# METODOLOGÌA DE IMPLEMENTACIÓN

Para llevar a cabo la implementación del Sistema de Gestión de Seguridad de la Información, se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar):

De acuerdo a esto, se definen las siguientes fases de implementación:

1. Diagnosticar
2. Planear
3. Hacer
4. Verificar
5. Actuar



*Fuente: Modelo de Seguridad y Privacidad de la Información emitida por MinTIC*

# CUMPLIMIENTO DE IMPLEMENTACIÒN

De acuerdo a las fases mencionadas anteriormente, se describe a continuación los dominios que se deben desarrollar y los plazos de implementación establecidos:

1. Política de Seguridad
2. Aspectos organizativos de la seguridad de la información
3. Seguridad Ligada a los recursos humanos
4. Gestión de Activos
5. Control de accesos
6. Cifrado
7. Seguridad física y ambiental
8. Seguridad en la operativa
9. Seguridad en las telecomunicaciones
10. Adquisición, desarrollo y mantenimiento de los sistemas de información
11. Relaciones con los proveedores
12. Gestión de Incidentes de Seguridad de la Información
13. Aspectos de seguridad de la información en la gestión de continuidad del negocio

# NIVELES DE MADUREZ

**Fase I – Diagnostico**

**Fase II – Planeación**

Dentro de esta fase se relacionan los siguientes entregables:

* Diagnostico
* Alcance
* Actualizar manual de políticas de seguridad y privacidad de la información, debidamente aprobadas y socializadas al interior de la Entidad, por la alta Dirección.
* Inventario de activo de información.
* Informe de análisis de riesgos, matriz de riesgos, plan de tratamiento de riesgos
* Declaración de aplicabilidad
* Documento con el plan de comunicación, sensibilización y capacitación, con los respectivos soportes.
* Plan y estrategia de transición de IPv4 a IPv6

**Fase III – Implementación:**

* Documento con la estrategia de planificación y control operacional.
* Documento con el informe del plan de tratamiento de riesgos, que incluya la implementación de controles de acuerdo con lo definido en la declaración de aplicabilidad.
* Ejecutar y presentación de análisis de vulnerabilidades
	+ Resultado de análisis de vulnerabilidades
	+ Resultado de entrevistas con los responsables de los procesos y administradores de la plataforma tecnológica y Sistemas de Información.
	+ Matriz de Riesgos
	+ Plan de tratamiento de los riesgos
* Indicadores de gestión y de cumplimiento.
* Documento con el informe de la implementación del plan y la estrategia de transición de IPv4 a IPv6.

**Fase IV – Evaluación del Desempeño de la seguridad implementada en SII,**

* Plan de seguridad, evaluación y análisis del SGSI
* Auditoría Interna
* Evaluación del Plan de Tratamiento de Riesgo.

**Fase V – Mejora Continua.**

* Plan de seguimiento, evaluación y análisis para el SGSI
* Auditoría interna
* Comunicación de resultados y plan de mejoramiento
* Revisión y aprobación por la alta dirección

# INDICADORES

Dentro de los indicadores del Sistema de Gestión de Seguridad de la Información se definen los siguientes:

1. Nombre del indicador: Implementación del SGSI

Formula: % de Implementación de acuerdo con herramienta de diagnóstico.

Unidad: %

Meta: 80%

Periodicidad de medición: Trimestral

Entregables: Procedimientos, Formatos, Riesgos, Inventario de Activos, actas, programas y de más documentos generados dentro de la ejecución.

1. Nombre del indicador: Ejecución programa de capacitación y sensibilización

Formula: % de actividades programadas / actividades ejecutadas \* 100

Unidad: %

Meta: 90%

Periodicidad de medición: Trimestral

Entregables: Piezas gráficas. Listas de asistencias, programa de capacitación y sensibilización, presentaciones y demás que se generen.

**Elaboró: Aprobó:**

**YULI ANDREA PARRA AMAYA GLORIA ROCIO PEREIRA**

Oficial de Seguridad de la InformaciónJefe Subdirección de Desarrollo Organizacional