	MANUAL	
ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARIA DISTRITAL DE AMBIENTE — BOGOTÁ MEJOR PARA TODOS	**Código: 126MSGSI**	**Versión: 1.0**

Versión	Descripción de la modificación	Resolución
1.0	Adopción del Manual del Subsistema de Gestión de Seguridad de la Información (SGSI) de la SDA.	Resolución 548 del 27 de febrero de 2017

Elaboró	Revisó	Aprobó
Nombre: Yeandri Natalia Moreno López **Cargo:** Profesional Universitario **Fecha:** 15/Feb/2017	**Nombre:** Shirley Andrea Zamora Mora **Cargo:** Director de Planeación y Sistemas de Información Ambiental **Fecha:** 17/Feb/2017	**Nombre:** Carlos Arturo Puerta Cardenas **Cargo:** Subsecretario General y de Control Disciplinario **Fecha:** 27/Feb/2017

Responsables de la elaboración del documento	
Francisco Javier Díaz Méndez	Oficial de Seguridad de la Información
Shirley Andrea Zamora Mora	Director de Planeación y Sistemas de Información Ambiental
Yeandri Natalia Moreno López	
Ingrid Sánchez González	Profesional Universitario
Sandra Mora escalante	Profesional Universitario
Sandra Viviana Duarte Restrepo	Profesional Universitario
Juan Carlos Tribin Perea	Profesional Universitario
Carlos Mauricio Montenegro Hernandez	Técnico operativo Código 314 Grado 17
Jonatan Gabriel Arango Alzate	Profesional Universitario
Luz Dary Achury Aguilar	Profesional Universitario Dirección de Gestión Corporativa
Gabriel Rodriguez Rodriguez	Funcionario carrera administrativa Dirección de Gestión Corporativa

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La Secretaría Distrital de Ambiente en cumplimiento a la Norma Técnica Distrital del Sistema Integrado de Gestión para las entidades y organismos distritales NTD - SIG 001:2011 y la Norma NTC-ISO-IEC 27001:2013, inició la implementación del Subsistema de Gestión de la Seguridad de la Información (SGSI), como un componente del Sistema Integrado de Gestión de la entidad. Complementariamente, la entidad siguiendo los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) sobre la estrategia de Gobierno en línea (GEL), adoptó el conjunto orientaciones y guías técnicas, que proveen y promueven la puesta en marcha, supervisión, mejora y control para la implementación del Modelo de Seguridad y Privacidad de la información (MSPI).

Basados en lo anterior, se crea el presente Manual del Subsistema de Gestión de la Seguridad de la Información (SGSI) de la Secretaría Distrital de Ambiente, como herramienta documental que contiene la planificación e implementación de las políticas, procedimientos, gestión de riesgos, y los controles necesarios para cumplir los requisitos de seguridad y privacidad de la información, a fin de asegurar la confidencialidad, integridad, disponibilidad de los activos de información, y su divulgación no autorizada; agregando valor a la prestación de los trámites y servicios, generando confianza tanto a los servidores públicos, clientes y demás partes interesadas de la SDA, como a terceros interesados, a través de la mejora continua.

2. ALCANCE

El manual del Subsistema de Gestión de la Seguridad de la Información (SGSI) de la Secretaría Distrital de Ambiente, cubre todos los procesos y procedimientos asociados al Sistema Integrado de Gestión, siguiendo el estándar de la norma NTC-ISO-IEC 27001:2013 y los elementos complementarios del Modelo de Seguridad y Privacidad de la Información orientados por MINTIC.

3. DEFINICIONES

Para el propósito de este manual aplican los términos dados en los documentos asociados al modelo de seguridad y privacidad de la información, Norma NTC-ISO-IEC 27001:2013, lineamientos del MINTIC, manual GEL y los presentados a continuación:

- **Activo:** Es un bien que la entidad posee y que tiene valor para la misma.
- **Activo de información:** Elementos de Hardware y de Software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema específico o a la entidad. (NTC-ISO-IEC 27000).
- **Caracterización de Proceso:** Se refiere a la identificación, personalización y descripción de las características más importantes de un proceso tales como: entradas, actividades, salidas, clientes, etc.
- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
- **Confidencialidad:** los activos de información solo pueden ser accedidos y custodiados por usuarios que tengan permisos para ello.
- **Disponibilidad:** Los activos de información sólo pueden ser obtenidos a corto plazo por los usuarios que tengan los permisos adecuados.
- **Estrategia:** Se centra en definir políticas, objetivos y lineamientos para el logro de la calidad y satisfacción del cliente. Estas políticas y objetivos deben estar alineados a los resultados que la organización desee obtener.
- **Integridad:** El contenido de los activos de información debe permanecer inalterado y completo. Las modificaciones realizadas deben ser registradas asegurando su confiabilidad.
- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.
- **Modelo de Seguridad y Privacidad de Información - MSPI:** El Modelo de Seguridad y Privacidad de la Información entrega una guía para construir un Sistema de Gestión de Seguridad de la Información (SGSI), buscando generar una conciencia colectiva sobre la importancia de clasificar, valorar y asegurar los activos de información de la entidad.
- **Proceso:** Secuencia de pasos dispuesta con algún tipo de lógica que se enfoca en lograr un resultado específico.
- **Recurso:** Son todos aquellos elementos que pueden utilizarse como medios a efectos de alcanzar un fin determinado.
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (NTC-ISO-IEC 27000).
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información.
- **Subsistema de Gestión de Seguridad de la Información - SGSI:** Conjunto de políticas de administración de la información el cual consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

4. REFERENCIAS NORMATIVAS

Los requisitos, delimitaciones legales, y contractuales se describen en el siguiente normograma desarrollado para el Subsistema de Gestión de Seguridad de la Información y, en el listado maestro de documentos externos de la SDA.

Resolución 305 de 2008: Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre
Ley 1581 de 2012: Ley de protección de datos personales
Ley 1712 de 2014: Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional
CONPES 3701 de 2011: Estrategia Nacional de de Ciberseguridad y Ciberdefensa
Decreto 2573 de 2014: Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones

5. CONTEXTO DE LA ENTIDAD

La entidad determina su contexto estratégico para identificar factores internos y externos que puedan generar riesgos que afecten el cumplimiento de la misión y objetivos institucionales.

En la Secretaría Distrital de Ambiente se utiliza la aplicación de la matriz DOFA – Debilidades, Oportunidades, Fortalezas y Amenazas, para analizar cada uno de los procesos de la entidad, las cuales se encuentran documentadas como Contexto Estratégico en el módulo Riesgos DAFP y en el módulo MECI - Administración del Riesgo.

Dentro de estas matrices DOFA de cada uno de los procesos, se identifican los elementos DOFA relacionados con la gestión del riesgo de Seguridad de la Información, los cuales se alinea a la misión y estrategias de la Secretaría Distrital de Ambiente, determinando los requisitos de los clientes y las partes interesadas pertinentes a la seguridad de la información, bajo los lineamientos de la norma NTC ISO/IEC 27001:2013 y MINTIC. Dentro de la Matriz DOFA se identifican estos elementos relacionados, señalándolos con las siglas del Subsistema de Gestión de Seguridad de la Información (SGSI)

Las matrices DOFA y la competencia de su elaboración, revisión y aprobación están documentadas en los lineamientos de operación del procedimiento Administración del Riesgo, código 126PG01-PR09.

5.1 COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LOS CLIENTES Y LAS PARTES INTERESADAS

Se identifican los clientes y las partes interesadas que son pertinentes y relevantes del Subsistema de Gestión de Seguridad de la Información, los cuales se articulan con los numerales 5.4. Clientes de la Secretaría Distrital de Ambiente. y 5.5. Partes interesadas documentados en el Manual del Sistema Integrado de Gestión - código 126MSIG, así como en el formato 126PG01-PR08-F-3 Identificación de partes interesadas o grupos de interés.

Manual de Sistema Integrado de Gestión

6. SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La Secretaria Distrital de Ambiente establece, implementa, mantiene y mejora continuamente el Subsistema de Gestión de la Seguridad de la Información (SGSI), por medio de lo establecido en la política, objetivos y en las metas e indicadores de gestión asociados a los objetivos definidos en la política específica del sistema.

6.1 DOCUMENTACIÓN DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Entre las actividades propias a desarrollar al abordar la implantación del SGSI se debe desarrollar la siguiente documentación básica: Los procedimientos obligatorios por la ISO/IEC 27001:2013 (incluyendo los controles del Anexo A de ésta norma) y las guías MINTIC se documentarán e implementarán de acuerdo a los lineamientos recibidos por la Alta Consejería de las TIC, el Ministerio de las TIC y al cronograma designado por dicha entidad.

- Activos de información
- Definición del alcance
- Definición de una Política de Seguridad
- Identificación de riesgos

- Evaluación de los posibles tratamientos del riesgo
- Elaboración de una Declaración de Aplicabilidad de controles y requisitos
- Definición de métricas e indicadores de la eficiencia de los controles
- Desarrollo de programas de formación y concienciación en seguridad de la información.
- Gestión de recursos y operaciones
- Elaboración de procedimientos y documentación asociada
- Inventario de activos transición IPv4 a IPv6

6.2 POLÍTICA GENERAL DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La Secretaria Distrital de Ambiente establece la política general de la seguridad de la información del SGSI, la cual es adecuada al propósito de la organización y busca garantizar la identificación y protección de los activos de información, implementando los mecanismos y controles para asegurar confidencialidad, integridad, disponibilidad de los activos de información, y la divulgación no autorizada de la información institucional acorde con sus riesgos.

La Política aplica en todo el ámbito de la Secretaría Distrital de Ambiente, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

Cubre todos los aspectos administrativos y de control que deben ser cumplidos por los funcionarios y contratistas de la Secretaría Distrital de Ambiente, para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información relacionada.

POLITICA GENERAL DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Consciente de las necesidades derivadas de sus actividades, la Secretaría Distrital de Ambiente adopta el Subsistema de Gestión de Seguridad de la Información como una herramienta para garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información, administrando los riesgos, cumpliendo con la legislación vigente, y generando una cultura de seguridad de la información en los servidores públicos y demás partes interesadas.

6.3 OBJETIVO GENERAL

Mantener la confidencialidad, integridad, disponibilidad de los activos de información, y la protección de datos personales, mediante la gestión los riesgos, que permita establecer un marco de confianza a las partes interesadas en concordancia con la misión y visión de la entidad.

6.4 OBJETIVOS ESPECÍFICOS

1. Proteger los activos de información, con base en los criterios de confidencialidad, integridad, disponibilidad, mediante la implementación de controles en los procesos de la entidad de manera coordinada con las partes interesadas.

2. Gestionar los riesgos asociados con la pérdida de confidencialidad, integridad, disponibilidad y privacidad de la información dentro del alcance del Subsistema de Gestión de Seguridad de la Información (SGSI).

3. Garantizar el tratamiento de los datos personales obtenidos en la entidad a los titulares de la información, en el ejercicio pleno de sus derechos.

4. Sensibilizar y entrenar al personal de la entidad en el Subsistema de Gestión de Seguridad de la Información (SGSI).

6.5 POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Politica general y políticas especificas del SGSI

6.6 COMPROMISO Y LIDERAZGO DE LA DIRECCIÓN

La Alta Dirección de la Secretaría Distrital de Ambiente está comprometida con la influencia y responsabilidad directa del Subsistema de Gestión de Seguridad de la Información - SGSI.

Se cuenta con el compromiso y concurso de todos los servidores públicos de la entidad, para el mantenimiento y mejora continua en nuestro SIG, los procesos y productos, para así cumplir con las necesidades y expectativas de nuestros clientes y partes interesadas, tal y como está documentado en el Manual del SIG.

De igual manera, a través de la implementación y seguimiento del Plan Estratégico Institucional 2012-2016, será imprescindible la participación y esfuerzo de todo el capital humano de la entidad, alineándose con la estrategia definida y actuando con el compromiso no sólo de hacer las cosas bien, sino de hacerlas con una permanente preocupación de satisfacer las necesidades de sus usuarios y con la seguridad y la confianza del beneficio del Distrito Capital.
La Alta Dirección de la SDA garantizará por medio de las auditorías que los objetivos establecidos y medidos con sus respectivas metas e indicadores corresponden con la Política General implementada y alineada al SGSI.

La Secretaría Distrital de Ambiente establece como máxima autoridad del Subsistema de Gestión de Seguridad de la Información al Comité del Sistema Integrado de Gestión quien es responsable de la orientación estratégica para la administración de los activos de información, la sostenibilidad y mejora del Subsistema en la Entidad. En este sentido, el liderazgo está en cabeza de la Alta Dirección de la SDA en cumplimiento de las funciones establecidas en el Artículo 2 de la Resolución SDA No. 00291 de 2017 “Por la cual se modifica parcialmente la Resolucion 176 de 2015 "Por la cual se crea el comité del Sistema Integrado de Gestión, y se dictan otras discposiciones" y la resolución 362 de 2016 "Por la cual se modifica parcialmente la Resolución 176 de 2015""; y como líder del Subsistema de Gestión de Seguridad de la Información SGSI a la Dirección de Planeación y Sistemas de Información Ambiental.

El numeral 4.3 de la Norma Técnica Distrital del SIG establece los requisitos en materia de Compromiso de la Alta Dirección, y en su literal c establece que “La alta dirección debe designar uno o varios miembros del grupo directivo con responsabilidades específicas en el Sistema Integrado de Gestión y con independencia de otras responsabilidades que le sean asignadas”, en este sentido la SDA documentó en la Resolución SDA No. 176 de 2015 Artículo 9, que cuando se trate de un tema específico asociado a un subsistema en particular, el representante de cada subsistema ejercerá la relatoría necesaria para la sesión correspondiente, como apoyo a la Secretaría Técnica, es así como para el Subsistema de Gestión de Seguridad de la Información (SGSI), será la Dirección de Planeación y Sistemas de Información Ambiental - DPSIA, quien desarrolle estas tareas.

La Alta Dirección asegura que las responsabilidades y autoridades para los roles pertinentes a la seguridad y privacidad de la información se asignen y comuniquen correctamente.

7. PLANIFICACIÓN Y CONTROL OPERACIONAL DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Las etapas definidas para el desarrollo y la implementación del Subsistema de Gestión de Seguridad de la Información son:

1. Planear y documentar el sistema
2. Implementar el sistema
3. Evaluar el sistema a través de auditorías internas y externas
4. Mejorar continuamente la eficacia del sistema a través de del análisis de datos

7.1 ADMINISTRACIÓN DEL RIESGO

La administración del riesgo (lo cual incluye la identificación, clasificación, valoración y tratamiento de los riesgos en Seguridad de la Información), se realizará de acuerdo al procedimiento Administración de Riesgos y Oportunidades: 126PG01-PR09.

7.2 DECLARACIÓN DE APLICABILIDAD

La Declaración de Aplicabilidad es un documento que lista los objetivos y controles que se van a implementar en la Entidad, Para el caso del SGSI de la SDA se enlistan los controles de seguridad establecidos en el Anexo A de la norma estándar NTC-ISO-IEC 27001:2013 (114 controles agrupados en 35 objetivos de control, en la versión de NTC-ISO-IEC 27001:2013 de esta norma de seguridad).

En el documento perteneciente a la SDA, se pueden enlistar cada uno de los controles exigidos por el Anexo A de la norma NTC-ISO-IEC 27001:2013, junto a la determinación de aplicabilidad del mismo; la información que convierte este registro en un documento vivo es la determinación del estado de cada uno de los controles y la evidencia de dicho estado. Por lo anterior, esta Declaración de Aplicabilidad debe ser alimentada periódicamente con las evidencias y evoluciones del SGSI.

La Declaración de Aplicabilidad se encuentra contemplada como un producto del procedimiento Administración de Riesgos y Oportunidades: 126PG01-PR09.

Declaración de Aplicabilidad SGSI

7.3 INDICADORES Y MEDICIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Con el fin de verificar el cumplimiento de la implementación de los objetivos específicos y el compromiso adquirido por la entidad en la política general del Subsistema de Gestión de Seguridad de la Información se establecen los indicadores, de acuerdo con la siguiente tabla:

COMPROMISO DE LA POLITICA GENERAL	OBJETIVO	NOMBRE DEL INDICADOR	TIPOLOGÍA	META A 2018
La SDA adopta el SGSI como herramienta como una herramienta para garantizar la confidencialidad, integridad, disponibilidad	Proteger los activos de información, con base en los criterios de confidencialidad, integridad, disponibilidad, mediante la implementación de controles en los procesos de la entidad de manera coordinada con las partes interesadas	Avance en la implementación de los controles de la NTC-ISO 27001:2013, en la Secretaría Distrital de Ambiente.	Eficacia	114 controles de la NTC-ISO 27001:2013 implementados
La SDA administra sus riesgos de Gestión de Seguridad de la Información.	Gestionar los riesgos asociados con la pérdida de confidencialidad, integridad, disponibilidad y privacidad de la información dentro del alcance del Subsistema de Gestión de Seguridad de la Información (SGSI).	Reducción del reporte de eventos relacionados con los riesgos de seguridad de la información	Efectividad	Reducción del 20% de los eventos de seguridad de la información, a partir de la línea base construida.
La SDA adopta el SGSI como herramienta para garantizar privacidad de la información	Garantizar el tratamiento de los datos personales obtenidos en la entidad a los titulares de la información, en el ejercicio pleno de sus derechos.	Avance en la implementación de lineamientos y controles para el manejo de datos personales en la Secretaría Distrital de Ambiente.	Eficacia	Implementación de 100% de la normativa vigente en el tema aplicable para el manejo de datos personales a la Secretaría Distrital de Ambiente.
La SDA genera una cultura de seguridad de la información en los funcionarios y contratistas y demás partes interesadas.	Socializar y entrenar al personal de la entidad en el Subsistema de Gestión de Seguridad de la Información (SGSI).	Servidores públicos de la Secretaría Distrital de Ambiente, sensibilizados en el Subsistema de Gestión de Seguridad de la Información	Eficacia	Sensibilizar el 80% de los Servidores públicos de la Secretaría Distrital de Ambiente, en el Subsistema de Gestión de Seguridad de la Información

8. SOPORTE

8.1 RECURSOS

La Secretaria de Ambiente Distrital proporciona los recursos necesarios para el establecimiento, implementación, mantenimiento y mejoramiento continuo del Subsistema de Gestión de Seguridad de la Información -.SGSI.

La Alta Dirección garantizará los recursos en cumplimiento de su Política del SIG, numeral 6.2 del documento Manual SIG:126MSIG, para ello la SDA mantendrá y fortalecerá los sistemas de información y tecnología adecuados, administrará y conservará los documentos de archivo producidos en el ejercicio de su gestión, mantendrá recursos humanos idóneos y competentes, identificará y controlará continuamente sus aspectos ambientales significativos, racionalizará el uso de los recursos naturales en todos los niveles de su organización, respondiendo a la satisfacción de sus clientes y partes interesadas promoviendo un ambiente de responsabilidad social.

8.2 COMPETENCIA

El equipo de personas que tendrá a cargo el soporte tecnológico del SGSI, tendrá un adecuado nivel de competencia basados en un Rol, Educación, Formación y Experiencia profesional orientada

a la seguridad de la información. La definición de esta matriz de competencias debe estar alineada con el acto administrativo en que la entidad resuelva para adoptar la escala de honorarios para los contratos de prestación de servicios profesionales y de apoyo a la gestión, en la cual se determina categoría, estudio y experiencia, así como equivalencias y excepciones.

Desde la vinculación del personal a la SDA se deben tener controles que permitan verificar la idoneidad e identidad, ética profesional y conducta. Se establecen las competencias correspondientes en la siguiente tabla.

MATRIZ DE COMPETENCIAS SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN- SGSI			
ROL	EDUCACIÓN	FORMACIÓN	REQUERIMIENTO
Gerente de Proyectos	Título de formación profesional en: Administración de Empresas, Administración Pública, Arquitectura; Ingeniería Ambiental, Ingeniería de Petróleos, Ingeniería Industrial, Ingeniería Geográfica Ingeniería Civil, Ingeniería Sanitaria, Ingeniería Catastral y Geodesia, Ingeniería Geográfica, Ingeniería Agronómica, Ingeniería Agrícola, Ingeniería Química, Ingeniería Forestal, Biología, Ecología o Ingeniería de Recursos Hídricos. Título en posgrado en áreas relacionadas con el cargo.	Tres (3) años de experiencia profesional.	Tarjeta o matrícula profesional en los casos reglamentados por la Ley
Asesor tecnológico	Título de formación profesional en: Ingeniería de Sistemas o Telecomunicaciones con Posgrado en áreas relacionadas con el cargo.	Nueve (9) años y hasta Diez (10) años de experiencia profesional relacionada, para contribuir con la aplicación de estándares y buenas prácticas para el manejo de información.	Tarjeta o matrícula profesional en los casos reglamentados por la Ley
Chief Information Security Officer - CISO	Título de formación profesional en: Ingeniería de Sistemas, Telecomunicaciones, o Electrónico; con tarjeta profesional vigente. Certificación ISO 27001:2013 Vigente. Certificación CRISK o PMI-RMP (opcionales) Certificación ISO 22301 o BS 25999-2 (opcionales)	Cuatro (4) años de experiencia profesional, formación específica como Oficial de seguridad, o auditor líder ISO27001:2013 Conocimiento en formulación e implementación de Planes de Continuidad de Negocio (BCP) preferiblemente y Recuperación de Desastres (DRP) preferiblemente Sistema de Gestión de Seguridad de la Información	Tarjeta o matrícula profesional en los casos reglamentados por la Ley
Profesionales de apoyo	Profesionales especializados	Tres (3) años de experiencia profesional.	Tarjeta o matrícula profesional en los casos reglamentados por la Ley

8.3 TOMA DE CONCIENCIA Y COMUNICACIÓN

La SDA desarrolla a través del proceso estratégico de Comunicaciones: 126PG02-CP01, los procedimientos necesarios para la comunicación organizacional o interna e informativa o externa, con el fin de promover la construcción de una visión compartida, facilitar los procesos de rendición de cuentas y suministrar información de manera oportuna.

Los funcionarios y contratistas tendrán los medios y recursos para la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes a su labor asociada a la SDA. Se hará seguimiento a través de los indicadores establecidos para la medición de los objetivos del SGSI.

El contenido de la comunicación del Subsistema parte de desarrollar campañas, capacitaciones, talleres y charlas de socialización referente al Subsistema de Gestión de Seguridad de la Información, que ayuden a la sensibilización y capacitación sobre seguridad de la información, además deberá:

- Definir los temas para la capacitación en seguridad de la información, de acuerdo con el público objetivo.
- Establecer la metodología que les permita evidencias cuales son las necesidades de capacitación para la SDA.
- Construir materiales para sensibilización y entrenamiento.
- Evaluar, medir y cuantificar, si el programa implementado genera impacto en el desarrollo de las actividades de la SDA.

En el marco del plan de socializaciones del SIG, en cumplimiento a lo establecido en la política del SIG de la entidad la cual se comunica y difunde a los servidores públicos a través de campañas internas, reuniones y talleres de sensibilización, medios electrónicos e impresos tales como carteleras virtuales, página Web, folletos, entre otros establecidos en los procedimientos de comunicación interna y externa adoptados.

El proceso de difusión irá de acuerdo a la implementación de lo definido en la planeación del SGSI. Se utilizará los canales de comunicación y las diferentes herramientas de difusión que posee la SDA fomentando la cultura de la seguridad y privacidad de la información de manera didáctica y amena, favoreciendo el cumplimiento de las políticas establecidas dentro del sistema. La comunicación será a todos funcionarios, contratistas y terceros de la Secretaría Distrital de Ambiente SDA.

Corresponde a la Oficina Asesora de Comunicaciones en coordinación con la Dirección de Planeación y Sistemas de Información, la elaboración del Plan de Comunicación del SGSI, a fin de divulgar las políticas de seguridad establecidas al interior de la entidad, para garantizar el conocimiento de los servidores públicos y contratistas, con el fin de que apoyen y cumplan estos preceptos, los cuales ayudan y redundan en beneficio y mejora de los niveles de seguridad de la información.

8.4 INFORMACIÓN DOCUMENTADA

- MANUAL DEL SUBSISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN - SGSI con código 126MSGSI
- CONTROL DE LA INFORMACIÓN DOCUMENTADA: Es concordante con el manual integrado de gestión con código 126MSIG y más específicamente con su sección 126PA06-CP01: GESTIÓN DOCUMENTAL en el numeral 126PA06-PR01 Control de la información documentada del Sistema Integrado de Gestión-SIG.
- CONTROL DE LA CONSERVACIÓN DE LA INFORMACIÓN DOCUMENTADA:Es concordante con el manual integrado de gestión con código 126PA06-PR02 y más específicamente con su sección 5. Documentación en el numeral 5.1 Procedimientos y documentos reglamentarios.
- Procedimientos y documentos reglamentarios. los procedimientos y demás documentos pertinentes a la implementación del SGSI para la SDA se encuentran listados en el Control de Documentos existente para el Sistema Integrado de Gestión de la entidad, y harán parte integral del Listado Maestro de Documentos.

8.5 CONTROL OPERACIONAL

Se establecerán acuerdos de nivel de servicio que permitan mitigar posibles riesgos de seguridad de la información en la entidad.

Las políticas de seguridad informática serán fijadas mediante planes, mecanismos y procedimientos que deberá adoptar la SDA para salvaguardar sus sistemas y la información que estos contienen

8.6 GESTIÓN DE ACTIVOS

La gestión de activos en la SDA se realizó teniendo en cuenta el cumplimiento del lineamiento décimo primero de la Secretaría General sobre Inventario de activos de información, los cuatro puntos principales descritos en el dominio 8 de la Tabla 2 – de la guía Controles del Anexo A del estándar NTC-SO-IEC 27001:2013 y la guía No. 5 de Gestión y Clasificación de activos de MINTIC.

Basados en lo anterior, la SDA cuenta con dos instrumentos: primero el formato 126PA06-PR02-F-1 Cuadro de caracterización documental - registro de activos de información - índice de información clasificada y reservada. El segundo instrumento es la Tabla de Retención Documental, de acuerdo con el procedimiento de control de la conservación de la información documentada: 126PA06-PR02, basados en la Ley General de Archivos No. 594 de 2000 y La Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional No. 1712 de 2014.

La articulación del formato 126PA06-PR02-F-1 Cuadro de caracterización documental - registro de activos de información - índice de información clasificada y reservada conlleva a contar con un insumo único, tanto para la caracterización de la producción documental como para el enlistamiento y clasificación de los activos de información no documentales (hardware, software y servicios). Asimismo, consolida la base para la construcción de otros instrumentos archivísticos y de gestión de la información pública.

Se determina en el siguiente link, 126PA06-PR02-F-1 Cuadro de caracterización documental - registro de activos de información - índice de información clasificada y reservada.

Inventario y clasificación de Activos de información no documentales

9. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

Se realizará seguimiento a los indicadores de medición y evaluación asociados a los objetivos del SGSI, documentados en el numeral 7.4 de este Manual, de acuerdo con el procedimiento Formulación, medición y evaluación de indicadores de gestión: 126PG01-PR07.

Además de la medición y seguimiento con los Indicadores, se podrá evaluar el desempeño de la seguridad de la información y la eficacia del SGSI, a partir de las herramientas de verificación establecidas en el ciclo PHVA de cada una de las caracterizaciones de los procesos de la entidad como: Auditorías, Autoevaluación de Control, Autoevaluación de la Gestión, Encuestas, Revisión por la Dirección, Derechos de petición, quejas y reclamos, documentadas en las caracterizaciones de los procesos y en el módulo de control de evaluación y seguimiento del MECI.

Adicional a las herramientas internas de verificación, se desarrollarán las metodologías de análisis y evaluación que dispongan los entes de control y agentes externos como la Alta Consejería de las TIC y el Ministerio de las TIC, con el fin de establecer el nivel de madurez que tenga la entidad frente a la seguridad y privacidad de la información. Se conocen las siguientes:

- Herramientas de auditorías regulares o especiales de los entes de control.
- Diagnóstico de SGSI de la Alta Consejería para las TIC.
- Herramienta e identificación del nivel de madurez de la entidad para el Modelo de Seguridad y Privacidad de la información de MINTIC.

9.1 AUDITORÍAS

La SDA a través de su proceso de Control y Mejora fomenta el autocontrol y determinar oportunidades de mejoramiento continuo a partir de las evaluaciones, auditorías internas y seguimientos.
Corresponde a la Oficina de Control Interno de la SDA la realización de Auditoria Interna, de acuerdo a lo establecido en el procedimiento 126PE01-PR03, en el cual se planifica, ejecuta e informa los resultados de dichas verificaciones, a fin de mantener y mejorar el Sistema Integrado de Gestión y sus respectivos subsistemas.
Corresponde a la Oficina de Control Interno de la SDA ejecutar la programación y planeación de las auditorías, ejecución de las evaluaciones, informes, planes de mejoramiento, planes de manejo del riesgo y seguimiento a su cumplimiento, de acuerdo con el proceso Control y Mejora: 126PE01-CP01.
El equipo Auditor deberá conocer de manera práctica y a profundidad la norma NTC-ISO-IEC 27001:2013, certificados como Auditores Internos por un ente certificador autorizado. En los casos que la OCI requiera el apoyo de un Experto Técnico para la realización de la auditoría, se podrá solicitar acompañamiento personal interno o externo.

9.2 REVISIÓN POR LA DIRECCIÓN

Se realiza la revisión por la Dirección con el objeto de asegurar la conveniencia, adecuación, eficacia, eficiencia y efectividad del SGSI como integrante del Sistema de Integrado de Gestión de la SDA, de acuerdo a lo establecido en el procedimiento Revisión por la Dirección: 126PG01-PR08, además los resultados se deberán retener y mantener como información documentada.

Los resultados de la revisión por la dirección deben incluir todas las decisiones y acciones relacionadas con la mejora de la eficacia, eficiencia y efectividad del Sistema Integrado de Gestión y sus procesos; la mejora del producto o servicio en relación con los requisitos del cliente; las necesidades de recursos; posibles cambios en la política, objetivos, metas y otros elementos de la gestión, coherentes con el compromiso de mejora continua, el informe de revisión por la dirección y el acta de Revisión por la Dirección.

10. MEJORA CONTINUA

LA SDA busca implementar de manera adecuada y efectiva el Subsistema de Gestión de Seguridad de la Información - SGSI, por medio de la utilización, cumplimiento y socialización de la Política General, las interiorización y aplicación de las políticas específicas de Seguridad de la Información, de manera articulada e integrada con el Sistema de Gestión de Calidad de la SDA.

Producto del seguimiento, evaluación, análisis y monitoreo de los indicadores y metas asociados a cada uno de los objetivos desarrollados, se evaluarán y analizarán en mesas de trabajo establecidas, para corregir de ser necesario, los errores cometidos, así como mejorar las acciones llevadas a cabo en las fases anteriores, llevando a cabo el plan de mejoramiento continuo de seguridad y privacidad de la información, de acuerdo a lo establecido en el procedimiento Plan de Mejoramiento por procesos: 126PE01-PR05, y en el procedimiento Plan de Mejoramiento Institucional: 126PE01-PR08, cuando se trate de evaluar la pertinencia y el cumplimiento de la respuesta institucional a los hallazgos generados por los diferentes entes de control.
La mejora continua es uno de los elementos más importantes de un sistema de gestión y con ella la implementación de acciones correctivas y preventivas que eliminen las causas de las situaciones, reales o potenciales, que afecten la eficacia del sistema, con estas acciones u oportunidades de mejora desarrolladas, ayudarán a prevenir posibles no conformidades, además se identificarán las posibles modificaciones a los riesgos encontrados y se buscará su correcto manejo de mitigación.

10.1 NO CONFORMIDADES Y ACCIONES CORRECTIVAS

El establecimiento de las acciones correctivas deben buscar la eliminación de las causas que conllevaron a la identificación de una no conformidad u observaciones, para ello la entidad tiene documentado el Instructivo para realizar el análisis de causas: 126PE01-PR05-I-A3, en el cual se determinan dos tipos de herramientas de análisis de causa (5 por qué y Diagrama causa efecto – Espina de pescado).

Para la mejora continua del SGSI se debe implementar las acciones necesarias revisando la eficiencia de las acciones correctivas llevadas a cabo. Si llegara a ser necesario, se tienen que realizar cambios en el Sistema de Gestión de la Calidad.

Todas las acciones correctivas o si es una corrección puntual de conformidad con las definiciones, deben ser las apropiadas según los efectos que generen las no conformidades que han sido encontradas.

Los responsables de procesos y/o jefes de dependencia evaluarán, en coordinación con la Oficina de Control Interno, la pertinencia de la reformulación de las acciones que se encuentren vencidas, hasta garantizar la eliminación de la causa del hallazgo.

11. PROTOCOLO IPV6

Una dirección IP es como un número telefónico o una dirección de una calle. Cuando hay una conexión a Internet, el dispositivo (computadora, teléfono celular, tableta) le es asignado con una dirección IP, así como también cada sitio que se visita tiene una dirección IP. El sistema de direccionamiento que se ha estado usado desde que nació Internet es llamado IPv4, y el nuevo sistema de direccionamiento es llamado IPv6. La razón por la cual se debe reemplazar el sistema IPv4 (y en última instancia opacarlo) con el IPv6 es porque Internet se está quedando sin espacio de direcciones IPv4, e IPv6 provee una exponencialmente larga cantidad de direcciones IP

Adicional a los controles y dominios de la NTD ISO 27001:2013, la Secretaria Distrital de Ambiente en cumplimiento de los componentes solicitados por el Ministerio de las TIC, realizará un análisis

de la posible transición de IPV4 a IPv6 para Colombia basados en la siguiente situación real: “Desde hace más de tres décadas, las redes de telecomunicaciones han venido creciendo exponencialmente generando mayor demanda de servicios y oportunidades en la red mundial de internet; con el aumento de las tecnologías computacionales y de comunicaciones, ha aumentado el proceso de innovación tecnológica en los diversos dispositivos tanto alámbricos como inalámbricos, como por ejemplo, celulares, puntos de acceso, tabletas, servidores, equipos de almacenamiento entre otros, que comenzaron a incrementar la conectividad en muchas redes en el mundo y para ello han tenido que hacerlo con direcciones de internet que permiten establecer conexiones para cada elementos conectado a la red, estas direcciones se conocen como direcciones IP (Internet Protocol Versión 4), que en estos momentos entraron a una fase de agotamiento final”.

Debido a esta situación, la entidad debe entrar en un proceso de aseguramiento del protocolo IPv6 para los servicios o elementos que priorice a fin de facilitar la conectividad en banda ancha, ofreciendo mejores servicios poniéndolos al alcance de toda la población a fin de estimular y ofrecer mejores oportunidades para el desarrollo mundial. Así mismo, para cumplir con los objetivos de innovación tecnológica que exige el país, las entidades del país deben entrar en el proceso de transición del protocolo IPv4 hacia el nuevo protocolo IPv6 siguiendo las instrucciones descritas en la Circular 002 del 6 de julio de 2011 del Ministerio de Tecnologías de la Información y las Comunicaciones, que busca promover la adopción de IPv6 en Colombia.

Inventario de los activos de información que podrán pasar del protocolo IPv4 a IPv6

La SDA documenta un inventario de los activos de información que podrán pasar del protocolo IPv4 a IPv6, para lo cual revisó su actual infraestructura, y posteriormente validará todos los componentes de hardware y software de que se disponga, revisando los servicios que se prestan, los sistemas de información, revisará estándares y políticas para conocer el impacto de adopción de la nueva versión del protocolo IP, para determinar un posible plan de transición.