**INSTITUTO DISTRITAL DE LA PARTICIPACIÓN Y ACCIÓN COMUNAL**



**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

**Bogotá, D.C. 2018-2019**

Tabla de Contenido

[1. INTRODUCCIÓN 5](#_Toc519085130)

[2. OBJETIVOS 5](#_Toc519085131)

[2.1. Objetivo General 5](#_Toc519085132)

[2.2. Objetivos Específicos 5](#_Toc519085133)

[3. Alcance 6](#_Toc519085134)

[4. Plan de Acción del Modelo de Seguridad y Privacidad de la Información – MSPI 6](#_Toc519085135)

[4.1. Fase 1: Diagnóstico 7](#_Toc519085136)

[4.2. Fase 2: Planificación 7](#_Toc519085137)

[4.2.1. Política de seguridad y privacidad de la información 9](#_Toc519085138)

[4.2.2. Manual de Políticas de Seguridad y Privacidad de la Información 9](#_Toc519085139)

[4.2.3. Líder de Seguridad y Privacidad de la Información 9](#_Toc519085140)

[4.2.4. Procedimientos de seguridad de la información 10](#_Toc519085141)

[4.2.5. Roles y responsabilidades de seguridad y privacidad de la información 10](#_Toc519085142)

[4.2.6. Inventario de activos de información 10](#_Toc519085143)

[4.2.7. Integración del MSPI con el Sistema de Gestión documental 11](#_Toc519085144)

[4.2.8. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 11](#_Toc519085145)

[4.2.9. Principio de Responsabilidad Demostrada (LPDP) 11](#_Toc519085146)

[4.2.10. Guía de contingencias de TI para la continuidad del negocio 11](#_Toc519085147)

[4.2.11. Declaración de Aplicabilidad de Seguridad de la Información 12](#_Toc519085148)

[4.2.12. Plan de Comunicaciones 12](#_Toc519085149)

[4.2.13. Plan de transición de IPv4 a IPv6 12](#_Toc519085150)

[4.3. Fase 3: Implementación 12](#_Toc519085151)

[4.3.1. Planificación y control operacional 13](#_Toc519085152)

[4.3.2. Implementación del Plan de Tratamiento de Riesgos 13](#_Toc519085153)

[4.3.3. Indicadores de gestión 13](#_Toc519085154)

[4.3.4. Plan de Transición de IPv4 a IPv6 13](#_Toc519085155)

[4.4. Fase 4: Evaluación de desempeño 14](#_Toc519085156)

[4.4.1. Plan de revisión y seguimiento a la implementación del MSPI 14](#_Toc519085157)

[4.4.2. Plan de auditorías internas 15](#_Toc519085158)

[4.5. Fase 5: Mejora continua 15](#_Toc519085159)

[4.5.1. Plan de mejora continua 15](#_Toc519085160)

[5. Responsables 16](#_Toc519085161)

[5.1. Dirección General o delegado 16](#_Toc519085162)

[5.2. Líder Oficial de Seguridad y Privacidad de la Información 16](#_Toc519085163)

[5.3. Equipo de trabajo de seguridad y privacidad de la información 16](#_Toc519085164)

Índice de Tablas

[Tabla 1. Plan de Acción Fase 1 6](#_Toc519085165)

[Tabla 2. Plan de Acción Fase 2 6](#_Toc519085166)

[Tabla 3. Plan de Acción Fase 3 11](#_Toc519085167)

[Tabla 4. Plan de Acción Fase 4 13](#_Toc519085168)

[Tabla 5. Plan de Acción Fase 5. 14](#_Toc519085169)

# INTRODUCCIÓN

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información contiene el plan de acción requerido para la gestión de los riesgos de seguridad y privacidad de la información, en función de la implementación de controles que permitan al Instituto disminuir la probabilidad y el impacto de materialización de este tipo de riesgos, con el fin de preservar la seguridad e integridad de los activos de información institucionales.

En este sentido, acorde con lo establecido en el Modelo de Seguridad y Privacidad de la Información – MSPI, en la Guía No. 7 – Guía de Gestión de Riesgos y Guía No. 8 – Controles de Seguridad y Privacidad de la Información, en el presente Plan se estipulan directrices, fechas de ejecución y responsables para lograr un adecuado proceso de administración y evaluación de los riesgos de seguridad y privacidad de la información.

Este Plan es elaborado en concordancia con lo establecido en el objetivo estratégico “*Incrementar los mecanismos y controles para la preservación de la seguridad, confidencialidad, privacidad, integridad y disponibilidad de la información institucional, protegiendo los activos de la información en su ciclo de vida, así como las acciones que impliquen el tratamiento de datos personales que sean recogidos por la entidad en el ejercicio de su misionalidad*”.

# OBJETIVOS

## Objetivo General

Desarrollar e implementar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, acorde con lo establecido en el Modelo de Privacidad y Seguridad de la Información – MSPI, la Guía No. 7 – Guía de Gestión de Riesgos y la Guía No. 8 – Controles de Seguridad y Privacidad de la Información, con el propósito de adoptar medidas y acciones encaminadas a modificar, reducir o eliminar esta tipologia de riesgos relacionada con la infraestructura de tecnologías de la Información de la Entidad.

## Objetivos Específicos

* Identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos de seguridad y privacidad de la información, los controles y acciones de prevención, y las medidas de contingencia establecidas para la gestión de esta tipología de riesgos.
* Proteger los activos de información del Instituto Distrital de la Participación y Acción Comunal – IDPAC, con base en los criterios de confidencialidad, integridad y disponibilidad.
* Administrar los riesgos de seguridad de la información para mantenerlos en niveles aceptables.
* Sensibilizar y capacitar a los servidores públicos, proveedores y partes interesadas acerca de la Gestión de Riesgos de Seguridad y Privacidad de la Información, fortaleciendo el nivel de conciencia en cuanto a la necesidad de salvaguardar los activos de información institucionales.
* Implementar acciones de mejora que contribuyan al permanente fortalecimiento de los controles establecidos y para el continuo fortalecimiento de la metodología de gestión y administración de riesgos de seguridad y privacidad de la información.

# ALCANCE

Los requisitos, lineamientos y acciones establecidas en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información son aplicables de forma anualizada a los procesos estratégicos, misionales, de apoyo y de evaluación, por lo cual deberán ser conocidos y cumplidos por todos los funcionarios, contratistas, recursos de infraestructura tecnológica para el tratamiento de la información y terceras partes vinculadas a la Entidad que accedan a los activos de información, sistemas de información e instalaciones físicas del Instituto.

# PLAN DE ACCIÓN PARA EL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para la formulación del presente Plan se toma como base la “Guía para la Administración del Riesgo” del Departamento Administrativo de la Función Pública – DAFP, de acuerdo con lo establecido en el Modelo de Privacidad y Seguridad de la Información – MSPI, la Guía No. 7 – Guía de Gestión de Riesgos y la Guía No. 8 – Controles de Seguridad y Privacidad de la Información; con el fin de que en la Entidad se maneje una metodología de gestión y administración de riesgos integral, que contemple todas las tipologias de riesgos que conciernen a la Entidad.

Ilustración 1. Proceso para la administración de riesgos



Fuente: Guía para la Administración del Riesgo - DAFP

Sin embargo, cabe resaltar que acorde con lo establecido en la NTC-ISO/IEC 27005 el proceso de gestión de riesgos de seguridad y privacidad de la información puede ser iterativo para las acciones de valoración y tratamiento. Este enfoque contribuye a incrementar la profundidad y el detalle de las valoraciones en cada iteración.

Ilustración 1. Proceso para la administración de riesgos de seguridad y privacidad de la información



Fuente: NTC-ISO/IEC 27005

En concordancia, teniendo en cuenta lo establecido en la guía IDPAC-PE-GU-01 “Guía metodológica para la administración del riesgo” y el marco conceptual anterior, las acciones definidas en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Instituto Distrital de la Participación y Acción Comunal – IDPAC son las siguientes.

Tabla 1. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

| Acción | Fecha inicio | Fecha fin |
| --- | --- | --- |
| Definir el equipo de trabajo para la administración de los riesgos de seguridad y privacidad de la información | 01/02/2019 | 10 /02/2019 |
| Revisar y actualizar la IDPAC-PE-OT-01 "Guía Metodológica para la Administración del Riesgo" con el propósito de validar el cumplimiento de los lineamientos establecidos en el Modelo de Seguridad y Privacidad de la Información – MSPI. | 11/02/2019 | 20/02/2019 |
| Actualizar el contexto estratégico como insumo para la identificación y gestión de los riesgos de seguridad y privacidad de la información | 21/02/2019 | 05/03/2019 |
| Realizar acompañamiento a los procesos del lDPAC en la identificación de los riesgos de seguridad y privacidad de la información, por procesos | 06/03/2019 | 15/04/2019 |
| Realizar acompañamiento a los procesos del lDPAC para el análisis de los riesgos de seguridad y privacidad de la información identificados | 16/04/2019 | 15/05/2019 |
| Realizar acompañamiento a los procesos del lDPAC para la valoración de los controles establecidos para los riesgos de seguridad y privacidad de la información | 16/05/2019 | 15/06/2019 |
| Realizar acompañamiento a los procesos del lDPAC para la formulación de las acciones de intervención y contingencia, requeridas para el tratamiento de los riesgos de seguridad y privacidad de la Información | 16/06/2019 | 17/08/2019 |
| Elaborar y publicar la Matriz de Riesgos de Seguridad y Privacidad de la Información en la página web y en la intranet de la Entidad. | 18/08/2019 | 20/09/2019 |
| Divulgar interna y externamente el Mapa de Riesgos de Seguridad y Privacidad de la Información del IDPAC a través de diferentes medios, al inicio de la vigencia y cuando se realicen ajustes al mismo | 24/09/2019 | 31/12/2019 |
| Realizar seguimiento considerando los elementos de la ficha técnica para la gestión de riesgos con el fin de evaluar la eficacia y efectividad de los controles establecidos mediante la ejecución de las actividades | 26/09/2018 | 31/12/2019 |
| Monitorear y revisar continuamente los riesgos establecidos en la Matriz de Riesgos de Seguridad y Privacidad de la Información | 24/09/2019 | 31/12/2019 |
| Realizar la evaluación anual de la Administración del Riesgo de Seguridad y Privacidad de la Información | 26/12/2019 | 31/12/2019 |

Fuente: Elaboración propia

## Definir el equipo de trabajo para la administración de los riesgos de seguridad y privacidad de la información

Para la ejecución anual de este Plan se deberá conformar el equipo de trabajo designado para esta labor. Es indispensable que se designe un representante de cada proceso y que los líderes de proceso participen en estas acciones.

Cabe resaltar que este equipo de trabajo puede ser el mismo que se designa para la gestión de todos los riesgos de la Entidad; aunque el liderazgo de la ejecución del Plan estará a cargo del proceso de Gestión de Tecnologías de la Información, con el acompañamiento de la Oficina Asesora de Planeación.

## Revisar y actualizar la IDPAC-PE-OT-01 "Guía Metodológica para la Administración del Riesgo" con el propósito de validar el cumplimiento de los lineamientos establecidos en el Modelo de Seguridad y Privacidad de la Información – MSPI

Dentro del marco de seguridad del Modelo de Seguridad y Privacidad de la información la Gestión de Riesgos se debe realizar con base en lo establecido en la “Guía para la Administración del Riesgo” del Departamento Administrativo de la Función Pública – DAFP, buscando que la administración de riesgos de seguridad y privacidad de la información se integre a lo que se ha desarrollado en la Entidad para la gestión de las otras tipologías de riesgos.

En este sentido, teniendo en cuenta que el Instituto desarrolló para la gestión de riesgos el documento metodológico IDPAC-PE-OT-01 "Guía Metodológica para la Administración del Riesgo", se debe realizar la revisión de este documento con el fin de validar que los requisitos para la administración de riesgos de seguridad y privacidad de la información definidos en la Guía No. 7 – Guía de Gestión de Riesgos y en la Guía No. 8 – Controles de Seguridad y Privacidad de la Información, se encuentren incluidos en su totalidad.

Una vez se realice la actualización de la IDPAC-PE-OT-01 "Guía Metodológica para la Administración del Riesgo", se debe realizar su socialización interna y externa.

## Actualizar el contexto estratégico como insumo para la identificación y gestión de los riesgos de seguridad y privacidad de la información

## Evaluación de riesgos de seguridad y privacidad de la información

Para la evaluación de riesgos de seguridad y privacidad de la información se tomará como insumo la matriz de Activos de Información, sobre la cual se implementará el presente Plan sobre los Activos de Información que tengan un nivel alto de clasificación al evaluar los criterios de confidencialidad, integridad y disponibilidad, según los siguientes criterios.

Ilustración 2. Criterios de Clasificación



Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482\_G7\_Gestion\_Riesgos.pdf

Ilustración 3. Niveles de Clasificación



Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482\_G7\_Gestion\_Riesgos.pdf

En esta fase se pretende elaborar el Plan de Seguridad y Privacidad de la Información a partir de los resultados generados en la fase de diagnóstico y garantizando su alineación con la planeación estratégica de la Entidad.