**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 Seguridad y Privacidad de la Información contiene el plan de acción requerido para diagnosticar, planificar, implementar, gestionar y mejorar continuamente el Modelo de Seguridad y Privacidad de la Información – MSPI de la Entidad, y estipula directrices, fechas de ejecución y responsables para lograr un adecuado proceso de administración y evaluación.

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 Modelo de Privacidad y Seguridad de la Información de acuerdo con los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, con el propósito de preservar la confidencialidad, integridad y disponibilidad de la información, y la privacidad de los datos de los ciudadanos y funcionarios.

## Objetivos Específicos

* 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 lo establecido en el Modelo de Seguridad y Privacidad de la Información – MSPI, fortaleciendo el nivel de conciencia en cuanto a la necesidad de salvaguardar los activos de información institucionales.
* Monitorear el cumplimiento de los requisitos de seguridad y privacidad de la información, mediante el uso de herramientas de diagnóstico y auditorías internas programadas a intervalos regulares.
* Implementar acciones de mejora que contribuyan al permanente fortalecimiento del Modelo de Seguridad y Privacidad de la Información – MSPI.

# Alcance

Los requisitos y lineamientos establecidos en el Modelo de Seguridad y Privacidad de la Información son aplicables 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.

Mediante la adopción del Modelo de Seguridad y Privacidad de la Seguridad se busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base para la aplicación del concepto de Seguridad Digital.

# Plan de Acción del Modelo de Seguridad y Privacidad de la Información – MSPI

El Modelo de Seguridad y Privacidad de la Información contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten gestionar adecuadamente la seguridad y privacidad de los activos de información. Cabe resaltar que se establecen seis (6) niveles de madurez, que corresponden a la evolución de la implementación del modelo de operación.

Ilustración 1. Ciclo de operación del Modelo de Seguridad y Privacidad de la Información - MSPI



Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482\_Modelo\_de\_Seguridad\_Privacidad.pdf

## Fase 1: Diagnóstico

En esta fase se pretende identificar el estado actual del Instituto Distrital de la Participación y Acción Comunal – IDPAC con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

Tabla 1. Plan de Acción Fase 1

|  |  |  |  |
| --- | --- | --- | --- |
| Acción | Producto | Fecha inicio | Fecha fin |
| Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad | Herramienta de diagnóstico diligenciada | 01/02/2019 | 15/02/2019 |
| Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad | Nivel de madurez identificado y documentado | 16/08/2018 | 28/02/2019 |
| Identificar vulnerabilidades técnicas y administrativas a partir de la realización de pruebas que permitan medir la efectividad de los controles existentes | Documentación de los hallazgos encontrados en las pruebas de vulnerabilidad | 01/03/2019 | 30/03/2019 |

Fuente: Elaboración propia

## Fase 2: Planificación

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.

Tabla 2. Plan de Acción Fase 2

| Acción | Producto | Fecha inicio | Fecha fin |
| --- | --- | --- | --- |
| Formular y publicar la Política de Seguridad y Privacidad de la Información | Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad | Actualmente publicada  | Actualmente publicada |
| Revisar, validar y/o actualizar el manual de Políticas de Seguridad y Privacidad de la Información | Manual con las políticas de seguridad y privacidad de la información, actualizado, aprobado por la alta dirección y socializado al interior de la Entidad | 01/04/2019 | 20/04/2019 |
| Designar el Líder de Seguridad y Privacidad de la Información | Líder de Seguridad y Privacidad de la Información  | 15/04/2019 | 30/04/2019 |
| Elaborar los procedimientos de seguridad de la información | Procedimientos documentados, aprobados y socializados | 21/04/2019 | 20/08/2019 |
| Definir roles y responsabilidades de seguridad y privacidad de la información | Acto administrativo a través del cual se asignan los temas de seguridad y privacidad de la información en la entidad, revisado y aprobado. | 15/04/2019 | 30/04/2019 |
| Actualizar el inventario de activos de información | Documento con la metodología para la identificación, clasificación y valoración de activos de información, revisado y aprobado. Matriz con la identificación, valoración y clasificación de activos de información. | 21/08/2019 | 15/09/2019 |
| Integrar el MSPI con el Sistema de Gestión Documental | Integración del MSPI con el sistema de gestión documental  | 16/09/2019 | 15/12/2019 |
| Elaborar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información | Documento con la metodología de gestión de riesgos. Documento con el análisis y evaluación de riesgos. Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad. Documentos revisados y aprobados por la Alta Dirección. | 01/02/2019 | 16/07/2019 |
| Implementar el Principio de Responsabilidad Demostrada (LPDP) | Documentos de soporte que evidencien la implementación del Principio de Responsabilidad Demostrada (LPDP) | 01/02/2019 | 31/12/2019 |
| Definir el Plan de Continuidad del Negocio | Plan de continuidad del negocio | 18/07/2019 | 30/10/2019 |
| Definir Declaración de Aplicabilidad de Seguridad y Privacidad de la Información | Documentación de la declaración de aplicabilidad de seguridad y privacidad de la información | 01/11/2019 | 30/11/2019 |
| Elaborar el Plan de Comunicaciones | Documento con el plan de comunicación, sensibilización y capacitación  | 16/07/2019 | 27/07/2019 |
| Plan de transición de IPv4 a IPv6 | Plan de diagnóstico para la transición de IPv4 a IPv6 | 01/06/2019 | 31/12/2019 |

Fuente: Elaboración propia.

### Política de seguridad y privacidad de la información

La Política de Seguridad y Privacidad del Instituto Distrital de la Participación y Acción Comunal – IDPAC contendrá la voluntad de la Alta Dirección para apoyar la Implementación del Modelo de Seguridad y Privacidad de la Información – MSPI.

Esta política contendrá de manera específica la declaración general por parte de la Alta Dirección, en cuanto a los objetivos, alcance y nivel de cumplimiento.

Esta política deberá ser aprobada y divulgada al interior de la Entidad.

### Manual de Políticas de Seguridad y Privacidad de la Información

El Instituto Distrital de la Participación y Acción Comunal establece las Políticas de Seguridad y Privacidad de la Información, con el fin de garantizar el adecuado uso de los activos de información, asegurando el cumplimiento de los principios de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.

 Estas políticas se aplicaran cuando el Instituto Distrital de la Participación y Acción Comunal ejecute y realice actividades que impliquen la recolección o captura, procesamiento, almacenamiento, distribución y captura de información, para el desarrollo de la misión institucional y el cumplimiento de sus objetivos estratégicos.

### Líder de Seguridad y Privacidad de la Información

Este líder será el responsable de la Seguridad y Privacidad de la Información en la Entidad, algunas de sus responsabilidades son identificar la brecha entre los requerimientos del Modelo de seguridad y privacidad de la información y la situación actual de la entidad, liderar la implementación del Modelo de Seguridad y Privacidad de la Información, liderar el equipo de trabajo que implementará y mantendrá el Modelo de Seguridad y Privacidad de la Información – MSPI, definiendo roles, responsabilidades, entregables y tiempos, representar a la Entidad en temas de Seguridad y Privacidad frente a requerimientos externos, etc.

La designación del Líder Oficial de Seguridad de la Información será realizada por la Dirección General.

### Procedimientos de seguridad de la información

Se realizará la revisión de los actuales procedimientos, con el objeto de identificar las necesidades de documentación y/o actualización de procedimientos en el marco de la implementación del Modelo de Seguridad y Privacidad de la información.

El propósito de esta actividad se fundamenta en desarrollar y formalizar procedimientos que permitan gestionar la seguridad y privacidad de la información en todos los procesos de la Entidad.

### Roles y responsabilidades de seguridad y privacidad de la información

La Dirección General deberá garantizar la asignación de roles y responsabilidades en todos los niveles (directivo, de procesos, operativo), para lo cual acorde con lo establecido en el Modelo Integrado de Planeación y Gestión – MIPG se deberán designar al Comité Institucional de Gestión y Desempeño como el organismo encargado de la gestión y toma de decisiones.

También se debe conformar el equipo de trabajo que apoyará al Oficial de Seguridad y Privacidad de la Información durante la implementación y mantenimiento del Modelo de Seguridad y Privacidad de la Información – MSPI, para lo cual se debe establecer y dar a conocer el perfil y responsabilidades de los integrantes del equipo de trabajo.

El equipo de trabajo designado se encargará de tomar las medidas necesarias para planear, implementar y hacer seguimiento a todas las actividades incluidas en el presente Plan para la adopción del Modelo de Seguridad y Privacidad de la Información al interior de la Entidad, así mismo, estará encargado de planear las actividades necesarias para una adecuada administración y sostenibilidad del Modelo.

### Inventario de activos de información

El Instituto Distrital de la Participación y Acción Comunal desarrolló una metodología para la identificación, clasificación, mantenimiento y actualización del inventario de activos de información, entendiendo que hace parte de la debida diligencia que a nivel estratégico se ha definido en el Modelo de Seguridad y Privacidad de la Información

En concordancia, el inventario de activos de la información se registra en la matriz definida por la Entidad incluyendo la información pertinente respecto a los propietarios, custodios y usuarios de los activos de información identificados en cada vigencia.

### Integración del MSPI con el Sistema de Gestión documental

El Instituto Distrital de la Participación y Acción Comunal realizará la alineación de la documentación relacionada con seguridad y privacidad de la información con el sistema de gestión documental generado o emitido conforme a los parámetros emitidos por el Archivo General de la Nación.

### Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

El Instituto Distrital de la Participación y Acción Comunal elaborará este Plan con el fin de establecer la metodología y las actividades de gestión de riesgos tecnológicos que permitan identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados a la seguridad y privacidad de los activos de información..

Para conseguir una integración adecuada entre el MSPI y la guía de gestión del riesgo emitida por el DAFP respecto a este procedimiento, se emplearán los criterios de evaluación (impacto y probabilidad) y niveles de riesgo emitidos por esta entidad.

### Principio de Responsabilidad Demostrada (LPDP)

Como parte de la implementación de este Modelo el Instituto Distrital de la Participación y Acción Comunal realizará la adopción de un Programa Integral de Gestión de Datos Personales a partir del cual se establezcan medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012.

### Plan de continuidad del negocio

El Instituto Distrital de la Participación y Acción Comunal establecerá los lineamientos de respuesta necesarios para atender en forma oportuna los incidentes que puedan alterar el normal funcionamiento de la infraestructura de tecnologías de la información, afectando la operación diaria de la Entidad.

Para eso, se desarrollarán las guías para la recolección de los datos, las finalidades de uso y la relevancia de los datos para su tratamiento y la definición de medidas de seguridad apropiadas.

### Declaración de Aplicabilidad de Seguridad y Privacidad de la Información

Se elaborará un documento para el registro de los controles y medidas de seguridad aplicadas después de la evaluación y tratamiento de riesgos.

### Plan de Comunicaciones

Establecer las actividades y programas para la capacitación, sensibilización y comunicación al interior de la Entidad de las políticas implementadas de Seguridad y Privacidad de la Información, con el propósito de generar cultura organizacional, competencias y hábitos, en todos los niveles de la Entidad.

### Plan de transición de IPv4 a IPv6

Para llevar a cabo el proceso de transición de IPv4 a IPv6, se cumplirá con la fase de planeación establecida en la Guía No 20 - Transición de IPv4 a IPv6 para Colombia que indica las actividades específicas a desarrollar.

## Fase 3: Implementación

Con base en las actividades definidas para esta fase se realizará la implementación de las acciones desarrolladas en las fases anteriores.

Tabla 3. Plan de Acción Fase 3

| Acción | Producto | Fecha inicio | Fecha fin |
| --- | --- | --- | --- |
| Definir la planificación y el control operacional | Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección | 01/06/2019 | 30/12/2019 |
| Implementar el Plan de Tratamiento de Riesgos | Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso | 13/01/2019 | 14/04/2019 |
| Formular los indicadores de gestión | Hoja de vida de los indicadores de gestión de seguridad y privacidad de la información | 28/07/2019 | 17/08/2019 |
| Plan de Transición de IPv4 a IPv6 | Documento con las estrategias del Plan de Implementación de IPv6 | 15/06/2019 | 30/12/2019 |

Fuente: Elaboración propia.

### Planificación y control operacional

Se realizará la planificación, implementación y control a los procesos necesarios para cumplir con los requisitos de seguridad y privacidad de la información, garantizando que permitan implementar las acciones determinadas en el plan de tratamiento de riesgos.

Además, se documentará la información necesaria que contribuya a evidenciar que los procesos se han llevado a cabo según lo planificado, adicionalmente, se llevará un control de cambios que apoye la toma de acciones para mitigar efectos adversos cuando sea necesario.

### Implementación del Plan de Tratamiento de Riesgos

Se implementará el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, en el cual se identifica el control a aplicar para llevar cada uno de los riesgos a un nivel aceptable para la Entidad.

### Indicadores de gestión

El Instituto Distrital de la Participación y Acción Comunal establecerá indicadores de gestión de Seguridad y Privacidad de la Información con el propósito de medir la efectividad, eficacia y eficiencia de los procedimientos, políticas y lineamientos desarrollados en el Modelo de Seguridad y Privacidad de la Información.

### Plan de Transición de IPv4 a IPv6

Se elaborará el documento detallado con el Plan de Transición e Implementación del Protocolo IPv6 en la Entidad. Las guías de apoyo para esta labor son “Guía de Transición de IPv4 a IPv6 para Colombia” y “Guía de Aseguramiento del Protocolo IPv6”

## Fase 4: Evaluación de desempeño

El proceso de seguimiento y monitoreo del MSPI se realizará con base en los resultados de los indicadores de gestión de seguridad y privacidad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas.

Tabla 4. Plan de Acción Fase 4

|  |  |  |  |
| --- | --- | --- | --- |
| Acción | Producto | Fecha inicio | Fecha fin |
| Elaborar el plan de revisión y seguimiento a la implementación del MSPI | Plan de revisión y seguimiento del MSPI revisado y aprobado por la alta Dirección | 15/06/2019 | 15/08/2019 |
| Elaborar el plan de auditorías internas | Plan de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección | 15/07/2019 | 30/08/2019 |

Fuente: Elaboración propia.

### Plan de revisión y seguimiento a la implementación del MSPI

En esta acción el Instituto Distrital de la Participación y Acción Comunal creará un plan que contemple las siguientes actividades:

* Revisión de la efectividad de los controles establecidos y su apoyo al cumplimiento de los objetivos de seguridad.
* Revisión de la evaluación de los niveles de riesgo y riesgo residual después de la aplicación de controles y medidas administrativas.
* Seguimiento a la programación y ejecución de las actividades de autorías internas y externas del MSPI.
* Seguimiento al alcance y a la implementación del MSPI.
* Seguimiento a los registros de acciones y eventos / incidentes que podrían tener impacto en la eficacia o desempeño de la seguridad de la información al interior de la entidad.
* Medición de los indicadores de gestión del MSPI.
* Revisiones de acciones o planes de mejora (solo aplica en la segunda revisión del MSPI)

Este plan deberá permitir la consolidación de indicadores periódicamente y su evaluación frente a las metas esperadas; permitiendo analizar causas de desviación y su impacto en el cumplimiento de las metas y objetivos del MSPI.

### Plan de auditorías internas

El Instituto Distrital de la Participación y Acción Comunal revisará y actualizará el Plan Anual de Auditorías Internas con el propósito de incluir las auditorías internas que se defina programar, especificando la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de informes.

Estas auditorías y revisiones independientes a intervalos planificados permitirán identificar si el MSPI es conforme con los requisitos, está implementado adecuadamente y se mantiene de forma eficaz; también permitirán identificar las debilidades y amenazas existentes, como insumo para establecer acciones de mejora.

Los resultados de la ejecución de las auditorías deberán socializarse con las partes interesadas.

## Fase 5: Mejora continua

En esta fase se consolidan los resultados obtenidos en la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

Tabla 5. Plan de Acción Fase 5.

|  |  |  |  |
| --- | --- | --- | --- |
| Acción | Producto | Fecha inicio | Fecha fin |
| Elaborar el plan de mejora continua | Documento con el plan de mejoramiento.Documento con el plan de comunicación de resultados. | 01/09/2019 | 11/11/2019 |

Fuente: Elaboración propia.

### Plan de mejora continua

En esta fase se definirá y ejecutará el Plan de Mejora Continua con base en los resultados de la fase de evaluación del desempeño. Este plan incluirá:

* Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI.
* Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI.

Utilizando los insumos anteriores, se efectuarán los ajustes a los entregables, controles y procedimientos dentro del MSPI. Estos insumos tendrán como resultado un plan de mejoramiento y un plan de comunicaciones de mejora continua, revisados y aprobados por la Alta Dirección. La revisión por la Alta Dirección hace referencia a las decisiones, cambios, prioridades etc. tomadas en sus comités y que impacten el MSPI.

# Responsables

## Dirección General o delegado

La responsabilidad de asegurar la implementación del Plan de Seguridad y Privacidad de la Información es la Dirección General y del Comité Institucional de Gestión y Desempeño, quienes deben garantizar la asignación de recursos y el compromiso de designación del equipo de trabajo.

## Líder Oficial de Seguridad y Privacidad de la Información

Responsable de liderar todos los temas asociados a la Seguridad y Privacidad de la Información de la Entidad; deberá guiar la implementación del Plan de Seguridad y Privacidad de la Información asegurando la calidad de los entregables y el cumplimiento del plan en su totalidad.

## Equipo de trabajo de seguridad y privacidad de la información

Responsables de tomar las medidas necesarias para planear, implementar y hacer seguimiento a todas las acciones establecidas para adoptar el Modelo de Seguridad y Privacidad de la Información a partir del presente plan.

Este equipo de trabajo deberá conformarse con los directivos y representantes de las áreas misionales.