PLAN DE SEGURIDAD DE LA INFORMACIÓN 2025 - SDA

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA DE AMBIENTE
BOGOTÁ

TABLA DE CONTENIDO

Tabla de contenido

1. INTRODUCCIÓN

Con la evolución de los ataques informáticos y los avances tecnológicos, es necesario establecer e implementar directivas y controles que permitan el aseguramiento de la información y proteger sus criterios de confidencialidad, integridad y disponibilidad de la misma, es así como a nivel gubernamental se define el Modelo de Seguridad y Privacidad de la Información (MSPI).

Dentro del Modelo de Seguridad y Privacidad de la Información, se contemplan un conjunto de actividades desarrolladas en las siguientes fases:

1. **Diagnóstico**: Realizar un análisis GAP, cuyo objetivo es identificar el estado actual de la Entidad respecto a la adopción del MSPI.
2. **Planificación**: Determinar las necesidades y objetivos de seguridad y privacidad de la información teniendo en cuenta su mapa de procesos, el tamaño y en general su contexto interno y externo.
3. **Operación**: Implementar los controles que van a permitir disminuir el impacto o la probabilidad de ocurrencia de los riesgos de seguridad de la información identificados en la etapa de planificación.
4. **Evaluación de desempeño**: Determinar el sistema y forma de medir el nivel de la adopción del modelo.
5. **Mejoramiento Continuo**: Establecer procedimientos para identificar desviaciones en las reglas definidas en el modelo y las acciones necesarias para su solución y no repetición. Cada una de las fases se dará por completada, cuando se cumplan todos los requisitos definidos en cada una de ellas.

De acuerdo con lo anterior se desarrolla el presente plan describiendo las acciones que permiten implementar el Sistema de Seguridad de la Información, contribuyendo a fortalecer la seguridad de la información de la SDA.

2. OBJETIVO

Trazar y planificar la manera como la SDA realizará o continuará con la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).

2.1 Objetivos Estratégicos.

Los objetivos estratégicos que se quieren alcanzar con este plan son:

- Implementar y proteger los activos de información de la SDA, con base en los principios de confidencialidad, integridad y disponibilidad.
- Sensibilizar a los servidores públicos y contratistas de la Entidad en Seguridad de la Información, fortaleciendo el nivel de conciencia de estos, en cuanto a la necesidad de salvaguardar los activos de información críticos de la entidad.
- Monitorear el cumplimiento de controles de seguridad tales como instalación de antivirus en los equipos de la entidad, uso de VPN para acceso seguro, creación de listas negras y blancas para el envío y recepción de correos, entre otros, mediante el uso de herramientas de seguridad perimetral y antivirus.
- Implementar acciones correctivas y de mejora para del Modelo de Seguridad y Privacidad de la Información de Gobierno Digital.
- Gestionar los incidentes de seguridad de la información, con el fin de prevenir el impacto negativo para la entidad. En cuanto a pérdidas económicas, sanciones disciplinarias, legales, entre otras.

3. ALCANCE

Definir las iniciativas, dentro del marco del proyecto IT03 - PR10 (Robustecer la seguridad informática, la seguridad y privacidad de la información y la ciberseguridad), definido en el PETI 2024-2028, orientados a la implementación del Subsistema de Gestión de Seguridad de la Información (SGSI), y la política de la información en la cual se indica que la SDA adopta, establece, implementa, opera, verifica y mejora el Modelo de Seguridad y Privacidad de la Información (MSPI), de MinTIC para todos sus procesos: estratégicos, misionales, de apoyo y de control, conforme con su misión y visión.

4. NORMATIVIDAD (BASE LEGAL)

En la siguiente tabla se relacionan la normatividad vigente que aplica para el presente documento:

Norma (número y fecha)	Descripción
Constitución Política de Colombia. Artículos 15, 209 y 269.	Resalta como todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos, además establece que la función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, mediante la

Norma (número y fecha)	Descripción
	descentralización, la delegación y la desconcentración de funciones.
Ley 1581 de 2012.	Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto 2609 de 2012.	Mediante el que se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
CONPES 3701 de 2011	Estrategia de ciberseguridad y ciberdefensa.
Decreto 1377 de 2013 (Compilado en el Decreto 1081 de 2015)	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Ley 1712 de 2014	Transparencia y Derecho de Acceso a la Información Pública.
Decreto 886 de 2014	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.
Decreto 1074 de 2015.	Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparte instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
Decreto 1078 de 2015.	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1083 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública, el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de 11. Gobierno Digital, antes Gobierno en Línea y 12. Seguridad Digital.
Decreto 103 de 2015	por el cual se reglamenta parcialmente la Ley 1712 de 2014 y el acceso a la información pública.
CONPES 3854 de 2016	Política Nacional de Seguridad digital
Decreto 612 de 2018.	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
Decreto 1008 de 2018	Política de Gobierno Digital (MinTIC).
Decreto 2106 de 2019	Establece la disposición de una estrategia de seguridad digital acorde con los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones MinTic.

Norma (número y fecha)	Descripción
CONPES 3995 de 2020	Política Nacional de Confianza y Seguridad Digital
Resolución 1519 de 2020.	Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos".
Ley 2088 de 2021.	Por la cual se regula el trabajo en casa y se dictan otras disposiciones.
Directiva presidencial 03 de 2021.	Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.
Resolución 500 de 2021.	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital
Decreto 338 de 2022	contiene lineamientos generales para fortalecer la gobernanza de la seguridad digital.
Modelo Integrado de Planeación y Gestión	Dimensión Seguridad Digital.
Directiva presidencial 02 de 2022	Lineamientos para el uso de servicios en la nube, actualización de catálogos de servicios, sistemas de información, bases de datos, activos de información, infraestructura; Implementar una estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos, conformación de un equipo o Grupo de Seguridad Digital.
Resolución 460 de 2022.	Por la cual se expide el Plan Nacional de Infraestructura de Datos y su hoja de ruta en el desarrollo de la Política de Gobierno Digital, y se dictan los lineamientos generales para su implementación.
Superintendencia de Industria y comercio: Circular externa 002 de 2024	Establece lineamientos específicos para el tratamiento de datos personales en sistemas de inteligencia artificial (IA).
ISO 22301	Norma desarrollada por ISO que especifica los requisitos para un sistema de gestión encargado de proteger a una empresa de incidentes que provoquen una interrupción en la actividad, reducir la probabilidad de que se produzcan y garantizar la recuperación de la empresa.
ISO 27001	Establece los requisitos para una gestión eficaz de los riesgos que pueden afectar a la confidencialidad, la integridad y la disponibilidad de la información.

Tabla 1. Normatividad (MINTIC 2021)

5. DEFINICIONES

Se describen los términos utilizados en el documento con una explicación más detallada.

- **Activos de Información y recursos**: Se refiere a 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. (CONPES 3854 de 2016).
- **Amenazas**: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Análisis de Riesgo**: Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo. (ISO/IEC 27000).
- **Auditoría**: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).
- **Bases de Datos Personales**: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)
- **Ciberseguridad**: Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.
- **Control**: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Datos Personales**: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- **Datos Personales Públicos**: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)
- **Datos Personales Privados**: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)
- **Datos Personales Mixtos**: Para efectos de este documento es la información que contiene datos personales públicos junto con datos privados o sensibles.
- **Datos Personales Sensibles**: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la

orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

- **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. (ISO/IEC 27000).
- **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
- **Información Pública Reservada**: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
- **Mecanismos de protección de datos personales**: Lo constituyen las distintas alternativas con que cuentan las Entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.
- **Plan de continuidad del negocio**: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
- **Plan de tratamiento de riesgos**: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- **Registro Nacional de Bases de Datos**: Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)
- **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. (ISO/IEC 27000).
- **Seguridad de la información**: Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).
- **Seguridad digital**: Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.
- **Titulares de la información**: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)
- **Tratamiento de Datos Personales**: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
- **Trazabilidad**: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o Entidad. (ISO/IEC 27000).

- **Vulnerabilidad**: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).
- **Partes interesadas (Stakeholder)**: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

6. RESPONSABILIDAD Y AUTORIDAD

En la tabla que se muestra a continuación, se definen los roles responsables o con un grado de autoridad de aplicación del presente documento, se describe brevemente la responsabilidad o autoridad relacionada:

Rol	Responsabilidad
Seguridad de la información - Profesional responsable. Seguridad de la información - Profesional Enlace Sistema Integrado de Gestión	Articular los esfuerzos, recursos, metodologías y estrategias para asegurar la implementación y mantenimiento del MSPI.
Director de Planeación y Sistemas de Información Ambiental Asesor TI	Revisar que el contenido garantiza que los servicios tecnológicos, que soportan la gestión de información, conservan los criterios de seguridad, transparencia, oportunidad y calidad.
Comité Institucional de Gestión y Desempeño	Aprobar verificando que el documento se ajusta a la razón de ser de la Entidad, comprometiéndose a brindar todo el apoyo para la implementación del SGSI.

Tabla 2. Responsabilidad y Autoridad

7. PLAN DE SEGURIDAD DE LA INFORMACIÓN

En el Plan de Seguridad de la información se enuncia el ámbito de gestión, objetivo, resultado(s) esperado(s), responsables y estimación del momento de entrega de los principales productos necesarios para continuar con la implementación del Subsistema de Seguridad de la información en la SDA para tal efecto se parte de unos antecedentes que nos brindan unos lineamientos de aquellos puntos más importantes a mejorar.

7.1. Antecedentes

Dentro del PETI se hace referencia y apoyo a todo lo definido en la iniciativa de fortalecer (Modernizar y ampliar) la disposición, operación y soporte infraestructura tecnológica con un enfoque híbrido y bajo estándares de seguridad de la información, seguridad informática y ciberseguridad, las acciones definidas en el proyecto: Robustecer la seguridad informática, la seguridad y privacidad de la información y la ciberseguridad

Algunas debilidades detectadas en el PETI son:

- No se ha implementado una estrategia y un procedimiento para definir los esquemas de disponibilidad orientados a contingencias y alta disponibilidad según la criticidad de los servicios.
- En términos de seguridad informática, a partir de la identificación de activos de información, se comenzó con la gestión de los riesgos asociados a su infraestructura tecnológica y servicios tecnológicos. Sin embargo, se deben fortalecer las actividades relacionadas con el fin de cubrir todos los procesos involucrados.
- Documentación e implementación de los controles a que se hace mención en los dominios que se referencian en el Modelo de Seguridad y Privacidad de la Información – MSPI.

También durante el 2024 la Oficina de Control Interno de la SDA realizó una auditoría interna con el objetivo de evaluar la implementación y/o los criterios de cumplimiento de los controles propuestos al Plan Estratégico de Tecnologías de la Información - PETI, al Modelo de Seguridad y Privacidad de la Información - MPSI y a la Accesibilidad y Usabilidad Web, existentes en la Secretaría Distrital de Ambiente - SDA. Evaluar la implementación y/o los criterios de cumplimiento de los controles propuestos al Plan Estratégico de Tecnologías de la Información - PETI, al Modelo de Seguridad y Privacidad de la Información - MPSI y a la Accesibilidad y Usabilidad Web, existentes en la Secretaría Distrital de Ambiente - SDA, los hallazgos de esta auditoría contemplan aspectos como:

- Debilidad en la implementación de las “Condiciones mínimas técnicas y de seguridad digital” estipuladas en el Anexo N° 3 de la Resolución 1519 de 2020, este hallazgo debe llevar a que en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2025 se tengan tareas específicas para la verificación de estos controles.
- Debilidad en la identificación, evaluación y tratamiento de los riesgos de Seguridad de la Información, relacionados con los Activos de Información identificados en la SDA, se deben realizar tareas específicas para identificar y valorar los riesgos de seguridad de la información en la entidad.

Otro punto importante a analizar es la cantidad de incidentes de seguridad reportados por los colaboradores de la SDA, que para el año 2024 se tiene un registro de 18 incidentes, donde el 90% tiene que ver con reporte de posibles correos electrónicos de phishing, como se muestra en la siguiente gráfica.

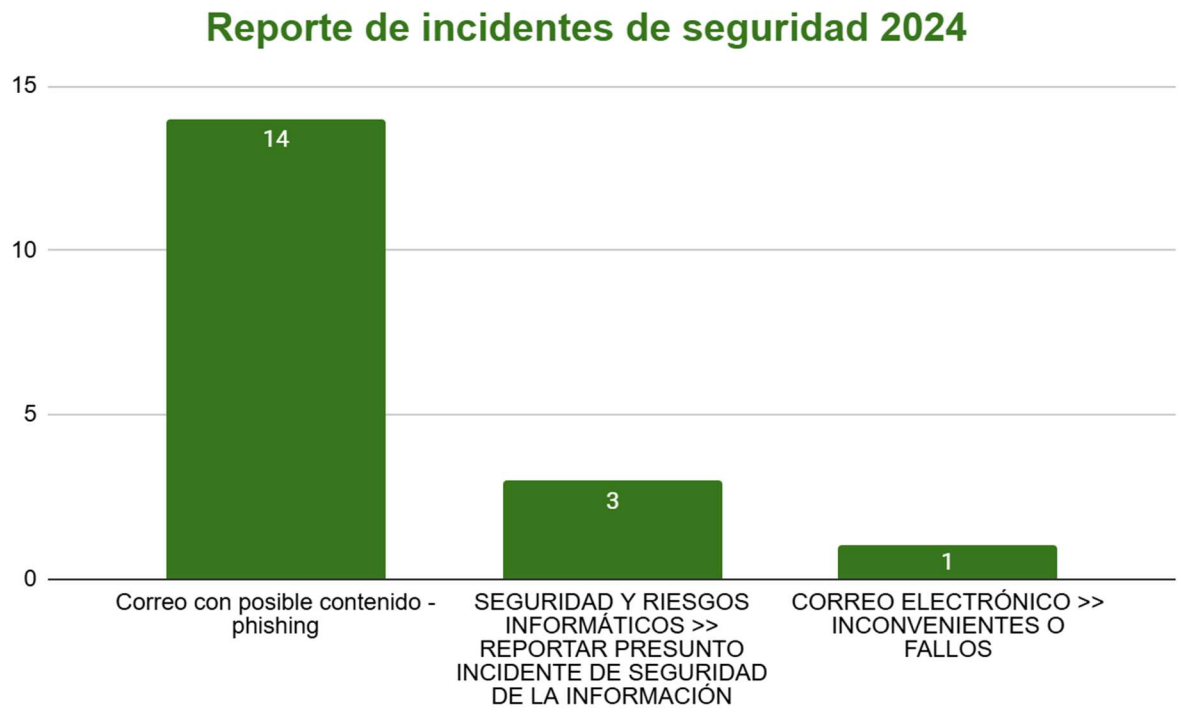

Ilustración 1. Reporte de incidentes de seguridad 2024

Se deduce de este reporte la necesidad de seguir haciendo campañas de sensibilización sobre phishing y del reporte de incidentes por parte de los colaboradores de la SDA en la herramienta ARANDA.

7.2. Hitos del Plan de Seguridad de la información

Con base en el Plan Estratégico de Tecnologías de la Información 2024 – 2027 de la SDA y de los diferentes hallazgos reportados en auditorías internas, los resultados de la fase de diagnóstico del SGSI a fin de propiciar el cierre primario de brechas de este, así como las recomendaciones de mejora dadas por la oficina de Control Interno, se describen, en la siguiente tabla, los hitos más importantes a desarrollar.

Ámbito	Objetivo	Resultado	Responsable(s)	Tiempo de entrega
Diagnóstico	Hacer el diagnóstico del subsistema de Seguridad de la Información.	Instrumento de diagnóstico de la implementación del SGSI actualizado.	Equipo de Seguridad de la Información. Responsable de dependencia.	Marzo y septiembre de cada año
Planificación	Definir y publicar el Plan de Seguridad de la Información.	Plan de seguridad de la información. Tiempo de atención a auditoría interna si aplica	Equipo de Seguridad de la Información. Asesor TI Responsable de procesos	Febrero de cada año
Planificación	Planear los controles y las políticas que se van a verificar durante el periodo.	Plan anual efectividad de los controles. * Verificar controles del MSPI * Verificar políticas de seguridad. * Seguimiento a los planes de mejoramiento de riesgos de seguridad de la información. * Verificar Anexo N° 3 Resolución 1519 de 2020 * Competencia del recursos humano	Equipo de Seguridad de la Información. Responsable de procesos.	Marzo de cada año
Planificación	Programar los DRP que se deben ejecutar en el año	Programación de los DRP a ejecutar.	Equipo de Seguridad de la Información. Toda la entidad.	Marzo de cada año

Ámbito	Objetivo	Resultado	Responsable(s)	Tiempo de entrega
Planificación	Desarrollar el plan de sensibilización de Seguridad de la Información	Plan de sensibilización.	Equipo de Seguridad de la Información. Dominio Uso y apropiación	Enero de cada año
Planificación	Actualizar las actividades de Continuidad de cada uno de los procesos de la SDA ante los escenarios planteados en el BCP.	Formatos que deben diligenciar los procesos con las tareas a ejecutar en caso de materializarse un escenario de contingencia.	Equipo de Seguridad de la Información.	Marzo 2025
Planificación	Crear nueva versión del manual de Seguridad de la información ampliando y profundizando en la Comprensión de la organización y su contexto.	Manual de Seguridad de la Información, con la definición entre otros de: contexto, las necesidades y la definición de expectativas de los interesados y la definición del alcance del SGSI, procedimiento de gestión de activos de información, entre otros. Procedimiento de gestión de incidentes de seguridad.	Equipo de Seguridad de la Información.	Agosto 2025
Operación	Ejecutar el plan de sensibilización de Seguridad de la Información	Evidencia de cada una de las tareas ejecutadas durante el periodo	Equipo de Seguridad de la Información.	Diciembre de cada año (desde el 2025)

Ámbito	Objetivo	Resultado	Responsable(s)	Tiempo de entrega
Operación	Verificar la ejecución de los ejercicios de continuidad de negocio DRP. Mínimo uno por año.	Minutograma con las actividades y responsables de las actividades realizadas.	Equipo de Seguridad de la Información. Profesional responsable de dominio.	Informe diciembre de cada año.
Operación	Ejecutar Plan anual efectividad de los controles.	Reporte de los controles verificados.	Equipo de Seguridad de la Información.	Reporte al final de año.
Operación	Reporte de las actividades desarrolladas en los planes que define el Subsistema de SGSI PAYS Plan de Seguridad de la Información Plan de tratamiento de riesgos plan de sensibilización Plan anual de efectividad de controles	Informe trimestral de avance de adopción del MSPI en la SDA.	Equipo de Seguridad de la Información.	Informe Trimestral (marzo, junio sept, dic).
Operación	Índice de Información Reservada y Clasificada (LEY 1712 DE 2014)	Acompañar la publicación periódica del índice de información clasificada previamente verificada y autorizada por la entidad.	Equipo de Seguridad de la Información. Gestión Documental.	Diciembre de 2025.

Ámbito	Objetivo	Resultado	Responsable(s)	Tiempo de entrega
Operación	Registro Nacional de Bases de Datos – RNBD.	Acompañar la definición de cómo se hace el registro, la publicación y actualización periódica del RNBD previamente verificada y autorizada por la entidad.	Equipo de Seguridad de la Información. Profesional responsable de dominio.	Diciembre de 2025.
Operación	Recopilar y generar reporte de las actividades desarrolladas durante el año por cada proceso para la definición de sus BCP	Reporte de los procesados con tareas documentadas y actualizadas.	Equipo de Seguridad de la Información. Responsable de proceso.	Diciembre de cada año
Evaluación de desempeño	Evaluar el desempeño de seguridad de la información y la eficacia del SGSI.	Hoja de vida de indicadores. Informe con la evaluación y medición de la efectividad de la implementación de los controles definidos en el plan de tratamiento de riesgos.	Equipo de Seguridad de la Información. Enlace Sistema de Gestión.	Diciembre de cada año
Evaluación de desempeño	Analizar el resultado de las auditorías internas y de los sistemas de monitoreo de seguridad con el fin de obtener información sobre el cumplimiento del SGSI y la efectividad de los controles.	Reporte con la evaluación de auditorías y monitoreo de sistemas para la seguridad perimetral.	Equipo de Seguridad de la Información. Responsable de control y mejora.	Octubre de cada año

Ámbito	Objetivo	Resultado	Responsable(s)	Tiempo de entrega
Evaluación de desempeño	Revisión del SGSI por parte de la alta dirección (comité de gestión institucional), en los intervalos planificados.	Acta y documento de Revisión por la alta Dirección con los puntos a mejorar, si existen.	Equipo de Seguridad de la Información. Comité Institucional de Gestión y Desempeño	Noviembre de cada año
Mejoramiento continuo	Identificar las acciones asociadas a la mejora continua del SGSI y de sus procedimientos.	Informe anual con los puntos de mejora.	Equipo de Seguridad de la Información. Enlace Sistema de Gestión	Diciembre de cada año
Mejoramiento continuo	Adquisición del soporte de los equipos de seguridad perimetral con el fin de proteger la seguridad tanto interna como externa de la entidad	Actualización de 2 FORTIGATE 601E 2 FORTIWEB 400D 1 FORTISANDBOX 1000D 1 FORTIANALYZER 400E Plataforma de Log y reports. Configuración y activación de 1 FIREWALL VIRTUAL MACHINE 1450 licenciamiento de Fortimail para buzones de correo.	Equipo de Seguridad de la Información. Líder de infraestructura Equipo jurídico DPSI DGC	Noviembre de cada año
Mejoramiento continuo	Adquisición de antivirus para la entidad	Adquisición de licenciamiento y soporte de endpoint protection de nueva generación con sistema XDR para proteger los equipos informáticos (endpoints, servidores y dispositivos móviles) de la SDA.	Equipo de Seguridad de la Información. Líder de infraestructura Equipo jurídico DPSI	Noviembre de cada año

Ámbito	Objetivo	Resultado	Responsable(s)	Tiempo de entrega
			DGC	

Tabla 3. Plan de Seguridad de la Información

REFERENCIAS BIBLIOGRÁFICAS

MINTIC, Ministerio de Tecnologías de la Información y las Comunicaciones. 2021. Documento maestro del Modelo de Seguridad y privacidad de la Información. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

MINTIC, Ministerio de Tecnologías de la Información y las Comunicaciones. junio de 2020. Marco de la Transformación Digital para el Estado Colombiano. https://gobiernodigital.mintic.gov.co/692/articles-179145_Marco_Transformacion_Digital.pdf

Oficina De Control Interno. SDA. 2023 informe Final de Auditoría al Proceso de Gestión Tecnológica. https://drive.google.com/drive/folders/1sIuxUIbdtqmln8YbCIGbQgmGJz-d0ou7

SDA. Estrategia de sensibilización en temas de seguridad de la información en la Secretaría Distrital de Ambiente vigencia 2023. 2023. https://docs.google.com/file/d/1PJIOXNDsxGQfoXRVU-HgDeAoR2V7kc-R/edit

Aprobado en el Comité Institucional de Gestión y Desempeño – CIGD del 28 de enero de 2025