Seguridad y privacidad de la Información

Informe trimestral Plan de Tratamiento de riesgos

I trimestre 2025

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

Tabla de contenido

Contenido

1. INTRODUCCIÓN 3
2. OBJETIVO 3
3. ALCANCE 3
4. NORMATIVIDAD (BASE LEGAL) 4
5. DEFINICIONES 6
6. RESPONSABILIDAD Y AUTORIDAD 6
7. AVANCE DE IMPLEMENTACIÓN 9
7.1 METODOLOGÍA DE RIESGO 14
8. CONCLUSIONES Y RECOMENDACIONES 15

1. INTRODUCCIÓN

La Secretaría Distrital de Ambiente (SDA) presenta este informe con el propósito de ser transparente y comunicar a la ciudadanía nuestras acciones para proteger la información que gestionamos. En un entorno digital en constante evolución, donde los riesgos cibernéticos son una preocupación creciente, es fundamental garantizar la confidencialidad, integridad y disponibilidad de toda la información.

Este documento busca asegurar la confianza pública en el uso de las tecnologías digitales y en la gestión de nuestra entidad. A través del Plan de Tratamiento de Riesgos, identificamos, analizamos y gestionamos proactivamente las amenazas a nuestra información, asegurando que se mantenga protegida y disponible para el servicio a los ciudadanos.

2. OBJETIVO

Evidenciar el seguimiento a las actividades realizadas para dar cumplimiento al El Plan de Tratamiento de Riesgos de Seguridad de la Información de la Secretaría Distrital de Ambiente (SDA)

3. ALCANCE

Este documento describe el desarrollo de las actividades establecidas en el El Plan de Tratamiento de Riesgos de Seguridad de la Información de la Secretaría Distrital de Ambiente 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. incluye:

- Inicio: El proceso inicia con la identificación y valoración de los riesgos de seguridad que podrían afectar nuestra información y nuestros procesos. Se presta especial atención a aquellos riesgos clasificados como Extremos, Altos o Moderados, los cuales superan el nivel de riesgo aceptable para la SDA. Esta etapa es fundamental para comprender las posibles amenazas y vulnerabilidades.
- Acciones: Continuamos con la definición e implementación de acciones y controles específicos para tratar y mitigar estos riesgos identificados. Esto incluye la aplicación de medidas de prevención para reducir la probabilidad de ocurrencia de incidentes, así como estrategias de mitigación para disminuir sus consecuencias en caso de que lleguen a materializarse.
- Seguimiento: El proceso finaliza con el seguimiento continuo y la evaluación periódica de la efectividad de las acciones implementadas.

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 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.

Norma (número y fecha)	Descripción
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.
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

Norma (número y fecha)	Descripción
	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.
Guía para la administración del riesgo y el diseño de controles en entidades públicas -V6: noviembre 2022.	Establece la metodología para la administración del riesgo, los criterios para el análisis de probabilidad e impacto identificado y su respectivo nivel de severidad. En la versión 5 se actualizaron y precisaron algunos elementos metodológicos para mejorar el ejercicio de identificación y valoración del riesgo.

Tabla 1. Normatividad

5. DEFINICIONES

- Plan de Tratamiento de Riesgos: Documento que contiene las actividades planificadas y organizadas para abordar los riesgos de seguridad y privacidad de la información que han sido identificados y valorados. Su objetivo principal es asegurar que los niveles de riesgo residual (es decir, el riesgo que queda después de aplicar los controles) sean aceptables para las diferentes áreas de la entidad.

- Plan de Seguridad y Privacidad de la Información: Documento donde se define la planeación del tiempo, recursos y presupuesto de las actividades que va a desarrollar relacionadas con el MSPI.

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. Para lograrlo, hemos establecido roles y responsabilidades claras, enmarcadas en un modelo de Tres Líneas de Defensa, un esquema que permite gestionar los riesgos de manera

integral y eficiente. 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

La Secretaría Distrital de Ambiente (SDA) reafirma su compromiso con la seguridad y privacidad de la información, un pilar fundamental para garantizar la confianza de los ciudadanos y la transparencia en su gestión. Para ello, la SDA ha adelantado acciones adoptado e implementado 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). Este sistema, que se basa en el estándar internacional ISO/IEC 27001:2013, busca asegurar la confidencialidad, integridad y disponibilidad de toda la información de la entidad, gestionando proactivamente los riesgos y cumpliendo con la legislación vigente.

Durante el primer trimestre, el equipo de seguridad de la información de la SDA adelantó acciones en el análisis, planeación y la evaluación de la pertinencia de actualización de los activos de información, riesgos de seguridad y planes de continuidad.

Se han identificado oportunidades de mejora en la formalización de procedimientos de gestión de seguridad informática, incluyendo el análisis y gestión de riesgos, e implementación de controles de seguridad para los servicios tecnológicos.

La siguiente tabla ilustra los controles de la Norma ISO 27001 aplicables a los sistemas de información de la SDA. Documentados en la Matriz de Administración de Riesgos de Seguridad de la Información 2025.

Control Anexo A (ISO27001)	Acciones
5.18 - Derechos de acceso	Permisos que se deben otorgar, revisar o derogar a los usuarios para crear, modificar, eliminar o leer la información de cada uno de los activos del proceso, es decir definir e implementar la tabla de accesos con su respectiva revisión regularmente.
5.3 - Segregación de funciones	Asegurar que las funciones incompatibles estén asignadas a diferentes cargos/personas (Ej. las siguientes tareas deben estar separadas: registrar con autorizar, autorizar con pagar) Estas definiciones se deben reflejar en las tablas de acceso (ver numeral 5.18)
5.14 - Transferencia de información	Aplica si se transfiere información a otras entidades, se deben definir políticas y controles y divulgarlas a los terceros, donde se incluya: Controles de cifrado para prevenir intersecciones, accesos no autorizados, destrucción o denegación del servicio. Asegurar la trazabilidad y la no repudiación, incluido el mantenimiento de la cadena de custodia durante el tránsito. Identificación de los contactos apropiados relacionados con la transferencia donde se considere propietarios del activo, propietarios de riego, oficiales de seguridad y los custodios de la información. Responsabilidades en caso de incidentes de seguridad de la información. Fiabilidad y disponibilidad del servicio de transferencia. Uso aceptable de la información. Manejo de firmas electrónicas.

5.19 - Seguridad de la información en las relaciones con los proveedores	1. Implementar una política y procedimientos divulgados donde se considere: a) Identificar y documentar los tipos de proveedores que pueden afectar la confidencialidad, integridad y disponibilidad de la información en los diferentes procesos de la organización. b) Establecer cómo evaluar y seleccionar proveedores según la sensibilidad de la información, los productos y los servicios (Ej. Análisis de mercado, referencias de clientes, revisión de documentos, evaluaciones in situ, certificaciones) c) Evaluar y seleccionar los productos o servicios del proveedor que tengan controles adecuados de seguridad de la información y revisarlos, en particular la integridad y exactitud de los controles implementados por el proveedor, que garanticen la seguridad de la información. d) Definir la información de la organización, los servicios de TIC y la infraestructura física a la que los proveedores pueden acceder, supervisar, controlar y utilizar. e) Definir los tipos de componentes y servicios de la infraestructura de TIC proporcionados por los proveedores que puedan afectar la seguridad de la información. f) Gestionar los riesgos de seguridad de la información relacionados con el uso de la información por parte del proveedor, el mal funcionamiento o las vulnerabilidades de los productos o servicios prestados por los proveedores (incluir componentes y subcomponentes de software utilizados en los productos) g) Supervisar el cumplimiento de los requisitos de seguridad establecidos para cada tipo de proveedor. h) Mitigación de la no conformidad, independiente de los medios usados para su detección. i) Manejo de incidentes y contingencias asociados con productos y servicios del proveedor, incluyendo las responsabilidades de las dos partes. j) Resiliencia y, si es necesario, medidas de recuperación y contingencia. l) Gestionar la transferencia de información, según las necesidades. m) Requisitos para asegurar una terminación segura de la relación con el proveedor, incluyendo: Retiro de permisos. Tratamiento de la información. Determinar la titularidad de la propiedad intelectual desarrollada durante el contrato. Portabilidad de la información en caso de cambio de

	proveedor o recurso interno. Gestión de documentos. Devolución de activos. Disposición segura de la información y otros activos asociados. Requisitos de confidencialidad continuos." n) Nivel de seguridad del personal y seguridad física que se espera por parte del proveedor. 2. Los procedimientos para continuar con el tratamiento de la información en caso de que el proveedor no pueda suministrar sus productos o servicios (Ej. incidente, el proveedor ya no está en el negocio)

5.30 -Preparación de las TIC para la continuidad de la actividad	Identificar e implementar controles para asegurar la continuidad de los servicios del proceso cuando los sistemas o servicios de TI no estén disponibles. Documentar los procesos, procedimientos e instructivos con el detalle de las actividades y responsables, así como los sistemas/herramientas utilizadas para garantizar la continuidad de la operación por cualquier colaborador.
5.34 -Protección y privacidad de la información de carácter personal	Controles para dar cumplimiento a la ley de protección de datos personales.
7.10 -Medios de almacenamiento	Aplica si la información es extraída a discos externos o USB.
8.10 -Eliminación de la información	Controles para la disposición final de la información alineados con los requisitos legales, reglamentarios y contractuales para la eliminación de la información, considerar: Selección del método de borrado seguro. Registro/evidencia de los resultados de la eliminación. Si se utiliza un proveedor, asegurar cláusulas de confidencialidad, y establecer como entregable evidencia de los resultados de la eliminación.
8.13 -Copias de seguridad de la información	Definir los registros, ubicación, periodicidad para realizar backups, periodo de retención de la copia, responsable de realizar la copia, responsable de custodiar la copia, periodicidad para realizar pruebas de restauración de las copias, incluyendo el registro/evidencia del resultado de la prueba. Controles para asegurar la confidencialidad de la información almacenada en las copias de respaldo.

7.1 METODOLOGÍA DE RIESGO

Metodología para la identificación y valoración de riesgos de seguridad de la información:

IDENTIFICACIÓN DEL RIESGO			
CAMPO	**DEFINICIÓN**	**INSTRUCTIVO**	**RESPONSABLE DE DILIGENCIAMIENTO**
No. de Riesgo	Número del riesgo a identificar y valorar.	NO diligenciar es automático.	N/A
Proceso	Proceso sobre el cual se está llevando a cabo la identificación y valoración de riesgos	Seleccione el nombre del proceso.	Líder de proceso / funcionario designado
Activo de Información	Campo que permite el registro del nombre o denominación de un activo de información. Diligencie este campo cuando requiera realizar una valoración de riesgos específica sobre un activo. *No registre activos de información que no se hayan identificado de manera previa en la matriz de activos de información.* Ej. Base de datos nómina, Servidor principal, Actas de reunión o aprobación.	Registre el nombre o denominación de un activo de información. Diligencie este campo cuando requiera realizar una valoración de riesgos específica sobre un activo. *No registre activos de información que no se hayan identificado de manera previa en la matriz de activos de información.* Ej. Base de datos nómina, Servidor principal, Actas de reunión o aprobación.	Líder de proceso / Colaborador designado
Tipo de activo	Campo que permite seleccionar entre las diferentes categorías o grupos de activos de información que se encuentran definidos tanto dentro del inventario de activos de información.	Seleccione la categoría de activos a la que pertenece el activo que ha diligenciado en el campo anterior sobre la cual desea evaluar el riesgo	Líder de proceso / Colaborador designado
Amenazas (Causa Inmediata)	Campo que permite seleccionar de un conjunto de amenazas para cada activo de información. EJ. [A01] Acceso no autorizado o [A06] Divulgación no autorizada de datos o información.	Seleccione una amenaza del listado de amenazas posibles	Líder de proceso / Colaborador designado
Vulnerabilidades (Causa raíz)	Campo que permite seleccionar las vulnerabilidades de las cuales se puede aprovechar la amenaza identificada y así causar la materialización del riesgo.	Selección una vulnerabilidad de la lista que pueda aprovechar la amenaza identificada en el campo anterior	Líder de proceso / Colaborador designado
Tipo de riesgo	Campo que define si es un riesgo de confidencialidad, integridad o disponibilidad.	Selección el tipo de riesgo de la lista	Líder de proceso / Colaborador designado
Descripción del Riesgo	Campo donde se describe el riesgo	Describa el riesgo, Ej.: *"Pérdida de integridad de la información del proceso contenida en la carpeta compartida por modificación no autorizada causando reprocesos".*	Líder de proceso / Colaborador designado
Clasificación riesgo	Campo que describe las posibles clasificaciones que puede tener el riesgo de seguridad de la información	Seleccione a cuál se puede asociar el riesgo identificado.	Líder de proceso / Colaborador designado

8. CONCLUSIONES Y RECOMENDACIONES

Durante el primer trimestre de 2025, la SDA ha avanzado en el análisis, la planificación y la evaluación para la actualización de sus activos de información, riesgos de seguridad y planes de recuperación. Estas acciones se enmarcan en la adopción del Sistema de Gestión de Seguridad de la Información (SGSI), basado en el estándar internacional ISO/IEC 27001:2013 y el Modelo de Seguridad y Privacidad de la Información (MSPI) de MinTIC. Esto implica un abordaje continuo y sistemático en áreas clave como la actualización continua del autodiagnóstico (Análisis GAP) el cual es fundamental para identificar el estado actual de la entidad respecto a la adopción del MSPI, usando el "instrumento de evaluación MSPI" para identificar controles implementados y faltantes.

- La actualización del autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) es una acción fundamental para la Secretaría Distrital de Ambiente (SDA). Este análisis de brechas es el paso inicial y esencial para identificar el estado actual y el nivel de madurez de la entidad en seguridad y privacidad de la información.
- Actualización de activos de información: Este proceso es fundamental para la gestión de riesgos y la continuidad del negocio, permitiendo una operación más segura, eficiente
- Realizar la actualización de los planes de recuperación BIA BCP Y DRP: La actualización de escenarios y estrategias de recuperación, asegurando que los planes sean probados regularmente (al menos una vez al año) para verificar su viabilidad y familiarizar al personal con sus roles.
- Garantizar el cumplimiento con los estándares y lineamientos de seguridad digital, particularmente las condiciones mínimas técnicas y de seguridad digital definidas en el Anexo N° 3 de la Resolución 1519 de 2020 del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).