PLAN DE SEGURIDAD
DE LA INFORMACIÓN

TABLA DE CONTENIDO

INTRODUCCIÓN

La Alcaldía Distrital de Santa Marta reconoce que la información es uno de los activos más estratégicos para el cumplimiento de su misión institucional, la prestación eficiente de los servicios públicos, la toma de decisiones basadas en datos y la implementación efectiva de la Política de Gobierno Digital. En un contexto de transformación tecnológica acelerada, incremento de amenazas digitales y creciente dependencia de sistemas de información para el funcionamiento del Distrito, se hace indispensable fortalecer la seguridad y la privacidad de la información como pilares fundamentales para garantizar la confianza, la continuidad operativa y la protección de los derechos de la ciudadanía.

El Plan de Desarrollo Distrital "Santa Marta 500+" establece como prioridades estratégicas aspectos esenciales como el acceso al agua potable, la seguridad ciudadana, la sostenibilidad ambiental, el cierre de brechas entre zonas urbanas y rurales, el fortalecimiento del desarrollo económico y la consolidación de un gobierno abierto, participativo y transparente. Estas prioridades constituyen habilitadores claves del desarrollo, y su implementación depende cada vez más de sistemas digitales, datos confiables, plataformas seguras y un ecosistema tecnológico resiliente.

En este marco, la seguridad y la privacidad de la información se convierten en elementos críticos para garantizar la correcta ejecución de dichos propósitos, especialmente en áreas de alto impacto como la gestión de agua, la seguridad ciudadana, la infraestructura, los programas sociales, el ambiente y la participación ciudadana. La protección de los datos que soportan estos sistemas no solo preserva la confidencialidad, integridad y disponibilidad de la información, sino que asegura la continuidad de los servicios esenciales para la comunidad.

Este Plan de Seguridad y Privacidad de la Información se formula en alineación con los lineamientos definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), a través del Modelo de Seguridad y Privacidad de la Información – MSPI, el cual orienta a las entidades públicas hacia la adopción de buenas prácticas, estándares internacionales y una gestión integral del ciclo de vida de la seguridad de la información. Asimismo, se articula con el Modelo Integrado de Planeación y Gestión (MIPG) y con la normatividad vigente, garantizando la incorporación de la seguridad digital en todos los procesos, trámites, servicios y sistemas de información del Distrito.

La Alcaldía reafirma su compromiso institucional con la construcción de un entorno digital seguro, confiable y robusto, que permita avanzar hacia una Santa Marta moderna, sostenible, inclusiva y preparada para los retos del presente y del futuro, especialmente en el marco de la conmemoración de los 500 años de la ciudad. Este plan establece las directrices, responsabilidades, estrategias y controles necesarios para proteger los activos de información, gestionar los riesgos, prevenir incidentes y asegurar que la ciudad continúe fortaleciendo su transformación digital con enfoque de seguridad, transparencia y servicio al ciudadano.

Estado Actual del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI)

La Alcaldía Distrital de Santa Marta ha venido desarrollando un Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) que incorpora políticas, lineamientos y prácticas de protección de la información institucional. Este sistema se enmarca en los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones y avanza hacia su consolidación conforme al Modelo de Seguridad y Privacidad de la Información –

MSPI, el cual orienta a las entidades públicas en la implementación de buenas prácticas y estándares internacionales en seguridad digital.

El análisis institucional evidencia importantes progresos y, al mismo tiempo, diversas áreas con potencial de fortalecimiento, lo cual representa una oportunidad para evolucionar hacia un sistema más robusto, integrado y alineado con las necesidades del Distrito y las exigencias del entorno digital actual. Este enfoque coincide con la práctica utilizada por el MinTIC, donde los planes de seguridad incluyen un diagnóstico para orientar ajustes, priorización de inversiones y mejora continua.

A continuación, se presenta una visión general del estado actual, destacando las capacidades institucionales existentes y los aspectos que se proyecta mejorar para elevar la madurez del SGSPI.

La Alcaldía cuenta con políticas institucionales de seguridad de la información y roles definidos para la gestión tecnológica. Esto constituye una base importante para continuar formalizando un modelo de operación del SGSPI, que integre de forma más amplia a las dependencias, promueva la coordinación interinstitucional y refuerce la toma de decisiones estratégicas en temas de seguridad, tal como lo recomiendan los lineamientos del MinTIC.

La Alcaldía dispone de un inventario de activos de información y una clasificación basada en los lineamientos de la Ley 1712. Como parte del proceso de modernización, se plantea reforzar su actualización permanente y asegurar una articulación más estrecha entre la clasificación y los controles aplicados, especialmente para sistemas estratégicos para el Distrito en ámbitos como la gestión del agua, la seguridad ciudadana y los servicios al ciudadano, coherentes con las prioridades del Plan de Desarrollo Santa Marta 500+

La infraestructura tecnológica cuenta con protecciones fundamentales como antivirus, firewall y mecanismos de respaldo. La entidad se encuentra en proceso de fortalecer estas capacidades mediante la evolución hacia soluciones más integradas y mecanismos avanzados de protección, monitoreo continuo y gestión de actualizaciones, tal como promueven los modelos de seguridad adoptados por el MinTIC.

Actualmente existe un mecanismo de reporte de incidentes a través de la Mesa de Ayuda. Como parte de la mejora continua, se proyecta evolucionar hacia un ciclo más completo de gestión de incidentes que incluya análisis, documentación, retroalimentación y recuperación estructurada, alineado con las buenas prácticas señaladas en los planes oficiales de seguridad digital.

La entidad promueve de manera transversal la sensibilización en buenas prácticas de uso seguro de la información. Se proyecta consolidar un Plan de Capacitación formal y regular, con enfoque en roles y competencias, como sugieren las guías de MinTIC en temas de fortalecimiento de capacidades institucionales en seguridad digital

La Alcaldía aplica los lineamientos legales fundamentales relacionados con protección de datos personales, transparencia y Gobierno Digital. Como parte del proceso de mejora, se contempla fortalecer la matriz de cumplimiento regulatorio, la articulación con la política de datos personales y los procesos de auditoría interna del SGSPI.

El SGSPI de la Alcaldía Distrital de Santa Marta se encuentra en un proceso continuo de consolidación, con bases sólidas y una hoja de ruta clara para su fortalecimiento. Las oportunidades de mejora identificadas permitirán evolucionar hacia un sistema más integral, alineado con el MSPI, con mayor capacidad de prevención, respuesta y resiliencia frente a los riesgos digitales, y con un enfoque estratégico que contribuye al logro de los propósitos del Plan de Desarrollo Distrital Santa Marta 500+.

1. OBJETIVOS

Fortalecer la gestión de la seguridad y privacidad de la información en la Alcaldía Distrital de Santa Marta, garantizando la confidencialidad, integridad, disponibilidad y trazabilidad de los activos institucionales, mediante la implementación de controles, políticas, procesos y mecanismos que permitan prevenir, gestionar y mitigar los riesgos que puedan afectar el cumplimiento de la misión distrital y las prioridades estratégicas definidas en el Plan de Desarrollo.

- **Gestionar riesgos de seguridad digital:** Implementar un proceso formal, continuo y sistemático para la identificación, análisis, valoración y tratamiento de riesgos, conforme a los lineamientos del MinTIC y del MSPI, con el fin de reducir su impacto sobre los servicios institucionales y los sistemas críticos.

- **Prevenir y gestionar incidentes:** Establecer un proceso de gestión de incidentes que permita su detección temprana, respuesta oportuna, mitigación, recuperación y registro, generando lecciones aprendidas que impulsen la mejora continua del SGSI.

- **Identificar, evaluar y clasificar activos de información:** Identificar, clasificar, valorar y asegurar los activos de información, incluyendo sistemas, bases de datos, infraestructura tecnológica y documentación, aplicando medidas técnicas, administrativas y físicas proporcionales a su criticidad.

- **Fortalecer la cultura de seguridad**: Promover la sensibilización, capacitación y formación continua en temas de seguridad, privacidad de datos y ciberseguridad, para todos los funcionarios, contratistas y terceros, fomentando la corresponsabilidad y las buenas prácticas.

- **Garantizar el cumplimiento normativo y regulatorio**: Asegurar que la entidad cumpla con las leyes, decretos, guías y estándares aplicables, incluyendo la normativa de protección de datos personales, las disposiciones del MinTIC y los lineamientos de Gobierno Digital.

- **Impulsar la modernización y transformación digital segura:** Alinear la seguridad de la información con los proyectos estratégicos del Distrito, especialmente aquellos relacionados con agua potable, seguridad ciudadana, sostenibilidad ambiental, movilidad, transparencia y gobierno abierto, garantizando que los sistemas involucrados operen de manera segura y confiable.

2. ALCANCE

El presente Plan de Seguridad y Privacidad de la Información aplica a todos los procesos, dependencias, servicios, sistemas, activos y actores que intervienen en la gestión, tratamiento, almacenamiento y uso de la información en la Alcaldía Distrital de Santa Marta. Su alcance abarca toda la infraestructura tecnológica institucional, los datos generados o administrados por la entidad, y las actividades operativas necesarias para garantizar la protección de la información conforme a los lineamientos del MinTIC, el Modelo MSPI y la normativa vigente.

Cubre todos los aspectos de la información, los datos electrónicos, los datos físicos y cualquier forma de comunicación.

- Se aplica a todos los empleados, contratistas, proveedores y cualquier entidad que interactúe con la información de la organización.
- Incluye todos los sistemas de TI, redes, dispositivos y cualquier infraestructura relacionada que gestione los datos.
- Se enfoca en la protección de datos sensibles y críticos de la entidad, como la información personal, la financiera, la propiedad intelectual, entre otros.
- Considera las normativas y leyes aplicables a la industria y la región específica de la organización.

TÉRMINOS Y DEFINICIONES

Acceso remoto: capacidad de acceder a datos, correo, información y aplicaciones desde fuera del entorno de la entidad.

Activos: cualquier cosa que tenga valor para la entidad se considera un activo; en este caso, la información es un activo.

Activo de información: cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de la Alcaldía Distrital de Santa Marta y, en consecuencia, debe ser protegido.

Amenaza: causa potencial de un incidente no deseado, que puede producir un daño a un sistema

Análisis de riesgos de seguridad de la información: proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

Centros de cableado: son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

Centro de cómputo: Es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.

Ciberseguridad: es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. El término se aplica en diferentes contextos, desde los negocios hasta la informática móvil, y puede dividirse en algunas categorías comunes.

Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados; se encuentra resguardada o salvaguardada en nuestros centros de datos con control de acceso a los usuarios a cada información.

Control: es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

Disponibilidad: es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

Dispositivo móvil: tipo de computadora que presenta las siguientes características:

- Movilidad: puede ser transportado con frecuencia y facilidad.
- Tamaño pequeño: esta característica está ligada a la anterior, para que sea fácil de transportar, su tamaño es pequeño.
- Comunicación inalámbrica: tiene la capacidad de enviar y recibir datos sin ningún tipo de cableado.
- Capacidad de interacción con las personas mediante pantalla y/o teclado.

Equipo de cómputo: dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

Incidente de Seguridad: es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerar, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

Licencia de software: es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

Política: su objetivo es establecer, a partir de la observación de hechos de la realidad política, principios generales acerca de su funcionamiento.

Recursos tecnológicos: son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la Alcaldía Distrital de Santa Marta.

Riesgo: el riesgo es la posibilidad de que ocurra algún evento que impacte los objetivos institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias.

Seguridad de la Información: se entiende el conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información. Dicho de otro modo, son todas aquellas políticas de uso y medidas que afectan al tratamiento de los datos que se utilizan en una organización.

Sistema de Gestión de Seguridad de la Información SGSI: Es el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

Sistema de información: Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software, ya sea de origen interno, es decir, desarrollado por la Alcaldía Distrital de Santa Marta, o de origen externo ya sea adquirido por la entidad como un producto estándar de mercado o desarrollado para las necesidades de esta.

Teletrabajo: trabajo que se realiza desde fuera de las oficinas de la entidad, mediante sistemas de telecomunicación.

Terceros: personas o entidades que se reconocen como independientes.

Usuario: Es la persona que utiliza una utilidad o servicio. Un usuario es un conjunto de permisos y recursos a los que se tiene acceso.

3. RESPONSABLES Y MODELO DE OPERACIÓN SGSPI

La gestión de la seguridad y privacidad de la información en la Alcaldía Distrital de Santa Marta es un esfuerzo institucional que involucra a todas las dependencias, servidores públicos, contratistas y terceros que acceden a los activos de información. El modelo de gobernanza y responsabilidades se fundamenta en las directrices del MinTIC y del Modelo de Seguridad y Privacidad de la Información – MSPI, los cuales establecen la necesidad de estructuras claras de liderazgo, roles definidos, mecanismos de coordinación y procesos de seguimiento continuo.
Este capítulo define los roles, responsabilidades y estructura de operación que permitirán fortalecer la gestión integral del SGSPI y garantizar su sostenibilidad en el tiempo.

3.1. Modelo de Operación del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI)

El SGSPI de la Alcaldía Distrital de Santa Marta se operará bajo un modelo estructurado que articula las etapas del ciclo de vida de la seguridad de la información definidas por el MSPI: Planear, Implementar, Evaluar y Mejorar. Este modelo se compone de instancias de liderazgo, equipos operativos y flujos de gestión que permiten mantener un sistema coordinado y eficiente.

3.2. Estructura del Modelo de Operación

a. Comité Institucional de Seguridad de la Información
es la instancia estratégica responsable de:

- Aprobar políticas, planes y proyectos del SGSPI.
- Definir prioridades institucionales en materia de seguridad digital.
- Hacer seguimiento al avance de indicadores y brechas.
- Articular decisiones con el Comité Institucional de Gestión y Desempeño, en concordancia con MIPG.

Este órgano sigue el equivalente de gobernanza que los planes del MinTIC describen como instancia de dirección del SGSI

b. Responsable de Seguridad de la Información (RSI)

La Alcaldía designará un responsable de la seguridad de la información que tendrá a su cargo:

- Liderar la implementación del SGSPI.
- Coordinar actividades técnicas y administrativas con las dependencias.
- Mantener actualizado el estado del SGSI, riesgos, incidentes y controles.
- Facilitar la adopción del MSPI y los lineamientos del MinTIC.

Este rol corresponde al "líder del modelo" definido en los documentos del MinTIC.

c. Dirección de Tecnologías de la Información y las Comunicaciones (Dirección TIC)

Es la instancia operativa responsable de:

- Administrar la infraestructura tecnológica y los sistemas de información.
- Implementar controles técnicos de seguridad.
- Gestionar incidentes y operar herramientas de monitoreo, antivirus y firewall.
- Soportar técnicamente el plan de continuidad y recuperación ante desastres.

Conforme al MinTIC, esta área es actor clave en la ejecución del modelo.

d. Líderes de Proceso

Cada dependencia deberá:

- Administrar los activos de información bajo su control.
- Clasificar y actualizar la información según su naturaleza y criticidad.
- Reportar necesidades, incidentes, cambios o riesgos detectados.
- Garantizar la adopción de prácticas seguras en su equipo de trabajo.

Este rol está definido como fundamental en la gestión descentralizada del MSPI.

e. Servidores públicos, contratistas y terceros

Todos los usuarios con acceso a información o sistemas de la Alcaldía deben:

- Cumplir con las políticas institucionales de seguridad y privacidad.
- Hacer uso responsable de los recursos asignados.
- Reportar incidentes o anomalías a través de la Mesa de Ayuda.
- Participar en procesos de formación y sensibilización.

Los planes MinTIC destacan que la seguridad es responsabilidad de toda la organización.

3.3. Ciclo de Operación del SGSPI

El SGSPI se gestionará bajo el siguiente ciclo continuo:

3.4. Planear

- Identificación y valoración de riesgos.

- Definición de objetivos, políticas y controles.
- Construcción del portafolio de proyectos del SGSPI.

3.5. Implementar

- Ejecución de controles técnicos, físicos y administrativos.
- Operación de sistemas de monitoreo, copias de respaldo y acceso seguro.
- Capacitación de usuarios y socialización institucional.

3.6. Evaluar

- Seguimiento a indicadores.
- Evaluación del cumplimiento normativo.
- Auditorías internas del SGSPI.

3.7. Mejorar

- Actualización de políticas y procedimientos.
- Ajustes derivados de incidentes, vulnerabilidades o hallazgos.
- Revisión anual del SGSPI.

Este ciclo corresponde directamente a la estructura del MSPI y los planes MinTIC.

3.8. Responsabilidades Institucionales

3.8.1. Alta Dirección

- Impulsar la seguridad de la información como habilitador estratégico.
- Garantizar los recursos para la operación del SGSPI.
- Aprobar políticas, planes y medidas propuestas.
- Integrar el SGSPI con el MIPG y el Plan de Desarrollo Distrital

3.8.2. Secretaría General

- Asegurar la articulación normativa y contractual.
- Incorporar requisitos de seguridad en procesos administrativos y en contratos con terceros.

3.8.3. Dirección TIC (responsable técnico)

- Implementar soluciones tecnológicas de protección.
- Administrar infraestructura y sistemas.
- Monitorear eventos, alertas y vulnerabilidades.
- Coordinar el soporte técnico ante incidentes.

3.8.4. Líderes de Proceso

- Administrar, custodiar y clasificar sus activos de información.
- Garantizar cumplimiento de políticas en sus dependencias.
- Gestionar riesgos operativos dentro de su área.

3.8.5. Oficina Jurídica / Protección de Datos

- Orientar el cumplimiento de la Ley 1581 de 2012.
- Acompañar la gestión de autorizaciones, tratamiento y protección de datos personales.

3.8.6. Oficina de Planeación

- Integrar el SGSPI en la planeación estratégica institucional.
- Asegurar la alineación del plan con el presupuesto y el Plan de Desarrollo Distrital.

3.8.7. Todos los funcionarios y terceros

- Cumplir las políticas.
- Proteger los dispositivos y la información que administran.
- Reportar incidentes oportunamente.
- Participar en procesos de formación.

4. MARCO NORMATIVO

- MINTIC: Seguridad y Privacidad de la Información - Guía No. 2
- Ley 1581 de 2012: Protección de datos personales.
- Ley 1712 de 2014: Transparencia y acceso a la información pública.
- MIPG: Modelo Integrado de Planeación y Gestión

5. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Plan de Seguridad y Privacidad de la Información de la Alcaldía Distrital de Santa Marta establece el conjunto de acciones, políticas, controles y mecanismos institucionales que permitirán proteger los activos de información, garantizar la continuidad de los servicios esenciales y fortalecer la confianza digital en la gestión pública. El plan se fundamenta en los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y en el Modelo de Seguridad y Privacidad de la Información – MSPI, los cuales orientan la adopción de buenas prácticas en toda la administración pública colombiana.

El propósito general del Plan es asegurar que la información institucional se gestione con los principios de **confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad**, contemplando riesgos emergentes, amenazas digitales y las necesidades estratégicas del Distrito consagradas en el Plan de Desarrollo “Santa Marta 500+”.

El Plan está construido bajo un marco estratégico que prioriza:

- La protección de activos críticos asociados a servicios esenciales (agua, seguridad, movilidad, sostenibilidad, servicios ciudadanos).
- La consolidación del SGSPI bajo un modelo de gobernanza definido (Comité, roles, responsables).
- La adopción progresiva de controles técnicos y administrativos modernos.
- La articulación del SGSPI con el MIPG, Gobierno Digital y el MSPI.
- La evolución continua mediante evaluación, auditoría, indicadores y mejora permanente.

5.1. Componentes del Plan de Seguridad y Privacidad de la Información

5.2. Líneas Estratégicas del Plan

El Plan se desarrolla en torno a seis líneas estratégicas, coherentes con los lineamientos de los planes oficiales de MinTIC:

5.3. Fortalecimiento del Modelo de Gobernanza del SGSPI

Incluye acciones para estructurar el modelo de operación, fortalecer el Comité de Seguridad y asegurar la participación de los líderes de proceso en las decisiones estratégicas.

6. Gestión Integral de Riesgos de Seguridad de la Información

Adopción de la metodología MinTIC para riesgos, registro unificado, seguimiento a controles, valoración periódica y articulación con el MIPG.

7. Protección de Activos de Información

Mejoras en la clasificación, inventario, controles de acceso, protección de datos, almacenamiento seguro y gestión de la información durante todo su ciclo de vida.

8. Implementación de Controles Técnicos Avanzados

Modernización tecnológica en seguridad digital alineada a las recomendaciones MinTIC: gestión de incidentes, telemetría, monitoreo continuo, parches, protección perimetral y autenticación reforzada.

9. Continuidad Operativa y Recuperación ante Desastres

Planes actualizados, pruebas programadas, escenarios críticos y priorización de servicios esenciales del Distrito.

10. Cultura Institucional en Seguridad y Privacidad

Programa anual de formación, campañas de sensibilización y fortalecimiento de capacidades.

6.2 Componentes del Plan

Siguiendo la estructura utilizada por el MinTIC, el Plan se organiza en los siguientes componentes:

6.3.1 Identificación

Incluye inventario de activos, clasificación, análisis de riesgos y determinación de controles.

6.3.2 Protección

Acciones preventivas: controles técnicos, acceso seguro, seguridad física, protección de datos personales y gestión de usuarios.

6.3.3 Detección

Monitoreo permanente de eventos, detección de anomalías, telemetría y alertas asociadas a amenazas.

6.3.4 Respuesta

Procedimiento de gestión de incidentes, comunicación, escalamiento y acciones correctivas.

6.3.5 Recuperación

Restauración de servicios, continuidad operativa, recuperación ante desastres y pruebas periódicas.

6.3.6 Mejora Continua

Evaluación del SGSPI, auditorías internas, indicadores, lecciones aprendidas y actualización de políticas.

11. POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Formalizar, documentar y difundir las políticas y procedimientos a todos los funcionarios, aprendices, practicantes, contratistas y proveedores que trabajen directa e indirectamente con la entidad es el primer paso para poder implementar una adecuada seguridad de la información.

La Alcaldía Distrital de Santa Marta reconoce la importancia de identificar y proteger los activos de información de la entidad. Para ello, evitará la destrucción, divulgación, modificación, acceso y utilización no autorizados de toda la información que produce y/o utiliza, independientemente de su soporte, comprometiéndose a implantar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información, mediante el cual se desarrollarán los controles necesarios que permiten salvaguardar los principios de:

- **Confidencialidad:** asegurar que sólo quienes estén autorizados puedan acceder a la información.
- **Integridad**: asegurar que la información y sus métodos de proceso sean exactos y completos.
- **Disponibilidad:** asegurar que los usuarios autorizados tengan acceso a la información cuando lo requieran.
- **Autenticidad:** verificación de identidades y fuentes.
- **Trazabilidad:** registro verificable de actividades y eventos.

La Alcaldía Distrital de Santa Marta declara el cumplimiento de la normativa y legislación vigente en relación con aspectos de seguridad de la información.

Para gestionar la seguridad de la información, la alcaldía conformará un comité de seguridad de la información que tendrá como principal objetivo promover, difundir y apoyar la seguridad de la información, garantizando que la misma sea parte del proceso de planificación, definiendo las estrategias, así como aprobar los planes, políticas y todo aquello que incremente y mejore la seguridad de la información.

Además, designará un responsable de la seguridad de la información, quien se encargará de la guía, implementación, mantenimiento y revisión del sistema de gestión de seguridad de la información.

Es política de la entidad:

- Establecer objetivos relacionados con la seguridad de la información, elaborar y actualizar el plan de acción para la obtención de estos objetivos.
- Desarrollar un proceso de evaluación y tratamiento de riesgos de seguridad e implementar las acciones correctivas y preventivas adecuadas de acuerdo con su resultado.
- Clasificar y proteger la información de acuerdo con la normativa vigente y los criterios de valoración relacionados con la importancia que posee para la entidad.
- Sensibilizar a todo el personal en materia de seguridad de la información.
- Contar con una política de gestión de incidentes de seguridad de la información de acuerdo con los lineamientos establecidos.
- Establecer que todo el personal es responsable de reportar las violaciones a la seguridad, confirmadas o sospechadas, de acuerdo con los procedimientos correspondientes.

- Establecer los medios necesarios para garantizar la continuidad de las operaciones.

Esta política de seguridad de la información se integrará a la normativa de la institución.

Responsabilidades

- La Dirección de TIC será responsable de presentar ante el comité institucional de gestión y desempeño, la documentación, estrategia y propuestas para el mantenimiento y fortalecimiento del SGSI.
- Las secretarías son responsables de apoyar la difusión de la política de seguridad de la información toda vez que el responsable de seguridad de la información así lo solicite y brindar los recursos necesarios para el cumplimiento de esta.
- Todas las dependencias son responsables de la implementación de la política de seguridad de la información y de la adhesión del personal a su cargo.
- El personal, sin importar su relación contractual, es responsable de la adhesión a la política de seguridad de la información de la entidad.

11.1. ACCESO REMOTO

La Alcaldía Distrital de Santa Marta debe garantizar la seguridad de la información cuando se accede remotamente a los sistemas de información de la entidad, tanto por el personal interno (funcionarios, practicantes, contratistas) como proveedores autorizados a trabajar en esta modalidad, y definir las condiciones y restricciones del teletrabajo.

- Definir servicios y sistemas accesibles remotamente.
- Mantener un inventario de accesos remotos autorizados.
- Utilizar comunicaciones seguras y protección contra el software malicioso.
- Revisar periódicamente los accesos remotos y sus condiciones de uso.

11.2. SEGURIDAD FÍSICA Y ACCESO A LAS ÁREAS SEGURAS

La Alcaldía Distrital de Santa Marta establecerá lineamientos generales para controlar el acceso físico a las áreas seguras de la entidad, con el objetivo de minimizar el riesgo de accesos no autorizados.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y la demás infraestructura de soporte a los sistemas de información y comunicaciones, tales como centros de datos (MDF e IDF), se consideran áreas de acceso restringido.

- Proteger servidores, estaciones de trabajo, dispositivos móviles y equipos de red.
- Mantener sistemas actualizados con parches de seguridad.
- Utilizar herramientas corporativas de antivirus, firewall y telemetría.
- Proteger equipos en desplazamiento y trabajo remoto.

11.3. GESTION DE ACTIVOS

La Alcaldía Distrital de Santa Marta debe establecer los criterios de clasificación de la información que esté en poder del organismo sin importar el medio que la soporte.

- Mantener un inventario actualizado de activos (información, infraestructura, aplicaciones y documentos).
- Clasificar la información conforme a su criticidad, riesgos y normativa vigente.
- Aplicar controles adecuados según el nivel de clasificación.

La clasificación de los activos de información en la Alcaldía Distrital de Santa Marta se establece de acuerdo con la Ley 1712 de 2014 de transparencia y del derecho de acceso a la información pública, la cual determina que la información producida por las entidades del estado es de naturaleza pública y en sus artículos 18 y 19, establece su clasificación en pública clasificada y pública reservada.

El nivel de clasificación se determina basado en la confidencialidad como principio rector en la selección, estableciendo un nivel bajo para la información pública, nivel medio para la información pública clasificada y alto para la información pública reservada.

Los lineamientos para la clasificación de la información en la Alcaldía Distrital de Santa Marta se establecen en el Manual de Gestión de Activos de Información (codificación).

Los líderes de proceso son los responsables de clasificar los activos pertenecientes a su proceso. La Dirección de TIC apoya a los líderes de proceso en la clasificación de sus activos dándoles a conocer la metodología de clasificación y aplicación de esta.

Dicha información, permanecerá con tal carácter hasta un período determinado desde su clasificación. Además, su carácter pasará a ser público cuando se extingan las causas que dieron lugar a su clasificación. Sólo se ampliará el periodo de reserva sobre cierta documentación cuando permanezcan y se justifiquen las causas que le dieron origen.

El organismo debe implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad, disponibilidad requeridos, en el marco de lo establecido en la presente política.

11.4. SEGURIDAD PARA LOS EQUIPOS INSTITUCIONALES.

Los equipos que conforman la infraestructura tecnológica de la Alcaldía Distrital de Santa Marta, tales como, servidores, estaciones de trabajo, equipos de redes y telecomunicaciones, central telefónica virtual, dispositivos de almacenamiento, que procesen información, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado, adoptando los controles necesarios para mantener estos equipos alejados de sitios que puedan tener riesgo de amenazas físicas y/o ambientales.

Las medidas tomadas deberán ser proporcionales a los riesgos identificados.

En caso de pérdida o robo de un equipo, el responsable del activo se deberá comunicar con la Dirección de TIC para que esta pueda informar inmediatamente a la autoridad correspondiente y al responsable de seguridad de la información para que lo registre como incidente de seguridad de la información y realice el tratamiento que corresponda.

Alcance

Afecta a toda la infraestructura tecnológica de la entidad, en especial a los centros de datos y áreas relacionadas.

Responsabilidades

- Las secretarías deben velar por el cumplimiento de la presente política y realizar las revisiones oportunas.
- Los directores, coordinadores, jefes de oficinas, líderes de procesos son responsables de disponer de los recursos necesarios para la implementación de la presente política.
- Todos los funcionarios, aprendices, practicantes, contratistas y proveedores son responsables de cumplir con los procedimientos y políticas orientados a la protección y aseguramiento del equipamiento en su poder.

Descripción

Todos los trabajadores son responsables de velar por la seguridad de los equipos propiedad de la entidad, que se encuentren fuera de las instalaciones, siguiendo las siguientes directrices:

- No dejar los equipos de cómputo desatendidos en lugares públicos o a la vista.
- Los equipos de infraestructura deben ser transportados con las medidas de seguridad apropiadas, que garanticen su integridad física.
- Los equipos portátiles siempre deben ser llevados como equipaje de mano.
- El retiro de equipamiento propiedad de la entidad fuera de las instalaciones, debe seguir los procedimientos establecidos, contemplando cláusulas de confidencialidad e integridad de la información sensible que esté contenida en este.

Eliminación o reutilización segura de equipos y medios: La entidad debe identificar los riesgos potenciales que puede generar destruir, reparar o eliminar equipos y medios de almacenamiento. Para ello, debe definir e implementar los mecanismos y controles adecuados para que la información sensible contenida en ellos sea eliminada de manera segura, alineados a la política de destrucción de información.

Cuando un equipo sea reasignado o dado de baja, se deberá asegurar la información para luego eliminarla, con el fin de evitar pérdida y/o recuperación no autorizada de la misma.

11.5. CONTINUIDAD OPERATIVA Y RECUPERACIÓN ANTE DESASTRES

La Alcaldía Distrital de Santa Marta deberá planificar y gestionar la continuidad operativa de los procesos críticos de la entidad ante la eventualidad de ocurrencia de eventos anormales que afecten personas, oficinas y edificios, tecnología, información y proveedores, provocando la disrupción de las operaciones.

Esta política aplica a todos los procesos críticos de la entidad, los recursos que se utilizan para su ejecución, la información que éstos generan o usan, y las instalaciones donde se desarrollan.

Responsabilidades

- Las secretarías son responsables por generar las condiciones adecuadas para la ejecución y comunicación de la presente política, así como por establecer el alcance para su aplicación. Así mismo, de la aprobación de los planes de respuesta, de la designación de un vocero para las comunicaciones externas e internas en ocasión de un incidente disruptivo, y de aprobar el contenido de dichas comunicaciones.
- Los directores, coordinadores, jefes de oficinas y líderes de programas son responsables por la identificación de los procesos críticos, los activos y sistemas que los soportan. Así mismo, de la realización de un análisis de impacto en caso de que los procesos críticos de sus áreas se vieren afectados.
- El comité de seguridad de la información es responsable de revisar el plan de contingencia y de recuperación ante desastres, coordinar formalmente a los diferentes actores para la realización de las pruebas y revisar los informes de las pruebas para establecer el plan de mejora.
- La Dirección de TIC debe participar en la planificación técnica del plan de contingencia y recuperación en caso de desastres, en coordinación con el responsable de la oficina de gestión del riesgo
- Los funcionarios de la entidad deben cumplir con lo establecido en la presente política y deben participar, previa coordinación con las secretarías, en las pruebas que se realicen al plan de contingencia y recuperación ante desastres.

Descripción

La Alcaldía Distrital de Santa Marta comprende que es necesario contar con un plan formal de continuidad operativa y un plan de recuperación en caso de desastres ante eventos anormales, teniendo como premisas fundamentales la seguridad y protección de las personas, los recursos y la información.

- Desarrollar y mantener un plan de continuidad operativa:
  - Procesos críticos relacionados con agua, seguridad, movilidad y servicios ciudadanos.
  - Escenarios de contingencia.
  - Pruebas y ejercicios periódicos.
  - Restauración y retorno gradual a la operación.
- Realizar pruebas periódicas del plan de recuperación ante desastres.

El plan de continuidad operativa deberá considerar el riesgo de interrupción de actividades por eventos tecnológicos, humanos y naturales, originados por causas internas o externas, los que estarán debidamente documentados siguiendo lo establecido en la política de gestión de riesgos. El plan deberá definir la contingencia para los procesos críticos incluyendo ventanas de tolerancia, así como un plan de recuperación para el retorno a la operativa normal de la entidad.

El comité realizará la coordinación formal de las pruebas con los planes con todas las partes involucradas, facilitando la coordinación que deba realizar para la seguridad de la información. Éste será el encargado, en conjunto con las secretarías que sea necesario para la ejecución de las pruebas al plan de contingencia y recuperación en caso de

desastres, informar al alcalde y al comité el resultado de estas, registrar las lecciones aprendidas y confeccionar el plan de acción para la mejora.

11.6. CICLO DE VIDA DE LA INFORMACIÓN

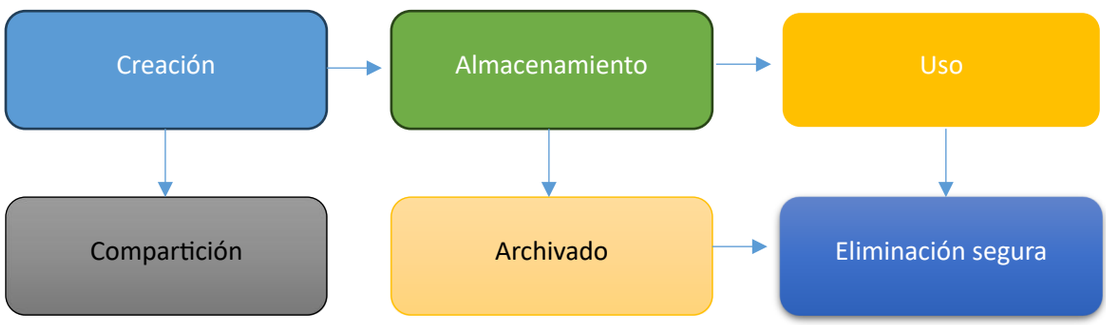
La Dirección de TIC debe garantizar que toda información de la entidad, o en poder de esta, cualquiera que sea su medio de almacenamiento y de acuerdo con su ciclo de vida, sea eliminada de forma segura.

Alcance

Esta política aplica a toda la información de propiedad de la entidad o en poder de esta, según su ciclo de vida.

Responsabilidades

- La Dirección de TIC debe proporcionar los recursos necesarios a fin de contribuir con una adecuada gestión de la información.
- Las secretarías son responsables de velar por el cumplimiento de la presente política y las revisiones que correspondan.
- El propietario del activo de información, o quien este designe, deberá asegurar el adecuado registro del proceso realizado, dejando evidencia del método utilizado e indicando si la operación resultó satisfactoria. Deberá también, informar a La Dirección de TIC para mantener actualizado el inventario de activos indicando la información que fue eliminada.



Descripción

Para completar el ciclo de vida de la información es necesario pasar por el proceso de destrucción de esta. Por lo tanto, se deben definir métodos formales de eliminación segura de la información, de acuerdo con su medio de almacenamiento.

- Gestionar la información desde su creación hasta su eliminación segura.

Se deberán utilizar métodos de borrado seguro de forma que garantice que la información y/o los medios que la contienen no se puedan recuperar. Posibles métodos de borrado seguro son: trituración, desintegración, pulverización, fusión e incineración, des magnetización, sobre escritura, entre otras. Otros métodos, como la utilización de comandos de borrado del sistema operativo algunos tipos de formateo podrían ser métodos no seguros de destrucción de información y permitirían su recuperación.

Durante la destrucción de la información, se debe velar por el cumplimiento del conjunto de políticas que afecten a la información, especialmente las vinculadas a divulgación y acceso.

Registro de las operaciones de borrado

- Deberá existir una solicitud formal, dirigida al propietario del activo de información, indicando en forma unívoca, el medio o la información que requiere destrucción.
- El propietario del activo, o quien éste designe, deberá evaluar si corresponde la destrucción de dicha información tomando en cuenta en los decretos, leyes y otra normativa vigente.
- En cada proceso de destrucción se debe generar un reporte que identifique al personal actuante, la metodología empleada para la destrucción de la información y toda observación que se considere pertinente. Se deberá identificar claramente que el proceso se ha efectuado.
- Aquellas situaciones donde la destrucción de la información no se pueda realizar correctamente, deberán ser documentadas.
- En caso de traslados de soportes físicos, lógicos y/o información almacenada externa a la entidad, hay que asegurar que se cumple la cadena de custodia de estos, para evitar fugas de información, y las demás políticas vinculadas.

11.7. DISPOSITIVOS MÓVILES

La Alcaldía Distrital de Santa Marta deberá proteger la información de la entidad, o en poder de ésta, almacenada o accesible desde los dispositivos móviles.

Evitar que los dispositivos móviles sean foco de infección y distribución de código malicioso dentro de la entidad y prevenir que éstos sean el origen de accesos no autorizados a las redes o recursos privados.

Alcance

Esta política aplica a todos los dispositivos móviles que manejen o accedan a información de la entidad.

Responsabilidades

- Las secretarías son responsables de velar por el cumplimiento de la presente política, así como de establecer los mecanismos de revisión apropiados.
- Los directores, coordinadores, jefes de oficinas, líderes de procesos son responsables de planificar acciones de sensibilización a su personal y proveedores autorizados respecto a la importancia de esta política.
- La Dirección de TIC es responsable por proveer los medios técnicos para el cumplimiento de la presente política.
- El personal y proveedores autorizados para utilizar dispositivos móviles son responsables por cumplir con lo establecido en la presente política.

11.8. FINALIZACIÓN O CAMBIO EN LA RELACIÓN LABORAL

Los servidores públicos y contratistas de la Alcaldía Distrital de Santa Marta deben cumplir con las responsabilidades y deberes de seguridad de la información.

Alcance

Todo el personal, independientemente de su rol funcional o su relación contractual.

Responsabilidades

- Las secretarías son responsables de difundir la presente política a todo el personal, independientemente del cargo que desempeñen.
- El responsable de seguridad de la información debe velar por la difusión y cumplimiento de la política, siendo el director, el responsable principal y último sobre dicho cumplimiento.
- La Dirección de Capital Humano será responsable de comunicar en tiempo y forma las finalizaciones o cambios en los vínculos a la unidad de sistemas de información y al servicio de seguridad del edificio, para que se deshabiliten los accesos lógicos y físicos que correspondan.

Descripción

Deberán retirarse los permisos de accesos lógicos y físicos, y niveles de autorización a toda persona que finalice o cambie su relación funcional o contractual. Todo usuario de servicios que posean claves de acceso o niveles de autorización y que finalizan su relación laboral ya sea en forma definitiva o transitoria (ej. destitución, renuncia, licencia sin goce de sueldo por períodos prolongados, finalización de contrato); así como aquellos que cambien su relación funcional (ej. pase en comisión, comisión de servicio “permanente”, traslados.) se le deberán retirar los permisos y niveles de autorización que ostenten hasta ese momento.

Este retiro deberá incluir:

- Correo Institucional: se dará de baja la cuenta de correo electrónico que para los fines institucionales se le otorgó oportunamente.
- Se eliminará el usuario de las listas de distribución de correo electrónico y grupos de trabajo.
- Otras aplicaciones: el usuario será dado de baja de todos los accesos a las diferentes aplicaciones en las que se encuentre activo
- Acceso a la red institucional: se bloqueará el acceso a la nube institucional, y toda otra forma de acceso a archivos, carpetas y otra información compartida.
- Ingreso Físico: se le retirará a la persona el acceso a las diferentes áreas físicas de la entidad a las que estaba autorizado a acceder.

La inhabilitación (ya sea temporal o definitiva) debe realizarse inmediatamente al momento del cese, por lo cual las comunicaciones deberán efectuarse oportunamente, siendo responsables las áreas intervinientes.
Se debe definir un procedimiento específico que garantice el cumplimiento de la presente política.

11.9. PROTECCIÓN CONTRA SOFTWARE MALICIOSO

La Dirección de TIC se asegurará de que la información y los sistemas informáticos que la procesan estén protegidos contra software malicioso (por ejemplo: virus, gusanos, troyanos, spyware, adware intrusivo, crimeware, entre otros).

Alcance

Todos los sistemas informáticos que soporten los procesos de la entidad.

Responsabilidades

- Las secretarías son responsables de velar por el cumplimiento de la presente política y realizar las revisiones oportunas.
- La Dirección de TIC es responsable de la gestión técnica relacionada con la presente política.
- Los funcionarios, aprendices, practicantes, contratistas y proveedores deben cumplir con lo establecido en la presente política.

Descripción

Se debe utilizar una solución de antivirus corporativo que cumpla con los siguientes:

- Incluir dispositivos móviles como parte de la solución.
- Implementar la seguridad en la navegación por la web y el correo electrónico.
- Que cuente con un firewall como escudo de seguridad.
- Implementar y actualizar medidas de protección contra software malicioso.

La entidad debe:

- Definir procedimientos y responsabilidades de gestión para la protección de los sistemas ante software malicioso.
- Brindar capacitación al personal afectado en la operación y uso de la solución antivirus, así como cualquier otro mecanismo utilizado para la detección de software malicioso.
- Concientizar a los usuarios finales sobre las formas en las que se puede adquirir el software malicioso, los riesgos y problemas que acarrea, así como sobre el procedimiento que se debe seguir en caso de sospechar o constatar estar afectado (tanto en los equipos informáticos a los cuales accede regularmente como en otros en los que haya detectado su presencia). Este procedimiento debe estar formalizado y difundido a nivel de todo el organismo.
- Contar con controles que prevengan y detecten el uso de software no autorizado (por ejemplo, lista blanca de aplicaciones), ya que estos pueden abrir la puerta a software malicioso.
- Contar con controles que eviten el acceso a sitios web maliciosos y/o no autorizados (por ejemplo, listas negras).
- Analizar periódicamente los sistemas informáticos en búsqueda de software malicioso.
- Analizar periódicamente los logs de los sistemas en búsqueda de actividades inusuales.

Todo equipo informático, tanto de escritorio, portátil, estaciones de trabajo y/o servidores, debe estar protegido por una solución técnica residente en el equipo contra software malicioso, gestionado de forma centralizada. Esta solución técnica, así como la base de datos y registro de las amenazas a detectar, deben estar actualizadas y acompañarse de un procedimiento que coadyuve hacia un comportamiento preventivo de los usuarios, así como del personal especializado de TI.

11.10. GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

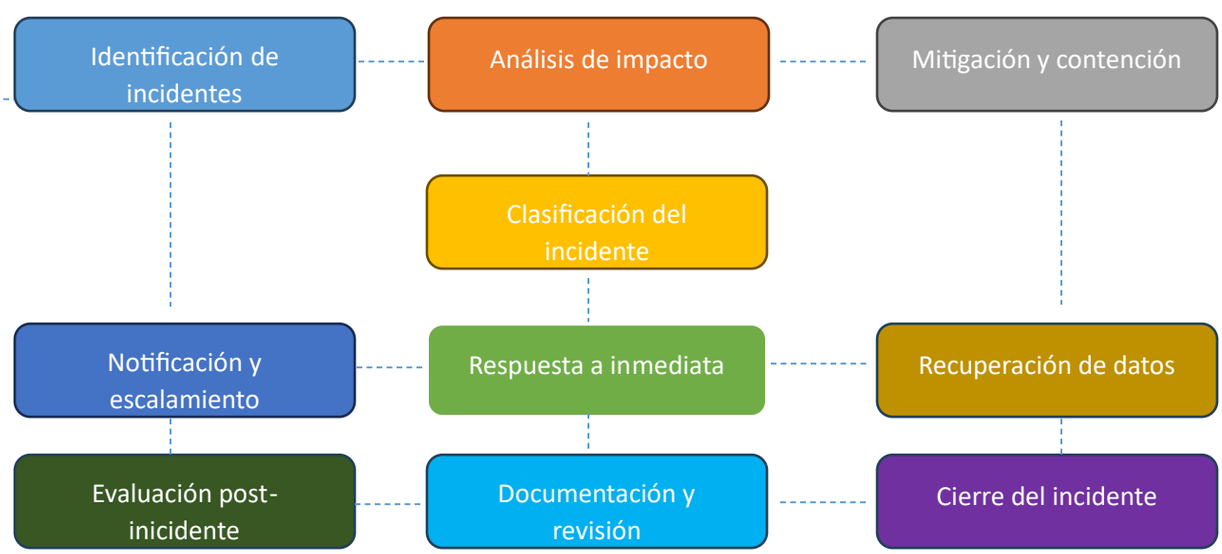
La Alcaldía Distrital de Santa Marta debe establecer lineamientos generales para la gestión de incidentes de seguridad de la información, con el fin de prevenir y mitigar el impacto de estos; basándose en el contexto de la entidad, concientización, reducción en tiempos de respuesta, estrategias para la recuperación y la generación de una base de conocimientos con lecciones aprendidas de eventos e incidentes.

Alcance

Toda persona que tenga legítimo acceso a los activos de información de la entidad, incluso aquellos gestionados mediante contratos con terceros y lugares relacionados.

Responsabilidades

- Todas las secretarías de la entidad son responsables por difundir la presente política a todo el personal, independientemente del cargo que desempeñe o su relación contractual y de brindar los recursos necesarios para el cumplimiento de esta.
- Los directores, coordinadores, jefe de oficinas son responsables de la seguridad de la información, la ejecución de los planes y demás actividades vinculadas a la gestión de incidentes y debe velar por el cumplimiento de esta política y realizar las revisiones periódicas y oportunas.
- Los funcionarios, aprendices, practicantes, contratistas y proveedores son responsables por dar cumplimiento a la presente política y reportar los eventos de seguridad que detecten, siguiendo los procedimientos operativos establecidos para tal fin.



Descripción

Es responsabilidad de cada uno de los funcionarios, contratistas, aprendices y practicantes de la entidad reportar de forma inmediata los eventos, incidentes o debilidades en cuanto a la seguridad de la información por medio de la mesa de ayuda.

- Establecer un proceso claro para la gestión de incidentes de seguridad.

11.11. CORREO ELECTRÓNICO

La Alcaldía Distrital de Santa Marta, entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre los funcionarios y terceras partes. Por lo anterior proporcionará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

- Definir políticas de uso seguro del correo electrónico e internet.

Alcance

Todo funcionario y/o contratista que tenga legítimo acceso al uso del correo electrónico institucional.

Responsabilidades

La Dirección de TIC debe establecer e implantar controles o filtros que permitan detectar y proteger la plataforma de correo electrónico contra contenido o código malicioso que pudiera ser adherido y/o transmitido a través de los mensajes.

Descripción

Los mensajes y la información contenida en los correos electrónicos que sean emitidos desde la Alcaldía Distrital de Santa Marta a su entidad adscrita, dirigidos a direcciones de correo electrónico externas, que contengan información confidencial con el desarrollo de las labores y funciones de cada usuario en apoyo al objetivo misional de la Alcaldía Distrital de Santa Marta, deben incluir una nota (Disclaimer) como: *La información contenida en este mensaje es confidencial y tiene como único destinatario la persona a quien está dirigida* y en su defecto: *El sistema para el control de virus implementado, no asume ninguna responsabilidad por virus que pueda llevar este mensaje o sus anexos*. El correo institucional no debe ser utilizado para actividades personales.

Los mensajes y la información contenida en los buzones de correo son propiedad de la Alcaldía Distrital de Santa Marta y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

Los usuarios de correo electrónico institucional tienen prohibido el envío de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición

humana y resulten ofensivas para los funcionarios de la institución y el personal provisto por terceras partes.

No es permitido el envío de archivos que contengan extensiones ejecutables, en ninguna circunstancia; a excepción de los que, por su importancia, envíen los proveedores y/o contratistas que brindan soporte a los sistemas de información bajo contrato vigente.

Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definidos por la Alcaldía Distrital de Santa Marta y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

11.12. INTERNET

La Alcaldía Distrital de Santa Marta debe regular el uso de Internet en la entidad. Se considera Internet como una herramienta valiosa para la entidad, por lo que su uso está permitido y se promueve en tanto es compatible y contribuye al cumplimiento de las metas y objetivos estratégicos. Sin embargo, su uso indebido representa un riesgo por el impacto negativo que puede tener. Por tanto, deberán monitorearse y controlarse las conexiones que se realicen.

Alcance

Esta política aplica a todas las personas (ej.: personal, proveedor, organismos públicos, organismos internacionales, etc.) con acceso al servicio de Internet de la entidad.

Trazabilidad de registros

Toda actividad que se realice a través de Internet será monitoreada y se generarán registros con la trazabilidad de las conexiones, los cuales podrán ser revisados y analizados en oportunidad de un incidente o para análisis estadístico.
Estos registros serán entregados al responsable de seguridad de la información o al secretario que los solicite, bajo petición escrita y fundada, y su contenido será de conocimiento de los referidos y del personal técnico responsable de extraerlos de los sistemas de información.
Dichos informes no podrán ser divulgados y se tomarán las previsiones pertinentes respecto a su archivo y custodia.

Disponibilidad de servicios

Se proporcionará acceso a Internet con una serie de servicios básicos que incluyen:

- Libre navegación por los sitios cuyo contenido no esté comprendido dentro de las prohibiciones o limitaciones dadas por una norma legal aplicable o por esta política.
- Acceso a servicio de correo electrónico.
- Acceso al Servicio de Mensajería Instantánea.

La ampliación de servicios asignados a las personas alcanzadas por esta política debe gestionarse por escrito por el jefe o supervisor donde se desempeña y deberá obtener el aval técnico del área que corresponda.

La ampliación o reducción de servicios de internet, es revocable en cualquier momento por disposición del jefe de oficina y a petición fundada de los supervisores o el responsable de seguridad de la información.

Uso aceptable

El uso de Internet:

- Debe estar acorde con el marco legal vigente, respetando pautas establecidas.
- Debe tener como principal utilidad servir como herramienta para cumplir las tareas asignadas. El uso fuera de esta situación no debe interferir con el desarrollo de la actividad laboral.
- Debe estar regido por los principios de buenas prácticas, la moral y ética, así como en procura de un mejor desempeño y productividad de quien lo haga.

Uso inaceptable

El uso de Internet considerado inaceptable puede comprender la pérdida del acceso, dar lugar a la revocación de permisos sobre internet, una investigación administrativa y/o las sanciones legales aplicables.

Sin ser una lista taxativa, se consideran uso inaceptable del servicio de internet los siguientes:

- Descargar material con expresa y manifiesta propiedad intelectual u otros derechos necesarios para dicha descarga o uso, sin los permisos necesarios, las licencias que correspondan o cualquier otro formalismo que deba cumplirse y se omite intencionalmente.
- Utilizar Internet para almacenamiento, divulgación o transmisión de cualquier información, archivos, documentos, imágenes, sonidos u obras que puedan infringir el marco normativo vigente referido a propiedad intelectual, marcas o patentes.
- Involucrarse o participar de cualquier manera en actividades ilícitas en cualquier sitio y desde cualquier dispositivo conectado a la red desde el servicio de Internet.
- Divulgación de información deliberadamente falsa, sensible o difamatoria sobre personas o instituciones en cualquier sitio o herramienta disponible en línea (correo electrónico, webs, wiki, redes sociales, chat, foros, etc.).
- Hacer uso del servicio de internet sin contar con herramientas básicas de resguardo y seguridad, instaladas en el computador o dispositivo a emplear, a saber: antivirus y las actualizaciones del sistema operativo que posea el computador o dispositivo. La validación de estas condiciones será determinada y pueden consultarse en el área técnica.
- Hacer uso de herramientas de software instaladas que habiliten servicios potencialmente riesgosos para la entidad. La validación de estas condiciones debe consultarse con el área técnica.
- El uso del servicio de internet en situaciones que afecten la dignidad humana tenga carácter discriminatorio u ofensivo, sean usados para amenazar y generar persecuciones a personas o empresas, generen situaciones de acoso laboral, sexual, contrarias a la moral, pornografía o similares.

Recursos institucionales de conectividad

La Alcaldía Distrital de Santa Marta se reserva el derecho de establecer la prioridad para la prestación del servicio de acceso a Internet y sus servicios en función de necesidades propias. Los usuarios del servicio aceptan tácitamente esta pauta de prestación de este.

11.13. USO INSTITUCIONAL DE REDES SOCIALES

La Alcaldía Distrital de Santa Marta debe gestionar de manera segura los perfiles de redes sociales utilizados por la entidad.

- Regular el uso de redes sociales para proteger la imagen y la información de la entidad.

Alcance

Todos los perfiles de carácter institucional utilizados por la entidad en las redes sociales.

La Alcaldía Distrital de Santa Marta, puede crear su perfil oficial en las redes sociales (por ejemplo: Instagram, Facebook, Twitter, YouTube) para dar a conocer sus programas, actividades y otros temas de interés, y para tener un contacto directo con la ciudadanía o clientes, y de esta manera poder conocer sus necesidades y requerimientos. No obstante, se debe cumplir con los lineamientos expresados a continuación.

- La entidad no se hace responsable de los sitios web no propios a los que se puede acceder mediante vínculos (links) desde nuestros perfiles o de cualquier contenido puesto a su disposición por terceros, que incluyan fotos, documentos, vídeos y otros contenidos.
- Si se detecta un contenido potencialmente inseguro, se debe reportar al responsable de seguridad de la información y eliminar si corresponde.
- Se debe tener claramente identificadas las personas (y sus correspondientes usuarios) con acceso a los perfiles en redes sociales, debiendo estos corresponder con cuentas institucionales y no personales.
- Las cuentas utilizadas para la recuperación de los datos de acceso deben ser institucionales.
- Se deberá seguir las pautas y procedimientos definidos por la entidad, para el traspaso de usuarios en casos de cambio o desvinculación de los administradores de los perfiles.
- Siempre que la red social lo permita, se debe verificar la cuenta, de manera de garantizar a los ciudadanos o clientes que es la cuenta oficial de la entidad.
- La contraseña utilizada en cada cuenta de red social debe ser diferente; la misma deberá ser una contraseña segura conforme a las pautas establecidas en las políticas vigentes.

Responsabilidades

- Las secretarías son responsables por difundir la presente política a todo el personal, independientemente del cargo que desempeñe o de su relación contractual.

- El responsable de seguridad de la información debe velar por el cumplimiento de la presente política. Deberá identificar y promover los controles de seguridad de la información para habilitar el acceso a un proveedor a los activos de información.
- La Oficina de Comunicaciones Estratégicas debe velar por el contenido de lo que se publica en las redes sociales de carácter institucional.

11.14. COPIAS DE RESPALDO

Esta política define la estrategia para gestionar las copias de respaldo de información y de las aplicaciones de la Alcaldía Distrital de Santa Marta y tiene como objetivo asegurarse de obtener un respaldo de la información contenida en los servidores a fin de que, en caso de una eventualidad, se pueda continuar con la operación de la entidad.

La información de los servidores y demás sistemas será respaldada mediante un método de copia de seguridad adecuado, igualmente, se debe utilizar un medio de almacenamiento apropiado o cualquier otro medio reconocido.

- Realizar y mantener copias de respaldo de la información crítica.

Alcance

Toda la información generada y/o procesada por la entidad de carácter institucional, con previa autorización del propietario o custodio del activo.

Responsabilidades

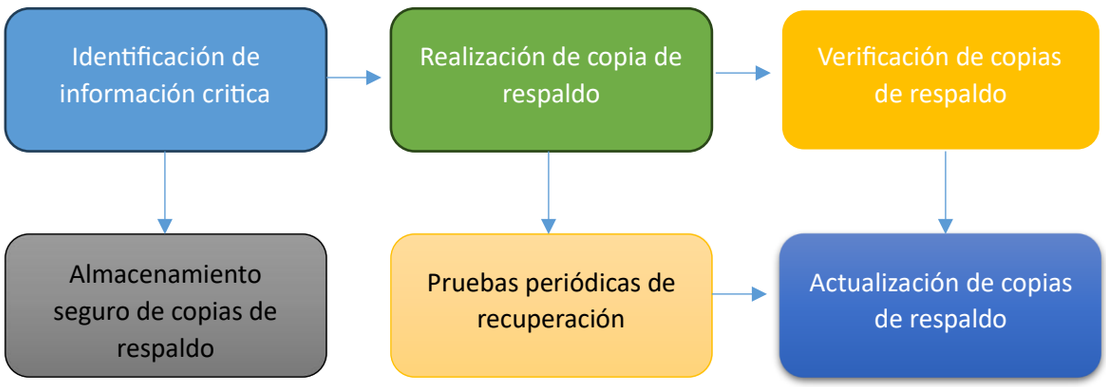
- Las secretarías son responsables por difundir la presente política a todo el personal, independientemente del cargo que desempeñe o de su relación contractual.
- Los funcionarios y contratistas de la alcaldía Distrital de Santa Marta son responsables del respaldo de su información y de verificar que los respaldos de información se ejecuten correctamente, estos deben ser realizados en medios de almacenamiento digitales y entregados al custodio o jefe de cada área de la entidad.
- La Dirección de TIC es responsable de mantener custodiadas copias idénticas de respaldo de sistemas operativos que respondan a eventos de contingencia y disminuyan el impacto en caso de una falla, así como las copias de seguridad de los correos electrónicos que generan alto volumen de almacenamiento.

Respaldo de la información

La data de cada sistema de información debe ser respaldado regularmente sobre un medio de almacenamiento, tales como, nube de respaldo, cinta, CD, DVD, de acuerdo con lo definido con el propietario del activo. Los medios de almacenamiento deben ser custodiados con mecanismos de protección ambiental como detección de humo, incendio, humedad y mecanismos de control de acceso físico, de acuerdo con los procedimientos establecidos.

Se deben realizar pruebas periódicas de verificación de la información almacenada en los medios con el fin de verificar su integridad y disponibilidad, de acuerdo con los establecido en los procedimientos.

Todas las solicitudes de restauración de copia de seguridad y respaldos, así como la restauración, las debe realizar el propietario o custodio de los activos a través de la Mesa de Ayuda colocando el respectivo caso por correo electrónico. Las copias de respaldo y restauraciones realizadas deben ser registradas en los formatos elaborados para el control y ejecución de citado proceso.



La Dirección de TIC debe realizar las copias de seguridad de:

- Correos electrónicos con el límite de almacenamiento en la nube lleno.
- Bases de datos en producción.
- Software de aplicaciones.
- Sistemas operativos de los servidores.
- Software base de la Alcaldía Distrital de Santa Marta.

11.15. TELEFONIA IP

La Alcaldía Distrital de Santa Marta cuenta con un sistema de Telefonía IP conformado por una planta telefónica virtualizada bajo sistema operativo Linux, lo cual permite tener capacidad para 150 extensiones telefónicas.

Alcance

Aplica a toda la infraestructura de telefonía IP instalada en todas las dependencias de la entidad.

Responsabilidades

La Dirección de TIC es responsable de monitorear la plataforma de telefonía IP virtualizada, realizando el respectivo seguimiento y Up Time a la operación de la planta y las extensiones.

Las tareas de configuración, tales como, cambios de nombre, número, asignación de cuentas SIP, traslados, configuración de privilegios de todas las extensiones son realizadas por el operador privado que administra el servicio bajo contrato vigente.

12. DIRECTRIZ DE SUPERVISIÓN DE CONTRATOS CON TERCEROS

La Alcaldía Distrital de Santa Marta reconoce que los terceros, contratistas, proveedores y entidades aliadas que participan en actividades de soporte, desarrollo, administración tecnológica, procesamiento de datos o acceso a información institucional representan un componente fundamental dentro del ecosistema digital del Distrito. Por esta razón, la supervisión de dichos contratos constituye un elemento crítico del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI).
Esta directriz se fundamenta en los lineamientos del **Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)** respecto al control de terceros dentro del SGSI, los cuales establecen que las entidades públicas deben garantizar que todas las relaciones contractuales incluyan requisitos claros de seguridad, responsabilidades definidas y mecanismos de verificación y seguimiento. Asimismo, se alinea con el **Modelo MSPI**, que exige el aseguramiento de la cadena de valor de la información, incluyendo los servicios gestionados por terceros.

12.1. Objetivo de la Directriz

Establecer las condiciones, controles y responsabilidades necesarias para garantizar que todos los terceros que tienen acceden, procesan, almacenan o administran información institucional cumplan con las políticas de seguridad y privacidad de la Alcaldía, así como con la normatividad vigente.

8.1 Alcance

Esta directriz aplica a:

- Contratos de prestación de servicios tecnológicos.
- Proveedores de sistemas de información o infraestructura.
- Operadores externos que administren plataformas, datos o redes institucionales.
- Consultores, desarrolladores, integradores, soporte técnico y outsourcing.
- Convenios o alianzas que impliquen intercambio de información.

8.2 Requisitos de Seguridad para Terceros

Todos los contratos que involucren acceso a información institucional deberán incluir cláusulas explícitas sobre:

a) Confidencialidad y protección de datos

- Compromiso de reserva, confidencialidad y no divulgación.
- Protección de datos personales conforme a la Ley 1581 de 2012.

b) Cumplimiento de políticas institucionales

El proveedor deberá cumplir íntegramente con las políticas de seguridad de la Alcaldía, incluyendo:

- Control de acceso.
- Clasificación de la información.
- Protección contra programas malignos.
- Gestión segura de la infraestructura.
- Uso aceptable de TIC.

c) Controles de acceso y manejo de credenciales

- Creación de cuentas para terceros autorizados.
- Vigencia temporal del acceso.

- Eliminación de cuentas al finalizar el contrato.
- Prohibición del uso compartido de credenciales.

d) Gestión de incidentes

- Obligación de reportar incidentes de seguridad que afecten servicios o información del Distrito.
- Participación en la investigación y acciones de respuesta.

e) Manejo seguro de la información

- Entrega de información, respaldos o medios al finalizar el contrato.
- Destrucción certificada cuando aplique.
- Prohibición de uso no autorizado de la información institucional.

f) Evaluación de proveedores críticos

Para proveedores con acceso a sistemas o datos sensibles:

- Evaluación de cumplimiento previo.
- Revisión de certificaciones o niveles de seguridad.
- Auditorías o verificaciones periódicas.

8.3 Responsabilidades de Supervisión

a. Supervisor del contrato

El supervisor designado por la Alcaldía deberá:

- Verificar el cumplimiento de cláusulas de seguridad del contrato.
- Validar que el proveedor aplique los controles establecidos.
- Documentar actividades de seguimiento y resultados.
- Notificar al responsable de Seguridad de la Información sobre incidentes o incumplimientos.

b. Dirección TIC

La Dirección TIC será responsable de:

- Validar requisitos técnicos de seguridad antes de firmar contratos.
- Revisar configuraciones, accesos, integraciones y conexiones remotas.
- Coordinar actividades de monitoreo, pruebas, auditorías o revisiones técnicas.
- Asegurar que el proveedor cumpla con los lineamientos del MSPI.

c. Responsable de Seguridad de la Información

- Evaluar los riesgos asociados a terceros.
- Proponer controles adicionales cuando sea necesario.
- Realizar seguimiento de cumplimiento y documentación.

8.4 Finalización del Contrato y Retiro de Accesos

Una vez finalizado el contrato, se deberá garantizar que:

- Todas las credenciales del proveedor sean deshabilitadas inmediatamente.
- Se retiren accesos, permisos, llaves criptográficas o autenticaciones remotas.
- Se reciba la información institucional bajo formato seguro.
- Se certifique la destrucción de copias de trabajo cuando corresponda.

Este control debe realizarse junto con la Dirección TIC y el supervisor del contrato.

8.5 Incumplimientos

El incumplimiento de los requisitos de seguridad por parte del proveedor podrá resultar en:

- Suspensión del servicio.
- Acciones disciplinarias o contractuales.
- Reporte ante autoridades competentes si procede.

13. ARTICULACION CON MIPG

La seguridad y privacidad de la información es un habilitador transversal dentro de la gestión pública y constituye un componente esencial del **Modelo Integrado de Planeación y Gestión (MIPG)**. En este marco, la Alcaldía Distrital de Santa Marta integra su Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) con las dimensiones, políticas de gestión y componentes estratégicos del MIPG, garantizando coherencia institucional, mejora continua y cumplimiento normativo.

Los lineamientos del **Modelo de Seguridad y Privacidad de la Información – MSPI**, parte de la Política de Gobierno Digital, señalan que todas las entidades públicas deben articular sus procesos de seguridad con los instrumentos de planeación, gestión del desempeño, gestión del riesgo, control interno y talento humano.
Esta articulación asegura que la seguridad de la información no opere como un sistema aislado, sino como un elemento integrado que soporta el logro de metas institucionales, especialmente en los habilitadores estratégicos del Plan de Desarrollo Distrital **"Santa Marta 500+"**, tales como acceso al agua, seguridad, sostenibilidad y gobierno abierto

8.6 Integración con la Gestión Estratégica del Distrito

La seguridad de la información se considera un habilitador del desarrollo y contribuye directamente a metas estratégicas del Distrito, entre ellas:

- Confiabilidad en los sistemas que soportan la gestión del agua.
- Protección de información sensible asociada a seguridad ciudadana.
- Soporte tecnológico seguro para movilidad y servicios sociales.
- Transparencia y confianza en iniciativas de gobierno abierto.

8.7 Beneficios de la Articulación con el MIPG

La integración del SGSPI con el MIPG permite:

- Mayor coherencia en la toma de decisiones.
- Priorización adecuada de inversiones.
- Fortalecimiento de la seguridad en procesos estratégicos.
- Mejor capacidad de respuesta ante incidentes y riesgos.
- Transparencia y rendición de cuentas.
- Mejora continua del desempeño institucional.

8.8 Compromiso Institucional

La Alcaldía Distrital de Santa Marta reafirma su compromiso con la aplicación de los principios del MIPG, promoviendo:

- Un enfoque articulado e interdependiente en la gestión pública.

- La integración de la seguridad como parte del direccionamiento estratégico.
- El fortalecimiento de la institución a través de una visión preventiva, colaborativa y orientada al ciudadano.

14. POLÍTICA DE CUMPLIMIENTO

La Alcaldía Distrital de Santa Marta se compromete a asegurar el cumplimiento de todas las obligaciones legales, reglamentarias, contractuales y normativas relacionadas con la seguridad y privacidad de la información. Esta política establece el marco para que la entidad actúe conforme a las disposiciones nacionales, lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y estándares aplicables en la administración pública.

Los planes de Seguridad y Privacidad del MinTIC establecen que el cumplimiento normativo es un componente transversal del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) y que todas las entidades deben adoptar procesos que garanticen la observancia de las leyes y directrices relacionadas con el tratamiento y protección de la información. Asimismo, el **Modelo MSPI** exige que el cumplimiento sea verificado, documentado y supervisado como parte del ciclo de mejora continua del SGSPI.

8.9 Objetivo de la Política de Cumplimiento

Asegurar todos los procesos, sistemas, funcionarios, contratistas y terceros que intervienen en la gestión de información para que cumplan con:

- La normatividad colombiana aplicable en materia de seguridad digital, protección de datos, transparencia y gobierno digital.
- Las políticas internas de la Alcaldía.
- Los lineamientos del MSPI y el MinTIC como autoridad rectora de la política pública digital.

8.10 Marco Normativo Aplicable

La Alcaldía garantizará el cumplimiento de, entre otras:

- Ley 1581 de 2012 sobre protección de datos personales.
- Ley 1712 de 2014 sobre transparencia y acceso a la información pública.
- Decreto 767 de 2022 (Política de Gobierno Digital).
- Guías del MinTIC, en especial las relacionadas con seguridad y privacidad de la información.
- Normatividad contractual y de derecho administrativo aplicable.

8.11 Responsabilidades para el Cumplimiento

Alta Dirección

- Garantizar la adopción y cumplimiento de las normas aplicables.
- Proveer recursos para implementar controles que aseguren conformidad normativa.

- Aprobar políticas, lineamientos y actualizaciones requeridas.

Responsable de Seguridad de la Información

- Supervisar el cumplimiento de las políticas del SGSPI.
- Realizar seguimiento y reporte de hallazgos de cumplimiento.
- Coordinar acciones correctivas y preventivas.

Dirección TIC

- Verificar que la infraestructura tecnológica cumpla con estándares y obligaciones técnicas vigentes.
- Asegurar la protección de sistemas, datos y plataformas según los lineamientos MinTIC.

Líderes de Proceso

- Aplicar los controles y procedimientos definidos para garantizar el tratamiento seguro de la información.
- Identificar y reportar posibles incumplimientos dentro de su área.

Oficina Jurídica

- Verificar la correcta aplicación del marco jurídico relacionado con seguridad de la información y datos personales.
- Revisar contratos para asegurar la inclusión de cláusulas de seguridad.

Todos los servidores públicos y terceros

- Cumplir las políticas de seguridad.
- Participar en procesos de formación y sensibilización.
- Reportar incidentes o prácticas que puedan constituir incumplimientos.

8.12 Mecanismos de Seguimiento y Control

La Alcaldía implementará mecanismos formales para verificar el cumplimiento, tales como:

- Auditorías internas y externas del SGSPI.
- Revisión periódica del cumplimiento normativo.
- Monitoreo de indicadores de seguridad y cumplimiento.
- Registro de evidencias de conformidad (actas, reportes, controles aplicados).
- Evaluaciones anuales del SGSPI, según el ciclo de mejora del MSPI.

15. MONITOREO

El monitoreo constituye un componente esencial del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI), permitiendo observar de manera continua el funcionamiento de los controles, detectar anomalías, prevenir incidentes, evaluar la efectividad de las medidas implementadas y asegurar la mejora continua del sistema. Su propósito es garantizar que la seguridad de la información opere de forma proactiva y que cualquier desviación sea detectada y atendida oportunamente.

Los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) establecen que las entidades públicas deben realizar un seguimiento permanente de los elementos críticos de su infraestructura tecnológica, políticas, procesos y sistemas de seguridad, como parte integral de los planes de seguridad de la información. Asimismo, el **Modelo MSPI** determina que el monitoreo y la evaluación son fases obligatorias dentro del ciclo de vida de la seguridad (Evaluar y Mejorar)

Alcance del Monitoreo

El monitoreo abarcará:

- Infraestructura de red, equipos activos, servidores y firewalls.
- Plataformas, sistemas de información, aplicaciones y servicios digitales.
- Registros de eventos, logs de auditoría y accesos de usuarios.
- Controles de autenticación, permisos y actividades privilegiadas.
- Estado de antivirus, parches, actualizaciones y políticas aplicadas.
- Copias de respaldo y procesos de restauración.
- Accesos remotos y dispositivos móviles autorizados.

8.13 Indicadores de Monitoreo

La Alcaldía establecerá indicadores para evaluar el desempeño del SGSPI, tales como:

- Número de incidentes de seguridad atendidos.
- Tiempo promedio de respuesta y recuperación.
- Disponibilidad de sistemas críticos.
- Porcentaje de activos inventariados y clasificados.
- Cumplimiento de políticas y controles.
- Nivel de actualización de infraestructura y aplicaciones.

8.14 Registro y Evidencias

Todos los eventos, hallazgos y actividades de monitoreo deberán quedar documentados en:

- Bitácoras de seguridad.
- Informes de incidentes y análisis.
- Reportes de disponibilidad y continuidad.
- Evidencias de cumplimiento y verificación de controles.

La documentación será consolidada por la Dirección TIC y el responsable de Seguridad de la Información.

16. REVISIÓN

La revisión del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) es un proceso indispensable para garantizar su actualización, efectividad y la mejora continua. La Alcaldía Distrital de Santa Marta realizará revisiones periódicas y sistemáticas del SGSPI con el fin de asegurar que las políticas, lineamientos, controles, riesgos y mecanismos de protección se mantengan vigentes y alineados con:

- La normatividad nacional aplicable.
- Los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).
- El Modelo de Seguridad y Privacidad de la Información (MSPI).
- Los objetivos institucionales definidos en el Plan de Desarrollo Distrital y en el modelo MIPG.

La revisión permite identificar oportunidades de mejora, detectar desviaciones, ajustar controles y asegurar la efectividad del sistema frente a riesgos emergentes y cambios tecnológicos.

8.15 Frecuencia de la Revisión

La revisión del SGSPI se realizará:

- **Anualmente**, como parte del ciclo de planeación institucional.
- **Cuando existan cambios significativos**, tales como:
  - actualización de normatividad,
  - implementación de nuevas tecnologías,
  - aparición de amenazas relevantes,
  - cambios estratégicos o reorganizaciones internas.
- **Después de incidentes mayores de seguridad**, para incorporar lecciones aprendidas y ajustar controles.

8.16 Resultados de la Revisión

Los resultados serán documentados y deberán incluir:

- Conclusiones sobre la efectividad del SGSPI.
- Actualización de riesgos y recomendaciones de tratamiento.
- Acciones preventivas y correctivas por implementar.
- Ajustes a políticas, controles, procesos o roles.
- Necesidades de recursos y fortalecimiento de las capacidades.
- Impacto en el modelo de operación y en proyectos del SGSPI.

Estos resultados alimentarán la mejora continua del sistema y se utilizarán para actualizar el Plan de Seguridad y Privacidad de la Información, la matriz de riesgos y el portafolio de proyectos.

17. VALIDEZ DE LA POLITICA

La presente Política de Seguridad y Privacidad de la Información entra en vigor a partir de la fecha de su aprobación por la Alcaldía Distrital de Santa Marta y permanecerá activa hasta que sea modificada, actualizada o reemplazada por una nueva versión debidamente autorizada. Su aplicación es obligatoria para todas las dependencias, los servidores públicos, los contratistas y los terceros que tengan acceso a los activos de información de la entidad.

En coherencia con los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), las políticas de seguridad deben mantenerse vigentes mientras el Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) continúe en operación y hasta que su revisión periódica determine la necesidad de realizar ajustes, de acuerdo con los cambios normativos, tecnológicos o institucionales del Distrito.

Asimismo, conforme al **Modelo de Seguridad y Privacidad de la Información – MSPI**, la validez de esta política está directamente relacionada con el ciclo de vida del SGSPI, que contempla procesos de evaluación y mejora continua, destinados a asegurar su

pertinencia y efectividad. Cualquier actualización deberá seguir el procedimiento de revisión formal establecido por la Alcaldía y contar con la aprobación del Comité de Seguridad de la Información.

El incumplimiento de esta política podrá dar lugar a acciones administrativas, disciplinarias o contractuales, según corresponda, debido a la importancia de proteger los activos de información y garantizar la seguridad digital de la entidad.

18. REFERENCIAS

- Función Pública. (2022). Guía para la Administración del Riesgo y el diseño de controles en entidades públicas - Versión 6. https://www.funcionpublica.gov.co/documents/28587410/34299967/Guia_administracion_riesgos_capitulo_riesgo_fiscal.pdf

- **Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.** (2024). *Plan de Seguridad y Privacidad de la Información – Versión 8.* Disponible en: https://mintic.gov.co/portal/715/articles-135830_plan_seguridad_privacidad_informacion_2024_20240125.pdf
- Función Pública. (2014). Ley 1712 de 2014 - Transparencia y del derecho de acceso a la información pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=56882

- **Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.** (2025). *Plan de Seguridad y Privacidad de la Información – Versión 10 y 11.* Disponible en:– https://mintic.gov.co/portal/715/articles-35830_Plan_de_Seguridad_y_Privacidad_de_la_Informacion_Vigencia_2025_PDF_descargable_20250919.pdf
– https://mintic.gov.co/portal/715/articles-135830_Plan_de_Seguridad_y_Privacidad_de_la_Informacion_2025.pdf

- Función Pública. (2012). Ley 1581 de 2012 - Protección de datos personales. https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=49981

- **Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.** (s.f.). *Modelo de Seguridad y Privacidad de la Información – MSPI.* Disponible en: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/w3-propertyvalue-49984.html

- Función Pública. (s.f.). MIPG https://www1.funcionpublica.gov.co/web/mipg

- **Ley 1581 de 2012.** *Ley de Protección de Datos Personales.*
Disponible en el portal de Función Pública.
- **Ley 1712 de 2014.** *Ley de Transparencia y del Derecho de Acceso a la Información Pública.*
Disponible en el portal de Función Pública.
- **Decreto 767 de 2022.** *Política de Gobierno Digital.*
Publicado por el Ministerio de Tecnologías de la Información y las Comunicaciones.
- **Función Pública.** (2022). *Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – Versión 6.*
Disponible en: https://www.funcionpublica.gov.co/

- MinTIC. (2016). Seguridad y Privacidad de la Información - Elaboración de la política general de seguridad y privacidad de la información. Guia No. 2 https://mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

➢ **Referentes internacionales:**
– ISO 27001: Sistemas de Gestión de Seguridad de la Información.
– ISO 27002: Controles de Seguridad de la Información.
– NIST Cybersecurity Framework (CSF).

➢ NQA. (2013) ISO 27001:2013 Guía de Implantación para la seguridad de la información https://www.nqa.com/medialibraries/NQA/NQA-Mediahttps://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish QRFs and PDFs/NQA-ISO-27001-Guia-de-implantacion.pdfLibrary/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-dehttps://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish QRFs and PDFs/NQA-ISO-27001-Guia-de-implantacion.pdfimplantacion.pdf

➢ NTC-ISO 9001:2015 - Sistemas de Gestión de la Calidad. Fundamentos y Vocabulario.

➢ NTC-ISO 9001:2015 - Sistemas de gestión de la calidad. Requisitos. https://www.guadalupanolasalle.edu.co/sgc/ISO9001-2015-Requisitos.pdf

➢ Villamizar, Carlos. (2023). Global Suite. Los principales cambios de la actualización de la norma ISO 27002:2022 https://www.globalsuitesolutions.com/es/cambios-norma-iso-27002-2022/

19. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS	
Versión	**Descripción de la modificación**
1	Creación del documento
2	Ajustes año 2024 de acuerdo con la articulación MIPG y normas de MINTC
3	Ajustes año 2026 según avances y los lineamientos de MINTC

ELABORÓ	REVISÓ / VBNO	APROBÓ
Nombre: **Luis Salas Ibarra** Cargo: **Profesional Universitario** Nombre: **Jhon Fredy Velázquez** Cargo: Profesional Especializado Fecha: **enero 20 de 2026**	Nombre: **Jhon Fredy Velázquez** Cargo: Profesional Especializado Fecha: 22 de enero de 2026 **Nombre: Cristián Silva Usaquén** **Cargo: Director TIC** **Fecha: 29 de enero de 2026**	**COMITÉ GESTION DE DESEMPEÑO**