Seguridad y privacidad de la Información en la SDA

Informe trimestral Plan de Seguridad de la información

I trimestre 2025

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

Tabla de contenido

1. INTRODUCCIÓN 3
2. OBJETIVO 3
3. ALCANCE 3
4. NORMATIVIDAD (BASE LEGAL) 3
5. DEFINICIONES 10
6. RESPONSABILIDAD Y AUTORIDAD 10
7. AVANCE DE IMPLEMENTACIÓN 13

1. INTRODUCCIÓN

El presente informe detalla el progreso de la Secretaría Distrital de Ambiente en la implementación de su Plan de Seguridad de la Información, el cuál es un compromiso fundamental para salvaguardar los datos que gestionamos. Nuestro enfoque se alinea al Sistema de Gestión de Seguridad de la Información-SGSI siguiendo las recomendaciones dispuestas en el Modelo de Seguridad y Privacidad de la Información - MSPI del Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC y los principios de la norma ISO 27001:2013, pilares que nos guían en la protección de la confidencialidad, integridad y disponibilidad de toda la información. Presentamos este balance para informar a la ciudadanía sobre las acciones que estamos llevando a cabo para garantizar un entorno digital seguro y confiable para todos.

2. OBJETIVO

Evidenciar el seguimiento a las actividades realizadas para dar cumplimiento al Plan de Seguridad y Privacidad de la Información, de la Secretaría Distrital de Ambiente.

3. ALCANCE

Este documento describe el desarrollo de las actividades establecidas en el Plan de Seguridad de la Información que fue previamente sometido a consideración y aprobado por el Comité Institucional de Gestión y Desempeño (CIGD) durante el primer trimestre de su implementación, permitiendo una evaluación de los avances y el cumplimiento de las metas establecidas.

4. NORMATIVIDAD (BASE LEGAL)

A continuación, se detalla la normativa que rige el Plan de Seguridad de la Información de la SDA, categorizada para mayor claridad:

1. Constitución Política y Leyes Fundamentales	
Constitución Política de Colombia (Artículos 13, 15, 20, 21, 22, 44, 209, 269)	Consagra el derecho a la intimidad personal y familiar, al buen nombre, a conocer, actualizar y rectificar información en bases de datos, y establece que la administración pública debe diseñar y aplicar métodos y procedimientos de control interno.
Ley 23 de 1982	Establece aspectos relacionados con los derechos de autor.
Ley 962 de 2005	Ley de simplificación y racionalización de trámites, que incluye atributos de seguridad en la información electrónica de entidades públicas.
Ley 594 de 2000 (Ley General de Archivos)	Define acciones para la administración, custodia, conservación y salvaguarda de la información.
Ley 527 de 1999	Define y reglamenta el acceso y uso de mensajes de datos, comercio electrónico y firmas digitales.
Ley 1221 de 2008	Regula y promueve el Teletrabajo a nivel nacional y territorial.
Ley 1266 de 2008	Regula el habeas data financiero.
Ley 1273 de 2009 (Ley de delitos informáticos)	Modifica el Código Penal creando un nuevo bien jurídico tutelado la protección de la información y los datos, aplicable en la sanción de violaciones.
Ley 1341 de 2009	Establece el marco general para la formulación de políticas públicas en el sector de las Tecnologías de la Información y las Comunicaciones (TIC).
Ley 1437 de 2011 (Código de Procedimiento Administrativo y de lo Contencioso Administrativo)	Establece disposiciones relativas a sedes electrónicas.
Ley 1581 de 2012	Dicta disposiciones generales para la protección de datos personales.

Ley Estatutaria 1621 de 2013	Expedida para fortalecer el marco jurídico que permite a los organismos de inteligencia y contrainteligencia cumplir su misión.
Ley 1712 de 2014 (Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional)	Regula el derecho de acceso a la información pública, los procedimientos para su ejercicio y las excepciones a la publicidad de la información.
Ley 1952 de 2019	Expedición del Código General Disciplinario.
Ley 2052 de 2020	Establece disposiciones para simplificar la interacción con el Estado y promueve el intercambio de información y el uso de servicios digitales.
Ley 2088 de 2021	Regula el trabajo en casa.
2. Normativa Específica de TIC y Seguridad Digital	
CONPES 3701 de 2011	Estrategia de ciberseguridad y ciberdefensa.
Decreto 1377 de 2013 (compilado en el Decreto 1081 de 2015)	Relacionado con la protección de datos personales.
Decreto 1078 de 2015 (Decreto Único Reglamentario del Sector TIC)	Es un marco de referencia fundamental que compila la normatividad del sector TIC y contiene lineamientos sobre la Política de Gobierno Digital y Seguridad y Privacidad de la Información como habilitador transversal.
Decreto 1080 de 2015	Establece directrices para la clasificación de información pública, reservada y clasificada.
Decreto 1083 de 2015 (Decreto Único Reglamentario del Sector Función Pública)	Establece políticas de Gestión y Desempeño Institucional, incluyendo Gobierno Digital y Seguridad Digital.
Decreto 415 de 2016	Adiciona lineamientos para el fortalecimiento institucional en Tecnologías de la Información y las Comunicaciones.

CONPES 3854 de 2016 (Política Nacional de Seguridad Digital)	Fortalece capacidades para gestionar y mitigar riesgos de seguridad digital.
Decreto 612 de 2018	Fija directrices para la integración de los planes institucionales y estratégicos al Plan de Acción.
Decreto 1008 de 2018	Política de Gobierno Digital del MinTIC.
Decreto 2106 de 2019	Establece la disposición de una estrategia de seguridad digital acorde con los lineamientos del MinTIC.
CONPES 3995 de 2020 (Política Nacional de Confianza y Seguridad Digital)	Formula medidas para ampliar la confianza y seguridad digital en Colombia.
Decreto Nacional 620 de 2020	Desarrolla los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
Resolución 1519 de 2020 (MinTIC)	Define estándares y directrices para publicar información, y requisitos en materia de acceso a la información pública, accesibilidad web, seguridad digital y datos abiertos. Es importante destacar que, según la información más precisa, el Anexo N° 3 de esta Resolución, a pesar de que uno de los documentos fuente lo describe para información financiera, en realidad define las "Condiciones mínimas técnicas y de seguridad digital" relevantes para el mantenimiento de la infraestructura tecnológica.
Directiva Presidencial 03 de 2021	Establece lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.
CONPES 4023 de 2021	Plantea la necesidad de acelerar y fortalecer los habilitadores digitales en el sector público.
CONPES 4070 de 2021	Establece lineamientos de política para la implementación de un modelo de Estado Abierto.

Resolución 500 de 2021 (MinTIC)	Establece los lineamientos y estándares para la estrategia de seguridad digital y adopta el MSPI como habilitador de la política de Gobierno Digital.
Decreto 338 de 2022	Contiene lineamientos generales para fortalecer la gobernanza de la seguridad digital.
Directiva Presidencial 02 de 2022	Provee lineamientos para el uso de servicios en la nube, actualización de catálogos de servicios, sistemas de información, bases de datos, activos de información, infraestructura; y para implementar una estrategia de seguridad digital.
Resolución 460 de 2022 (MinTIC)	Expedida para el Plan Nacional de Infraestructura de Datos (PNID) y su hoja de ruta en el desarrollo de la Política de Gobierno Digital.
Decreto 1389 de 2022	Adiciona el Decreto 1078 de 2015, estableciendo lineamientos para la gobernanza en la infraestructura de datos y creando el Modelo de gobernanza.
Superintendencia de Industria y Comercio (SIC)	Circular Externa 002 de 2024 Establece lineamientos específicos para el tratamiento de datos personales en sistemas de inteligencia artificial (IA)
Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la Información. Diseño de Controles en Entidades Públicas (DAFP)	Establece la metodología para la administración del riesgo.
Resolución 02239 del 24 de junio de 2024 (MinTIC)	Actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios en el Ministerio/Fondo Único de TIC.
3. Estándares y Modelos Internacionales/Nacionales	
Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC	Es la guía principal para construir y gestionar el SGSI.

ISO/IEC 27001 (versiones 2013 y 2022)	Es el estándar internacional clave que proporciona los requisitos para establecer, implementar, mantener y mejorar continuamente un SGSI, centrándose en la gestión de riesgos y la aplicación de controles.
Familia de normas ISO/IEC 27000	Incluye ISO/IEC 27000 (vocabulario), ISO/IEC 27002 (guía de implementación de controles), ISO/IEC 27003 (guía de implementación SGSI), ISO/IEC 27004 (métricas SGSI), ISO/IEC 27005 (gestión del riesgo SI).
ISO 22301	Norma para el sistema de gestión de continuidad del negocio, que sirve de base para el Plan de Recuperación de Desastres (DRP) y el Análisis de Impacto al Negocio (BIA).
ISO 25000	Norma que se utiliza como marco de referencia para la calidad y seguridad de los sistemas de información.
ISO 31000	Proporciona directrices generales para la gestión del riesgo, alineada con la apreciación y tratamiento de riesgos de seguridad de la información.
Modelo Integrado de Planeación y Gestión (MIPG)	Un marco de referencia para la gestión y el desempeño de las entidades públicas, articulando políticas como la de gobierno digital y seguridad digital.
Marco de Referencia de Arquitectura Empresarial (MRAE) V3.0	Orienta a las entidades públicas en la implementación del enfoque de arquitectura empresarial para la gestión y gobierno de las TIC.
Guías del MSPI de MinTIC	Incluyen la "Guía para la preparación de las TIC para la continuidad del negocio" y la "Guía para realizar el Análisis de Impacto de Negocios BIA".
4. Normatividad Distrital (Bogotá)	
Decreto Distrital 57 de 2002	Establece el Sistema de Información Distrital (SDI) para verificar y hacer seguimiento a la gestión de las entidades.

Decreto Distrital 109 de 2009	Modifica la estructura de la Secretaría Distrital de Ambiente.
Acuerdo Distrital 130 de 2004	Establece la Infraestructura Integrada de Datos Espaciales para el Distrito Capital.
Acuerdo Distrital 257 de 2006	Dicta normas básicas sobre la estructura, organización y funcionamiento de los organismos y entidades de Bogotá D.C..
Decreto Distrital 807 del 24 de diciembre de 2019	Indica que la institucionalidad del MIPG en el Distrito Capital está conformada por el Comité Institucional de Gestión y Desempeño.
Decreto Distrital 189 de 2020	Expide lineamientos generales sobre transparencia, integridad y medidas anticorrupción.
Acuerdo Distrital 761 de 2020	Establece el propósito de "Construir Bogotá-Región con gobierno abierto, transparente y ciudadanía consciente".
Acuerdo 822 de 2021	Dispone lineamientos para la promoción del ciclo virtuoso de la seguridad, uso y aprovechamiento de los datos en Bogotá.
Acuerdo 002 de 2023 (Alcaldía Mayor de Bogotá, D.C. - Comisión Distrital de Transformación Digital)	Obliga a las entidades del Distrito a realizar Evaluaciones de Impacto de Privacidad (PIA).
Decreto Distrital 050 de 2023	Regula el Teletrabajo y trabajo en casa a nivel distrital.
Decreto Distrital 575 de 2023	Establece los lineamientos para la gobernanza en la infraestructura de datos en Bogotá, promoviendo la transformación digital basada en datos.
Circular N° 007 del 16 de diciembre de 2024 (Oficina Consejería Distrital de TIC, Secretaría General de la Alcaldía Mayor de Bogotá, D. C.)	Establece lineamientos generales y específicos para la planificación, ejecución y seguimiento de proyectos de TI.

Tabla 1. Normatividad

Estos documentos establecen el marco de referencia legal y técnico dentro del cual la SDA opera su SGSI y define las directrices y controles específicos para la seguridad y privacidad de su información

5. DEFINICIONES

- **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).

6. RESPONSABILIDAD Y AUTORIDAD

La protección de la información en la Secretaría Distrital de Ambiente (SDA) es una responsabilidad compartida por toda la entidad, desde su dirección hasta cada funcionario y contratista. Nuestro compromiso es garantizar la confidencialidad, integridad y disponibilidad de la información que gestionamos. La SDA adoptó el Sistema de Gestión de Seguridad de la Información (SGSI) siguiendo las recomendaciones del Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), con el fin de administrar los riesgos y generar una cultura de seguridad.

Alta Dirección y Comité Institucional de Gestión y Desempeño (Línea Estratégica):

- Este Comité es responsable de la orientación estratégica para la administración de los activos de información, buscando la sostenibilidad y mejora del sistema en la entidad.
- La Alta Dirección establece y apoya la política y los objetivos de seguridad de la información, asegurándose de que sean compatibles con la dirección estratégica de la organización.
- Garantiza que se dispongan los recursos necesarios (humanos, tecnológicos y económicos) para la implementación, mantenimiento y mejora continua del SGSI.
- Aprueba el Plan de Tratamiento de Riesgos de seguridad de la información y la aceptación de los riesgos residuales, así como los Planes de Continuidad de Negocio (BCP) y Recuperación ante Desastres (DRP).
- Revisa periódicamente el desempeño del SGSI para asegurar su eficacia continua, incluyendo los resultados de la evaluación de riesgos y el estado del plan de tratamiento de riesgos.
- La Dirección de Planeación y Sistemas de Información Ambiental (DPSIA), o quien la Alta Dirección delegue, es la única autorizada para reportar incidentes de seguridad a las autoridades externas y emitir comunicados oficiales.
- La Dirección de Planeación y Sistemas de Información Ambiental (DPSIA) y la Dirección de Gestión Corporativa (DGC) son responsables de gestionar el control de acceso a sistemas y servicios, y de mantener los registros y soportes que autorizan dichos accesos . La DGC también asegura la inclusión de cláusulas de confidencialidad y seguridad en los contratos con proveedores que manejan información sensible de la entidad.

Equipo de Seguridad de la Información (Segunda Línea de Defensa):

- El equipo de seguridad constituye la segunda línea de defensa de la entidad, coordinando la implementación y mantenimiento del Modelo de Seguridad y Privacidad de la Información (MSPI). El dominio de Seguridad y Privacidad de la Información lidera y gestiona el MSPI.
- Actúa como asesor y acompañante de los líderes de proceso en la identificación y valoración de riesgos de seguridad de la información, así como en la formulación de recomendaciones para mitigar dichos riesgos.
- Es el encargado de establecer e implementar los controles específicos necesarios para disminuir el impacto o la probabilidad de ocurrencia de los riesgos identificados. Esto incluye:
    - Hacer seguimiento sobre el cumplimiento de la política de control de acceso lógico y físico.
    - Proponer actividades para gestionar vulnerabilidades técnicas identificadas en las plataformas tecnológicas, de comunicaciones y de seguridad.
    - Adquirir licenciamiento y soporte de soluciones de seguridad perimetral (firewalls) y de protección de endpoints de nueva generación con sistema XDR (antivirus) para equipos informáticos, servidores y dispositivos móviles.
    - Asesorar en el uso de controles criptográficos para proteger información clasificada o reservada.
    - Monitorear continuamente los canales de servicio de internet y la red de la entidad.
    - Realiza diagnósticos periódicos para evaluar el estado actual de la implementación del SGSI, identificando controles implementados y faltantes.

- Lidera la actualización de los procedimientos para la identificación y valoración de activos de información, y colabora técnicamente con los líderes de proceso en esta tarea.
- Monitorea y evalúa continuamente la efectividad de los controles de seguridad implementados, incluyendo la verificación de los planes de continuidad y recuperación.
- Planifica y desarrolla las campañas de sensibilización en seguridad de la información para toda la entidad.

Líderes de Proceso (Primera Línea de Defensa):

- Son los dueños de los riesgos y tienen la responsabilidad principal de identificar y valorar los activos de información bajo su custodia.
- Participan activamente en la identificación y valoración de los riesgos de seguridad de sus respectivos procesos, asegurando su integración en el mapa de riesgos institucional.
- Deberán conocer, apropiar e implementar las directrices y lineamientos definidos en el plan de tratamiento de riesgos de la SDA .
- Enlace Sistema Integrado de Gestión (Enlace SIG):
  - Articula los esfuerzos, recursos, metodologías y estrategias para asegurar la implementación y el mantenimiento del Modelo de Seguridad y Privacidad de la Información (MSPI).
  - Apoya a los líderes de proceso en la identificación y actualización de los activos de información.
  - Participa en la evaluación del desempeño del SGSI y su efectividad.
  - Colabora en la identificación de acciones de mejora para el SGSI [Deducción basada en rol y evaluación del desempeño.

Todos los Funcionarios y Contratistas:

- Tienen la responsabilidad de cumplir con las políticas, procedimientos y lineamientos de seguridad de la información establecidos por la SDA.
- Proteger la información a la que tienen acceso, garantizando su confidencialidad, integridad y disponibilidad.
- Reportar cualquier evento o actividad sospechosa relacionada con la seguridad de la información, a través de los canales internos designados (Mesa de Servicio).
- Participar activamente en las capacitaciones y jornadas de sensibilización sobre seguridad de la información para fortalecer la cultura de seguridad en la entidad.
- Hacer uso adecuado y responsable de los recursos tecnológicos y de la información de la entidad, siguiendo las normas de control de acceso, uso de dispositivos móviles y comunicaciones seguras.Esto incluye:
  - Hacer buen uso de los dispositivos suministrados por la SDA.
  - Utilizar contraseñas robustas y realizar su cambio periódico.
  - Asegurar el adecuado almacenamiento y resguardo de medios removibles.
  - Ser responsable de la seguridad en su puesto de trabajo y del equipo de cómputo asignado.
  - Destruir de forma segura los documentos físicos clasificados como de uso clasificado y reservado.

- Asegurar y legalizar la devolución del activo de información bajo su custodia o responsabilidad al finalizar su vinculación.
- No acceder a áreas seguras sin autorización, a menos que sea en cumplimiento de sus obligaciones.
- Velar por la correcta utilización de la identificación física y la tarjeta de proximidad para el ingreso a la sede principal de la SDA

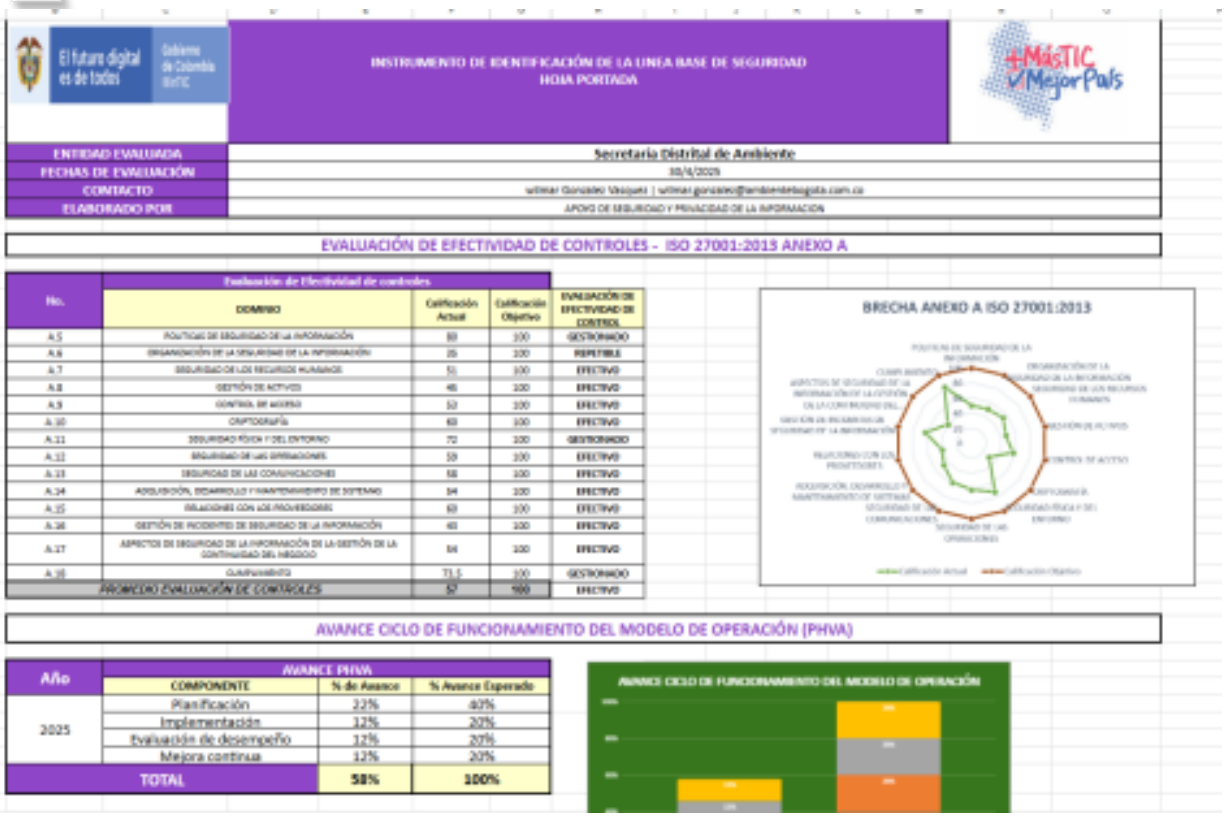
7. AVANCE DE IMPLEMENTACIÓN

OPERACIÓN: EJECUCIÓN DEL PLAN DE SENSIBILIZACIÓN DEL SGSI.

Durante el primer trimestre de 2025, la Secretaría Distrital de Ambiente (SDA) avanzó en el desarrolló el plan de sensibilización de su Sistema de Gestión de Seguridad de la Información (SGSI). Como parte de su ejecución, se realizó capacitación para los equipos de la Subdirección Financiera (SF), Subdirección Contractual (SC), Dirección de Gestión Corporativa (DGC) y Oficina de Participación, Educación y Localidades (OPEL). Adicionalmente, se entregaron piezas de sensibilización que serán utilizadas a partir de abril, lo que contribuye al fortalecimiento de la conciencia y apropiación de la seguridad de la información entre el personal de la entidad.

AUTODIAGNÓSTICO DEL SUBSISTEMA DE SEGURIDAD DE LA INFORMACIÓN.

El instrumento de autodiagnóstico del sistema SGSI de la SDA asociado al Modelo y Privacidad de la Seguridad de la Información fue actualizado en el primer trimestre de 2025. Esta renovación estratégica nos permite evaluar el nivel de madurez y el cumplimiento de la entidad basado en la norma ISO 27001 - 2013 de manera más precisa, facilitando la identificación de brechas y la formulación de acciones de mejora continua.Para este diagnóstico el resultado nos arroja un porcentaje de avance en la implementación de un 58 % donde se toma la sumatoria de los siguientes componentes planificacion, 22%, implementación 12 %, evaluación de desempeño 12%,mejora continua 12 %



INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD
HOJA PORTADA

ENTIDAD EVALUADA	Secretaría Distrital de Ambiente
FECHAS DE EVALUACIÓN	30/4/2025
CONTACTO	wilmar Gonzalez Vasquez | wilmar.gonzalez@ambientebogota.com.co
ELABORADO POR	APOYO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	80	100	GESTIONADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	35	100	REPETIBLE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	51	100	EFECTIVO
A.8	GESTIÓN DE ACTIVOS	48	100	EFECTIVO
A.9	CONTROL DE ACCESO	52	100	EFECTIVO
A.10	CRIPTOGRAFÍA	60	100	EFECTIVO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	72	100	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	59	100	EFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	58	100	EFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	64	100	EFECTIVO
A.15	RELACIONES CON LOS PROVEEDORES	60	100	EFECTIVO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	60	100	EFECTIVO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	64	100	EFECTIVO
A.18	CUMPLIMIENTO	71.5	100	GESTIONADO
	PROMEDIO EVALUACIÓN DE CONTROLES	57	100	EFECTIVO

AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)

Año	AVANCE PHVA		
	COMPONENTE	% de Avance	% Avance Esperado
2025	Planificación	33%	40%
	Implementación	12%	20%
	Evaluación de desempeño	12%	20%
	Mejora continua	12%	20%
TOTAL		58%	100%

Imagen 1. Autodiagnóstico del Modelo y Privacidad de la Seguridad de la Información (MPSI) de la SDA

Planeación de los controles y las políticas que se van a verificar durante el periodo.

Durante el primer trimestre de 2025, la Secretaría Distrital de Ambiente (SDA) ha avanzado en la planificación y ejecución inicial de las actividades del Plan anual de efectividad de los controles.
Específicamente:
• Se ha trabajado en la verificación de controles del Modelo de Seguridad y Privacidad de la Información (MSPI), incluyendo la incorporación y validación de controles de los dominios A.9 (Control de acceso), A.11 (Seguridad física y del entorno) y A.13 (Seguridad en las comunicaciones) de ISO 27001.
• Se han adelantado labores para la verificación de políticas de seguridad y el seguimiento a los planes de mejoramiento de riesgos de seguridad de la información.
• En cuanto a la verificación del Anexo N° 3 de la Resolución 1519 de 2020, se han iniciado acciones para abordar las debilidades previamente identificadas.

Se adelantarán acciones continuas y se consolidará el desarrollo de todos estos puntos durante el próximo trimestre para fortalecer integralmente el SGSI de la entidad.

PROGRAMACION DE LOS EJERCICIOS DE PRUEBA DE LOS DRP QUE SE DEBEN EJECUTAR EN EL AÑO

Durante el primer trimestre de 2025, la Secretaría Distrital de Ambiente (SDA) avanzó en la programación de los ejercicios de prueba de los Planes de Recuperación ante Desastres (DRP) que se ejecutarán durante el año. Esta actividad clave, enmarcada dentro del plan anual de efectividad de los controles del Sistema de Gestión de Seguridad de la Información (SGSI), tiene como fecha de cumplimiento el mes de marzo de cada año.

Como resultado de este proceso de planificación en el primer trimestre, se logró la definición y programación de los DRP a ejecutar. Estos planes son fundamentales para proteger y recuperar la infraestructura tecnológica de la entidad (hardware, software, aplicaciones, bases de datos y telecomunicaciones) en caso de interrupciones significativas. La programación se basa en el Análisis de Impacto al Negocio (BIA) previo, que clasifica la criticidad de los procesos y establece el orden de recuperación. La ejecución de estas programaciones busca asegurar la disponibilidad e integridad de los datos y la continuidad de las operaciones críticas de la SDA.

Actualizar las actividades de Continuidad de cada uno de los procesos de la SDA ante los escenarios planteados en el BCP

Durante el primer trimestre de 2025, TI- DPSIA adelantó actividades para actualizar la información de los documentos con los que cuenta la entidad: BIA, BCP y DRP alineada con con la actualización de activos de información, , con el objetivo de articular las acciones a desarrollar en caso tal que la operación de la entidad se vea afectada parcial o totalmente, para ser desarrolladas en los siguientes periodos.