MINMINAS

IPSE
Instituto de Planificación y Promoción de Soluciones Energéticas para las Zonas No Interconectadas

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Alineado con el propósito misional IPSE (Instituto de Planificación y Promoción de Soluciones Energéticas para las Zonas no Interconectadas, basado en el MSPI (Modelo de Seguridad y Privacidad de la Información) establecido por el Ministerio De TIC – Colombia.

IPSE
Instituto de Planificación y Promoción de Soluciones Energéticas para las Zonas No Interconectadas
No 2017-133-003938-2
Asunto DEYBER ERICKSON RODRIGUEZ
Fecha Radicado 05/10/2017 15:52:37
Destino COORDINACION DE TECNOLOGIA Y S
Remitente CIU DEYBER ERICKSONRODRIGUEZ
Bogotá D.C. Carrera 12 No. 84-12, 6449300
Sistema de Gestión - OrfeoGpl

Agosto 2017

IPSE

CONTROL DE CAMBIOS

VERSIÓN	FECHA	RESPONSABLE	DESCRIPCIÓN
1.0	1/8/2017	DEYBER ERICKSON RODRIGUEZ ALVAREZ	CREACIÓN DEL DOCUMENTO

DERECHOS DE AUTOR

Basándose en normas jurídicas, principios, derechos morales y patrimoniales de ley el copyright del texto incluido en este documento es propiedad del instituto de planificación y promoción de soluciones energéticas para las zonas no interconectadas **(IPSE),** por ello, la realización de copias no está permitida.

CONTENIDO

1. **OBJETIVOS** 2
2. **PLANTEAMIENTO DEL PROBLEMA** 2
3. **MARCO LEGAL** 3
4. **ALCANCE** 5
5. **NIVEL DE CUMPLIMIENTO** 5
6. **MARCO METODOLOGICO - DISEÑO METODOLOGICO - Ciclo PHVA** 6
7. **ESQUEMA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - IPSE** ..... ¡Error! Marcador no definido.
8. **PLANIFICACIÓN** 7

8.1 FASE DE DIAGNÓSTICO - ETAPAS PREVIAS A LA IMPLEMENTACIÓN 7
8.2 TAREAS PARA EJECUTAR FASE DIAGNOSTICO IPSE: 8
8.3 FASE DE PLANIFICACIÓN 8
8.4 TAREAS PARA EJECUTAR FASE PLANIFICACIÓN IPSE: 9
8.5 FASE DE IMPLEMENTACIÓN 10
8.6 TAREAS PARA EJECUTAR FASE IMPLEMENTACIÓN IPSE: 11
8.7 FASE DE EVALUACIÓN DE DESEMPEÑO 12
8.8 TAREAS PARA EJECUTAR FASE EVALUACIÓN IPSE: 12
8.9 FASE DE MEJORA CONTINUA 13
8.10 TAREAS PARA EJECUTAR FASE DE MEJORA CONTINUA IPSE: ..... **¡Error! Marcador no definido.**

TABLA DE IMÁGENES

Imagen 1 Modelo PHVA aplicado al Plan de Seguridad y Privacidad de la Información del IPSE *6*
Imagen 2 Esquema de Seguridad y Privacidad de la Información IPSE ..... ***¡Error! Marcador no definido.***
Imagen 3 Niveles de madurez *7*

1. OBJETIVOS

Objetivo Principal:

Crear un plan de Seguridad y Privacidad de la Información en el IPSE para la presente vigencia, con la intención de organizar y solucionar las necesidades de la entidad para la presente vigencia competentes.

Objetivos Específicos:

- Elaborar el diagnóstico de seguridad y privacidad de la información y de los sistemas de información basado en las nuevas estrategias elaboradas por el estado.
- Definir las políticas de seguridad y privacidad de la información, alineado con el propósito misional de la entidad y el MSPI expuesto por el MINTIC.
- Modernizar la Política de Seguridad Informática del IPSE implementada actualmente (Resolución No. 20131300004105 del 02/07/2013) alineada a los requerimiento de seguridad informática solicitada a entes de orden nacional.
- Planear actividades para la evaluación, monitoreo y mejoramiento continúo de los niveles de seguridad y privacidad de la información y los sistemas de información.
- Apoyar la innovación tecnológica.
- Implementar el Modelo de Seguridad y Privacidad de la información con base a las necesidades de la entidad y el nivel de madurez acorde a la respectiva vigencia.

2. PLANTEAMIENTO DEL PROBLEMA

ANTECEDENTES DEL PROBLEMA

- En la actualidad el punto de amenazas en cualquier entidad no se tipifica como personalizado, por el contrario estas amenazas se construyen de manera global, hecho que obliga a que las organizaciones se preparen para cualquier ataque y para eso cuente con elementos que prevengan los ataques como firewalls, antivirus, antispam, etc.
- Actualmente se tiene implementada la política de seguridad informática con Resolución No. 20131300004105 implementada desde el día 02/07/2013.

FORMULACIÓN DEL PROBLEMA

3 No existe a la fecha un plan de seguridad y privacidad de la información que comprometa y permita al personal del IPSE mantener unas condiciones estables de seguridad y privacidad de la información, para garantizar la confidencialidad, integridad y disponibilidad de la información.

3. MARCO LEGAL

El Estado Colombiano por medio de las diferentes entidades que lo representan establece una serie de lineamientos y guías que permiten a las entidades estatales planificar, implementar y desarrollar una serie de estrategias, con el fin de guardar la información como un tesoro, garantizando la seguridad de la información.

Para lograrlo y como lo estipula el decreto 1078 del 26 de mayo de 2015, cada organización estatal debe adoptar y dar cumplimiento a la normatividad que se ha impartido, de esta forma se le dé importancia a crear una cultura de Seguridad Informática en el sector y en todas las entidades del estado, ligada a un trato seguro de la información, para que la implantación de las diversas Políticas de Seguridad y Privacidad de la Información pueda generar sinergia interna y externamente.

Lineamientos recomendados en Norma la ISO IEC 27005 – 2009, y la ley 1712 de 2014 por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, dando cumplimiento a sus funciones; publica El Modelo de Seguridad y Privacidad de la Información (MSPI), el cual 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.

El Modelo de Seguridad y Privacidad para estar acorde con las buenas prácticas de seguridad será actualizado periódicamente; reuniendo los cambios técnicos de la norma 27001 del 2013, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información.
A nivel metodológico es importante tener presente que el (MSPI) cuenta con una serie de guías anexas que ayudarán a las entidades a cumplir lo solicitado permitiendo abordar de manera detallada cada una de las fases del modelo, buscando a su vez comprender cuáles son los resultados a obtener y como

desarrollarlos, incluyendo los nuevos lineamientos que permiten la adopción del protocolo IPv6 en el Estado Colombiano.

La implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, en la Entidad está determinado por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la misma, todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.

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

LA BIBLIOTECA DE SEGURIDAD[1] CONSTA DE:

- ✓ Instrumento de Evaluación MSPI
- ✓ Instructivo Instrumento de Evaluación MSPI
- ✓ Guía - Seguridad de la información Mipymes
- ✓ Guía 1 - Metodología de pruebas de efectividad
- ✓ Guía 2 - Política General MSPI v1
- ✓ Guía 3 - Procedimiento de Seguridad de la Información
- ✓ Guía 4 - Roles y responsabilidades
- ✓ Guía 5 - Gestión Clasificación de Activos
- ✓ Guía 6 - Gestión Documental
- ✓ Guía 7 - Gestión de Riesgos
- ✓ Guía 8 - Controles de Seguridad de la Información
- ✓ Guía 9 - Indicadores Gestión de Seguridad de la Información
- ✓ Guía 10 - Continuidad de Negocio
- ✓ Guía 11 - Análisis de Impacto de Negocio
- ✓ Guía 12 - Seguridad en la Nube
- ✓ Guía 13 - Evidencia Digital (En actualización)
- ✓ Guía 14 - Plan de comunicación, sensibilización, capacitación
- ✓ Guía 15 - Auditoria
- ✓ Guía 16 - Evaluación de Desempeño
- ✓ Guía 17 - Mejora continua

[1] Vinculo Biblioteca de seguridad Ministerio de TIC http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

- ✓ Guía 18 - Lineamientos terminales de áreas financieras de entidades públicas
- ✓ Guía 19 - Aseguramiento de protocolo IPv4_IPv6
- ✓ Guía 20 - Transición IPv4_IPv6
- ✓ Guía 21 - Gestión de Incidentes
- ✓ Modelo de Seguridad y Privacidad

4. ALCANCE

Tomando como base la herramienta diagnostico que se establece en el Modelo de Seguridad y Privacidad mencionado anteriormente para realizar una revisión completa de las necesidades que tiene la entidad interna y externamente.

Se aplicara el modelo de seguridad y privacidad de la información establecido por el ministerio de TIC, contemplando el ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

5. NIVEL DE CUMPLIMIENTO

Se debe dar cumplimiento a todas las estrategias mencionadas en el presente documento para garantizar que el plan de seguridad se pueda implementar correctamente, estas actividades se pueden ver comprometidas o afectadas por la disponibilidad del personal del IPSE ya que el desarrollo de las actividades es directamente proporcional con el tiempo de los empleados.

6. MARCO METODOLOGICO - DISEÑO METODOLOGICO - Ciclo PHVA

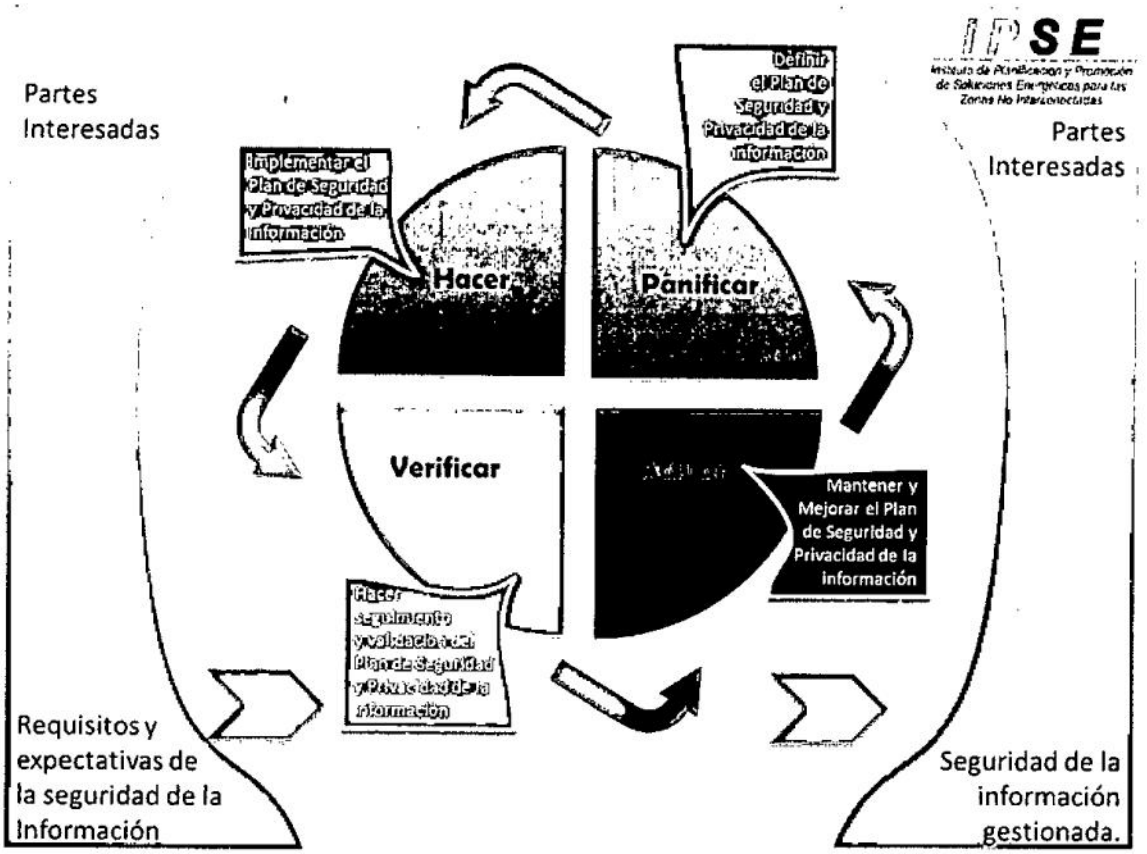
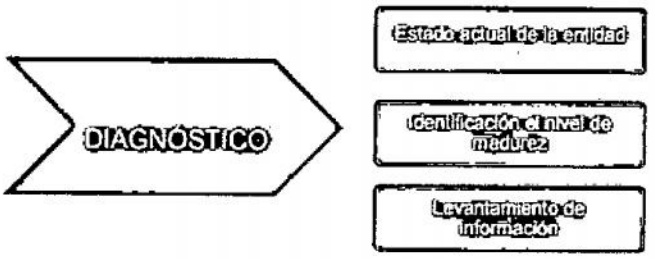


Imagen 1 Modelo PHVA aplicado al Plan de Seguridad y Privacidad de la Información del IPSE

7. PLANIFICACIÓN

Se debe realizar el diagnostico a toda la entidad para recolectar la información que permita establecer el nivel de madurez del IPSE y el estado actual estado actual de la gestión de seguridad y privacidad de la información internamente.

7.1 FASE DE DIAGNÓSTICO - ETAPAS PREVIAS A LA IMPLEMENTACIÓN



Diagnostico			
Metas	**Resultados**	**Instrumentos MSPI**	**Alineación MRAE**
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.	Diligenciamiento de la herramienta.	Herramienta de diagnóstico.	LI.ES.01 LI.ES.02 LI.GO.01 LI.GO.04 LI.GO.05 LI.GO.07 LI.ST.14
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.	Herramienta de diagnóstico	
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Documento con los hallazgos encontrados en las pruebas de vulnerabilidad.	Herramienta de diagnóstico	

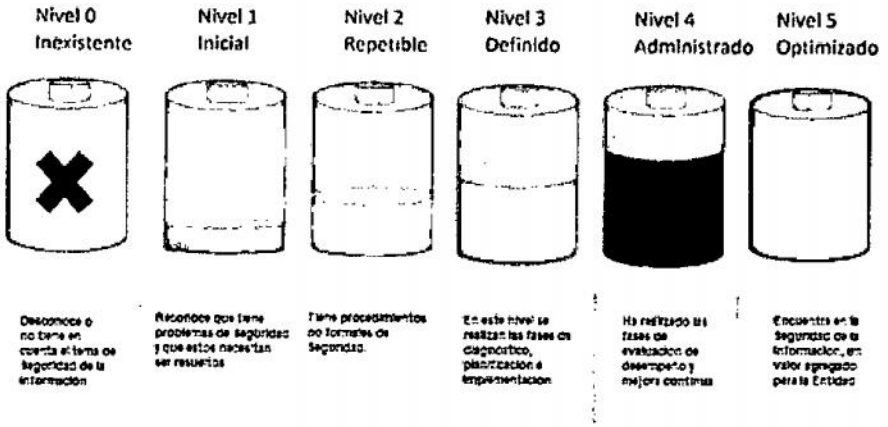
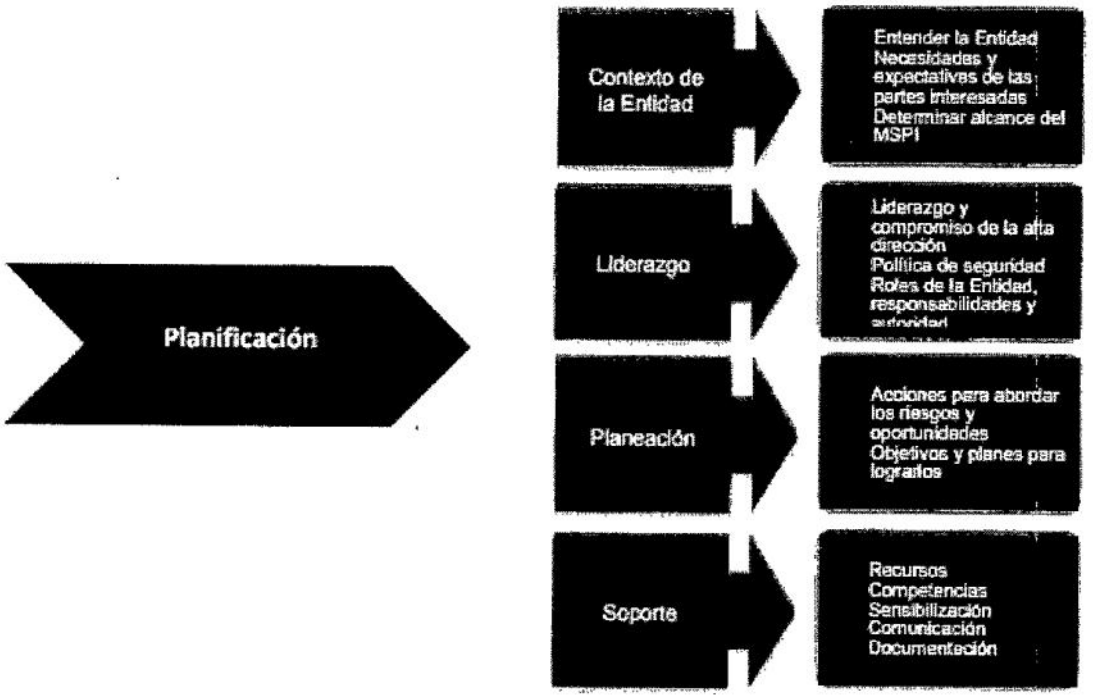


Imagen 2 Niveles de madurez

7.2 TAREAS PARA EJECUTAR FASE DIAGNOSTICO IPSE:

1. Diligenciar la herramienta de diagnóstico con nombre:
   Instrumento de evaluación MSPI 2016.xlsx
   Disponible en http://www.mintic.gov.co/gestionti/615/articles-5482_Instrumento_Evaluacion_MSPI.xlsx
2. Definir el nivel de madurez
3. Identificar hallazgos en las pruebas que se incluyen sobre la herramienta.
4. Realizar el reporte en el documento matriz de la política 4 del PDA con el cumplimiento del 100% del ítem de diagnóstico.

7.3 FASE DE PLANIFICACIÓN



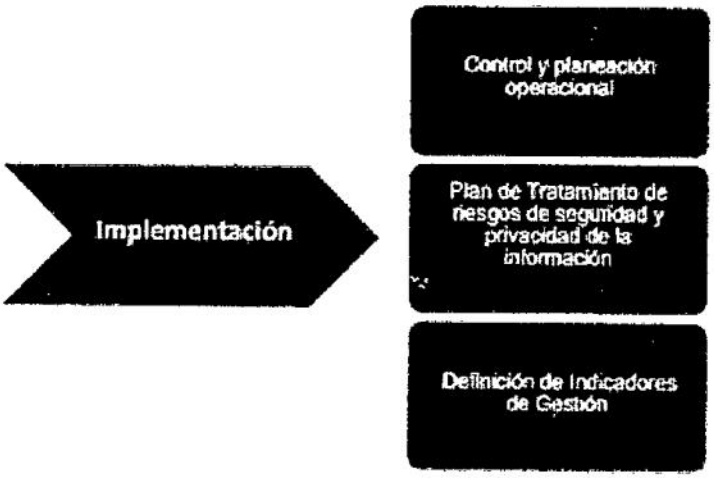
Planificación			
Metas	**Resultados**	**INSTRUMENTOS MSPI**	**MRAE**
Política de Seguridad y Privacidad de la Información	Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad.	Guía No 2 – Política General MSPI	LI.ES.02 LI.ES.06 LI.ES.07 LI.ES.08
Políticas de seguridad y privacidad de la información	Manual con las políticas de 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	LI.ES.09 LI.ES.10 LI.GO.01 LI.GO.04 LI.GO.07 LI.GO.08 LI.GO.09 LI.GO.10 LI.INF.01 LI.INF.02 LI.INF.09 LI.INF.10 LI.INF.11 LI.INF.14 LI.SIS.22 LI.SIS.23 LI.SIS.01 LI.ST.05 LI.ST.06 LI.ST.09 LI.ST.10 LI.ST.12 LI.ST.13 LI.ST.14 LI.UA.01 LI.UA.02 LI.UA.03 LI.UA.04 LI.UA.05 LI.UA.06
Procedimientos de seguridad de la información.	Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas 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.	
Inventario de activos de información.	Documento con la metodología para identificación, clasificación y valoración de activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por la alta dirección. Matriz con la identificación, valoración y clasificación de activos de información. Documento con la caracterización de activos de información, que contengan datos personales Inventario de activos de IPv6	Guía No 5 - Gestión De Activos Guía No 20 - Transición Ipv4 a Ipv6	
Integración del MSPI con el Sistema de Gestión documental	Integración del MSPI, con el 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. Documento con la declaración de aplicabilidad. 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	

7.4 TAREAS PARA EJECUTAR FASE PLANIFICACIÓN IPSE:

1. Identificar necesidades en la entidad.
2. Determinar el alcance del plan de seguridad y privacidad de la información.
3. Elaborar la Política de seguridad y privacidad de la información.

4. Crear el comité se seguridad y privacidad de la información.
5. Realizar la clasificación de activos de información utilizando la normatividad vigente.
6. Definir estrategias para recolectar riesgos. (Clasificación de riegos).
7. Definir controles para riesgos (Clasificación de controles).
8. Seleccionar los procedimientos de Seguridad de la Información que se consideren necesarios para aplicarlos en la entidad
9. Definir estrategias para utilizar los recursos disponibles que permitan sensibilizar, comunicar y documentar las actividades.
10. Elaborar la fase de planeación para IPV6 establecida en la Guía No 20 de la BIBLIOTECA DE SEGURIDAD publicada por el ministerio de TIC. (http://www.mintic.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf)
11. Alinear las actividades a ejecutar con el proyecto de arquitectura empresarial (Actividades consideradas necesarias).

7.5 FASE DE IMPLEMENTACIÓN

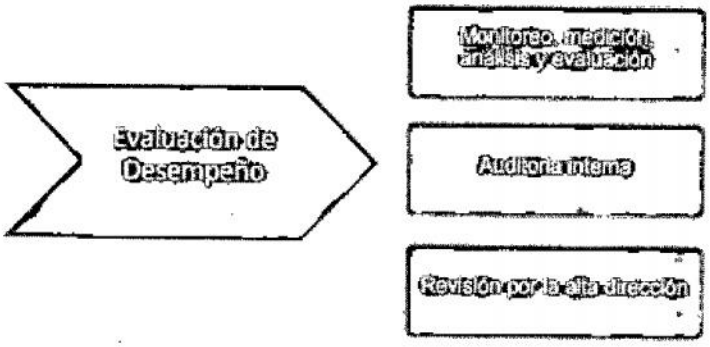


Planificación y Control Operacional.	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad.	LI.ES.09 LI.ES.10 LI.GO.04 LI.GO.09 LI.GO.10 LI.GO.14 LI.GO.15 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 la Oficina 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

7.6 TAREAS PARA EJECUTAR FASE IMPLEMENTACIÓN IPSE:

1. Elaborar documento con las estrategias que permitan implementar las acciones y actividades del plan de control o tratamiento de riesgos, tomando como insumo la clasificación de activos de información.
2. Elaborar y aprobar por cada líder de proceso del IPSE el Informe del plan de control o tratamiento de riesgos
3. Elaborar los indicadores de gestión de seguridad y privacidad de la información que se hayan seleccionados.
4. Elaboración del plan de transición de IPV4 a IPV6 (aprobado por la Coordinación del Grupo de Tecnología y Sistemas de Información)

7.7 FASE DE EVALUACIÓN DE DESEMPEÑO

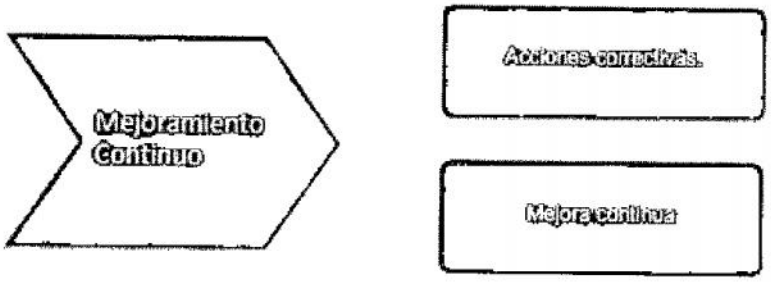


Evaluación del Desempeño			
Metas	Resultados	Instrumentos	
		MSPI	MRAE
Plan de revisión y seguimiento, a la implementación del MSPI.	Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección.	Guía No 16 – Evaluación del desempeño.	LI.ES.12 LI.ES.13 LI.GO.03 LI.GO.11 LI.GO.12 LI.INF.09 LI.INF.11 LI.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.	

7.8 TAREAS PARA EJECUTAR FASE EVALUACIÓN IPSE:

1. Realizar la evaluación de desempeño establecida en la guía 16 del MSPI establecido por el Ministerio de TIC
2. Apoyar y permitir que el área correspondiente o responsable en la entidad pueda realizar las actividades de auditoria y seguimiento a las labores planeadas en el presente plan alineada al cronograma del plan.

7.9 FASE DE MEJORA CONTINUA



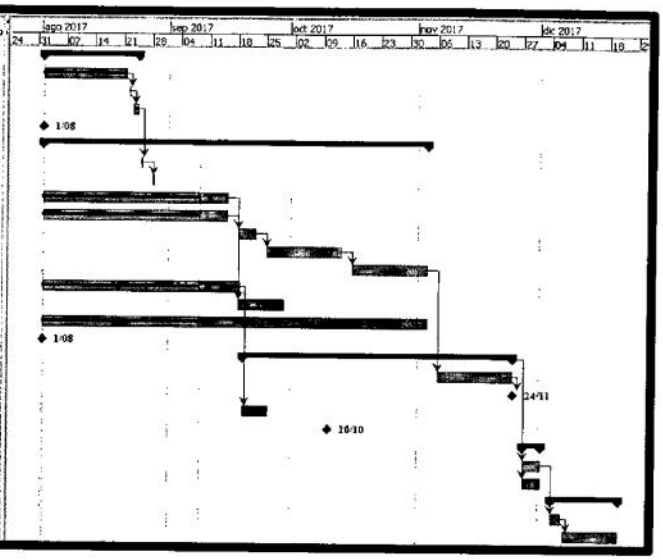
Mejora Continua			
Metas	Resultados	Instrumentos	
		MSPI	MRAE
Plan de mejora continua	Documento con el plan de mejoramiento. Documento con el plan de comunicación de resultados.	Resultados de la ejecución del Plan de Revisión y Seguimiento. a la Implementación del MSPI. Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI. Guía No 17 – Mejora Continua	LI.GO.03 LI.GO.12 LI.GO.13 LI.INF.14 LI.INF.15 LI.ST.15 LI.UA.9 LI.UA.10

7.10 TAREAS PARA EJECUTAR FASE DE MEJORA CONTINUA IPSE:

1. Realizar un análisis de resultados tomando como base las actividades planeadas y los resultados de la evaluación de desempeño (entregando un informe al líder de TIC para reorganizar la información).
2. Establecer estrategias que permitan planear mejoras sobre el plan de seguridad, tomando como insumo las actividades ejecutas y la evaluación de desempeño (se debe realizar un listado de la estrategias que se van a aplicar).

8. CRONOGRAMA

	Nombre	Duracion	Inicio	Terminado	Predecesores	Nomb
1	**7.2 TAREAS PARA EJECUTAR FASE DIAGNOSTICO IPSE:**	18 days?	**1/08/17 08:00 AM**	**24/08/17 05:00 PM**		
2	1. Diligenciar la herramienta de diagnóstico con nombre: Instrumento	15 days?	1/08/17 08:00 AM	21/08/17 05:00 PM		
3	2. Definir el nivel de madurez	1 day?	22/08/17 08:00 AM	22/08/17 05:00 PM	2	
4	3. Identificar hallazgos en las pruebas que se incluyen sobre la herra	2 days?	23/08/17 08:00 AM	24/08/17 05:00 PM	3	
5	4. Realizar el reporte en el documento matriz de la política 4 del PDA	0 days?	1/08/17 08:00 AM	1/08/17 08:00 AM		
6	**7.4 TAREAS PARA EJECUTAR FASE PLANIFICACIÓN IPSE:**	69 days?	**1/08/17 08:00 AM**	**3/11/17 05:00 PM**		
7	1. Identificar necesidades en la entidad.	1 day?	25/08/17 08:00 AM	25/08/17 05:00 PM	4	
8	2. Determinar el alcance del plan de seguridad y privacidad de la infor	1 day?	28/08/17 08:00 AM	28/08/17 05:00 PM	7	
9	3. Elaborar la Política de seguridad y privacidad de la información.	34 days?	1/08/17 08:00 AM	15/09/17 05:00 PM		
10	4. Crear el comité se seguridad y privacidad de la información.	34 days?	1/08/17 08:00 AM	15/09/17 05:00 PM		
11	5. Realizar la clasificación de activos de información utilizando la norm	5 days	18/09/17 08:00 AM	22/09/17 05:00 PM	10	
12	6. Definir estrategias para recolectar riesgos. (Clasificación de riesgos	15 days?	25/09/17 08:00 AM	13/10/17 05:00 PM	11	
13	7. Definir controles para riesgos (Clasificación de controles).	15 days?	16/10/17 08:00 AM	3/11/17 05:00 PM	12	
14	8. Seleccionar los procedimientos de Seguridad de la Información que	35 days?	1/08/17 08:00 AM	18/09/17 05:00 PM		
15	9. Definir estrategias para utilizar los recursos disponibles que permit	10 days?	18/09/17 08:00 AM	29/09/17 05:00 PM	9	
16	10. Elaborar la fase de planeación para a IPv6 establecida en la Guia No	69 days?	1/08/17 08:00 AM	3/11/17 05:00 PM		
17	11. Alinear las actividades a ejecutar con el proyecto de arquitectura e	0 days?	1/08/17 08:00 AM	1/08/17 08:00 AM		
18	**7.6 TAREAS PARA EJECUTAR FASE IMPLEMENTACIÓN IPSE:**	49 days?	**19/09/17 08:00 AM**	**24/11/17 05:00 PM**		
19	1. Elaborar documento con las estrategias que permitan implementar la	15 days?	6/11/17 08:00 AM	24/11/17 05:00 PM	13	
20	2. Elaborar y aprobar por cada líder de proceso del IPSE el Informe del	0 days?	24/11/17 05:00 PM	24/11/17 05:00 PM	19	
21	3. Elaborar los indicadores de gestión de seguridad y privacidad de la i	5 days?	19/09/17 08:00 AM	25/09/17 05:00 PM	14	
22	4. Elaboración del plan de transición de IPv4 a IPv6 (aprobado por la o	0 days?	10/10/17 08:00 AM	10/10/17 08:00 AM		
23	**7.8 TAREAS PARA EJECUTAR FASE EVALUACIÓN IPSE:**	5 days?	**27/11/17 08:00 AM**	**1/12/17 05:00 PM**		
24	1. Realizar la evaluación de desempeño establecida en la guía 16 del M	5 days?	27/11/17 08:00 AM	1/12/17 05:00 PM	18	
25	2. Apoyar y permitir que el área correspondiente o responsable en la e	5 days?	27/11/17 08:00 AM	1/12/17 05:00 PM	18	
26	**7.10 TAREAS PARA EJECUTAR FASE DE MEJORA CONTINUA IPS**	13 days?	**4/12/17 08:00 AM**	**20/12/17 05:00 PM**		
27	1. Realizar un análisis de resultados tomando como base las actividades	3 days?	4/12/17 08:00 AM	6/12/17 05:00 PM	24	
28	2. Establecer estrategias que permitan planear mejoras sobre el plan d	10 days?	7/12/17 08:00 AM	20/12/17 05:00 PM	27	



Elaboró	Aprobó
DEYBER ERICKSON RODRIGUEZ ALVAREZ	ANGELINA TOLOZA PABON
Firma:	Firma:

MINMINAS

IPSE
Instituto de Planificación y Promoción de Soluciones Energéticas para las Zonas No Interconectadas

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN