PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ALCALDÍA DE PEREIRA

PROCESO

PROMOCIÓN DEL DESARROLLO ECONÓMICO

SUBPROCESO

SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

ACTIVIDAD

GOBIERNO DIGITAL

Título:	**PLAN DE IMPLEMENTACIÓN DEL MSPI**				
Sumario	El presente documento denota el cronograma y orden de ejecución del habilitador transversal seguridad y privacidad contemplado en la Política de Gobierno Digital del Decreto 1008 de 2018, en este se encuentra de manera explícita y desglosada las actividades y tiempos aproximados para la ejecución de las actividades requeridas por el Modelo de Seguridad y Privacidad de la Información, dicho modelo fue elaborado por el Ministerio de Tecnologías de la Información y las Comunicaciones.				
Palabras Claves	Gobierno Digital Seguridad Digital Seguridad y Privacidad				
Formato:	PDF		Lenguaje:	Español	
Dependencia:	Secretaría de Tecnologías de Información y la Comunicación				
Código:	N/A	Versión	1.0	Estado	En Aprobación
Categoría	Documento Informativo: Implementación del habilitador transversal Seguridad y Privacidad de la Política de Gobierno Digital.				
	Componente:	TIC para EL ESTADO			
	Habilitador Transversal:	Seguridad y Privacidad			
	Lineamientos y Estándares:	Modelo de Seguridad y Privacidad de la Información			
Asesor:	Magister Carlos Mario Arteaga Pacheco Contratista Prestación de Servicios Profesionales Especializados				
Autor:	Ingeniero Julián Londoño Giraldo Contratista Prestación de Servicios Profesionales Ingeniera Rubialba Ocampo Foronda				
Revisó:	Carlos Andres Alvarez Palomino Director de Sistemas de Información y Servicios Digitales Alejandro Usma Vasquez Director de Infraestructura Tecnológica y Servicios Digitales				
Aprobó:	Fredy Eduardo Ruano López Secretario de Tecnología de Información y la Comunicación				

VERSIÓN	FECHA	CAMBIOS INTRODUCIDOS
1.0	26/03/2019	Emisión del documento
2.0	18/08/2020	Modificación de responsables e imagen institucional y cronograma

Tabla de contenido

Lista de figuras

Lista de tablas

Introducción

Las Tecnologías de la Información y las Comunicaciones TIC son un el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios, que permiten la compilación, procesamiento, almacenamientos, transmisión de información como: voz, datos, texto, video e imágenes (Art 6, Ley 1341 de 2009), es de vital importancia resguardar estos recursos en el entendimiento que la información es el activo más importante para cualquier organización máxime en una entidad pública como la Alcaldía de Pereira.

Los riesgos a que se ven asociados todos los activos de información son variados y están en constante cambio, estos no discriminan el tamaño de la entidad u otros factores externos e internos, los delincuentes cibernéticos y personas que deseen realizar ingeniería social con el fin de sustraer información están al acecho pudiendo ser víctima de fugas de información, interrupción en los servicios, fallas críticas en los sistemas de información o en resumen ser víctima de un incidente de seguridad de cualquier índole.

Este plan expresa el tiempo de ejecución estimado, actividades propuestas y demás hechos inherentes en la implementación del Modelo de Seguridad y Privacidad de la Información en la Alcaldía de Pereira, dando cumplimiento al Decreto 1008 de 2018 en su habilitador transversal seguridad y privacidad disminuyendo riesgos de seguridad y privacidad lo cual se traduce en entornos más seguros y eficientes en las organizaciones.

El soporte para la ejecución de dicho plan se centra en tres factores principales:

1. Marco legal vigente colombiano que de la materia trate.
2. Necesidades identificadas de la entidad.
3. Posible ocurrencia de incidentes de seguridad y privacidad de la información.

Conceptos

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, art4)
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.
Activo:	En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).
Amenaza:	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)
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 200, art 3)
Auditoría:	Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).
Bases de Datos Personales:	Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)
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)
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)
Confidencialidad:	Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizada

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 Personales Mixtos:	Para efectos de este manual es la información que contiene datos personales públicos junto con datos privados o sensibles.
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 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 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)
Datos Personales:	Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables (Ley 1581 de 2012, art 3)
Declaración de aplicación:	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 justificación de las exclusiones de controles del anexo A de ISO 27001.
Disponibilidad:	Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera
Gestión de incidente 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).
Guía:	Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares, buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

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. (Ley 1712 de 2014, art 6)
Información:	Datos relacionados que tienen significado para la entidad. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada.
Integridad:	Propiedad de salvaguardar la exactitud y estado completo de los activos.
Ley de Habeas Data:	Se refiere a la Ley Estatuaria 1266 de 2008.
Ley de Transparencia y Acceso a la Información Pública:	Se refiere a la Ley Estatuaria 1712 de 2014.
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.
Plan de tratamiento de riesgos:	Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptable e implementar los controles necesarios para proteger la misma. (ISO/IEC 27000).
Política:	Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.
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.

Procedimiento:	Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la entidad, los estándares, las mejores prácticas y las guías tan cerca cómo les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro de la dependencia donde ellos se aplican
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, además, otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad pueden estar involucradas.
Sistema de Gestión de Seguridad de la Información SGSI:	Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, política, 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).
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).
Usuario:	Cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la Unidad, para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información
Vulnerabilidad:	Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

Objetivos

I. Objetivo general

- Generar el cronograma de implementación con sus actividades y tiempos estimados en la implementación del Modelo de Seguridad y Privacidad de la Información en la Alcaldía de Pereira.

II. Objetivos específicos

- Identificar las fases del Modelo de Seguridad y Privacidad de la Información.
- Orientar el cumplimiento del MSPI.
- Garantizar un adecuado manejo de la información pública.
- Contribuir en la planeación institucional referente al MSPI.
- Promover la cultura de la seguridad y privacidad.
- Indicar los tiempos y porcentajes de cada fase.

Ciclo de operación MSPI

El ciclo operación del Modelo de Seguridad y privacidad de la Información está compuesto por cinco fases, permitiendo así que se gestione fase por fase de manera progresiva denotando que cada fase requiere actividades, cronogramas y recursos diferentes. Por ende, se abordará cada fase de manera individual, no obstante, el avance de cada fase se reflejará como el avance global del MSPI.

A continuación, se muestra el ciclo de operación del MSPI expresando cada fase y porcentaje que dicha fase tiene en el desarrollo o cumplimiento del 100% de la implementación del MSPI en la Alcaldía de Pereira.

Figura 1 Ciclo de operación del Modelo de Seguridad y Privacidad de la Información[1]

[1] *Figura tomada de la guía Modelo de Seguridad y Privacidad de la Información capítulo 8*

Porcentajes determinados para cada fase del MSPI

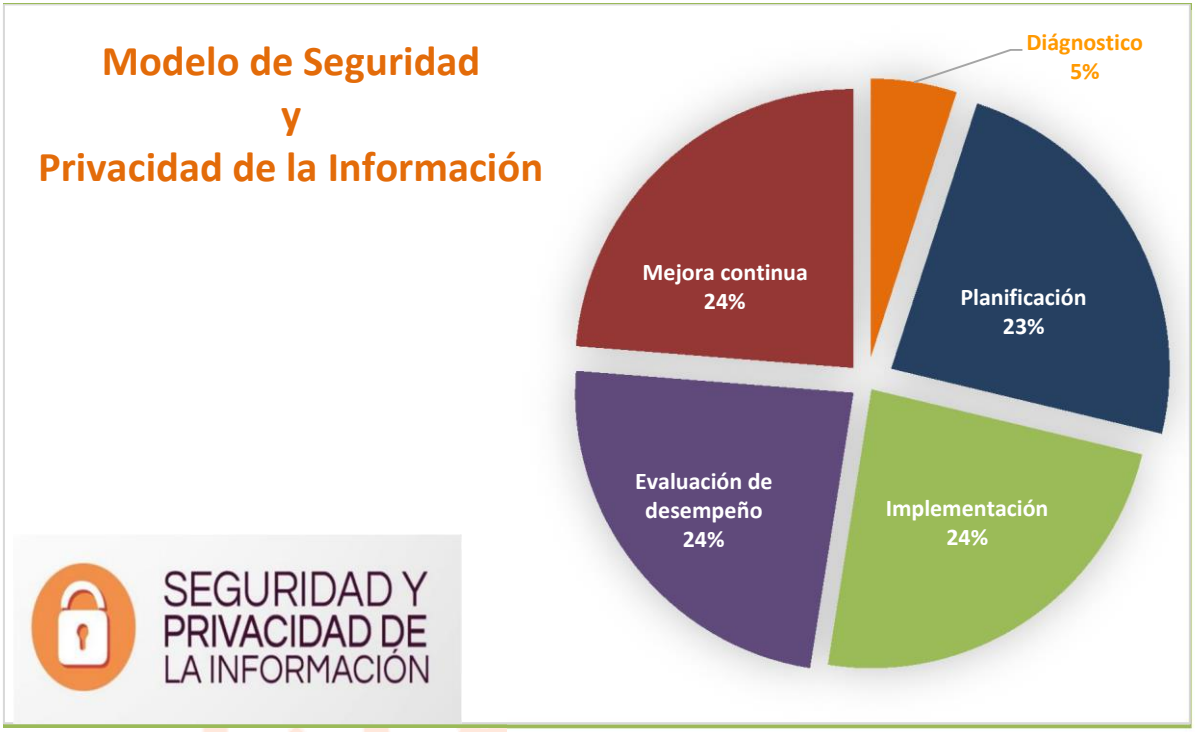


Figura 2 Porcentaje determinado para cada fase del MSPI[2]

En la anterior figura se puede denotar que cada fase de la implementación del Modelo de Seguridad y Privacidad de la Información tiene un porcentaje sobre el total de la implementación del MSPI en la Alcaldía de Pereira, dichos porcentajes fueron establecidos para la entidad como se determina en la figura y serán referencia de carácter interno para manifestar o denotar el avance del mismo en la Alcaldía de Pereira, por ende este porcentaje no se debe confundir con el porcentaje que arroje otros instrumentos como el autodiagnóstico del Modelo Integrado de Planeación y Gestión MIPG, o como el Instrumento de Evaluación del MSPI o como el reporte en el Formulario Único de Reporte Avance a la Gestión FURAG.

[2] *Fuente de elaboración propia*

I. Fase diagnóstico

La fase diagnóstica se ejecuta para conocer la situación actual de la entidad referente a la seguridad y privacidad de la información, en este caso se identifica el nivel de madurez, vulnerabilidades y otros aspectos que son relevantes y que demuestren la situación actual de la Alcaldía de Pereira. Esta fase se transforma en un insumo de vital importancia para la siguiente fase de planificación, entendiendo que cada fase está en concordancia con la siguiente siguiendo el ciclo de operación entre fases que se muestra en la Figura 1 Ciclo de operación del Modelo de Seguridad y Privacidad de la Información.

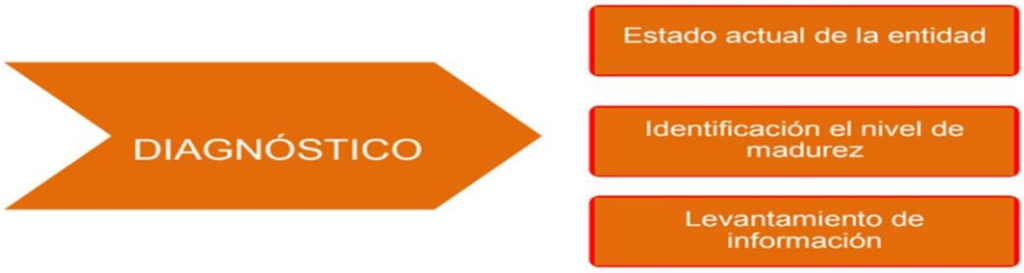


Figura 3 Fase de diagnóstico[3]

A continuación, se muestra en la Tabla 1 Avance fase diagnóstico, el tiempo estimado para la ejecución de la fase, las actividades que se deben ejecutar, la dependencia que lidera dicho proceso, las dependencias que por la envergadura de la fase se requiera de apoyo o complemento para la gestión y por último el porcentaje de avance específicamente para esta fase, es decir del 100% de la fase en que porcentaje se encuentra su desarrollo.

Avance fase diagnóstico	
Fecha estimada ejecución	2 meses
Cantidad de actividades a realizar	3 actividades
Dependencia líder	Secretaría TIC
Dependencias adicionales involucradas	Ninguna
Fase en ejecución	SI ✓ NO
Porcentaje de avance	100%

Tabla 1 Avance fase diagnóstico[4]

[3] *Figura tomada de la guía Modelo de Seguridad y Privacidad de la Información capítulo 8.1*

II. Fase planificación

La fase de planificación concierne en procesar la información suministrada en la fase anterior y planear al igual que ejecutar las actividades con base en las necesidades identificadas, la fase de planificación se ejecuta ajustando el MSPI a los objetivos, misión, visión, necesidades y demás requerimientos determinados para preservar la confidencialidad, disponibilidad, integridad y privacidad de los activos de información en la Alcaldía de Pereira, a la vez, requiere la conformación de equipos interdisciplinarios para ir dando cumplimiento a cada una de las actividades de cada fase.

En esta fase lo más importante es entender el contexto de la entidad y así generar acciones que suplan las necesidades y que estos procesos estén razonables a la realidad de la capacidad humana y económica para dicha implementación del MSPI. También demuestra el compromiso de la alta dirección para la implementación de este mediante la Política General de Seguridad y Privacidad de la Información.

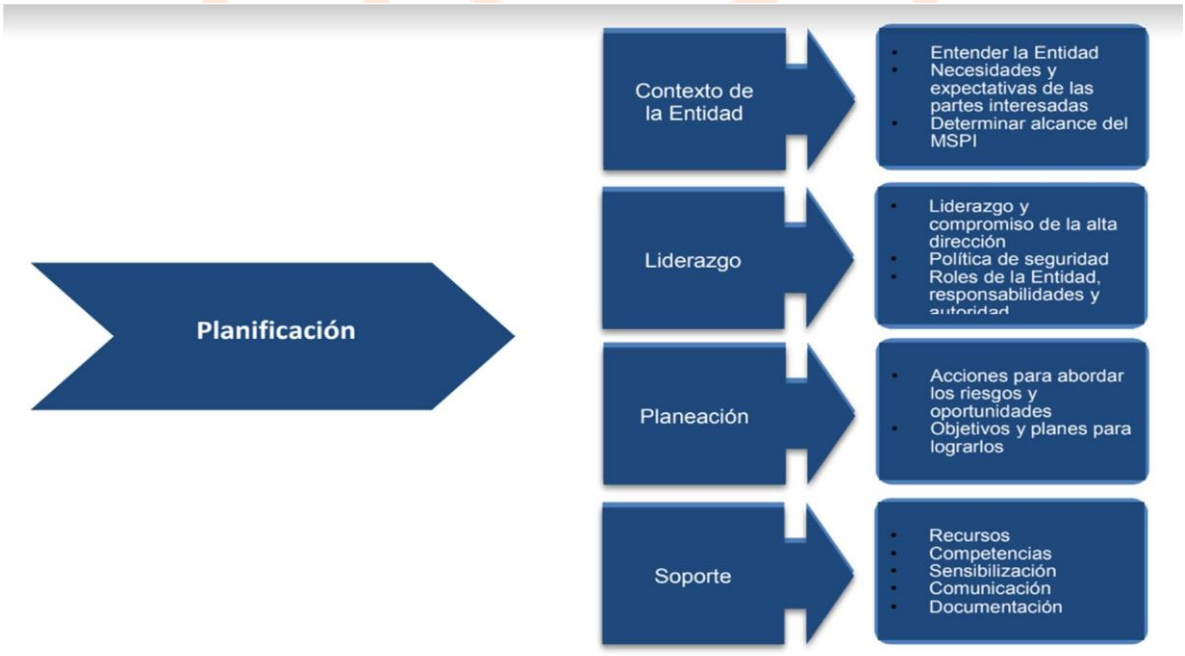


Figura 4 Fase de planificación[5]

[4] *Fuente de elaboración propia*

[5] *Figura tomada de la guía Modelo de Seguridad y Privacidad de la Información capítulo 8.2*

A continuación, se muestra en la Tabla 2 Avance fase de planificación, el tiempo estimado para la ejecución de la fase, las actividades que se deben ejecutar, la dependencia que lidera dicho proceso, las dependencias que por la envergadura de la fase se requiera de apoyo o complemento para la gestión y por último el porcentaje de avance específicamente para esta fase, es decir del 100% de la fase en que porcentaje se encuentra su desarrollo.

Avance fase planificación	
Fecha estimada ejecución	24 meses
Cantidad de actividades a realizar	8 actividades
Dependencia líder	Secretaría TIC
Dependencias adicionales involucradas	Secretaría de Desarrollo Administrativo, Secretaría Jurídica.
Fase en ejecución	SI ✓ NO
Porcentaje de avance	77%

Tabla 2 Avance fase de planificación[6]

III. Fase implementación

La fase de implementación permite instaurar lo que hasta el momento se ha planificado en la fase anterior, significando así que es la fase donde se genera el compromiso de la alta dirección con la implementación del Modelo de Seguridad y Privacidad de la Información ya que en esta fase se inician los controles y acciones necesarias para resguardar la información de la Alcaldía de Pereira. Iniciando también con todo lo concerniente a un plan trascendental para los sistemas de información y la entidad como tal de nombre Plan de Transición de IPv4 a IPv6.

[6] *Fuente de elaboración propia*

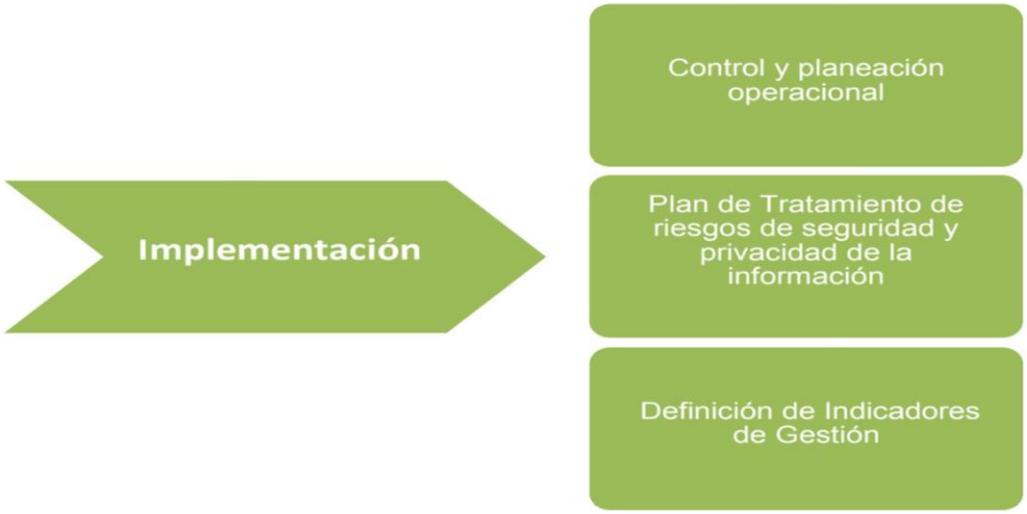


Figura 5 Fase de implementación[7]

A continuación, se muestra en la Tabla 3 Avance fase de implementación, el tiempo estimado para la ejecución de la fase, las actividades que se deben ejecutar, la dependencia que lidera dicho proceso, las dependencias que por la envergadura de la fase se requiera de apoyo o complemento para la gestión y por último el porcentaje de avance específicamente para esta fase, es decir del 100% de la fase en que porcentaje se encuentra su desarrollo.

Avance fase implementación	
Fecha estimada ejecución	13 meses
Cantidad de actividades a realizar	3 actividades
Dependencia líder	Secretaría TIC
Dependencias adicionales involucradas	Ninguna
Fase en ejecución	SI ✓ NO
Porcentaje de avance	10%

Tabla 3 Avance fase de implementación[8]

[7] *Figura tomada de la guía Modelo de Seguridad y Privacidad de la Información capítulo 8.3*

[8] *Fuente de elaboración propia*

IV. Fase evaluación de desempeño

En esta fase se compilan todos los resultados elaborados en las fases anteriores y se verifica o contrasta fase por fase verificando así el cumplimiento de los objetivos propuestos y que cada fase se haya desarrollado alienada a los objetivos, visión y misión de la Alcaldía de Pereira, identificando así acciones que se deben trasladar la fase siguiente.

De esta fase corresponde realizar seguimiento a los indicadores al igual que verificación del alcance propuesto en la fase de planificación, también el resultado de las auditorías internas y externas generando un gran insumo hacia la toma de decisiones del Modelo de Seguridad y Privacidad de la Información.

Figura 6 Fase de mejora continua[9]

A continuación, se muestra en la Tabla 4 Avance fase de evaluación de desempeño, el tiempo estimado para la ejecución de la fase, las actividades que se deben ejecutar, la dependencia que lidera dicho proceso, las dependencias que por la envergadura de la fase se requiera de apoyo o complemento para la gestión y por último el porcentaje de avance específicamente para esta fase, es decir del 100% de la fase en que porcentaje se encuentra su desarrollo.

[9] *Figura tomada de la guía Modelo de Seguridad y Privacidad de la Información capítulo 8.4*

Avance fase evaluación de desempeño	
Fecha estimada ejecución	11 meses
Cantidad de actividades a realizar	3 actividades
Dependencia líder	Secretaría TIC
Dependencias adicionales involucradas	Secretaría de Gestión Administrativa
Fase en ejecución	SI NO ✓
Porcentaje de avance	0%

Tabla 4 Avance fase de evaluación de desempeño[10]

V. Fase mejora continua

La fase de mejora continua nos permite entender las falencias, aciertos, ventajas y desventajas de las decisiones adoptadas en la fase de planificación e implementación del MSPI permitiendo así que ante de regresar nuevamente a la fase de panificación se entiendan las nuevas necesidades y se cubran o mejoren los aspectos que quedaron pendiente en el anterior ciclo de implementación.

Por ende, esta fase es de mucha relevancia ya que permite trazar nuevamente la hoja de ruta con unas lecciones aprendidas y así ir mejorando en conjunto la seguridad y privacidad de los activos de información en la Alcaldía de Pereira.

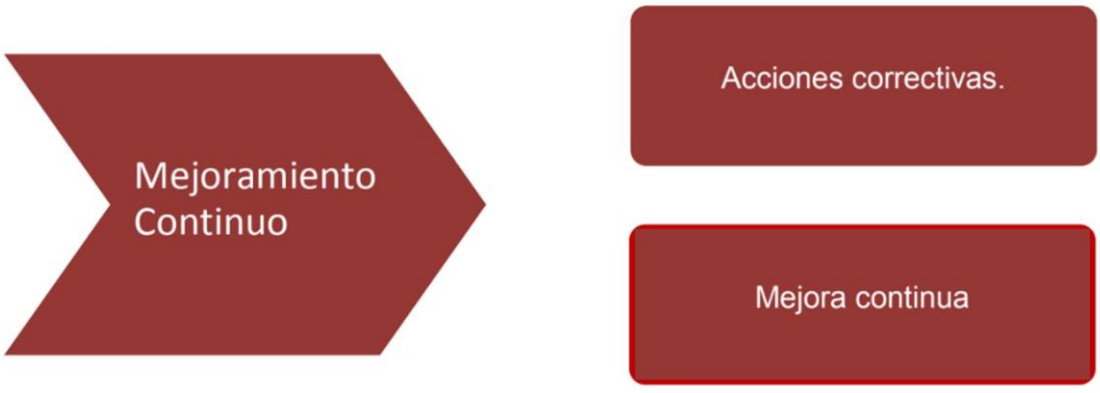


Figura 7 Fase de mejoramiento continuo[11]

[10] *Fuente de elaboración propia*

[11] *Figura tomada de la guía Modelo de Seguridad y Privacidad de la Información capítulo 8.5*

A continuación, se muestra en la Tabla 5 Avance fase de mejora continua, el tiempo estimado para la ejecución de la fase, las actividades que se deben ejecutar, la dependencia que lidera dicho proceso, las dependencias que por la envergadura de la fase se requiera de apoyo o complemento para la gestión y por último el porcentaje de avance específicamente para esta fase, es decir del 100% de la fase en que porcentaje se encuentra su desarrollo.

Avance fase mejora continua	
Fecha estimada ejecución	6 meses
Cantidad de actividades a realizar	2 actividades
Dependencia líder	Secretaría TIC
Dependencias adicionales involucradas	Secretaría de Gestión Administrativa
Fase en ejecución	SI NO ✓
Porcentaje de avance	0%

Tabla 5 Avance fase de mejora continua[12]

Cronograma del Modelo de Seguridad y Privacidad de la Información en la Alcaldía de Pereira

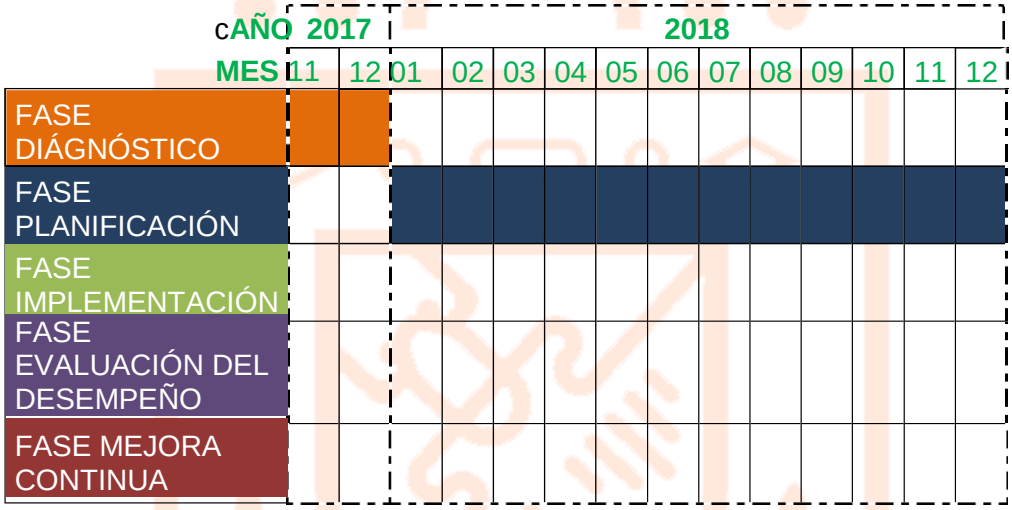
A continuación se desglosa el cronograma de ejecución de la implementación del Modelo de Seguridad y Privacidad de la Información desde la fase de diagnóstico hasta la fase de mejora continua, es decir abarcando todas las fases.

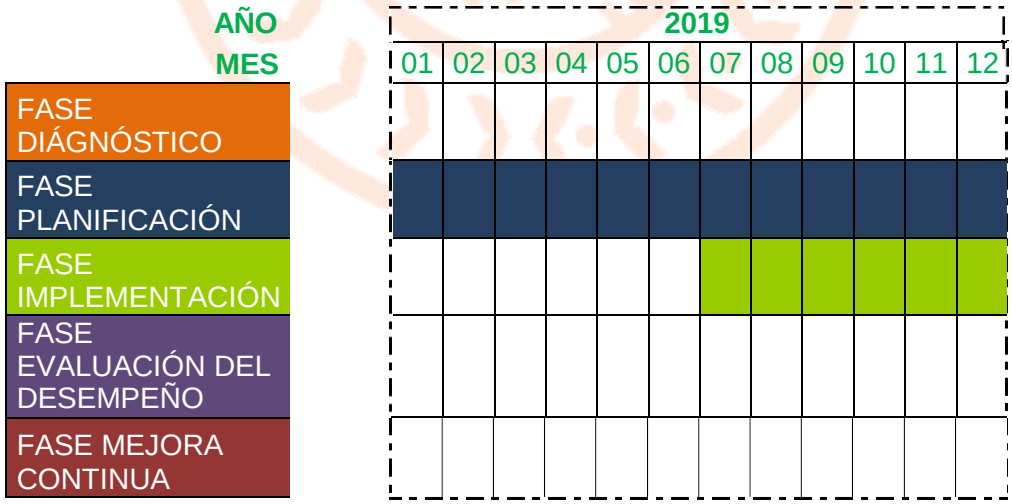
Se efectúa el cronograma detallando año por año con sus respectivos meses de ejecución indicados en las tablas de avance de cada fase.

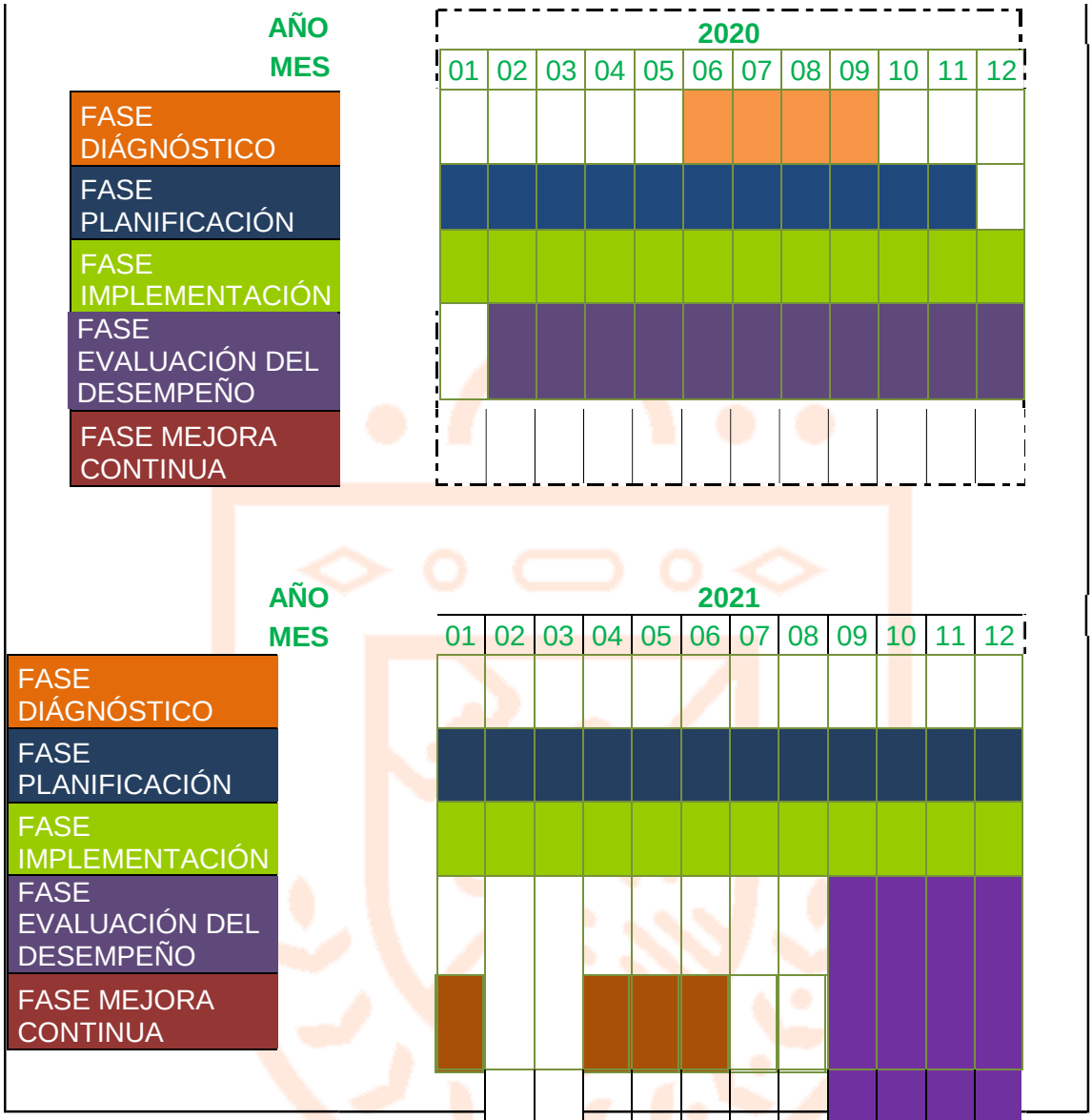
[12] *Fuente de elaboración propia*

ALCALDÍA DE PEREIRA

CRONOGRAMA PLAN DE IMPLEMENTACIÓN DEL MSPI







x

Tabla 6 Cronogr implementación del MSI