

**PLAN DE TRATAMIENTO A RIESGOS DE SEGURIDAD DE LA INFORMACIÓN - 2025**

**PROCESO GESTIÓN TECNOLÓGICA**

**Bogotá, D.C., enero de 2025**

Contenido

[**1. INTRODUCCIÓN 3**](#_Toc155902422)

[**2. OBJETIVO GENERAL 3**](#_Toc155902423)

[**3. OBJETIVOS ESPECÍFICOS 3**](#_Toc155902424)

[**4. ALCANCE 3**](#_Toc155902425)

[**5. DEFINICIONES 4**](#_Toc155902426)

[**6. LÍNEAMIENTOS 5**](#_Toc155902427)

[**7. DESARROLLO DEL PLAN DE TRATAMIENTO A RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y PRIVACIDAD 5**](#_Toc155902428)

[**8. CONCLUSIONES 8**](#_Toc155902429)

[**9. REFERENCIAS BIBLIOGRÁFICAS 8**](#_Toc155902430)

[**10. REGISTRO DE MODIFICACIONES 8**](#_Toc155902431)

# INTRODUCCIÓN

En cumplimiento del Decreto 612 del 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" y teniendo en cuenta el artículo 1, el cual establece que los planes institucionales deben estar publicados en la página web de la entidad a más tardar el 31 de enero de cada vigencia, la Secretaría Distrital de la Mujer ha actualizado el Plan de Tratamiento a Riesgos de Seguridad de la Información y Privacidad para la vigencia 2025.

Para la Secretaría Distrital de la Mujer es importante la identificación, clasificación y valoración de los riesgos, que pueden afectar la seguridad y privacidad de la información en todos los procesos y dependencias de la Entidad, con el propósito de gestionar la confidencialidad, integridad y disponibilidad de la información, por lo cual se establecen controles y medidas de seguridad que permitan asegurar la información de la Entidad en todos sus procesos, trámites, servicios, sistemas e infraestructura.

Durante la vigencia 2024, la Secretaría Distrital de la Mujer actualizó la “PG-PLT-1 Política Administración del Riesgo” en la cual está incluida las responsabilidades en materia de la gestión de riesgos de seguridad de la información. Adicionalmente, contiene la identificación y clasificación de activos, así como evaluación de riesgos de seguridad de la información considerando amenazas y vulnerabilidades en el contexto de la Entidad, usando referencias como el estándar ISO27005:2018.

# OBJETIVO GENERAL

Documentar el plan de tratamiento de riesgos de la Secretaría Distrital de la Mujer, mediante la definición de actividades específicas que faciliten el seguimiento continuo y la generación de alertas, con el fin de garantizar que los riesgos se mantengan dentro de niveles aceptables y gestionables.

# OBJETIVOS ESPECÍFICOS

* Presentar los resultados de la identificación, análisis y evaluación de riesgos de seguridad de la información y privacidad realizada durante el año 2024.
* Reportar las estrategias de tratamiento a los riesgos de seguridad de la información y privacidad, las cuales serán desarrolladas a partir del año 2025.

# ALCANCE

El Plan de Tratamiento a Riesgos de Seguridad de la Información y Privacidad aplica para la vigencia 2025 sobre todos los niveles y procesos de la Entidad teniendo en cuenta su responsabilidad como primera línea de defensa y la gestión transversal de los riesgos evaluados.

# DEFINICIONES

* **Activo de Información:** Datos o conocimiento que tienen valor para una organización.
* **Amenaza:** Causa potencial de un incidente no deseado, que puede resultar en daños a un sistema u organización.
* **Clasificación de la información:** Los responsables de los activos de información deben documentar la clasificación de seguridad de los activos de información de los cuales son responsables y designarán un custodio para cada activo, a su vez éste será responsable de la implementación de los controles de seguridad.
* **Confidencialidad:** Propiedad para que la información no esté disponible o divulgada a personas, entidades o procesos no autorizados.
* **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:** Propiedad de la información relacionada con ser accesible y utilizable a petición de una entidad autorizada.
* **Gestión de riesgos:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
* **Gobierno de seguridad de la información:** Es el conjunto de responsabilidades y prácticas ejercidas por el Grupo Directivo con el propósito de evaluar, dirigir, monitorear y comunicar todas las acciones y/o actividades relacionadas con la protección de la información de la Entidad, (ISO/IEC 27014:2013).
* **Impacto:** La magnitud del daño que se puede esperar como resultado de la divulgación, modificación no autorizada, destrucción, o pérdida de información.
* **Información:** Es un conjunto de datos ordenados, clasificados y almacenados en cualquier medio (magnético, papel, correo electrónico, conversación telefónica, chat, USB, etc.).
* **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.
* **Sistema de información:** Aplicaciones, servicios, activos de tecnología de la información u otros componentes de manejo de información.
* **SGSI - Sistema de Gestión de Seguridad de la Información:** 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.
* **Vulnerabilidad:** Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO IEC debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

# LÍNEAMIENTOS

Teniendo en cuenta la “PG-PLT-1 Política Administración del Riesgo” publicada en el sistema de integrado de gestión de la Secretaría Distrital de la Mujer, una vez realizada la valoración de los riesgos residuales de gestión y seguridad de la información, se deben aplicar los siguientes niveles de aceptación y estrategias para combatir el riesgo.



# DESARROLLO DEL PLAN DE TRATAMIENTO A RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y PRIVACIDAD

Los resultados detallados de la identificación y valoración de riesgos de seguridad de la información y privacidad realizada durante el año 2024 se encuentran bajo clasificación de información pública reservada en el sistema de integrado de gestión de la Secretaría Distrital de la Mujer.

A continuación, se presenta un resumen de los riesgos de seguridad de la información y privacidad evaluados y registrados para la Entidad:

|  |  |  |
| --- | --- | --- |
| **Nivel del Riesgo** | **Cantidad de Riesgos** | **Porcentaje** |
| **Bajo** | 2 | 7% |
| **Moderado** | 11 | 39% |
| **Alto** | 14 | 48% |
| **Extremo** | 1 | 4% |
| **TOTAL** | 28 | 100% |

A continuación, se presentan el listado de riesgos y la estrategia definida para combatirlos:

| **RIESGO** | **TIPO** | **FACTOR DE RIESGO** | **NIVEL DE RIESGO RESIDUAL** | **ESTRATEGIA** |
| --- | --- | --- | --- | --- |
| R13 | Continuidad | Fallas técnicas |  MODERADO | Mitigar |
| R14 | Continuidad | Fallas técnicas |  MODERADO | Mitigar |
| R15 | Continuidad | Perdida de servicios esenciales |  MODERADO | Mitigar |
| R16 | Seguridad de la Información | Acciones de personas |  MODERADO | Mitigar |
| R17 | Continuidad | Fallas técnicas |  ALTO | Mitigar |
| R18 | Seguridad de la Información | Fallas técnicas |  ALTO | Mitigar |
| R19 | Seguridad de la Información | Fallas técnicas |  ALTO | Mitigar |
| R20 | Seguridad de la Información | Fallas técnicas |  ALTO | Mitigar |
| R21 | Seguridad de la Información | Acciones de personas |  ALTO | Mitigar |
| R22 | Seguridad de la Información | Acciones de personas |  ALTO | Mitigar |
| R24 | Seguridad de la Información | Acciones de personas |  MODERADO | Mitigar |
| R25 | Seguridad de la Información | Acciones de personas |  ALTO | Mitigar |
| R26 | Seguridad de la Información | Compromiso de la información |  MODERADO | Mitigar |
| R27 | Seguridad de la Información | Acciones de personas |  ALTO | Mitigar |
| R28 | Seguridad de la Información | Acciones de personas |  MODERADO | Mitigar |
| R29 | Seguridad de la Información | Acciones de personas |  MODERADO | Mitigar |
| R30 | Seguridad de la Información | Acciones de personas |  BAJO | Aceptar |
| R31 | Seguridad de la Información | Acciones de personas |  ALTO | Mitigar |
| R32 | Seguridad de la Información | Acciones de personas |  EXTREMO | Reducir |
| R34 | Seguridad de la Información | Acciones de personas |  ALTO | Mitigar |
| R35 | Seguridad de la Información | Acciones de personas |  MODERADO | Mitigar |
| R36 | Seguridad de la Información | Acciones de personas |  MODERADO | Mitigar |
| R37 | Seguridad de la Información | Acciones de personas |  ALTO | Mitigar |
| R38 | Seguridad de la Información | Acciones de personas |  ALTO | Mitigar |
| R39 | Seguridad de la Información | Acciones de personas |  ALTO | Mitigar |
| R40 | Seguridad de la Información | Acciones de personas |  MODERADO | Mitigar |
| R41 | Seguridad de la Información | Acciones de personas |  ALTO | Mitigar |
| R42 | Seguridad de la Información | Acciones de personas |  BAJO | Mitigar |

# CONCLUSIONES

* La Secretaría Distrital de la Mujer durante el año 2024 realizó una evaluación destallada de los riesgos de seguridad de la información y conforme a los resultados obtenidos determinó la estrategia de mitigar o reducir 27 de los 28 riesgos valorados.
* Los factores de riesgo más relevantes son acciones de personas (con 20 de los 28 riesgos valorados) y fallas técnicas (con 6 de los 28 riesgos valorados).
* Los planes de tratamiento a todos los riesgos deben ser verificados y aceptados, definiendo fechas de compromiso en el Sistema Integrado de Gestión de la Entidad.
* Es importante que se realice seguimiento y monitoreo a las acciones definidas en los planes de tratamiento de riesgos a través de los seguimientos cuatrimestrales cumpliendo con la “PG-PLT-1 Política Administración del Riesgo”

# REFERENCIAS BIBLIOGRÁFICAS

* Estándar ISO 27001:2013
* Estándar ISO 27005:2018

**Control de cambios**

| **No.** | **CAMBIOS REALIZADOS** |
| --- | --- |
| 1 | Creación del documento. |

**Responsables de elaboración, revisión y aprobación**

|  |  |  |  |
| --- | --- | --- | --- |
| ELABORADO POR | APROBADO POR | REVISADO POR | AVALADO POR |
| NOMBRE: Cristian Camilo Calderón Tapia | NOMBRE:Carlos Alfonso Gaitán Sánchez | NOMBRE:Paula Vanessa Sosa Martin | NOMBRE:Carlos Alfonso Gaitán Sánchez |
| CARGO: Contratista OAP | CARGO: Jefe Oficina Asesora de Planeación | CARGO: Contratista OAP. | CARGO:Jefe Oficina Asesora de Planeación |