Políticas de seguridad de la información

Febrero 2020
ESSMAR E.S.P

Km 7 Troncal del Caribe
Calle 70 N° 12-418 Bodegas Gaira
Telefono: (57+5) 4358201
atencionalciudadano@essmar.gov.co
SantaMarta D.T.C.H.

1. OBJETIVO

Establecer las políticas que regulan 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.

2. ALCANCE

Las Políticas de Seguridad de la Información son aplicables para todos los aspectos administrativos y de control que deben 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. RESPONSABILIDAD

El personal del área TIC's es encargado de hacer cumplir dichas políticas y socializarlas con cada dependencia y personal externo que tenga algún tipo de vinculación.

4. GLOSARIO

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

- **Antivirus:** es una herramienta cuyo objetivo es ayudar a proteger la computadora de amenazas cibernéticas.

- **Virus:** Programas informáticos de carácter malicioso, que buscan alterar el normal funcionamiento de una red de sistemas o computador personal, por lo general su acción es transparente al usuario y este tardo tiempo en descubrir su infección; buscan dañar, modificar o destruir archivos o datos almacenados.

- **Almacenamiento en la Nube:** Del inglés cloud storage, 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, 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.

Km 7 Troncal del Caribe
Calle 70 N° 12-418 Bodegas Gaira
Telefono: (57+5) 4358201
atencionalciudadano@essmar.gov.co
SantaMarta D.T.C.H.

- **Computo forense:** El cómputo forense, también llamado informática forense, es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

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

- **Ingeniería Social:** Es la manipulación de las personas para conseguir que hagan que algo debilite la seguridad de la red o faciliten información con clasificación confidencial.

- **IPS:** Sistema de prevención de intrusos. Es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

- **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 o no controlada como Internet.

- **Ransomware:** Código malicioso para secuestrar datos, una forma de explotación en la cual 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. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN.

La empresa de servicios públicos del distrito de Santas Marta ESSMAR E.S.P., como entidad prestadora de servicios públicos de acueducto, alcantarillado, aseo y alumbrado público, establece que la información es vital para el desarrollo de las actividades del distrito, motivo por el cual, el área de TIC's 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 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

Km 7 Troncal del Caribe
Calle 70 N° 12-418 Bodegas Gaira
Telefono: (57+5) 4358201
atencionalciudadano@essmar.gov.co
SantaMarta D.T.C.H.

documento, fundamentados en la norma técnica colombiana NTC-ISO-27001:2013 y el modelo de seguridad y privacidad de la información.

Directrices:

Verificar que se definan, implementen, revisen y actualicen las políticas de seguridad de la información.

Todos los usuarios 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 manual.

Diseñar, programar y realizar los programas de auditoría del sistema de gestión de seguridad de la información - SGSI, los cuales estarán a cargo de la Oficina de Control Interno.

Los jefes de área o dependencia deben asegurarse 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. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

6.1. Política de estructura organizacional de seguridad de la información

El Área TIC's 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 y distribuidas.

6.2. Política de seguridad para los recursos humanos

El Área TIC's 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.

El funcionario o contratista debe entregar los activos de información de acuerdo procedimiento de terminación o cambio de empleo de acuerdo al formato de Entrega por retiro del servicio o el Informe final de supervisión, el cual deberá ser verificado por el supervisor del contrato.

6.3. Política de gestión de activos de Información

Km 7 Troncal del Caribe
Calle 70 N° 12-418 Bodegas Gaira
Telefono: (57+5) 4358201
atencionalciudadano@essmar.gov.co
SantaMarta D.T.C.H.

El Área TIC's es propietario de los activos de información y los administradores de estos activos son los funcionarios, contratistas o demás colaboradores que estén autorizados y sean responsables por la 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).

6.4. 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 a 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.

6.5. 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.

6.6. 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's, velando por la disponibilidad y confidencialidad de la información. Los medios y equipos donde se almacena, 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.

6.7. 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's.

6.8. 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's suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas

Km 7 Troncal del Caribe
Calle 70 N° 12-418 Bodegas Gaira
Telefono: (57+5) 4358201
atencionalciudadano@essmar.gov.co
SantaMarta D.T.C.H.

de información a los que hayan sido autorizados, las claves son de uso personal e intransferible.

6.9. 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 las TIC's.

6.10. Política de respaldo y restauración de información.

Proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y el 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's.

6.11. 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

6.12. Política para la Transferencia de Información.

Proteger la información transferida al interior y exterior de la empresa, el Área TIC's, realiza el control del uso de sistemas de transferencia de archivos con herramientas implementadas.

6.13. 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 Área TIC's. Los usuarios y claves suministrados por el jefe de TIC's 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 al rol asignado.

6.14. Políticas específicas para Webmaster.

Proteger la integridad de la página Web institucional, software y la información contenida.

Km 7 Troncal del Caribe
Calle 70 N° 12-418 Bodegas Gaira
Telefono: (57+5) 4358201
atencionalciudadano@essmar.gov.co
SantaMarta D.T.C.H.

6.15. Políticas específicas para funcionarios y contratistas del Área TIC's

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.

6.16. 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.

6.17. Política de Revisiones de Seguridad de la Información

Garantizar el funcionamiento del sistema de gestión de seguridad de la información de acuerdo a las políticas y procedimientos implementados por el área TIC's. 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.

6.18. Política de uso de mensajería instantánea y redes sociales.

El área TIC's 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.

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.

7. PROCEDIMIENTOS QUE APOYAN LA POLÍTICA DE SEGURIDAD

Los procedimientos son uno de los elementos dentro de la documentación del Manual de políticas de Seguridad de la Información. Un procedimiento describe de forma más detallada lo que se hace en las actividades de un proceso, en él, se especifica cómo se deben desarrollar las actividades, cuáles son los recursos, el método y el objetivo que se pretende lograr o el valor agregado que genera y caracteriza el proceso.

Km 7 Troncal del Caribe
Calle 70 N° 12-418 Bodegas Gaira
Telefono: (57+5) 4358201
atencionalciudadano@essmar.gov.co
SantaMarta D.T.C.H.

7.1. 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, porque 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 se evidencie la eficacia de las acciones correctivas, preventivas y de mejora que hacen que los procesos se ajusten y evolucionen; de igual manera que los documentos existentes en el momento de la evaluación y comprobación del cambio que se implementó como solución a un problema, riesgo o a una oportunidad se conserven.

7.2. 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.

7.3. 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 sistema y los procesos, de tal manera que se pueda evaluar la adecuación, la conveniencia y la eficacia del sistema de gestión. 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.

7.3.1. 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.

7.3.2. 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

Km 7 Troncal del Caribe
Calle 70 N° 12-418 Bodegas Gaira
Telefono: (57+5) 4358201
atencionalciudadano@essmar.gov.co
SantaMarta D.T.C.H.

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.

7.3.3. 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 su representante, 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.

8. 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 del Área de Talento 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 los computadores encendidos en horas no laborables.

Km 7 Troncal del Caribe
Calle 70 N° 12-418 Bodegas Gaira
Telefono: (57+5) 4358201
atencionalciudadano@essmar.gov.co
SantaMarta D.T.C.H.

- 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 la plataforma tecnológica institucional.

- 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 el área de las TIC's.

- Usar dispositivos de almacenamiento externo en los computadores, cuya autorización no haya sido otorgada por el Área TIC's.

- Permitir el acceso de funcionarios a la red corporativa, sin la autorización de Área TIC's.

- 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.

- El que destruya, dañe, borre, deteriore o suprima datos informáticos o un sistema de tratamiento de información.

- Permitir el acceso u otorgar privilegios de acceso a las redes de datos de la empresa de servicios públicos del distrito de Santas Marta 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 las estaciones de trabajo o equipos portátiles institucionales, cuyo uso no esté autorizado por el Área TIC's

- 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.

Km 7 Troncal del Caribe
Calle 70 N° 12-418 Bodegas Gaira
Telefono: (57+5) 4358201
atencionalciudadano@essmar.gov.co
SantaMarta D.T.C.H.

9. 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 debe prevenir el incumplimiento de las leyes, estatutos, regulaciones u obligaciones contractuales que se relacionen con los controles de seguridad.

10. 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.

11. 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.

Km 7 Troncal del Caribe
Calle 70 N° 12-418 Bodegas Gaira
Telefono: (57+5) 4358201
atencionalciudadano@essmar.gov.co
SantaMarta D.T.C.H.

- 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.

12. 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".

VERSIÓN:	FECHA:	PROYECTÓ	APROBÓ
0	Febrero 2020	Rafael Pineda Apoyo TICS ESSMAR E.S.P.	Carlos Sanabria P.E. TICS ESSMAR E.S.P.

Km 7 Troncal del Caribe
Calle 70 N° 12-418 Bodegas Gaira
Telefono: (57+5) 4358201
atencionalciudadano@essmar.gov.co
SantaMarta D.T.C.H.