PLAN DE SEGURIDAD Y PRIVACIDAD DE LAINFORMACION, TRATAMIENTO DE RIESGOS

	ACTUALIZÓ	REVISÓ	APROBÓ
FIRMA:			
NOMBRE:	**FERNANDO CELIS CLAROS**	**María Elvira Yagüe Hurtado**	**Oriana Sofía Peña Mazabel**
CARGO:	Líder Gestión de las Tecnologías	Subdirectora Administrativa y Financiera	Gerente
FECHA:	19/01/2022	19/01/2022	19/01/2022

Contenido

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION Y TRATAMIENTO DE RIESGOS

1. INTRODUCCION

En el proceso de implementación del modelo Institucional de Gestión y desempeño MIPG trae consigo una modernización del Estado Colombiano buscando como fin el mejoramiento en la prestación de servicios públicos para el pueblo, mejorando la calidad de vida de los ciudadanos en cada región.

La ESE MANUEL CASTRO TOVAR es una Entidad descentralizada del nivel territorial responsable de la prestación de servicios de salud de primer nivel de atención en la ciudad de Pitalito, por tanto, desarrolla la implementación de MIPG y en consecuencia los productos asociados a este modelo, uno de ellos es el PETI y los planes de seguridad y privacidad de la información y de tratamiento de riesgos de seguridad y privacidad de la información pertenecientes a la política de Gobierno digital.

En este aparte la ESE trabajara conjuntamente los planes de seguridad y privacidad de la información y lo articulara con el PETI.

La ESE es una entidad que apenas en este periodo está trabajando en la migración a la ejecución de actividades misionales haciendo uso de las tecnologías de la información desde sus procesos de planeación estratégica.

El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, es la entidad encargada de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones.

La estrategia de Gobierno en Línea, liderada por el Ministerio TIC, tiene como objetivo, garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de contribuir con la construcción de un Estado más participativo, más eficiente y más transparente. 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.

El Modelo de Seguridad y Privacidad de la Información – MSPI, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

A través del decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, se define el componente de seguridad y privacidad de la información, como parte integral de la estrategia GEL.

El Modelo de Seguridad y Privacidad de la Información se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.

2. DEFINICIONES IMPORTANTES

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).

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 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 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. (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.

3. OBJETIVOS

3.1 Objetivo General

Establecer un lineamiento en cuanto a seguridad y privacidad de la información que permita la ejecución de buenas prácticas por parte de los usuarios de las TI en la Entidad y los ciudadanos en general.

3.2 Objetivos Específicos

- ✓ Incremento de la transparencia de la Entidad publica

- ✓ Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.
- ✓ Orientar a los diferentes servicios de la E.S.E en las mejores prácticas en seguridad y privacidad.
- ✓ Optimizar la labor de acceso a la información pública al interior de la E.S.E

4 MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

El modelo de operación, contempla un ciclo de cinco (5) fases, las cuales permiten que La ESE MANUEL CASTRO TOVAR pueda gestionar adecuadamente la seguridad y privacidad de sus activos de información. En el presente Modelo de Seguridad y Privacidad de la Información se contemplan diferentes niveles de madurez, que corresponden a la evolución de la implementación del modelo de operación.

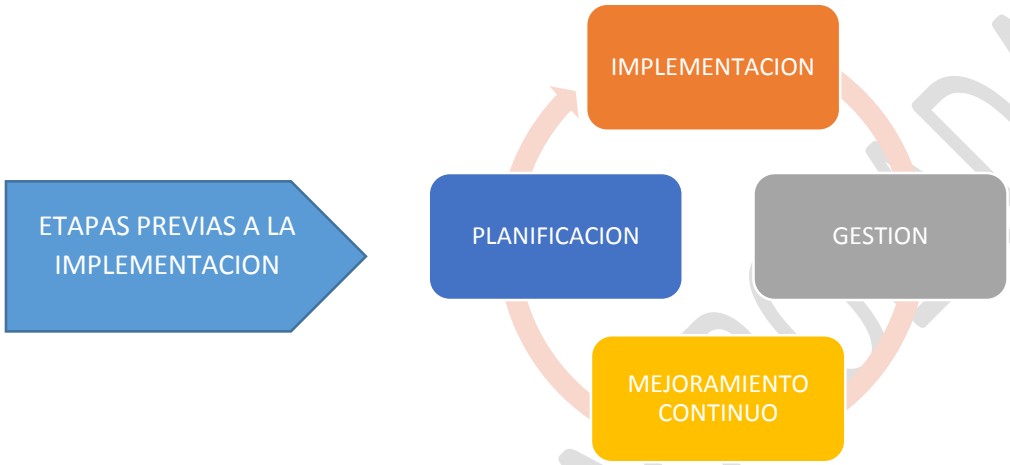
La seguridad y privacidad de la información, como componente transversal a la Estrategia de Gobierno en línea, permite alinearse al componente de TIC para la Gestión al aportar en el uso estratégico de las tecnologías de la información con la formulación e implementación del modelo de seguridad enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos de la entidad.

La Seguridad y Privacidad de la Información se alinea al componente de TIC para Servicios apoyando el tratamiento de la información utilizada en los trámites y servicios que ofrece la Entidad, observando en todo momento las normas sobre protección de datos personales, así como otros derechos garantizados por la Ley que exceptúa el acceso público a determinada información.

TIC para Gobierno Abierto y Seguridad y Privacidad de la Información se alinean en la construcción de un estado más transparente, colaborativo y participativo al garantizar que la información que se provee tenga controles de seguridad y privacidad de tal forma que los ejercicios de interacción de información con el ciudadano, otras entidades y la empresa privada sean confiables.

Para lograr que los sistemas de información de la administración pública estén conectados, articulados, cumplan estándares y adopten las mejores prácticas en cuanto a su desarrollo y al manejo de la información, se ha creado la Arquitectura TI Colombia, cuyo principal instrumento es el Marco de Referencia de Arquitectura Empresarial para la Gestión de TI. Con él se busca habilitar las estrategias de Gobierno en línea de TIC para Servicios, TIC para la Gestión, TIC para el Gobierno Abierto y Seguridad y la Privacidad de la Información.

Descripción del modelo



4.1 FASE- ETAPAS PREVIAS A LA IMPLEMENTACION

En esta fase se pretende identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información, que de ahora en adelante se denominará MSPI, el cual hace parte integral de la Estrategia de Gobierno en línea.

- ✓ Estado actual de la Entidad
- ✓ Identificar el nivel de madurez
- ✓ Levantamiento de la información

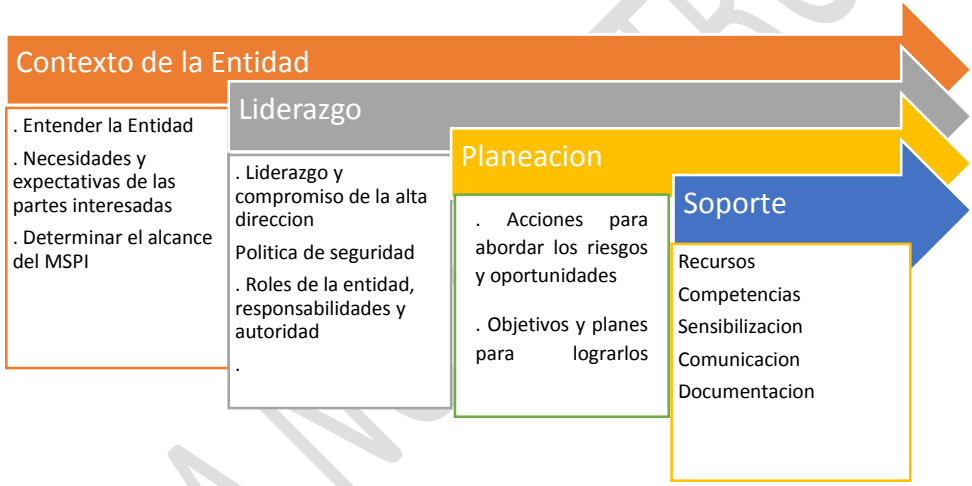
La guía del Mintic determina unos instrumentos para ser aplicados y definir el Estado actual de la Entidad, y su nivel de madurez , LA ESE MANUEL CASTRO TOVAR realmente está en un nivel muy bajo frente a este tema , inicialmente se tratara de estructura el área de TECNOLOGIAS y procesos de gestión de TI , el gobierno de TI para poder en la ejecución y formación de la estrategia TI trabajar de manera progresiva en la implementación del plan de seguridad y privacidad de la información y de los riesgos de los mismos.

Durante esta fase deben conseguir las siguientes metas:

Metas
1. Determinar el estado actual de la gestión de seguridad y privacidad de la información en la ESE
2. Identificar el nivel de madurez de la ESE según metodología

4.2 FASE- PLANIFICACION

Esta fase tiene la finalidad de generar un plan de seguridad y privacidad alineado con el propósito 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.
Para desarrollar esta fase se toman los resultados y las metas de la fase anterior como insumo para poder desarrollarla.



Resultados de la Fase de implementación

Instrumento	***Resultado***
Seguridad y privacidad de la información	Documento que contenga la Política de seguridad de la información
Procedimientos de seguridad de la información y privacidad y tratamiento de riesgos	Procedimientos documentados, adoptados y socializados
Plan de diagnóstico de transición de IPV4 A IPV6	Documento con proyecto de transición viabilizado
Integración del MSPI con el sistema de gestión	Proceso de integración de los dos modelos.

documental	

Descripción de la FASE DE PLANIFICACION

Procedimientos de Seguridad de la Información. En este Ítem se debe desarrollar y formalizar procedimientos que permitan gestionar la seguridad de la información en cada uno de los procesos definidos en la entidad. Esta actividad 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.

Política de seguridad y privacidad de la información. La Política de Seguridad y Privacidad de la información está 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 debe contener 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. 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 debe explicar 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.

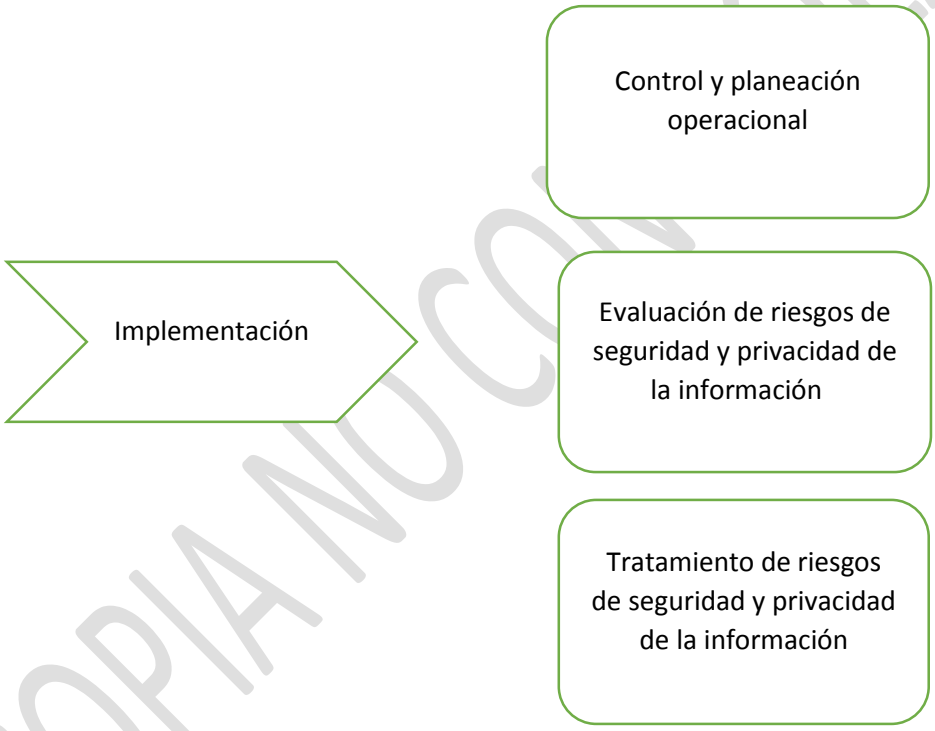
Integración del MSPI con el Sistema de Gestión documental. La entidad deberá alinear la documentación relacionada con seguridad de la información con el sistema de gestión documental generado o emitido conforme a los parámetros emitidos por el archivo general de la nación. Identificación, Valoración Y Tratamiento de Riesgos. La entidad debe definir una metodología de gestión del riesgo enfocada a procesos, que le permita identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que estén expuestos los activos, así como la declaración de aplicabilidad. Para conseguir una integración adecuada entre el MSPI y la guía de gestión del riesgo emitida por el DAFP respecto a este procedimiento, se recomienda emplear los criterios de evaluación (impacto y probabilidad) y niveles de riesgo emitidos por esta entidad. Para definir la metodología, la entidad puede

hacer uso de buenas prácticas vigentes tales como: ISO 27005, Margerit, Octave, ISO 31000 o la Guía No 7 - Gestión de Riesgos emitida por el MinTIC.

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.

4.3 FASE DE IMPLEMENTACION

E n esta fase se lleva a cabo la implementación de lo planeado en la fase anterior de manera gradual, teniendo en cuenta los aspectos más importantes determinados en la fase anterior.



Para desarrollar esta fase debe estar definido el nivel de madurez de la Entidad

Metas	Resultados
Planificación y control	Documento socializado y aprobado
Implementar el plan de tratamiento de riesgos	Documento que contenga soportes de ejecución
Plan de transición de IPV 4 A IPV6	Documento que contiene la estrategia de

	transición.

Teniendo en cuenta los resultados de las fases anteriores a la implementación y planificación del MSPI se elabora un plan de implementación y se ejecuta el plan de tratamiento de riesgos del MSPI

Plan de implementación.

La entidad debe planear, implementar y controlar los procesos misionales y de apoyo, validando la efectividad de los controles a implementar garantizando sus objetivos misionales. Dichos controles deben estar documentados y debe ser verificada su efectividad cada cierto tiempo. La entidad debe controlar que no se presenten cambios que afecten los procesos, tomando acciones para mitigar cualquier evento adverso, es decir se deben controlar sus procesos.

Implementación del plan de tratamiento de riesgos.

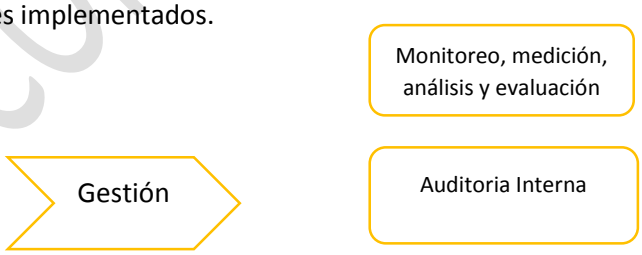
Se implementa el plan de tratamiento de riesgos de seguridad de la información, en el cual se identifica el control a aplicar para llevar cada uno de los riesgos a un nivel aceptable, en donde la base para ejecutar esta fase es el anexo A de la Norma ISO 27001:2013 y la guía de controles sobre privacidad del MSPI. Es preciso tener en cuenta que la aplicación del control sobre los riesgos detectados debe estar aprobados por los responsables de los procesos.

Plan de control operacional.

Es el plan que debe construir la entidad para efectuar el monitoreo y seguimiento a los controles de seguridad definidos para los procesos. Los entregables asociados a las metas en la Fase de Implementación deben ser revisados y aprobados por la alta Dirección.

4.4 FASE EVALUACION DE DESEMPEÑO

El proceso de seguimiento y monitoreo del MSPI se hace con base en los resultados que arroja los indicadores de la seguridad de la información propuestos para verificación de la eficacia y efectividad de los controles implementados.



Revisión por alta dirección

Metas	***Resultados***
Plan de seguimiento, evaluación y análisis del MSPI	Documento con el plan de seguimiento, evaluación, análisis y resultados del MSPI, revisado y aprobado por la alta Dirección
Plan de ejecución de Auditoria Interna.	Resultados de la auditoria interna al MSPI, de acuerdo a lo establecido en el plan de auditoría, revisado y aprobado por la alta Dirección.

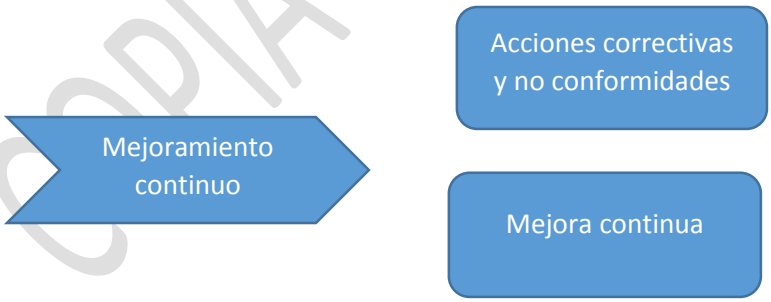
Seguimiento y evaluación al MSIP

En esta fase la Entidad debe diseñar instrumentos para hacer seguimiento al cumplimiento del MSIP y evaluar de manera general el funcionamiento del MSPI.

- ✓ Seguimiento y evaluación de la implementación del MSIP
- ✓ Revisión de los resultados de la medición de los riesgos según metodología
- ✓ Se deben medir los indicadores de gestión del MSIP
- ✓ Revisar controles definidos para mitigar riesgos

4.5 FASE DE MEJORA CONTINUA

Esta fase le permitirá a la Entidad, consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, que permita realizar el plan de implementación de las acciones correctivas identificadas para el MSPI.



Metas	*Resultados*
Plan de mejora continua	Documento con el plan de mejoramiento. Documento con el plan de comunicación de resultados.

FORMATO DE SEGUIMIENTO DE ACCIONES

E.S.E. MUNICIPAL MANUEL CASTRO TOVAR :MPRESA SOCIAL DEL ESTADO MUNICIPAL MANUEL CASTRO TOVAR
SEGUIMIENTO PLANES DE ACCIÓN PETI

PERSPECTIVA										
OBJETIVO ESTRATÉGICO										
ESTRATEGIA Y/O POLÍTICA	ACCIONES A 31 DICIEMBRE	RESPONSABLE	SEGUIMIENTO 1TRIMESTRE	%	SEGUIMIENTO 2 TRIMESTRE	%	SEGUIMIENTO 3 TRIMESTRE	%	SEGUMIENTO 4 TRIMESTRE	% TOTAL

CONTROL DE CAMBIOS

VERSIÓN	APROBACIÓN	DESCRIPCIÓN DEL CAMBIO
01		Versión inicial implementación SGC