# Tabla de Contenido



# Tabla de Ilustraciones

## 1. INTRODUCCIÓN

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Secretaría Distrital de la Mujer, tiene por objetivo definir un adecuado tratamiento de los riesgos de seguridad de la información, teniendo en cuenta los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) de Mintic, con lo cual se pretende minimizar la materialización de los riesgos.

La administración de los riesgos, consiste en identificar, analizar y gestionar los riesgos de seguridad de la información que se puedan presentar en el cumplimiento de la misionalidad de la entidad, lo cual involucra entre otros, el uso de la tecnología, equipos de cómputo, dispositivos móviles, red y canales de datos, infraestructura física y virtual, asociados cada uno de los procesos y dependencias que conforman la entidad y que pueden conllevar a pérdida, modificación, alteración, destrucción de la información entre otros, de otra parte la gestión de riesgos de seguridad de la información, consiste en realizar el análisis de identificación de riesgos, cuyo resultado conlleva a la formulación del plan de tratamiento y administración de los mismos.

El presente documento tiene en cuenta los lineamientos y directrices indicados por el Ministerio de las TIC en el Modelo de Seguridad y Privacidad de la Información – MSPI, el cual pertenece al habilitador transversal de la Política de Gobierno Digital y de la misma forma se tiene en cuenta los estándares de la ISO 27001:2013, cuyo objetivo es minimizar, gestionar y controlar los riesgos de seguridad de la información teniendo en cuenta las causas, probabilidad e impacto, velando así por la protección y seguridad de la información institucional. El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Secretaría Distrital de la Mujer, tiene como hoja de ruta la gestión de los riesgos de seguridad de la información, incorporando mecanismos, controles y acciones orientadas a minimizar los riesgos y sus efectos, con el propósito de garantizar la disponibilidad, integridad y confidencialidad de la información.

Es importante resaltar la necesidad de realizar una adecuada identificación, clasificación y valoración de los riesgos, que pueden afectar o comprometer la seguridad y privacidad de la información en los procesos y dependencias de la Entidad, con el propósito de garantizar la disponibilidad, integridad y confidencialidad de la información, por lo cual se deben establecer controles y medidas de seguridad, cuyo objetivo es asegurar la información de la Entidad en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y activos de información.

La implementación del Plan de Tratamiento de Riesgos de Seguridad de la Información en la Entidad, obedece a las necesidades objetivas, requisitos y acciones en materia de seguridad de la información, promoviendo así la implementación y apropiación de las mejores prácticas, definidas en el MSPI y en la norma ISO 27001 para la gestión e implementación de Sistemas de Gestión de Seguridad de la Información.

## 2. OBJETIVO GENERAL:

Definir Plan de Tratamiento de Riesgos de Seguridad de la Información de la Secretaría Distrital de la Mujer para la vigencia 2022, cuya finalidad es proteger los activos de información preservando su

integridad, disponibilidad y confidencialidad, alineado a la Política de Gestión del Riesgo, lo cual permitirá a los responsables de los procesos gestionar los riesgos en materia de seguridad y privacidad de la información, los cuales se identifican a partir del inventario de activos de información y se tratan en concordancia con su nivel de criticidad.

## 3. OBJETIVOS ESPECÍFICOS

- Proteger los activos de información de la Secretaría Distrital de la Mujer.
- Tratar y gestionar adecuadamente los riesgos de seguridad de la información que puedan afectar la confidencialidad, integridad y disponibilidad de la información.
- Realizar seguimiento a los planes de tratamiento de riesgos de seguridad de la información, por medio del mapa de riesgos de cada proceso.

## 4. ALCANCE

Plan de Tratamiento de Riesgos de Seguridad de la Información de la Secretaría Distrital de la Mujer define el plan de trabajo para ejecutar la administración y gestión de los riesgos de seguridad de la información a nivel de los procesos y dependencias de la Entidad con las actividades a desarrollar durante el periodo 2022.

## 5. MARCO NORMATIVO

| NORMA | DESCRIPCIÓN |
|---|---|
| Decreto 1078 de 2015 | Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones (Título 9, Capítulo 1). |
| 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 |
| Guía para la administración del riesgo y el diseño de controles en entidades públicas -V5 | 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. |
| Modelo de Seguridad y privacidad de la información - MSPI | Se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Política de Gobierno Digital, TIC para el Estado y TIC para la Sociedad. TIC, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales |

| | |
|---|---|
| NTC/ISO 27001 de 2013 | Sistemas de Gestión de Seguridad de la Información. Sistema de Gestión de Seguridad de la Información (SGSI) es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para alcanzar los objetivos de negocio. |

## 6. ROLES Y RESPONSABILIDADES

### 6.1. Oficina Asesora de Planeación

- Responsable de realizar seguimiento cuatrimestral a los Riesgos de Gestión, Corrupción y Seguridad de la Información.

### 6.2. Oficina Asesora de Planeación – Gestión Tecnológica

- El Plan de Tratamiento de Riesgos de Seguridad de la Información se encuentra bajo la responsabilidad de la Oficina Asesora de Planeación – Gestión Tecnológica, quien establece los lineamientos y directrices, necesarias para realizar el seguimiento, implementación de controles y acciones que servirán para el tratamiento y mitigación de los riesgos de Seguridad de la Información.
- Responsable de definir y ejecutar el plan de comunicación, sensibilización y capacitación en seguridad de la información, cuyo objetivo es concientizar a las servidoras, servidores y contratistas, en lo relacionado con el tratamiento de los riesgos de seguridad de la información en la Entidad.
- Responsable de apoyar a los procesos en las actividades conducentes a la identificación de los riesgos de seguridad de la información.

### 6.3. Responsables (Lideresas) de Procesos y Dependencias

- Son responsables de identificar los riesgos, establecer acciones y/o controles para mitigarlos y aprobar los planes de tratamiento de los riesgos identificados.
- Realizar seguimiento a la gestión y ejecución de los riesgos de seguridad de la información, de acuerdo con los lineamientos establecidos en la Entidad. Cabe aclarar que, para cumplir con la implementación del plan de tratamiento de riesgos de seguridad de la información es importante contar con el apoyo y el compromiso de líderes de procesos, el personal designado para tal fin (enlace) y de la Alta dirección.

## 7. METODOLOGÍA DEL PLAN TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La metodología para el tratamiento de los riesgos de seguridad de la información de los procesos de la entidad, busca planificar, identificar, valorar e implementar el tratamiento adecuado de los riesgos de

seguridad de la información, de forma tal que los riesgos se mantengan en niveles óptimos de control y así preparar a la entidad para una posible materialización de alguno de los riesgos y así gestionar el seguimiento, monitoreo, evaluación, o auditoría, según corresponda.

El Plan de Tratamiento de Riesgos de Seguridad de la Información, está basado en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, emitido por el Departamento Administrativo de Función Pública - DAFP (V5), en la Política de Administración del Riesgo de la Secretaría Distrital de la Mujer y en la norma técnica ISO/IEC 27001 - Sistemas de Gestión de Seguridad de la Información.

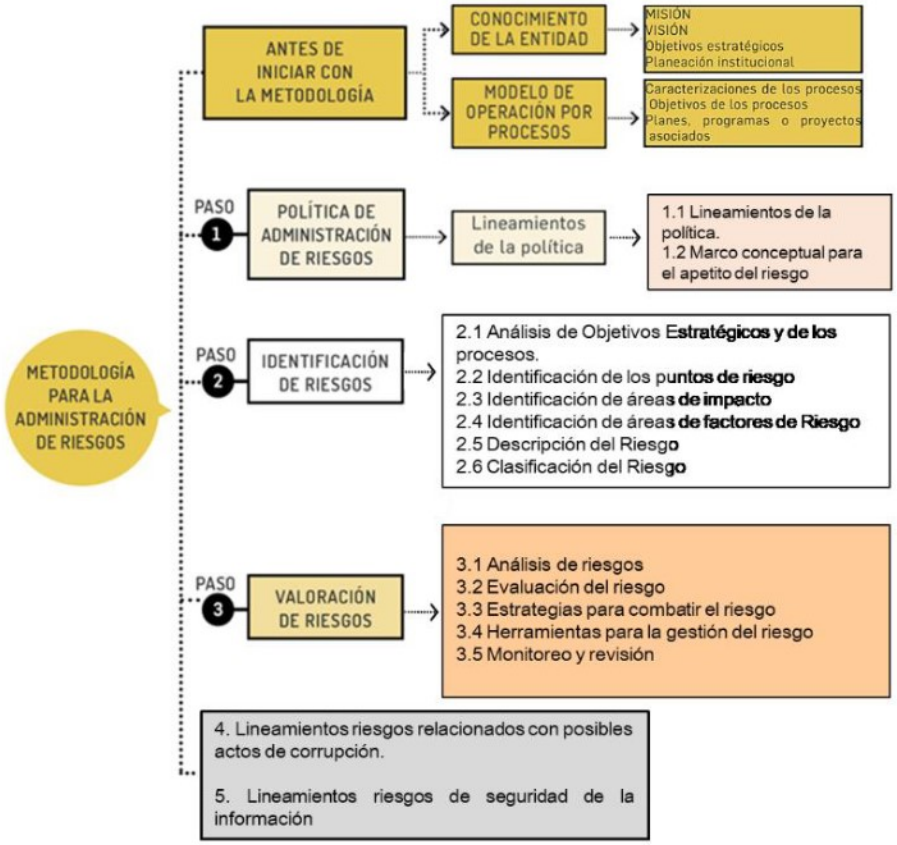


*Ilustración 1. Metodología administración del riesgo*
*Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas*

## 7.1. CAPACIDAD ORGANIZACIONAL

Partiendo de la identificación de las partes interesadas y la designación de los actores clave de cada proceso, es necesario evaluar la capacidad y estructura de los procesos oficiales que se encuentran definidos en el mapa de procesos de la entidad, cuya finalidad es identificar tempranamente debilidades

y obstáculos que permitan establecer las acciones a que haya lugar y se propicie el cumplimiento de los objetivos del plan.

La Entidad debe disponer de los recursos suficientes para el desarrollo de la gestión de riesgos de seguridad de la información, (capital, tiempo, personal, procesos, sistemas y tecnologías), con el fin de apoyar a los responsables en la implementación de controles y seguimiento de los riesgos de seguridad de la información.

La línea estratégica o alta dirección debe asignar entre otros, recursos tales como:

- Personal capacitado e idóneo para la gestión del riesgo de seguridad de la información.
- Recursos económicos para la implementación de controles de mitigación de riesgos.
- Recursos para los aspectos de mejora continua, monitoreo y auditorías.

## 7.2. MAPA DE PROCESOS

La Secretaría Distrital de la Mujer definió el siguiente mapa de procesos en concordancia con su misionalidad.

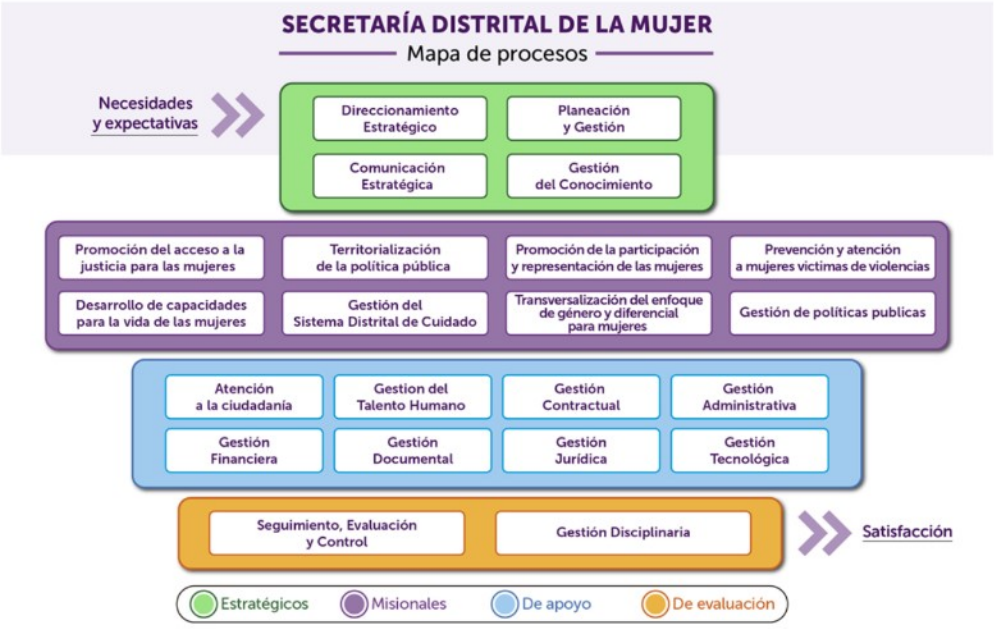


*Ilustración 2.MAPA DE PROCESOS*
*Fuente: Secretaría Distrital de la Mujer*

## 7.3. IDENTIFICAR Y VALORAR LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Para cada tipo de activo o grupo de activos de información, pueden existir una serie de riesgos de seguridad de la información, los cuales deben ser identificados, valorados y posteriormente tratados si

el nivel criticidad es "ALTO".

## 7.4. TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Una vez se han identificado los riesgos, se debe definir el tratamiento para cada uno de los riesgos analizados y evaluados. Este es un proceso cíclico, el cual involucra una selección de opciones para modificarlos, por lo tanto, puede tener en cuenta las opciones planteadas en la "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (V5) - DAFP:

## 7.5. TRATAMIENTO ZONA DE RIESGO FINAL:

- **Muy Alta:** Evitar
- **Alta:** Reducir el riesgo - Mitigar
- **Media:** Compartir
- **Baja, Muy Baja:** Aceptar

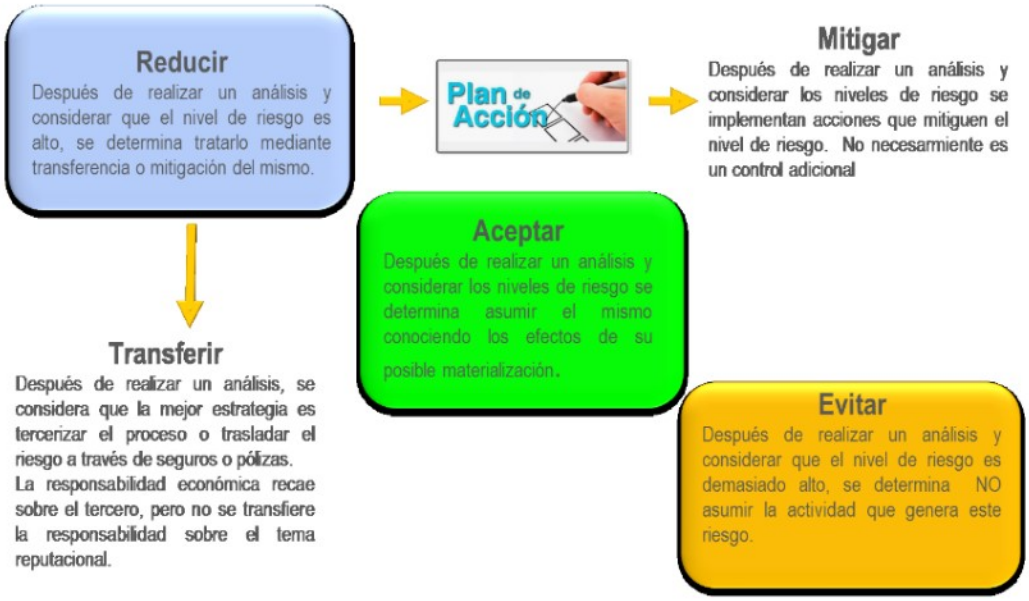


*Ilustración 3 Estrategias para combatir el riesgo*
*Fuente: Tomado de Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (V5)*

## 7.6. MONITOREO Y REVISIÓN

Se debe hacer seguimiento a los planes de tratamiento para determinar su efectividad, de acuerdo con lo definido a continuación:

- Realizar seguimiento y monitoreo al plan de acción en la etapa de implementación y finalización de los planes de acción.
- Revisar periódicamente las actividades de control para determinar su relevancia y actualizarlas de ser necesario.
- Realizar monitoreo de los riesgos y controles.
- Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos.

## 8. IMPLEMENTACIÓN DEL PLAN TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La etapa de implementación, se centra en la ejecución y cumplimiento de las actividades y objetivos acordados y aprobados, de la misma forma se tienen en cuenta los roles y responsabilidades y los tiempos establecidos por la Entidad en la Política de Administración del Riesgo. El resultado esperado de esta fase, es la adecuada implementación y cumplimiento de las actividades previstas en el Plan de Tratamiento de Riesgos de Seguridad de la Información.

En esta fase se requiere del apoyo y liderazgo del equipo directivo de la Secretaría Distrital de la Mujer, comprendiendo todos los requerimientos que se realicen, para logar la implementación y cumplimiento de las actividades del presente plan. Se reitera la necesidad de contar con el personal idóneo y conocedor de cada proceso, facultado para la toma de decisiones, así como también la ejecución eficiente de las actividades planificadas y su debida diligencia en la entrega oportuna de los productos esperados, con lo cual se garantiza la implementación y cumplimiento de los objetivos trazados en el presente plan.

### 8.1. ACTIVIDADES DEL PLAN DE TRATAMIENTO DE RIESGOS

Dando cumplimiento a las políticas de seguridad de la información y con el ánimo de fortalecer los niveles de Confidencialidad, Integridad y Disponibilidad de la Información, la Secretaría Distrital de la Mujer se apoya en los lineamientos y directrices que contribuyen al adecuado tratamiento y gestión de la información en los procesos institucionales, mediante la identificación y gestión de los riesgos de seguridad de la información, para el seguimiento y definición de controles técnicos y administrativos según corresponda.

| No. | ACTIVIDAD | PRODUCTO | FECHA INICIO | FECHA FIN | RESPONSABLE |
|---|---|---|---|---|---|
| 1 | **PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN** | | | | |
| 1.1 | Definir el Plan de Tratamiento de Seguridad de la Información | Plan de Tratamiento de Seguridad de la Información | 14 Enero | 25 Enero | Oficina Asesora de Planeación – Gestión Tecnológica |
| 1.2 | Aprobación del Plan de Tratamiento de | Plan de Tratamiento de Seguridad de la | 25 Enero | 28 Enero | Comité Institucional de Gestión y |

| | | | | | |
|---|---|---|---|---|---|
| | Seguridad de la Información por parte del Comité Institucional de Gestión y Desempeño | Información aprobado | | | Desempeño |
| 1.3 | Publicar el Plan de Tratamiento de Seguridad de la Información | Plan de Tratamiento de Seguridad de la Información publicado | 28 Enero | 31 Enero | Oficina Asesora de Planeación |
| **2** | **IDENTIFICACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN** | | | | |
| 2.1 | Definir y aprobar metodología de identificación de Riesgos de Seguridad de la Información | Metodología de identificación de Riesgos de Seguridad de la Información | 01 Febrero | 30 Marzo | Oficina Asesora de Planeación – Gestión Tecnológica |
| 2.2 | Socialización identificación de Riesgos de Seguridad de la Información | Socialización | Cuando se requiera | Cuando se requiera | Oficina Asesora de Planeación – Gestión Tecnológica |
| 2.3 | Apoyo en la identificación y análisis de riesgos de seguridad de la información | Mapa de riesgos de seguridad de la información | 01 Marzo | 30 Diciembre | Todos los procesos y dependencias de la entidad |
| 2.4 | Aprobación de riesgos de seguridad de la información | Mapa de riesgos de seguridad de la información | 30 Abril | 30 Diciembre | Responsables de los procesos y dependencias de la entidad |
| 2.5 | Seguimiento a los riesgos de seguridad de la información | Mapa de riesgos de seguridad de la información | 30 Abril | 30 Diciembre | Responsables de los procesos y dependencias de la entidad |
| **3** | **DECLARACIÓN DE APLICABILIDAD** | | | | |
| 3.1 | Actualización y aprobación de la declaración de aplicabilidad SOA | Declaración de aplicabilidad - SOA actualizada. | 02 Mayo | 30 Junio | Oficina Asesora de Planeación – Gestión Tecnológica |
| **4** | **PLAN DE SENSIBILIZACIÓN SEGURIDAD DE LA INFORMACIÓN** | | | | |
| 4.1 | Actualización del plan de | Plan de sensibilización en | 01 Abril | 30 Mayo | Oficina Asesora de Planeación – |

| | | | | | |
|---|---|---|---|---|---|
| | sensibilización en seguridad de la información | seguridad de la información | | | Gestión Tecnológica |
| 4.2 | Charlas de sensibilización en seguridad de la información para servidoras, servidores públicos y contratistas | Sensibilizaciones - Actas | 01 Junio | 30 Noviembre | Oficina Asesora de Planeación – Gestión Tecnológica |
| 4.3 | Envío de piezas comunicativas de seguridad de la información | Piezas comunicativas de seguridad por correo electrónico y/o boletina | 01 Marzo | 15 Diciembre | Oficina Asesora de Planeación – Gestión Tecnológica |
| **5** | **MESAS DE TRABAJO DE GOBIERNO DIGITAL Y SEGURIDAD DIGITAL - MTGD** | | | | |
| 5.1 | Realizar mesas de trabajo para tratar temas de Gobierno Digital y seguridad Digital en los comités de enlaces MIPG | Reunión Actas | 1 Febrero | 16 Diciembre | Oficina Asesora de Planeación – Gestión Tecnológica y enlaces de GD de todos los procesos/áreas de la entidad |

## 9. TÉRMINOS Y DEFINICIONES

**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).

**Alta dirección:** Persona o grupo de personas que dirige y controla una organización, al nivel más alto (ISO/IEC 27001:2013).

**Amenaza:** Potencial ocurrencia de un hecho que pueda manifestarse en un lugar específico, con una duración e intensidad determinadas. Cuando el Agente de riesgo selecciona una víctima contra la cual pretende cometer un acto delictivo, automáticamente se convierte en una amenaza para ella. Se puede considerar que es la materialización del riesgo.

**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.

**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.

**Causa:** Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

**Compromiso de la Dirección:** Alineamiento firme de la Dirección de la entidad con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI - Sistema de Gestión de Seguridad de la Información.

**Confidencialidad:** El acceso a la información es permitido exclusivamente al personal autorizado, sin revelar la misma a terceras partes y/o personas.

**Control:** Medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

**Custodio:** Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado. Tomado de https://www.mintic.gov.co/gestionti/615/articles-482_G5_Gestion_Clasificacion.pdf

**Dato Personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables (Ley 1581 de 2012 – Artículo 3).

**Disponibilidad:** En seguridad informática es un término hace referencia a la característica de poder acceder a la información en el momento que se requiera.

**Evaluación del riesgo:** Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

**Evento de seguridad de la información:** Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o falla de salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad (NTC-ISO/IEC 27001 2013).

**Gestión de la seguridad en los activos:** La Secretaría Distrital de la Mujer a través de los procesos Gestión Tecnológica y Gestión Administrativa deben establecer y divulgar los lineamientos específicos para la identificación, clasificación y buen uso de los activos de información de tipo información, datos, software, hardware y servicios, con el objetivo de garantizar su protección.

**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).

**Hardware:** Conjunto de equipos de cómputo, servidores, redes, equipos de seguridad, impresoras, scanner, equipos de almacenamiento, entre otros, que utiliza la Secretaría Distrital de la Mujer.

**Impacto:** Resultado de un incidente de seguridad de la información.

**Incidente de seguridad:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

**Incidente:** Según [ISO/lEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información

**Inventario de activos:** Los responsables de la información deben propender para que se mantenga actualizado el inventario de sus activos de información y hagan entrega de éste al menos una vez al año. La consolidación de dicho inventario está bajo la responsabilidad de la Dirección de Gestión Administrativa.

**Mapa de riesgos:** Documento con la información resultante de la gestión del riesgo.

**Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

**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.

**Riesgo inherente:** Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

**Riesgo residual:** Nivel restante de riesgo después del tratamiento del riesgo.

**Probabilidad:** Se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.

**Propietario de la Información:** Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso.

**SGSI - Sistema de Gestión de Seguridad de la Información:** Según [ISO/lEC 27001: 2013]: Sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura

de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.

**Seguridad de la Información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad pueden estar involucradas (NTC-ISO/IEC 27001:2013).

**Vulnerabilidad:** Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

## 10. REGISTRO DE MODIFICACIONES.

| VERSIÓN | FECHA | DESCRIPCIÓN DE LA MODIFICACIÓN |
|---|---|---|
| 1 | 20/01/2021 | Primera versión del Plan de Tratamiento de Riesgos de Seguridad de la Información de la Secretaría Distrital de la Mujer. |
| 2 | 31/01/2022 | Actualización general del documento y de las actividades Plan de Tratamiento de Riesgos de Seguridad de la Información 2022 de la Secretaría Distrital de la Mujer. |

| | NOMBRE | CARGO | FIRMA |
|---|---|---|---|
| ELABORÓ | Andrés Giovanny Cadena Herrera | Profesional Especializado - Contratista | |
| REVISÓ | Sandra Catalina Campos Romero | Jefe Oficina Asesora de Planeación | |
| APROBÓ | Sandra Catalina Campos Romero | Comité Institucional de Gestión y Desempeño | |