



Plan de Tratamiento de Riesgos 2025 - SDA



SECRETARÍA DE
AMBIENTE



Tabla de contenido

1. INTRODUCCIÓN.....	3
2. OBJETIVO.....	3
3. ALCANCE	4
4. NORMATIVIDAD (BASE LEGAL)	4
Tabla 1. Normatividad (MINTIC 2021)	7
5. DEFINICIONES	7
6. RESPONSABILIDAD Y AUTORIDAD.....	8
Tabla 2. Responsabilidad y Autoridad.....	9
7. PLAN DE TRATAMIENTOS DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN	9
7.1. Identificar y valorar los Riesgo de Seguridad de la Información.	10
Imagen 1. Total, activos de información. tomado del inventario de activos de información de la SDA.	10
Imagen 2. Activos críticos. tomado del inventario de activos de información de la SDA.	11
7.2. Riesgos del proceso Gestión Tecnológica.	11
Imagen 3. Activos críticos de Gestión de Tecnología. tomado del inventario de activos de información de la SDA.	12
7.3. Plan de tratamiento de Riesgos.	13
Tabla 3. Plan de tratamiento de Riesgos de Seguridad de la Información	14
REFERENCIAS BIBLIOGRÁFICAS	14

1. INTRODUCCIÓN

El plan de tratamiento de riesgos de Seguridad de la información de la Secretaría de Ambiente (SDA), define las actividades para identificar, analizar, tratar, evaluar y evaluar periódicamente los riesgos de seguridad de la información en cada uno de los procesos de la Entidad, permitiendo así mitigar los riesgos y mantener su valoración en un residual aceptable para la SDA, este plan se encuentra articulado con la política de riesgos de la entidad y busca contar con un plan de actividades que ayuden a mantener y mejorar la gestión de riesgos relacionados con seguridad de la información.

En Colombia, durante los últimos años se ha puesto a la vanguardia la lucha contra las amenazas en el ámbito digital con estrategias tales como:

- El Documento CONPES 3995 de 2020 y el Decreto Único Reglamentario del Sector TIC, Decreto 1078 de 2015, que señala la el habilitador de seguridad y privacidad de la Información, reglamentado por la 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.
- Adoptando, además las buenas prácticas y los lineamientos de los estándares ISO 27001, ISO 31000 y la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 6, emitida por el Departamento Administrativo de la Función Pública (DAFP).
- De la misma forma, el apoyo de diferentes organizaciones para la prevención y gestión de incidentes (MinTIC, Grupo de Respuestas a Emergencias Cibernéticas de Colombia ColCERT, Equipo de respuesta a incidentes de seguridad informática CSIRT, - Centro Cibernético Policial de la Policía Nacional), los mecanismos de investigación (fiscalía general de la Nación, Centro Cibernético Policial) y de judicialización (rama judicial).

2. OBJETIVO

Establecer las acciones para tratar de manera integral los riesgos relacionados con la seguridad y privacidad de la información a los que la Secretaría Distrital de Ambiente pueda estar expuesta; protegiendo y preservando la integridad, confidencialidad y disponibilidad de la información, con el fin de evitar materializaciones de situaciones que pueden afectar el cumplimiento de su misión y el logro de su visión estratégica.

2.1 Objetivos Estratégicos.

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

- Gestionar de manera integral los riesgos de seguridad y privacidad de la información para alcanzar los objetivos, la misión y la visión institucional.
- Contribuir al fortalecimiento y apropiación de conocimiento sobre la gestión de riesgos de seguridad y privacidad de la información
- Propiciar las acciones conducentes al cierre de brechas identificadas.
- Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana.

3. ALCANCE

El plan de tratamiento de riesgos de seguridad aplica a toda la Entidad, se enfoca en gestionar y tratar todos los riesgos de seguridad de la información, en especial los que se encuentran en la zona de riesgo Extremo, Alto o Moderado, los cuales superan el apetito de riesgo aceptable en la SDA, con la finalidad de generar mecanismos de prevención y mitigación de los mismos, fortalecer la toma de decisiones y la prevención frente a la materialización de incidentes de seguridad de la información que puedan afectar el logro de los objetivos institucionales.

Un adecuado tratamiento y gestión de los riesgos debe contar con la participación activa de todos los procesos de la SDA, con el fin de conocer, apropiar e implementar las directrices y lineamientos definidos y realizar el seguimiento o monitoreo correspondiente de acuerdo a la Política de Riesgos de la Entidad.

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,

Norma (número y fecha)	Descripción
	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.
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.

Norma (número y fecha)	Descripción
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 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

Norma (número y fecha)	Descripción
	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 (MINTIC 2021)

5. DEFINICIONES

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

- **Alta dirección:** persona o grupo de personas que dirige y controla una organización, al nivel más alto (ISO/IEC 27001:2013).
- **Activo de Información:** un activo de información es cualquier elemento que contenga, genere, adquiera, gestione y/o procese información, que tiene valor para uno o más procesos de la organización y debe protegerse (ISO/IEC 27001:2013).
- **Aceptación de riesgo:** decisión de asumir un riesgo. Amenazas: situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización. • **Amenaza:** es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo). (DAFP, 2022)
- **Análisis de Riesgo:** uso sistemático de la información para identificar fuentes y estimar el riesgo (Guía ISO/IEC 73:2002).
- **Apetito al riesgo:** magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener. (DAFP, 2022)
- **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo. (DAFP, 2022)
- **Control o medida:** acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad. (DAFP, 2022)

- **Evaluación del riesgo:** proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo. (DAFP, 2022)
- **Gestión de riesgos:** actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y su tratamiento. (ISO 27000, Glosario de términos y definiciones).
- **Impacto:** son las consecuencias que genera un riesgo una vez se materialice. • **Mapa de riesgos:** documento con la información resultante de la gestión del riesgo. (DAFP, 2022)
- **Probabilidad:** es la posibilidad de que la amenaza aproveche la vulnerabilidad para materializar el riesgo. (DAFP, 2022)
- **Riesgo:** es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos. (DAFP, 2022)
- **Riesgo de seguridad de la información:** combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas. (DAFP, 2022)
- **Riesgo inherente:** nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control. (DAFP, 2022)
- **Riesgo residual:** nivel restante de riesgo después del tratamiento del riesgo. (DAFP, 2022)
- **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos. (DAFP, 2022)

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	Articular los esfuerzos, recursos, metodologías y estrategias para asegurar la identificación y el tratamiento de riesgos de seguridad de la información.

Rol	Responsabilidad
Enlace Sistema Integrado de Gestión	
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 TRATAMIENTOS DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN

La SDA consciente de la responsabilidad e importancia del manejo de los riesgos asociados a los diferentes procesos definidos en el Sistema Integrado de Gestión, implementa el procedimiento PE03-PR02 Administración de riesgos donde se definen las actividades para administrar y gestionar los riesgos asociados a las actividades y procesos de la entidad, con el propósito de prevenir pérdidas y mitigar su impacto en caso de materialización, que afecte el cumplimiento de los objetivos institucionales a través de un enfoque sistemático establecido en las metodologías dispuestas para ello.

Durante la ejecución de este procedimiento se tiene como resultado al realizar la identificación, análisis y evaluación de los riesgos de seguridad de la información:

- Identificación, análisis y evaluación de los riesgos de seguridad de la información en el documento PE03-PR02-F2 Mapa de riesgos institucional usando como insumo el documento PA06-PR02-F2 Inventarios de activos de información no documental de cada uno de los procesos.
- Seleccionar activos críticos, para el año 2024 se identificaron como críticos los activos que cumplían los siguientes criterios:
 - Nivel de Confidencialidad: Alta
 - Nivel de Integridad: Alta

- Nivel de Disponibilidad: Alta
- Realizar mesas de trabajo con los procesos para identificar y valorar los riesgos.
- Actualizar el documento PE03-PR02-F1 Declaración de aplicabilidad de seguridad de la información y los demás documentos relacionados con la administración del riesgo de seguridad de la información.

7.1. Identificar y valorar los Riesgo de Seguridad de la Información.

La nueva versión del inventario de activos de información, creada a partir de la actualización de activos de información del año 2023, tiene una distribución, entre los 18 procesos de la SDA, como se muestra en la siguiente imagen.

Proceso	Total AI
COMUNICACIONES	3
CONTROL Y MEJORA	3
DIRECCIONAMIENTO ESTRATÉGICO	4
EVALUACIÓN CONTROL Y SEGUIMIENTO	93
GESTIÓN ADMINISTRATIVA	75
GESTIÓN AMBIENTAL Y DESARROLLO RURAL	2
GESTIÓN CONTRACTUAL	55
GESTIÓN DE TALENTO HUMANO	113
GESTIÓN DISCIPLINARIA	1
GESTIÓN DOCUMENTAL	17
GESTIÓN FINANCIERA	91
GESTIÓN JURÍDICA	5
METROLOGÍA MONITOREO Y MODELACIÓN	68
PA03-Gestión Tecnológica	49
PARTICIPACIÓN Y EDUCACIÓN AMBIENTAL	18
PLANEACIÓN AMBIENTAL	3
SERVICIO A LA CIUDADANÍA	5
SISTEMA INTEGRADO DE GESTIÓN	5
Suma total	610

Imagen 1. Total, activos de información. tomado del inventario de activos de información de la SDA.

En la siguiente imagen se muestran los activos que se consideran críticos, con los procesos propietarios de estos activos se realizó las actividades, durante el segundo semestre de 2024, para identificar y valorar sus riesgos de seguridad.

Activos de información críticos: Confidencial = Alta, Integridad = Alta, Disponibilidad = Alta	
Proceso	Cuenta de Confidencialidad
COMUNICACIONES	1
EVALUACIÓN CONTROL Y SEGUIMIENTO	9
GESTIÓN DE TALENTO HUMANO	4
GESTIÓN DISCIPLINARIA	1
GESTIÓN FINANCIERA	4
GESTIÓN JURÍDICA	1
METROLOGÍA MONITOREO Y MODELACIÓN	8
PA03-Gestión Tecnológica	18
PARTICIPACIÓN Y EDUCACIÓN AMBIENTAL	2
SERVICIO A LA CIUDADANÍA	2
Suma total	50

Imagen 2. Activos críticos. tomado del inventario de activos de información de la SDA.

para el primer reporte de entrega de las matrices por parte de los enlaces de sistema de Gestión, se identificaron 6 riesgos reportados por los procesos:

- Comunicaciones
- Participación y Educación Ambiental
- Gestión del talento humano
- Servicio a la ciudadanía

De estos riesgos 4 en la zona de riesgo inherente Alta y 2 en la zona de riesgo Moderada, después de aplicar controles se tiene:

- 2 riesgos en la zona de riesgo Alta
- 4 riesgos en la zona de riesgo moderada.

Para todos estos riesgos se definen planes de mejora que deben ser verificados durante el próximo año. Es necesario planear acciones que permitan tener la identificación y valoración de los riesgos para los procesos que faltan.

7.2. Riesgos del proceso Gestión Tecnológica.

Debido a que no se encontró evidencia de la realización de este ejercicio antes, para Gestión tecnológica, que tiene la mayor cantidad de activos de información críticos, se les propuso agruparlos como se muestra en la siguiente imagen.

Nombre AI	Descripción AI	Realiza/crea
Sistema de información Ambiental SIA -procesos y documentos. Forest BPMN	Servicio FOREST (Herramientas tecnológicas)	2023
Bases de datos en motor ORACLE	Servicios de Gestión de Bases de Datos	2023
Almacenamiento y acceso a archivos (FILESERVER)	Servicios de SERVIDOR DE ARCHIVOS (FILESERVER)	2023
Copias de respaldo BACKUPS	Servicios de SERVIDOR DE ARCHIVOS (FILESERVER)	2023
Conectividad cableada	Servicios de redes y conectividad	2023
Conectividad inalámbrica	Servicios de redes y conectividad	2023
DHCP Y DNS	Servicios de redes y conectividad	2023
Directorio Activo de la SDA	Servicio de Gestión de Usuarios	2023
Seguridad Perimetral	Servicios de seguridad Perimetral	2023
Servidores y almacenamiento	Servicio de Datacenter, servicio de almacenamiento local	2023
Red Privada Virtual (VPN)	Servicios de redes y conectividad	2023
WAN e INTERNET	Servicios de redes y conectividad	2023
Centro de datos (datacenter) de la SDA	Servicio de Datacenter	2023
Centro de operaciones de seguridad (SOC)	Servicios de seguridad Perimetral (control)	2023
Archivo confidencial de acceso para la administración de la infraestructura tecnológica de la SDA	Servicio de Datacenter (continuidad)	2023
Equipos físicos de conectividad	Servicios de redes y conectividad	2023
Tarjeta de acceso al Centro de datos de la SDA	Servicio de Datacenter (control)	2023
Bitacora de acceso al Centro de datos de la SDA	Servicio de Datacenter (control)	2023
Servicios en la nube: correo electrónico, Almacenamiento (DRIVE)	Servicios Google correo electrónico y Unidades Compartidas para almacenamiento de información para cada proceso.	2024
Antivirus	Servicios de seguridad Interna para detección de virus y aplicación de controles como autorización del uso de USB	2024

Imagen 3. Activos críticos de Gestión de Tecnología. tomado del inventario de activos de información de la SDA.

De esta forma Gestión tecnológica debe trabajar siete riesgos:

- Color naranja: Dominio de sistemas de información: controles que garantizan la seguridad en todas las soluciones tecnológicas que gestiona.
- Color naranja claro: Dominio de información: controles que garantizan la seguridad en todos los repositorios de información.
- Color amarillo: Dominio de servicios de TI: almacenamiento
- Color Verde: Dominio de servicios de TI: redes y comunicaciones
- Color azul claro: Dominio de servicios de TI: seguridad de componentes en sitio.
- Color morado: Dominio de servicios de TI: seguridad de componentes en la nube
- Color azul oscuro: Dominio de servicios de TI: seguridad de componentes de seguridad perimetral.

El activo de color rojo, se debe eliminar ya que no esté en uso, los dos últimos activos se adicionaron por recomendaciones de la auditoría y por el incidente de disponibilidad del correo electrónico en julio de 2024.

Es necesario definir acciones que permitan tener la definición de controles y planes de mejora para lograr el diseño y ejecución de los controles recomendados por la MSPI, el instrumento que se está usando queda en la ruta

<https://docs.google.com/spreadsheets/d/1sDy5uLZDTGmCOCK6xeF5BzjKiOotlUb53KstI7LyW6Q/edit?gid=1472333324#gid=1472333324>

7.3. Plan de tratamiento de Riesgos.

Las actividades relacionadas en este plan de tratamiento de riesgos de seguridad aplica a toda la SDA, se enfocan en gestionar y tratar todos los riesgos de seguridad de la información, en especial los que se encuentran en la zona de riesgo Extremo, Alto o Moderado, los cuales superan el apetito de riesgo aceptable en la SDA, con la finalidad de generar mecanismos de prevención y mitigación de los mismos, fortalecer la toma de decisiones y la prevención frente a la materialización de incidentes de seguridad de la información que puedan afectar el logro de los objetivos institucionales.

Ámbito	Objetivo	Resultado	Responsable(s)	Tiempo de ejecución
Planeación	Definir y publicar el Plan de Tratamiento de Riesgos de Seguridad de la Información.	Plan de Tratamiento de Riesgos de Seguridad de la Información.	Equipo de seguridad de la información Asesor TI Enlace SIG	Febrero de cada año
Operación	Apoyar que cada proceso revise y actualice, al menos una vez al año, su registro de activos e información.	Inventario de Activos de Información actualizado, identificando los activos críticos. Actualizar la versión de declaración de aplicabilidad.	Equipo de seguridad de la información Responsable de procesos.	Diciembre de cada año.
Operación	Apoyar que cada proceso revise y actualice, al menos una vez al año, sus Riesgos de Seguridad de la Información	Mapa de riesgos	Equipo de seguridad de la información Responsable de procesos.	Informe a diciembre de cada año de las sesiones que se programaron

Ámbito	Objetivo	Resultado	Responsable(s)	Tiempo de ejecución
Operación	Identificar y valorar los riesgos de seguridad de la información de los dominios de Tecnología.	Matriz de riesgos de tecnología	Equipo de Seguridad de la Información Profesional responsable de dominio	Diciembre de cada año.

Tabla 3. Plan de tratamiento de Riesgos 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/MSP/>

DAFP, Departamento Administrativo de la Función Pública. noviembre de 2022. Guía para la administración del riesgo y el diseño de controles en entidades públicas -V6. https://www1.funcionpublica.gov.co/documents/28587410/34299967/Guia_administracion_riesgos_capitulo_riesgo_fiscal.pdf

Oficina De Control Interno. SDA. 2023 Informe Final de Auditoría al Proceso de Gestión Tecnológica. <https://drive.google.com/drive/folders/1sluxUIbdtqmln8YbCIGbQgmGJz-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