través de la herramienta de gestión de requerimientos establecida por el área TIC. Soportado en el plan de copias de seguridad y plan de tratamiento de riesgo y privacidad de la información.

7.11 Política de gestión de vulnerabilidades

Evitar la utilización de vulnerabilidades técnicas de los sistemas de información y comunicaciones de la empresa, e implementando los lineamientos para gestión de vulnerabilidades. Soportado en el plan de tratamiento de riesgo y privacidad de la información.

7.12 Política para la Transferencia de Información.

Proteger la información transferida al interior y exterior de la empresa, el área TIC, realiza el control del uso de sistemas de transferencia de archivos con herramientas implementadas clave administrador, consola antivirus, entre otras.

7.13 Política de uso de correo electrónico.

Definir las pautas generales para asegurar una adecuada protección de la información de la empresa, en el uso del servicio de correo electrónico por parte de los funcionarios. Todo funcionario (usuario final) no debe dar a conocer su clave de usuario a terceros, sin previa autorización del jefe de área o el área TIC. Los usuarios y claves suministrados por TIC son de uso personal e intransferible. Debe emplearse obligatoriamente las contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación fuerte que posee la entidad de acuerdo con el rol asignado. Se entrega el formato de entrega de correo corporativo.

7.14 Políticas específicas para WEBMASTER.

Proteger la integridad de la página Web institucional, software y la información contenida. Solo tiene acceso el personal a cargo del área de TIC y líder de proceso del área de comunicaciones para gestionar las noticias de prensa.

7.15 Políticas específicas para funcionarios y contratistas del área TIC

Definir las pautas generales para asegurar una adecuada protección de la información de la empresa por parte de los funcionarios y contratistas de TI de la entidad.

7.16 Política de gestión de los incidentes de la seguridad de la información

Asegurar que los eventos e incidentes de seguridad que se presenten con los activos de información sean comunicados y atendidos oportunamente, empleando los procedimientos definidos, con el fin de tomar oportunamente las acciones correctivas. Soportado en el plan de tratamiento de riesgo y privacidad de la información.

7.17 Política de revisiones de seguridad de la información

Garantizar el funcionamiento del sistema de gestión de seguridad de la información de acuerdo con las políticas y procedimientos implementados por el área TIC. Esta área realiza auditorias al sistema de gestión de seguridad de la información, para la verificación y cumplimiento de

objetivos, controles, políticas y procedimientos de seguridad de la Información. Soportado en el plan de tratamiento de riesgo y privacidad de la información.

7.18 Política de uso de mensajería instantánea y redes sociales.

El área TIC define las pautas generales para asegurar una adecuada protección de la información de la empresa, en el uso del servicio de mensajería instantánea y de las redes sociales, por parte de los usuarios autorizados. Por ello se estructuran grupos autorizados para la debida divulgación de la información institucional o labores misionales.

La información que se publique o divulgue por cualquier medio de Internet, de cualquier funcionario, contratista o colaborador de la empresa, que sea creado a nombre personal en redes sociales como: Twitter®, Facebook®, Youtube® Linkedin®, blogs, Instagram®, etc, se considera fuera del alcance del SGSI y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.

8 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.

8.1 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; de igual manera que los documentos existentes en el momento de la evaluación y comprobación del cambio que se implemente como solución a un problema, riesgo o a una oportunidad se conserven. Soportado en el documento (TIC-P010 Procedimiento Gestión de Seguridad de la Información).

8.2 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 (TIC-P011 Procedimiento Gestión del Cambio).

8.3 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. Esta es la razón por la cual se recomienda siempre realizar auditorías internas antes de llevar a cabo la revisión gerencial, ya que para esta última se requiere información sobre el o (los) sistema(s) y los procesos, de tal manera que se pueda evaluar la adecuación, la conveniencia y la eficacia del sistema. 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 (TIC-P09 Procedimiento Formulación y Actualización de Políticas TI).

8.4 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 (TIC-P02 Procedimiento Administración y Mantenimiento de Sistemas de Información y TIC-P03 Procedimiento Mantenimiento Preventivo y Correctivo Hardware).

8.5 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 (TIC-P02 Procedimiento Administración y Mantenimiento de Sistemas de Información y TIC-P03 Procedimiento Mantenimiento Preventivo y Correctivo Hardware).

8.6 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 (TIC-P010 Procedimiento Gestión de Seguridad de la Información y TIC-P012 Procedimiento Gestión de Acceso a la Información).

9 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.

10 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.

11 CONTROLES

Este documento de Políticas de Seguridad de la Información de la empresa de servicios públicos del distrito de Santas Marta ESSMAR E.S.P esta soportado en un conjunto de procedimientos que se encuentran documentados en archivos complementarios.

12 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.

13 REQUISITOS TÉCNICOS

- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.

- Norma Técnica Colombiana NTC/ISO 17799 Código de práctica para la gestión de la seguridad de la información.

- Modelo Estándar de Control Interno MECI 1000 2da versión "Subsistema: Control de Gestión; Componente: Actividades de Control; Elemento: Monitoreo y Revisión e Información".

14 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