




 <p>Alcaldía Municipal <b>Ibagué</b> NIT.800113389-7</p>	<b>MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Código:</b>	
		<b>Versión:</b>	
	<b>PROCESO: GESTION DE RECURSOS FISICOS E INFRAESTRUCTURA TECNOLOGICA</b>	<b>Vigente desde:</b>	
		<b>Pág. 1 de 38</b>	

# MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

 <p>Alcaldía Municipal <b>Ibagué</b> NIT.800113389-7</p>	<b>MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	Código:	
		<b>PROCESO: GESTION DE RECURSOS FISICOS E INFRAESTRUCTURA TECNOLÓGICA</b>	
		Vigente desde:	
		Pág. 2 de 38	

## CONTENIDO



<b>1. DERECHOS DE AUTOR .....</b>	<b>3</b>
<b>2. AUDIENCIA.....</b>	<b>4</b>
<b>3. INTRODUCCION.....</b>	<b>5</b>
<b>4. GLOSARIO .....</b>	<b>6</b>
<b>5. OBJETIVOS .....</b>	<b>13</b>
5.1 Objetivo General.....	13
5.2 Objetivos Específicos .....	13
<b>6. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN .....</b>	<b>14</b>
6.1 Desarrollo del Ciclo de Operación .....	14
6.1.1 Diagnóstico.....	14
6.1.2 Planificación .....	16
6.1.3 Implementación .....	20
6.1.4 Evaluación de Desempeño.....	22
6.1.5 Mejora Continua .....	24
<b>7. MODELO DE MADUREZ .....</b>	<b>26</b>
<b>8. PRIVACIDAD DE LA INFORMACION .....</b>	<b>28</b>
8.1 Diagnóstico.....	30
8.2 Planificación .....	32
8.3 Implementación.....	33
8.4 Evaluación de Desempeño .....	33
8.5 Mejora Continua.....	34
<b>9. ADOPCION DEL PROTOCOLO IPv6.....</b>	<b>35</b>
9.1 Planeación.....	35
9.2 Implementación .....	36
9.3 Pruebas de Funcionalidad .....	37
<b>10.CONTROL DE CAMBIOS .....</b>	<b>38</b>

 <p>Alcaldía Municipal <b>Ibagué</b> NIT.800113389-7</p>	<b>MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Código:</b>	
		<b>Versión:</b>	
	<b>PROCESO: GESTION DE RECURSOS FISICOS E INFRAESTRUCTURA TECNOLOGICA</b>	<b>Vigente desde:</b>	
		<b>Pág. 3 de 38</b>	

## 1. DERECHOS DE AUTOR



Todas las referencias a los documentos del Modelo de Seguridad y Privacidad de la Información, con derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la estrategia de Gobierno en Línea.

Todas las referencias a las políticas, definiciones o contenido relacionado, publicadas en el compendio de las normas técnicas colombianas NTC ISO/IEC 27000 vigentes, así como a los anexos con derechos reservados por parte de ISO/CONTEC.

 <p>Alcaldía Municipal <b>Ibagué</b> NIT.800113389-7</p>	<p><b>MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b></p>	<p><b>Código:</b></p>	
	<p><b>PROCESO: GESTION DE RECURSOS FISICOS E INFRAESTRUCTURA TECNOLÓGICA</b></p>	<p><b>Versión:</b></p>	
		<p><b>Vigente desde:</b></p>	
		<p><b>Pág. 4 de 38</b></p>	

## 2. AUDIENCIA

El Modelo de Privacidad y Seguridad de la Información está orientado a la Alcaldía de Ibagué y son de obligatorio cumplimiento en los procesos que sean referenciados en el Alcance y por todos los servidores públicos, proveedores, ciudadanos, terceros y demás personas vinculadas que hacen parte de dichos procesos.

 <p>Alcaldía Municipal <b>Ibagué</b> NIT.800113389-7</p>	<b>MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	Código:	
		Versión:	
	<b>PROCESO: GESTION DE RECURSOS FISICOS E INFRAESTRUCTURA TECNOLOGICA</b>	Vigente desde:	
		Pág. 5 de 38	

### 3. INTRODUCCION



El Modelo de Seguridad y Privacidad de la Información – MSPI, tiene el propósito de preparar a la Entidad para la preservación de la confidencialidad, integridad y disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo que brinde confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

Con la implementación de un modelo de seguridad y privacidad de la información, la Alcaldía de Ibagué, busca garantizar el cumplimiento de los objetivos esenciales y la misión institucional. Esto incluye la transparencia misma de la gestión pública, y el establecimiento establecer los lineamientos para adoptar las mejores prácticas de seguridad para prevenir incidentes con un impacto negativo, identificando la infraestructura crítica en la entidad. Promueve además un mejor intercambio de la información pública, cumplir con la legislación relacionada con la protección de datos personales, logrando respetar los derechos de los titulares de los datos (privacidad) y optimizando la labor de acceso a la información pública

La planificación e implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, en la Entidad está determinado por las necesidades y objetivos, los requisitos de seguridad, los procesos misionales y el tamaño y estructura de la Entidad.

Este documento se elaboró siguiendo los lineamientos del Ministerio de las TIC en el marco de la estrategia de TI, denominado Modelo de Seguridad y Privacidad de la Información, el cual contiene la recopilación de las mejores prácticas nacionales e internacionales para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del MSPI; así mismo para estar acorde con las buenas prácticas de seguridad, se tomó como referencia un conjunto de documentos asociados al modelo que tiene disponible el Ministerio de las tic.

Para el desarrollo de cada uno de los productos y entregables de las diferentes etapas del ciclo de vida del MSPI, se toma como referencia las guías e instructivos dispuestos por el Ministerio de las TIC así como los documentos del marco de referencia de Arquitectura Empresarial

 <p>Alcaldía Municipal <b>Ibagué</b> NIT.800113389-7</p>	<b>MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Código:</b>	
	<b>PROCESO: GESTION DE RECURSOS FISICOS E INFRAESTRUCTURA TECNOLÓGICA</b>	<b>Versión:</b>	
		<b>Vigente desde:</b>	
		<b>Pág. 6 de 38</b>	

#### 4. GLOSARIO

##### **Acceso a la Información Pública:**

Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

##### **Activo**

En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).

##### **Activo de Información:**

En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

##### **Archivo:**



Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

##### **Amenazas**

Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

##### **Análisis de Riesgo**

Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

 <p>Alcaldía Municipal <b>Ibagué</b> NIT.800113389-7</p>	<b>MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Código:</b>	
	<b>PROCESO: GESTION DE RECURSOS FISICOS E INFRAESTRUCTURA TECNOLÓGICA</b>	<b>Versión:</b>	
		<b>Vigente desde:</b>	
		<b>Pág. 7 de 38</b>	

## **Auditoría**

Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

## **Autorización:**

Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

## **Bases de Datos Personales**

Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

## **Ciberseguridad**

Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

## **Ciberespacio**



Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

## **Control**

Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

## **Datos Abiertos**

Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con

 <p>Alcaldía Municipal <b>Ibagué</b> NIT.800113389-7</p>	<p><b>MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b></p>	<p><b>Código:</b></p>	
	<p><b>PROCESO: GESTION DE RECURSOS FISICOS E INFRAESTRUCTURA TECNOLÓGICA</b></p>	<p><b>Versión:</b></p>	
	<p><b>Vigente desde:</b></p>		
	<p><b>Pág. 8 de 38</b></p>		

el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)

### **Datos Personales**

Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

### **Datos Personales Públicos:**

Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

### **Datos Personales Privados:**

Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)

### **Datos Personales Mixtos:**

Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.



### **Datos Personales Sensibles:**

Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

### **Declaración de aplicabilidad**

Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la



 <p>Alcaldía Municipal <b>Ibagué</b> NIT.800113389-7</p>	<b>MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Código:</b>	
	<b>PROCESO: GESTION DE RECURSOS FISICOS E INFRAESTRUCTURA TECNOLOGICA</b>	<b>Versión:</b>	
		<b>Vigente desde:</b>	
		<b>Pág. 9 de 38</b>	

justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

### **Derecho a la Intimidad**

Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

### **Encargado del Tratamiento de Datos**

Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)

### **Gestión de incidentes de seguridad de la información**

Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

### **Información Pública Clasificada**



Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. ( art 6)

### **Información Pública Reservada**

Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

### **Ley de Habeas Data**

Se refiere a la Ley Estatutaria 1266 de 2008.

 <p>Alcaldía Municipal <b>Ibagué</b> NIT.800113389-7</p>	<b>MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Código:</b>	
	<b>PROCESO: GESTION DE RECURSOS FISICOS E INFRAESTRUCTURA TECNOLÓGICA</b>	<b>Versión:</b>	
		<b>Vigente desde:</b>	
		<b>Pág. 10 de 38</b>	

## **Ley de Transparencia y Acceso a la Información Pública**

Se refiere a la Ley Estatutaria 1712 de 2014.

**MRAE:** Marco de Referencia Arquitectura Empresarial

**MSPI:** Modelo de Seguridad y Privacidad de la Información

### **Mecanismos de protección de datos personales**

Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

### **Plan de continuidad del negocio**

Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

### **Plan de tratamiento de riesgos**

Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).



### **Privacidad**

En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

### **Protocolo IPV4**

El Protocolo de Internet versión 4, en inglés: Internet Protocolo versión 4 (IPv4), es la cuarta versión del Internet Protocolo (IP). Un protocolo de interconexión de redes basados en Internet, y fue la primera versión implementada para la producción de ARPANET, en 1983. Definida en el RFC 791

La versión vigente y controlada de este documento, solo podrá ser consultada a través de la plataforma PISAMI y/o de Intranet de la Administración Municipal. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es responsabilidad de la Alcaldía de Ibagué

 <p>Alcaldía Municipal <b>Ibagué</b> NIT.800113389-7</p>	<b>MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Código:</b>	
	<b>PROCESO: GESTION DE RECURSOS FISICOS E INFRAESTRUCTURA TECNOLÓGICA</b>	<b>Versión:</b>	
		<b>Vigente desde:</b>	
		<b>Pág. 11 de 38</b>	

## Protocolo IPv6

Es la versión 6 del Protocolo de Internet (IP por sus siglas en inglés, Internet Protocol), es el encargado de dirigir y encaminar los paquetes en la red, fue diseñado en los años 70 con el objetivo de interconectar redes; diseñado para reemplazar a Internet Protocolo versión 4 (IPv4) RFC 791, que a 2016 se está implementando en la gran mayoría de dispositivos que acceden a Internet.

## Registro Nacional de Bases de Datos:

Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

## Responsabilidad Demostrada:

Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

## Responsable del Tratamiento de Datos:

Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).



## Riesgo

Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

## Seguridad de la información

Preservación de la confidencialidad, integridad, y disponibilidad de la información.

La versión vigente y controlada de este documento, solo podrá ser consultada a través de la plataforma PISAMI y/o de Intranet de la Administración Municipal. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es responsabilidad de la Alcaldía de Ibagué

 <p>Alcaldía Municipal <b>Ibagué</b> NIT.800113389-7</p>	<b>MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Código:</b>	
	<b>PROCESO: GESTION DE RECURSOS FISICOS E INFRAESTRUCTURA TECNOLÓGICA</b>	<b>Versión:</b>	
		<b>Vigente desde:</b>	
		<b>Pág. 12 de 38</b>	

(ISO/IEC 27000).

## **Sistema de Gestión de Seguridad de la Información SGSI**

Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

### **Titulares de la información:**

Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

### **Tratamiento de Datos Personales:**

Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

### **Trazabilidad**



Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

### **Vulnerabilidad**

Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

### **Partes interesadas (Stakeholder)**

Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

 <p>Alcaldía Municipal <b>Ibagué</b> NIT.800113389-7</p>	<p><b>MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b></p>	<p><b>Código:</b></p>	
	<p><b>PROCESO: GESTION DE RECURSOS FISICOS E INFRAESTRUCTURA TECNOLÓGICA</b></p>	<p><b>Versión:</b></p>	
	<p><b>Vigente desde:</b></p>		
	<p><b>Pág. 13 de 38</b></p>		



## 5. OBJETIVOS

### 5.1 Objetivo General

Establecer las políticas, procedimientos y controles para garantizar la administración, manejo y control de la seguridad y privacidad de la información de la Alcaldía de Ibagué.

### 5.2 Objetivos Específicos

- Brindar lineamientos para la implementación de la gestión de la seguridad y privacidad de la información.
- Asignar roles y responsabilidades para garantizar la seguridad y privacidad de la
- Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.
- Alinear el Modelo de Seguridad y Privacidad de la Información con el Marco de Referencia de Arquitectura Empresarial de TI.
- Dar lineamientos para la implementación de mejores prácticas de seguridad que garanticen la privacidad, confidencialidad y disponibilidad de la información.
- Orientar a la Entidad para la construcción de una política de privacidad respetuosa de los datos personales de los titulares.
- Optimizar la gestión de la información al interior de la Alcaldía.
- Contribuir al incremento de la transparencia en la gestión pública.
- Administrar los riesgos de seguridad digital a fin de incrementar la confianza de las múltiples partes interesadas en el uso del entorno digital y del aseguramiento de los activos de información de la Entidad.

 <p>Alcaldía Municipal <b>Ibagué</b> NIT.800113389-7</p>	<b>MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Código:</b>	
	<b>PROCESO: GESTION DE RECURSOS FISICOS E INFRAESTRUCTURA TECNOLÓGICA</b>	<b>Versión:</b>	
		<b>Vigente desde:</b>	
		<b>Pág. 14 de 38</b>	

## 6. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El modelo de seguridad y privacidad de la información contempla un ciclo de operación que consta de cinco (5) fases, que permiten una adecuada gestión de la seguridad y privacidad de los activos de información.



Figura 1. Ciclo de operación Modelo de Seguridad y Privacidad de la Información



Fuente: Mintic. [http://estrategia.gobiernoonline.gov.co/623/articles-8258\\_recurso\\_1.pdf](http://estrategia.gobiernoonline.gov.co/623/articles-8258_recurso_1.pdf)

### 6.1 Desarrollo del Ciclo de Operación

#### 6.1.1 Diagnóstico

En esta fase se identifica el estado actual de la Alcaldía de Ibagué, con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información, y para tal efecto se utiliza la herramienta “Instrumento de Evaluación MSPI”, suministrada por el Ministerio de las TIC para efectuar el autodiagnóstico.

El “Instrumento de Evaluación MSPI” es una herramienta que fue creada por el Ministerio de Tecnologías de la Información y las Comunicaciones, con el fin de identificar el nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información, permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las Entidades Públicas, según lo definido en la Estrategia de Gobierno en Línea en su cuarto componente “Seguridad y Privacidad de la Información”.

 <p>Alcaldía Municipal <b>Ibagué</b> NIT.800113389-7</p>	<p><b>MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b></p>	<p><b>Código:</b></p>	
	<p><b>PROCESO: GESTION DE RECURSOS FISICOS E INFRAESTRUCTURA TECNOLÓGICA</b></p>	<p><b>Versión:</b></p>	
		<p><b>Vigente desde:</b></p>	
		<p><b>Pág. 15 de 38</b></p>	

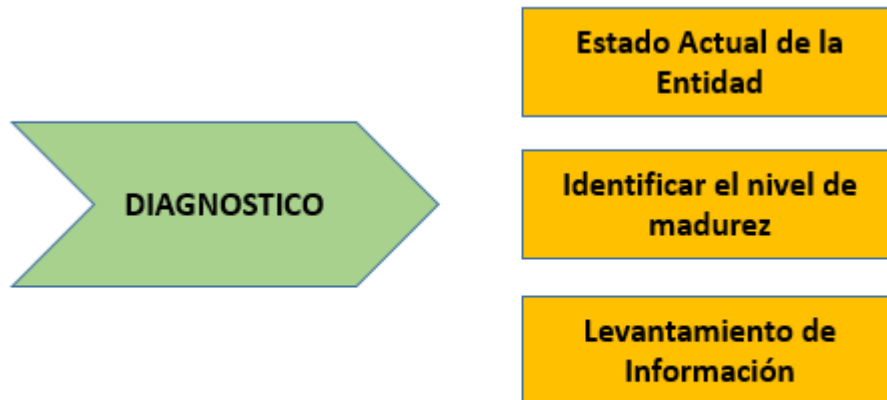


Figura 2. Etapas previas a la implementación

Fuente: MINTIC [http://estrategia.gobiernoenlinea.gov.co/623/articles-8258\\_recurso\\_1.pdf](http://estrategia.gobiernoenlinea.gov.co/623/articles-8258_recurso_1.pdf)



En la fase de diagnóstico del MSPI se pretende:

- Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.
- Determinar el nivel de madurez de los controles de seguridad de la información. (ver numeral 7.)
- Identificar el avance de la implementación del ciclo de operación al interior de la entidad.
- Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.
- Identificación del uso de buenas prácticas en ciberseguridad.

En esta etapa se tomarán como documentos fuente, los instrumentos suministrados por el Ministerio de las TIC:

- Instrumento de evaluación MPSI
- Instructivo para el diligenciamiento de la herramienta
- Guía No 1 - Metodología de Pruebas de Efectividad



 <p>Alcaldía Municipal <b>Ibagué</b> NIT.800113389-7</p>	<b>MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Código:</b>	
	<b>PROCESO: GESTION DE RECURSOS FISICOS E INFRAESTRUCTURA TECNOLÓGICA</b>	<b>Versión:</b>	
		<b>Vigente desde:</b>	
		<b>Pág. 16 de 38</b>	

**Tabla 1 - Metas, Resultados e Instrumentos de la fase etapas previas a la implementación**

<b>Nivel de Madurez: Preparación</b>		
<b>Metas</b>	<b>Resultados</b>	<b>MSPI</b>
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.	Diligenciamiento de la herramienta de autoevaluación	Instrumento de Evaluación MSPI
Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad	Diligenciamiento de la herramienta e identificación del nivel de madurez de la entidad.	Instrumento de Evaluación MSPI
Levantamiento de información para las pruebas que permitan establecer la efectividad de los controles existentes.	Documento con la preparación para el análisis de vulnerabilidades y de riesgo	Metodología de pruebas de efectividad

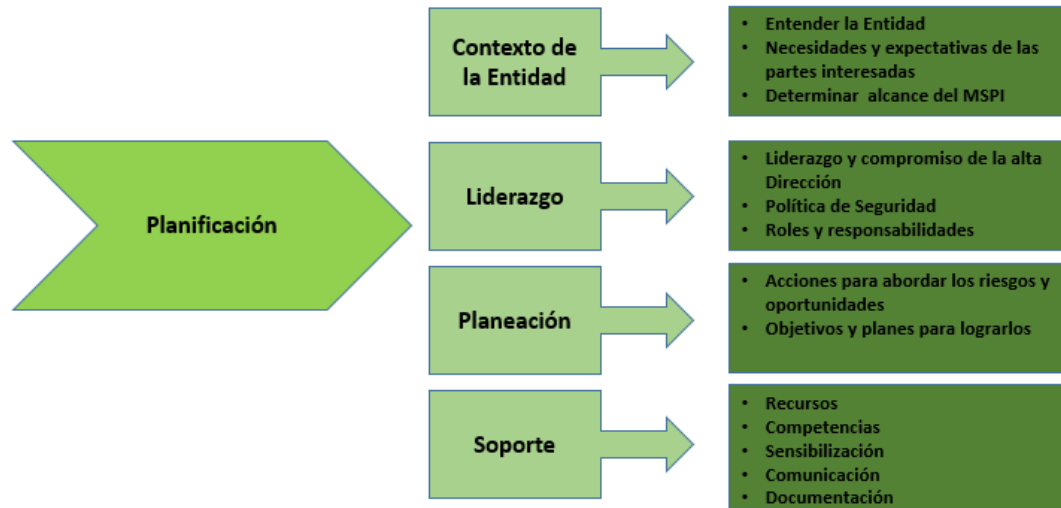
Una vez se tenga el resultado del diagnóstico inicial y se haya determinado el nivel de madurez de la entidad se procede al desarrollo de la fase de Planificación.

Los resultados asociados a la fase de Diagnostico previas a la implementación deben ser revisados y socializados por las partes interesadas.

### **6.1.2 Planificación**

Basados en los resultados de la etapa anterior, se procede a la elaboración el plan de plan de seguridad y privacidad de la información alineado con el objetivo misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo.







**Figura 3. Fase de Planificación**

Fuente: Mintic : [http://estrategia.gobiernoenlinea.gov.co/623/articulos-8258\\_recurso\\_1.pdf](http://estrategia.gobiernoenlinea.gov.co/623/articulos-8258_recurso_1.pdf)

**Tabla 2 - Metas, Resultados e Instrumentos de la fase de planificación**

Metas	Resultados	MSPI
Política de Seguridad general con objetivos y alcance de MSPI	Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad.	Guía No 2 – Política General MSPI
Políticas de seguridad y privacidad de la información	Documento con las políticas específicas seguridad y privacidad de la información, debidamente aprobadas por la alta dirección y socializadas al interior de la Entidad.	Guía no 2 - Política General MSPI
Procesos y Procedimientos de seguridad de la información debidamente definidos	Formatos de procesos y Procedimientos, debidamente definidos, establecidos y aprobados por el comité de gestión institucional.	Guía No 3 - Procedimientos de Seguridad y Privacidad de la Información.
Roles y responsabilidades de seguridad y privacidad de la información.	Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad.	Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información.



 <p>Alcaldía Municipal <b>Ibagué</b> NIT.800113389-7</p>	<b>MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Código:</b>	
	<b>PROCESO: GESTION DE RECURSOS FISICOS E INFRAESTRUCTURA TECNOLÓGICA</b>	<b>Versión:</b>	
		<b>Vigente desde:</b>	
		<b>Pág. 18 de 38</b>	

Metas	Resultados	MSPI
Inventario de activos de información.	Documento con la identificación, clasificación y valoración de los activos de información, revisado y aprobado por la alta Dirección.	Guía No 5 - Gestión De Activos
Integración del MSPI con el Sistema de Gestión documental	Plan de Integración del MSPI y sistema de gestión documental de la entidad.	Guía No 6 - Gestion Documental
Identificación, Valoración y tratamiento de riesgo.	Documento con la metodología de gestión de riesgos. Documento con el análisis y evaluación de riesgos. Documento con el plan de tratamiento de riesgos. Documentos revisados y aprobados por la Alta Dirección	Guía No 7 - Gestion de Riesgos Guía No 8 - Controles de Seguridad
Plan de Comunicaciones.	Documento con el plan de comunicación, sensibilización y capacitación para la entidad.	Guía No 14 - Plan de comunicación, sensibilización y capacitación
Plan de diagnóstico de IPv4 a IPv6.	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6.	Guía No 20 - Transición IPv4 a IPv6

A continuación, se explica de manera general los productos de la fase de planificación del Modelo de Seguridad y Privacidad de la Información:

**Política de seguridad y privacidad de la información.** La Política de Seguridad y Privacidad de la información estará contenida en un documento de alto nivel que incluye la voluntad de la Alta Dirección de la Entidad para apoyar la implementación del Modelo de Seguridad y Privacidad de la Información.

La política contendrá una declaración general por parte de la administración, donde se especifique sus objetivos, alcance, nivel de cumplimiento. La política debe ser aprobada y divulgada al interior de la entidad.

 <p>Alcaldía Municipal <b>Ibagué</b> NIT.800113389-7</p>	<b>MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Código:</b>	
	<b>PROCESO: GESTION DE RECURSOS FISICOS E INFRAESTRUCTURA TECNOLOGICA</b>	<b>Versión:</b>	
		<b>Vigente desde:</b>	
		<b>Pág. 19 de 38</b>	

**Políticas de Seguridad y Privacidad de la Información.** Manual de políticas, donde se describe los objetivos, alcances y el nivel de cumplimiento, que garanticen el adecuado uso de los Activos de información al interior de la Entidad; definiendo las responsabilidades generales y específicas para la gestión de la seguridad de la información.



En el manual de políticas de la entidad, se explica de manera general, las políticas, los principios de seguridad y la normatividad pertinente. La entidad debe evaluar los requerimientos necesarios para ser ajustados o desarrollados en la elaboración de las políticas de seguridad y privacidad, así como en la implementación.

**Procedimientos de Seguridad de la Información.** desarrollar y formalizar procedimientos que permitan gestionar la seguridad de la información en cada uno de los procesos definidos en la entidad. Para desarrollar esta actividad, se tomará como referencia la Guía No 3 - describe los procedimientos mínimos que se deberían tener en cuenta para la gestión de la seguridad al interior de la entidad.

**Roles y Responsabilidades de Seguridad y Privacidad de la Información.** La entidad debe definir mediante un acto administrativo (Resolución, circular, decreto, entre otros) los roles y las responsabilidades de seguridad de la información en los diferentes niveles (Directivo, De procesos y Operativos) que permitan la correcta toma de decisiones y una adecuada gestión que permita el cumplimiento de los objetivos de la Entidad. Para desarrollar estas actividades, se tomará como referencia la Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información.

**Inventario de activos de información.** La entidad desarrollará la metodología de gestión de activos de la Guía No.5, que le permita generar un inventario de activos de información exacto, actualizado y consistente, que a su vez permita definir la criticidad de los activos de información, sus propietarios, custodios y usuarios

**Integración del MSPI con el Sistema de Gestión documental.** La entidad deberá alinear la documentación relacionada con seguridad de la información con el sistema de gestión documental generado o emitido conforme a los parámetros emitidos por el archivo general de la nación. Para tal efecto tomará como referencia La Guía No 6 - Gestión Documental, la cual brinda información relacionada para poder llevar a cabo la realización de las actividades mencionadas previamente.

 <p>Alcaldía Municipal <b>Ibagué</b> NIT.800113389-7</p>	<p><b>MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b></p>	<p><b>Código:</b></p>	
	<p><b>PROCESO: GESTION DE RECURSOS FISICOS E INFRAESTRUCTURA TECNOLÓGICA</b></p>	<p><b>Versión:</b></p>	
		<p><b>Vigente desde:</b></p>	
		<p><b>Pág. 20 de 38</b></p>	

**Identificación, Valoración Y Tratamiento de Riesgos.** La entidad aplicará la metodología de gestión del riesgo de seguridad digital, según los lineamientos del DAFP y la Guía No 8 - Controles de Seguridad.

**Plan de Comunicaciones.** La Entidad debe definir un Plan de comunicación, sensibilización y capacitación que incluya la estrategia para que la seguridad de la información se convierta en cultura organizacional, al generar competencias y hábitos en todos los niveles (directivos, funcionarios, terceros) de la entidad. Este plan será ejecutado, con el aval de la Alta Dirección, a todas las áreas de la Entidad. Para estructurar se tomará como referencia la Guía No 14 – plan de comunicación, sensibilización y capacitación.

**Plan de transición de IPv4 a IPv6.** Para llevar a cabo el proceso de transición de IPv4 a IPv6 en las entidades, se debe cumplir 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.

### 6.1.3 Implementación

En esta fase la Entidad llevará a cabo las actividades de la fase de planeación.

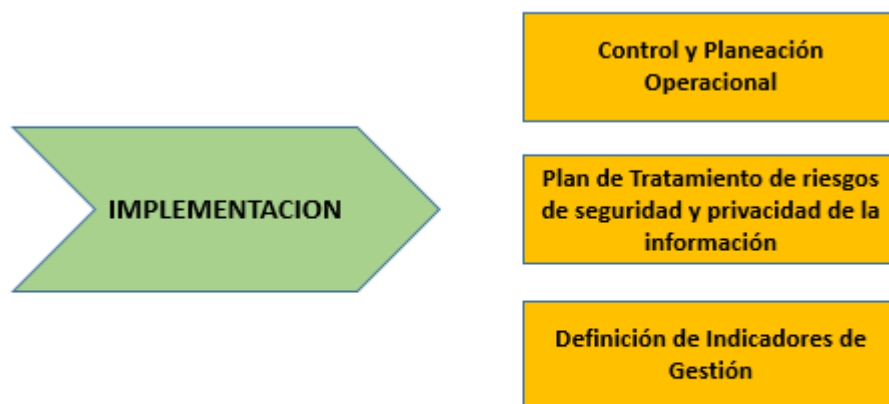


Figura 4. Fase de implementación

Fuente: MINTIC [http://estrategia.gobiernoenlinea.gov.co/623/articles-8258\\_recurso\\_1.pdf](http://estrategia.gobiernoenlinea.gov.co/623/articles-8258_recurso_1.pdf)





 <p>Alcaldía Municipal <b>Ibagué</b> NIT.800113389-7</p>	<b>MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	Código:	
		<b>PROCESO: GESTION DE RECURSOS FISICOS E INFRAESTRUCTURA TECNOLÓGICA</b>	
		Vigente desde:	
		Pág. 21 de 38	

Tabla 3 - Metas, Resultados e Instrumentos de la Fase de Implementación

Implementación			
Metas	Resultados	Instrumentos	
		MSPI	MRAE
Planificación y Control Operacional.	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad.	LI.ES.09 LI.ES.10 LI.GO.04 LI.GO.09 LI.GO.10 LI.GO.14 LI.GO.15 LI.INF.09 LI.INF.10 LI.INF.11 LI.INF.14 LI.INF.15 LI.SIS.22 LI.SIS.23 LI.ST.05 LI.ST.06 LI.ST.09 LI.ST.10 LI.ST.12
Implementación del plan de tratamiento de riesgos.	Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso.	Documento con la declaración de aplicabilidad. Documento con el plan de tratamiento de riesgos.	
Indicadores De Gestión.	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información.	Guía No 9 - Indicadores de Gestión SI.	
Plan de Transición de IPv4 a IPv6	Documento con las estrategias del plan de implementación de IPv6 en la entidad, aprobado por el área de TI	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6. Guía No 20 - Transición de IPv4 a IPv6 para Colombia. Guía No 19 – Aseguramiento del Protocolo IPv6.	LI.ST.13 LI.UA.01

Con base a los resultados de la fase de planeación, en la fase de implementación deberá

La versión vigente y controlada de este documento, solo podrá ser consultada a través de la plataforma PISAMI y/o de Intranet de la Administración Municipal. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es responsabilidad de la Alcaldía de Ibagué

 <p>Alcaldía Municipal <b>Ibagué</b> NIT.800113389-7</p>	<b>MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Código:</b>	
	<b>PROCESO: GESTION DE RECURSOS FISICOS E INFRAESTRUCTURA TECNOLOGICA</b>	<b>Versión:</b>	
		<b>Vigente desde:</b>	
		<b>Pág. 22 de 38</b>	

ejecutarse las siguientes actividades:

### **Planificación y Control Operacional.**

La entidad debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad y privacidad de la información que permitan implementar las acciones determinadas en el plan de tratamiento de riesgos.

La entidad debe tener información documentada en la medida necesaria para tener la confianza en que los procesos se han llevado a cabo según lo planificado, adicionalmente, deberá llevarse un control de cambios que le permitan tomar acciones para mitigar efectos adversos cuando sea necesario.

### **Implementación del plan de tratamiento de riesgos.**

Se debe implementar el plan de tratamiento de riesgos de seguridad digital, en el cual se identifica el control a aplicar para llevar cada uno de los riesgos a un nivel aceptable para la entidad, en donde la base para ejecutar esta actividad es la Guía de Administración del Riesgo que emita el DAFP.



### **Indicadores De Gestión.**

La entidad deberá definir indicadores que le permitan medir la efectividad, la eficiencia y la eficacia en la gestión y las acciones implementadas en seguridad de la información.

Los indicadores buscan medir:

- Efectividad en los controles.
- Eficiencia del MSPI al interior de la entidad.
- Proveer estados de seguridad que sirvan de guía en las revisiones y la mejora continua.
- Comunicar valores de seguridad al interior de la entidad.
- Servir como insumo al plan de control operacional.

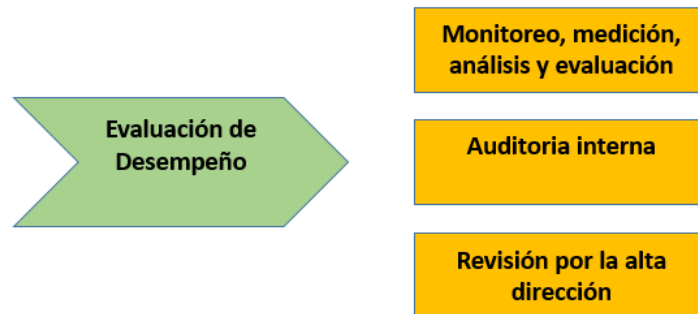
### **Plan de Transición de IPv4 a IPv6.**

 <p>Alcaldía Municipal <b>Ibagué</b> NIT.800113389-7</p>	<b>MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	Código:	
		<b>PROCESO: GESTION DE RECURSOS FISICOS E INFRAESTRUCTURA TECNOLÓGICA</b>	
		Vigente desde:	
		Pág. 23 de 38	

Se deberá generar el documento detallado con el plan de transición e implementación del protocolo IPv6 en la entidad.

### 6.1.4 Evaluación de Desempeño

El proceso de seguimiento y monitoreo del MSPI se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas.





**Figura 5. Figura 5 - Fase de Evaluación de desempeño**  
Fuente: MINTIC [http://estrategia.gobiernoonline.gov.co/623/articles-8258\\_recurso\\_1.pdf](http://estrategia.gobiernoonline.gov.co/623/articles-8258_recurso_1.pdf)

**Tabla 4 - Metas, Resultados e Instrumentos de la Fase de Evaluación de Desempeño**

Implementación			
Metas	Resultados	Instrumentos	
		MSPI	MRAE
Plan de revisión y seguimiento, a la implementación del MSPI.	Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección.	Guía No 16 – Evaluación del desempeño.	LI.ES.12,LI.ES.13 LI.GO.03,LI.GO.11 LI.GO.12,LI.INF.09 LI.INF.11 ,I.INF.13 LI.INF.14,LI.INF.15 LI.SIS.23 LI.ST.05 LI.ST.06 LI.ST.08 LI.ST.15 LI.UA.07 LI.UA.08
Plan de Ejecución de Auditorías	Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección.	Guía No 15 – Guía de Auditoría.	



 <p>Alcaldía Municipal <b>Ibagué</b> NIT.800113389-7</p>	<b>MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Código:</b>	
	<b>PROCESO: GESTION DE RECURSOS FISICOS E INFRAESTRUCTURA TECNOLÓGICA</b>	<b>Versión:</b>	
		<b>Vigente desde:</b>	
		<b>Pág. 24 de 38</b>	

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

En esta actividad la entidad debe crear 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 permitirá la consolidación de indicadores periódicamente y su evaluación frente a las metas esperadas; deben ser medibles permitiendo analizar causas de desviación y su impacto en el cumplimiento de las metas y objetivos del MSPI.

## Plan de Ejecución de Auditorías



La entidad debe generar un documento donde se especifique el plan de auditorías para el MSPI, donde especifique la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de informes. Este plan estará a cargo de la unidad administrativa que lidere el proceso de SIGAMI.

Se debe llevar a cabo auditorías y revisiones independientes a intervalos planificados que permitan identificar si el MSPI es conforme con los requisitos de la organización, está implementado adecuadamente y se mantiene de forma eficaz; así mismo es necesario difundir a las partes interesadas, los resultados de la ejecución de las auditorías. Es importante conservar la información documentada como evidencia de los resultados de las auditorías.

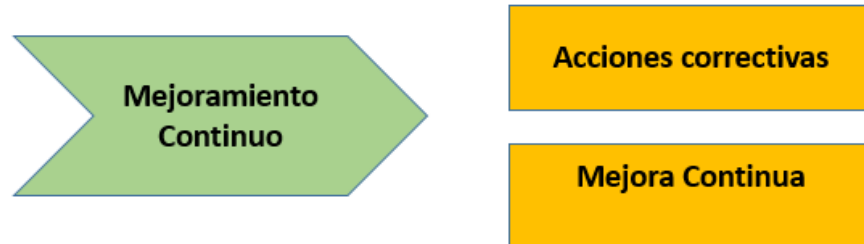
### 6.1.5 Mejora Continua

En esta fase la Entidad se consolida los resultados obtenidos de la fase de evaluación de



 <p>Alcaldía Municipal <b>Ibagué</b> NIT.800113389-7</p>	<b>MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Código:</b>	
	<b>PROCESO: GESTION DE RECURSOS FISICOS E INFRAESTRUCTURA TECNOLÓGICA</b>	<b>Versión:</b>	
		<b>Vigente desde:</b>	
		<b>Pág. 25 de 38</b>	

desempeño, y se diseña el plan de mejoramiento continuo, tomando las acciones oportunas para mitigar las debilidades identificadas.



**Figura 6 - Fase de Evaluación del Desempeño**

Fuente: MINTIC [http://estrategia.gobiernoenlinea.gov.co/623/articles-8258\\_recurso\\_1.pdf](http://estrategia.gobiernoenlinea.gov.co/623/articles-8258_recurso_1.pdf)

**Tabla 5 - Metas, Resultados e Instrumentos de la Fase de Mejora Continua**

<b>Implementación</b>			
<b>Metas</b>	<b>Resultados</b>	<b>Instrumentos</b>	
		<b>MSPI</b>	<b>MRAE</b>
Plan de Mejora Continua	<p><b>Documento con el plan de mejoramiento</b></p> <p><b>Documento con el plan de comunicación de resultados</b></p>	<p><b>Resultados de la ejecución del plan de Revisión y Seguimiento, a la implementación del MSPI</b></p> <p><b>Resultados del plan de ejecución de auditorías y reisiones independientes al MSPI</b></p> <p><b>Guía 17 Mejora Continua</b></p>	<p>LI.GO.03 LI.GO.12 LI.GO.13 LI.INF.14 LI.INF.15 LI.ST.15 LI.UA.9 LI.UA.10</p>

En esta fase la Entidad define y ejecuta el plan de mejora continua con base en los resultados de la fase de evaluación del desempeño. Este plan incluye:

- 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, la entidad puede efectuar 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 de la entidad. La revisión por la Alta Dirección hace referencia a las decisiones, cambios, prioridades etc. tomadas en sus comités y que impacten el MSPI.

## 7. MODELO DE MADUREZ

Este esquema permite identificar el nivel de madurez del MSPI en el que se encuentran la Entidad, midiendo la brecha entre el nivel actual de la entidad y el nivel optimizado. Es decir, se aplica en la fase de Diagnóstico y como herramienta de evaluación de los avances de la implementación del modelo

A continuación, la figura 7, muestra los diferentes niveles que hacen parte del modelo de madurez.



Figura 7- Niveles de madurez

Fuente: MINTIC [http://estrategia.gobiernoenlinea.gov.co/623/articles-8258\\_recurso\\_1.pdf](http://estrategia.gobiernoenlinea.gov.co/623/articles-8258_recurso_1.pdf)

El esquema que muestra los niveles de madurez del MSPI, busca establecer unos criterios de valoración a través de los cuales se determina el estado actual de la seguridad de la información en la Entidad.





 <p>Alcaldía Municipal <b>Ibagué</b> NIT.800113389-7</p>	<b>MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	Código:	
		<b>PROCESO: GESTION DE RECURSOS FISICOS E INFRAESTRUCTURA TECNOLOGICA</b>	
		Vigente desde:	
		Pág. 27 de 38	

Tabla 6 – Características de los Niveles de Madurez

Nivel	Descripción
Inexistente	<ul style="list-style-type: none"> <li>Se han implementado controles en su infraestructura de TI, seguridad física, seguridad de recursos humanos entre otros, sin embargo no están alineados a un Modelo de Seguridad.</li> <li>No se reconoce la información como un activo importante para su misión y objetivos estratégicos.</li> <li>No se tiene conciencia de la importancia de la seguridad de la información en la entidad.</li> </ul>
Inicial	<ul style="list-style-type: none"> <li>Se han identificado las debilidades en la seguridad de la información.</li> <li>Los incidentes de seguridad de la información se traan de forma reactiva.</li> <li>Se tiene la necesidad de implementar el MSPI, para definir políticas, procesos y procedimientos que den respuesta proactiva a las amenazas sobre seguridad de la información que se presentan en la Entidad.</li> </ul>
Repetible	<ul style="list-style-type: none"> <li>Se identifican en forma general los activos de información.</li> <li>Se clasifican los activos de información.</li> <li>Los servidores públicos de la entidad tienen conciencia sobre la seguridad de la información.</li> <li>Los temas de seguridad y privacidad de la información se tratan en los comités del modelo integrado de gestión.</li> <li>La entidad cuenta con un plan de diagnóstico para IPv6.</li> </ul>
Definido	<ul style="list-style-type: none"> <li>La Entidad ha realizado un diagnóstico que le permite establecer el estado actual de la seguridad de la información.</li> <li>La Entidad ha determinado los objetivos, alcance y límites de la seguridad de la información.</li> <li>La Entidad ha establecido formalmente políticas de Seguridad de la información y estas han sido divulgadas.</li> <li>La Entidad tiene procedimientos formales de seguridad de la Información</li> <li>La Entidad tiene roles y responsabilidades asignados en seguridad y privacidad de la información.</li> <li>La Entidad ha realizado un inventario de activos de información aplicando una metodología.</li> <li>La Entidad trata riesgos de seguridad de la información a través de una metodología.</li> <li>Se implementa el plan de tratamiento de riesgos.</li> <li>La entidad cuenta con un plan de transición de IPv4 a IPv6.</li> </ul>
Administrado	<ul style="list-style-type: none"> <li>Se revisa y monitorea periódicamente los activos de información de la Entidad.</li> <li>Se utilizan indicadores para establecer el cumplimiento de las políticas de seguridad y privacidad de la información.</li> <li>Se evalúa la efectividad de los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro.</li> <li>La entidad cuenta con ambientes de prueba para el uso del protocolo IPv6.</li> </ul>
Optimizado	<ul style="list-style-type: none"> <li>En este nivel se encuentran las entidades en las cuales la seguridad es un valor agregado para la organización.</li> <li>Se utilizan indicadores de efectividad para establecer si la entidad encuentra retorno a la inversión bajo la premisa de mejora en el cumplimiento de los objetivos misionales.</li> <li>La entidad genera tráfico en IPv6</li> </ul>

 <p>Alcaldía Municipal <b>Ibagué</b> NIT.800113389-7</p>	<b>MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	Código:	
		<b>PROCESO: GESTION DE RECURSOS FISICOS E INFRAESTRUCTURA TECNOLOGICA</b>	
		Vigente desde:	
		Pág. 28 de 38	

## 8. PRIVACIDAD DE LA INFORMACIÓN

Para cumplir con el objetivo del modelo de seguridad y privacidad de la información relacionado con garantizar el adecuado manejo de la información en poder de la entidad, la cual es uno de los activos más valiosos para la toma de decisiones, el MSPI propende por un doble enfoque, el del nivel de seguridad y el de privacidad de la información

A nivel de seguridad marca el derrotero para que se construyan políticas de seguridad a fin de salvaguardar la misma a nivel físico y lógico, de manera que se garantice su integridad, disponibilidad y autenticidad.

El nivel de seguridad se complementa con el nivel de privacidad para garantizar tanto la protección de los derechos a la intimidad y el buen nombre o a la salvaguarda de secretos profesionales, industriales o de información privilegiada de particulares en poder de la administración como el acceso a la información pública cuando esta no se encuentre sometida a reserva

Para ello se requiere dotar al modelo de seguridad de la información de un componente específico relacionado con la privacidad.



Es necesario tener claro que diferentes procesos relacionados con la recolección y uso de información son susceptibles de ser objeto de implementación de medidas de privacidad, como puede ser:

- La Implementación de un sistema de información que tenga la posibilidad de recolectar datos personales, tal como un sistema de seguridad a través de video vigilancia que capture imágenes, datos biométricos, etc.
- El Diseño y ejecución de un sistema de gestión documental
- El Desarrollo de políticas que impliquen la necesidad de recolectar y usar información personal, como por ejemplo políticas de atención de PQR's
- La Transferencia de información a terceros (otras entidades o países).

Se debe tener en cuenta los siguientes temas.

Contar con una herramienta de análisis sobre impacto en la privacidad

El MSPI es el instrumento que se pone a disposición de las entidades con el fin de realizar el análisis de impacto que en la privacidad de la información pueda presentarse a partir del desarrollo de las funciones administrativas o el desarrollo misional de cada entidad, teniendo como referente:

 <p>Alcaldía Municipal <b>Ibagué</b> NIT.800113389-7</p>	<b>MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Código:</b>	
	<b>PROCESO: GESTION DE RECURSOS FISICOS E INFRAESTRUCTURA TECNOLOGICA</b>	<b>Versión:</b>	
		<b>Vigente desde:</b>	
		<b>Pág. 29 de 38</b>	

- ✓ El marco legal vigente.
- ✓ Las necesidades de los clientes internos y externos de la entidad.
- ✓ La identificación de los posibles problemas recurrentes relacionados con la privacidad.

### **Descripción de los flujos de información**



La descripción de los flujos de información sirve para saber qué información está siendo recolectada, con qué propósito, cómo, en qué cantidad y si la misma es objeto de divulgación.

La fase de diagnóstico de privacidad puede servir como insumo al poder identificar qué información se tiene, dónde y en cabeza de quién. Este ejercicio tiene que ser complementado con la documentación de los procesos relacionados con gestión de la información que la entidad haya levantado, para poder hacer una valoración sobre la circulación de la información, identificando que en la misma no se afecten derechos de los titulares de información o se ponga en riesgo su privacidad.

### **Identificar los riesgos de privacidad**

Los riesgos en relación con la privacidad pueden ser de varios tipos:

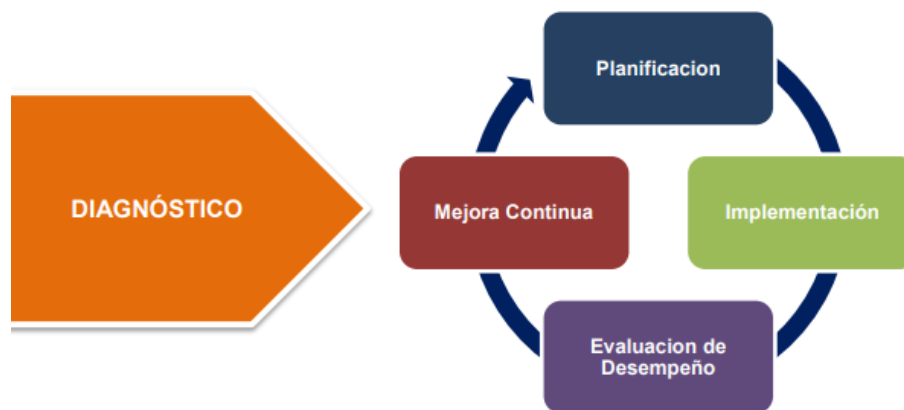
- ✓ En relación con la información personal de los individuos
  - Se expone información clasificada (datos personales no públicos) sin que medie autorización para ello.
  - Uso de sistemas de información o aplicaciones en la interacción con los ciudadanos que pueden ser intrusivos sobre su privacidad sin advertir previamente a los usuarios sobre ello (geolocalización)
  - Información que permanece en poder de la entidad por más tiempo de la vigencia que tiene la base de datos o en contra del ejercicio de derecho de supresión por parte del titular-ciudadano.
- ✓ En relación con la información de usuarios institucionales
  - Se divulga información que puede ser clasificada como secreto industrial o que pone en riesgo la imagen corporativa.

 <p>Alcaldía Municipal <b>Ibagué</b> NIT.800113389-7</p>	<p><b>MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b></p>	<p><b>Código:</b></p>	
	<p><b>PROCESO: GESTION DE RECURSOS FISICOS E INFRAESTRUCTURA TECNOLÓGICA</b></p>	<p><b>Versión:</b></p>	
	<p><b>Pág. 30 de 38</b></p>	<p><b>Vigente desde:</b></p>	

- ✓ En relación con los sistemas de información y programas usados o los procedimientos y procesos relacionados con la gestión administrativa a cargo.
  - Procesos no ajustados al sistema de gestión documental que garanticen medidas de protección sobre la información.
  - Adquisición de programas que no garanticen un nivel adecuado de privacidad, por ejemplo, que permitan recolección masiva de datos sin conocimiento de los usuarios.
  - Indebida utilización de datos personales en ejercicios de divulgación tales como procesos de rendición de cuentas, publicación de información en la página web, etc.



El análisis debe reflejarse en una matriz de riesgos ponderando la probabilidad de su ocurrencia y el impacto que puede generar su causación.

La implementación del componente de privacidad sigue el mismo ciclo de operación adoptado para seguridad de la información consistente en cinco fases o etapas así: diagnóstico, planeación, implementación, gestión y mejora continua.



Fuente: MINTIC [http://estrategia.gobiernoenlinea.gov.co/623/articles-8258\\_recurso\\_1.pdf](http://estrategia.gobiernoenlinea.gov.co/623/articles-8258_recurso_1.pdf)



 <p>Alcaldía Municipal <b>Ibagué</b> NIT.800113389-7</p>	<b>MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	Código:	
		<b>PROCESO: GESTION DE RECURSOS FISICOS E INFRAESTRUCTURA TECNOLÓGICA</b>	
		Vigente desde:	
		Pág. 31 de 38	

## 8.1 Diagnóstico



En esta fase se identifica cómo se está garantizando la privacidad sobre todo el ciclo de la información que tienen en su poder verificando la implantación o no de medidas que den cumplimiento a los requerimientos de las normas sobre protección de datos personales y que, adicionalmente contribuya a identificar la información pública sometida a reserva o clasificada en los términos de la Ley.

Para ello se utiliza el instrumento de diagnóstico y seguimiento a la implementación. A través del diligenciamiento de este instrumento se podrá conocer la realidad de la información relacionada con el manejo de los activos de la información que reposen en bancos de datos o archivos y a partir de allí determinar las medidas a nivel procedimental que deben adelantar la Entidad para otorgar un nivel adecuado de protección a esta información.

Tabla 7 - Metas, Resultados e Instrumentos de la Fase de Diagnostico

Diagnóstico			
Metas	Resultados	Instrumentos	
		MSPI	MRAE
Diagnostico	Realizar el diagnóstico de las condiciones en que se encuentran los activos de información administrados por la entidad.  Diligenciamiento de la herramienta.	Herramienta de diagnóstico.	
	Documento con el resultado del diagnóstico realizado por la entidad con la clasificación y distinción de los activos de información teniendo en cuenta la información con datos personales y aquellos que no lo son identificando la criticidad de la información clasificada o reservada.		

Con el resultado del diagnóstico se puede contar con un insumo frente a la identificación de aquella información que debe ser manejada como privada (clasificada en los términos de la Ley) para a partir de allí incorporar las medidas de seguridad proporcionales a su naturaleza como los procedimientos que lleven al cumplimiento de la normatividad de protección de datos, transparencia y acceso a la información pública soportado todo ello en la incorporación de un sistema de privacidad por diseño que responda a la realidad

 <p>Alcaldía Municipal <b>Ibagué</b> NIT.800113389-7</p>	<b>MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Código:</b>	
	<b>PROCESO: GESTION DE RECURSOS FISICOS E INFRAESTRUCTURA TECNOLÓGICA</b>	<b>Versión:</b>	
		<b>Vigente desde:</b>	
		<b>Pág. 32 de 38</b>	

presupuestal, humana y técnica de cada entidad.

## 8.2 Planificación



En esta segunda etapa se traza la estrategia con el objetivo de organizar el trabajo adelantado por la entidad a partir de las características recogidas en la fase de diagnóstico, para acercarlas a un nivel de cumplimiento adecuado para salvaguardar la información privada y de manera concomitante responder a los retos de disponibilidad a la información pública por parte de la ciudadanía, así como para ajustar los roles del personal designado para cumplir con las responsabilidades de seguridad y privacidad de la información.

Para ello deben ajustarse las políticas, los procesos y procedimientos ya definidos en el modelo de seguridad con el fin de incorporar la privacidad con el alcance mencionado.

Tabla 8 - Metas, Resultados e Instrumentos de la Fase de Planificación

Planificación			
Metas	Resultados	Instrumentos	
		MSPI	MRAE
Planificación	Documento con la política de privacidad, debidamente aprobada por la alta dirección y socializada al interior de la entidad.		
	Manual de políticas de seguridad y privacidad de la información, aprobada por la alta dirección y socializada al interior de la entidad.	Herramienta de diagnóstico. Guía No 4 - Roles y Responsabilidades de Seguridad y Privacidad de la Información.	
	Documento con el plan de gestión de la privacidad sobre la información, aprobado por la alta dirección de la entidad.	Guía No 2 – Política General.	
	Definición de roles en relación con la Información.		
	Procedimientos de privacidad.		
	Plan de capacitación al interior de la entidad		



 <p>Alcaldía Municipal <b>Ibagué</b> NIT.800113389-7</p>	<b>MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	<b>Código:</b>	
	<b>PROCESO: GESTION DE RECURSOS FISICOS E INFRAESTRUCTURA TECNOLÓGICA</b>	<b>Versión:</b>	
		<b>Vigente desde:</b>	
		<b>Pág. 33 de 38</b>	

### 8.3 Implementación

En esta fase se ejecutan las acciones trazadas en la etapa previa de planeación de manera que se diseñe un modelo de privacidad que permita cumplir con los mínimos legales y generar una política privacidad que permita la correcta gestión de la información.

De esta manera se da cumplimiento normativo, como: registro de bases de datos en el RNBD, índice de información clasificado y reservado revisado, procedimiento interno ajustado a la gestión de la privacidad de la información diseñada.

Tabla 9 - Metas, Resultados e Instrumentos de la Fase de Implementación

Implementación			
Metas	Resultados	Instrumentos	
		MSPI	MRAE
Implementación	<p>Documento con los riesgos contra la privacidad identificados y las medidas de solución adoptadas a partir de la implementación del plan de gestión de la privacidad de la información</p> <p>Documento que evidencie el registro de las Bases de datos,</p> <p>Documento con el índice de información clasificada, reservada, revisada y sus procedimientos ajustados</p>	<p>Herramienta de Diagnóstico. Guía No 7 – Gestion de Riesgos.</p>	

### 8.4 Fase de Evaluación del desempeño

Una vez implementadas las anteriores actividades el modelo de privacidad se evalúa, para medir la efectividad de las acciones tomadas a través de los indicadores definidos en la fase de implementación que debe incluir la correcta interacción entre el MSPI y la aplicación de la Ley de Transparencia y Acceso a la Información Pública.

Tabla 9 - Metas, Resultados e Instrumentos de la Fase de Evaluación de Desempeño

La versión vigente y controlada de este documento, solo podrá ser consultada a través de la plataforma PISAMI y/o de Intranet de la Administración Municipal. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es responsabilidad de la Alcaldía de Ibagué



Evaluación de Desempeño			
Metas	Resultados	Instrumentos	
		MSPI	MRAE
Evaluación del desempeño	<p>Documento con los resultados del plan de seguimiento</p> <p>Documento con el Plan de auditoría interna y resultados revisado y aprobado por el Comité de Gestión Institucional o el que haga sus veces</p> <p>Comunicación de los indicadores al público a través de la rendición de cuentas, informe a la PGN y al Congreso de la República.</p>	<p>Guía No 16 – Evaluación del Desempeño.</p> <p>Guía No 15 – Auditoría.</p> <p>Guía No 14 – Plan de Comunicación, sensibilización y capacitación.</p>	

### 8.5 Mejora Continua

Una vez se tengan los resultados del componente de evaluación del desempeño se toman los resultados obtenidos y se preparan los correctivos necesarios que permitan a la misma crecer en el nivel de responsabilidad demostrada.

Tabla 10 - Metas, Resultados e Instrumentos de la Fase de Mejora Continua

Mejora Continua			
Metas	Resultados	Instrumentos	
		MSPI	MRAE
Mejora Continua	<p>Documento con los resultados del plan de seguimiento</p> <p>Documento con los resultados del plan de mejoramiento revisado y aprobado por el Comité de Gestión Institucional o el que haga sus veces.</p> <p>Documento con el consolidado de las auditorías.</p>	<p>Guía No 16 – Evaluación del Desempeño.</p> <p>Guía No 17 - Mejora Continua.</p>	

 <p>Alcaldía Municipal <b>Ibagué</b> NIT.800113389-7</p>	<p><b>MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b></p>	<p><b>Código:</b></p>	
	<p><b>PROCESO: GESTION DE RECURSOS FISICOS E INFRAESTRUCTURA TECNOLÓGICA</b></p>	<p><b>Versión:</b></p>	
		<p><b>Vigente desde:</b></p>	
		<p><b>Pág. 35 de 38</b></p>	

## 9. ADOPCIÓN DEL PROTOCOLO IPv6

A continuación se mencionan las fases a cumplir para la transición del protocolo IPv4 a IPv6



Figura 8 - Fases del proceso de transición del protocolo IPv4 al IPv6  
Fuente: MINTIC [http://estrategia.gobiernoenlinea.gov.co/623/articles-8258\\_recurso\\_1.pdf](http://estrategia.gobiernoenlinea.gov.co/623/articles-8258_recurso_1.pdf)

### 9.1 Planeación

Se define el plan y la estrategia de transición de IPv4 a IPv6, en procura de los resultados que permitan dar cumplimiento con la adopción del nuevo protocolo.

En la Tabla No 11 se describen las metas, entregables e instrumentos para cumplir esta actividad, de conformidad con la Guía de Transición de IPV4 a IPV6.



 <p>Alcaldía Municipal <b>Ibagué</b> NIT.800113389-7</p>	<b>MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	Código:	
		<b>PROCESO: GESTION DE RECURSOS FISICOS E INFRAESTRUCTURA TECNOLÓGICA</b>	
		Vigente desde:	
		Pág. 36 de 38	

Tabla 11 - Metas, Resultados e Instrumentos de la Fase de Planeación

Planeación			
Metas	Resultados	Instrumentos	
		MSPI	MRAE
Plan y estrategia de transición de IPv4 a IPv6.	<p>Plan de diagnóstico que debe contener los siguientes componentes: Inventario de TI (Hardware y software) de cada Entidad diagnosticada, Informe de la Infraestructura de red de comunicaciones, recomendaciones para adquisición de elementos de comunicaciones , de cómputo y almacenamiento con el cumplimiento de IPv6, plan de direccionamiento en IPv6, plan de manejo de excepciones, definiendo las acciones necesarias en cada caso particular con aquellos elementos de hardware y software (aplicaciones y servicios) que sean incompatibles con IPv6, Informe de preparación (Readiness) de los sistemas de comunicaciones, bases de datos y aplicaciones.</p> <p>Documento que define la estrategia de para la implementación y aseguramiento del protocolo IPv6 en concordancia con la política de seguridad de las entidades.</p>	<p>Guía No 20 – Transición IPv4 a IPv6.</p> <p>Guía No 19 – Aseguramiento del protocolo IPv6.</p> <p>Circular 002 de 2011 del MinTIC.</p>	

## 9.2 Implementación

Actividades de habilitación del direccionamiento de IPv6, montaje, ejecución y corrección de configuraciones para pruebas piloto, activar las políticas de seguridad de IPv6, validar la funcionalidad de los servicios y aplicaciones de las entidades, entre otras.

En la Tabla No 12 se describen las metas, entregables e instrumentos para cumplir esta actividad, de conformidad con la Guía de Transición de IPV4 a IPV6 para Colombia



 <p>Alcaldía Municipal <b>Ibagué</b> NIT.800113389-7</p>	<b>MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b>	Código:	
		<b>PROCESO: GESTION DE RECURSOS FISICOS E INFRAESTRUCTURA TECNOLÓGICA</b>	
		Vigente desde:	
		Pág. 37 de 38	

Tabla 12 - Metas, Resultados e Instrumentos de la Fase de Implementación.



Implementación			
Metas	Resultados	Instrumentos	
		MSPI	MRAE
Implementación del plan y estrategia de transición de IPv4 a IPv6.	Documento con el informe de la implementación del plan y la estrategia de transición de IPv4 a IPv6, revisado y aprobado por la alta Dirección.	Guía No 20 – Guía Transición de IPv4 a IPv6 para Colombia Guía No 19 - Guía de Aseguramiento del Protocolo IPv6.	

### 9.3 Pruebas de Funcionalidad

Pruebas de funcionalidad y/o monitoreo de IPv6, en sistemas de información, de almacenamiento, de comunicaciones y servicios; frente a las políticas de seguridad perimetral, de servidores de cómputo, equipos de comunicaciones, de almacenamiento, entre otros. Así mismo se elabora un inventario final de servicios y sistemas de comunicaciones, bajo el nuevo esquema de funcionamiento de IPv6.

Tabla 13 - Metas, Resultados e Instrumentos de la Fase de Pruebas de Funcionalidad.

Pruebas de Funcionalidad			
Metas	Resultados	Instrumentos	
		MSPI	MRAE
Plan de Pruebas de funcionalidad IPV4 a IPV6	<p>Documento con los cambios detallados de las configuraciones realizadas, previo al análisis de funcionalidad realizado en la fase II de implementación</p> <p>Acta de cumplimiento a satisfacción de la Entidad con respecto al funcionamiento de los servicios y aplicaciones que fueron intervenidos en la implementación</p> <p>Documento de inventario final de la Infraestructura TI sobre el protocolo IPV6</p>	<p>Guía 20 – Guía ransición de IPV4 a IPV6 para Colombia</p> <p>Guía 19 – Guía de Aseguramiento del protocolo IPV6</p>	

 <p>Alcaldía Municipal <b>Ibagué</b> NIT.800113389-7</p>	<p><b>MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACION</b></p>	<p><b>Código:</b></p>	
	<p><b>PROCESO: GESTION DE RECURSOS FISICOS E INFRAESTRUCTURA TECNOLÓGICA</b></p>	<p><b>Versión:</b></p>	
		<p><b>Vigente desde:</b></p>	
		<p><b>Pág. 38 de 38</b></p>	

## 10. CONTROL DE CAMBIOS

VERSION	VIGENTE DESDE	OBSERVACION

REVISÓ	APROBÓ
<p><b>Nombre:</b> Doris Galeano Rodríguez <b>Cargo:</b> Profesional Universitario</p>	<p><b>Nombre:</b> María Antonia Gamboa Sandoval <b>Cargo:</b> Director</p>