



GOBIERNO DE COLOMBIA



ARCHIVO
GENERAL
DE LA NACIÓN
COLOMBIA

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (SG-SPI) 2019

GOBIERNO DIGITAL

Grupo de Sistemas

Subdirección de tecnologías de la información archivística y documento electrónico
Archivo General de la Nación Jorge Palacios Preciado



1. PRESENTACIÓN

El presente documento se realiza con el fin de dar a conocer cómo se realizará la implementación y socialización del sistema de gestión de seguridad y privacidad de la información SG-SPI, el cual se encuentra alineado con la política de Gobierno Digital y el modelo integrado de planeación y gestión – MIPG y las disposiciones de la ley 1581 de 2012, decreto 1377 de 2013 y el decreto 886 de 2014.

2. ALCANCE

La vigencia del presente plan es 2019 y aplica para los 13 procesos que hacen parte del mapa de procesos definido en el manual de calidad del Archivo General de la Nación, siendo un (1) proceso estratégico, siete (7) procesos de apoyo, cuatro (4) procesos misionales, un (1) proceso de evaluación independiente

3. OBJETIVOS

3.1. Objetivo general

Elaborar el plan de seguridad y privacidad de la información alineado con los planes estratégicos del Archivo General de la Nación, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los activos de información.

3.2. Objetivos específicos

- Realizar el plan de trabajo específico, conforme a los resultados obtenidos del instrumento MSPI de MINTIC vigencia 2018.
- Alinear el SG-SPI con la ley de protección de datos personales y transparencia y acceso a la información pública.
- Asegurar la concordancia y alineación de las políticas del MIPG y el SG-SPI con los objetivos institucionales y la medición del SIPG.

4. RECURSOS

- **Humano:** La dirección general, la subdirección de tecnologías de la información archivística y documento electrónico, el grupo de sistemas, los líderes de proceso, un profesional especializado en seguridad informática, oficina de control interno.
- **Físico:** Infraestructura tecnológica, controles de acceso físico y bodegas.



5. RESPONSABLES

- La Dirección general
- La Subdirección de tecnologías de la información archivística y documento electrónico
- Grupo de sistemas
- Líderes de proceso
- Enlaces SIPG
- Equipo Sistema Integrado de planeación y gestión (SIPG)
- Profesional Especializado en seguridad informática
- Oficina de control interno

6. METODOLOGÍA DE IMPLEMENTACIÓN

La implementación, gestión y mejora continua del Sistema de gestión de seguridad y privacidad de la información SG-SPI, toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar), el modelo MSPI de MINTIC, el modelo integrado de planeación y gestión – MIPG y la norma ISO 27001:2013.



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



6.1. Actividades y entregables de las fases de la metodología de implementación

Fase I – Diagnostico

Dentro de esta fase se relacionan las siguientes actividades:

- ✚ Realizar un análisis del Estado actual del Sistema de Gestión de Seguridad y Privacidad de la información.

Dentro de esta fase se relacionan los siguientes entregables:

- Herramienta de Diagnóstico

Fase II – Planeación

Dentro de esta fase se relacionan las siguientes actividades:

- ✚ Participar en las actividades que la oficina asesora de planeación determine en la alineación del MIPG con los requisitos de la norma ISO 27001:2013.

Dentro de esta fase se relacionan los siguientes entregables:

- Manual de políticas actualizado, incluyendo la política sobre las condiciones de uso de las conexiones remotas por VPN u otro software.
- Procedimientos de seguridad y privacidad de la información normalizados en el sistema de gestión de calidad.
 - Procedimiento para la gestión de medios de soporte removibles de acuerdo con el esquema de calificación adoptado por la Entidad.
- Acto administrativo por el cual se adopta el MIPG y se fijan responsabilidades de los sistemas de gestión entre ellos el SG-SPI
- Guía metodológica para la calificación de la información articulada con la ley 1581 del 2012 y la ley 1712 del 2014.
- Integración del MSPI con el Sistema de Gestión documental
 - Propuesta del documento de tablas de control de acceso de conformidad con la normatividad vigente y el índice de información clasificada y reservada.
 - Registro de activos de información de conformidad con las tablas de retención documental y cuadros de clasificación documental vigentes del AGN actualizado.
- Guía metodológica para la gestión del riesgo
- Documento con el plan de comunicación, sensibilización y capacitación



Fase III – Implementación:

Dentro de esta fase se relacionan las siguientes actividades:

- ✚ Alinear el SGSI con la legislación de protección de datos personales y transparencia y acceso a la información pública.
- ✚ Dar continuidad a la implementación del sistema de Seguridad y Privacidad de la Información (SG-SPI).

Dentro de esta fase se relacionan los siguientes entregables:

- Documento con la estrategia de planificación y control operacional.
 - Plan de seguridad y privacidad de la información
 - Plan de tratamiento de riesgos de seguridad y privacidad de la información
 - Declaración de aplicabilidad
- Mapa de riesgos de seguridad digital.
- Informe de ejecución del plan de tratamiento de riesgos.
- Indicadores de gestión y de cumplimiento.
- Registro Nacional de Bases de Datos: Documento evidencia del registro de las bases de datos en la plataforma de la SIC.

Fase IV – Evaluación del Desempeño

Dentro de esta fase se relacionan las siguientes actividades:

- ✚ Seguimiento y monitoreo al cumplimiento de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública aspectos relacionados con el SG-SPI.
- ✚ Elaborar informes de desempeño trimestrales para el sistema de gestión de seguridad y privacidad de la información siguiendo los lineamientos del supervisor y la dirección general.
- ✚ Realizar las auditorías internas del sistema de gestión de seguridad y privacidad de la información.

Dentro de esta fase se relacionan los siguientes entregables:

- Matriz de seguimiento aplicación ley de protección de datos personales, transparencia y acceso a la información pública en cuanto a los aspectos relacionados con el SG-SPI
- Informes de desempeño para el SG-SPI incluyendo el resultado de las auditorías.



Fase V – Mejora Continua.

Dentro de esta fase se relacionan las siguientes actividades:

- Realizar el plan de mejoramiento resultado de las auditorias.

Dentro de esta fase se relacionan los siguientes entregables:

- Comunicación de resultados y plan de mejoramiento

7. DESAGREGADO DEL PLAN

PLAN DE ACCIÓN POR DEPENDENCIAS		
SUBDIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN ARCHIVÍSTICA Y DOCUMENTO ELECTRONICO		
GRUPO DE SISTEMAS		
ACTIVIDADES Y/O OBLIGACIONES	PRODUCTOS O EVIDENCIAS	MES
3. Realizar actividades tendientes a la implementación y mantenimiento del SGSI	<ol style="list-style-type: none"> 1. Realizar un análisis del Estado actual del Sistema de Gestión de Seguridad de la información. 2. Alinear del SGSI con la legislación de la ley de protección de datos personales y transparencia y acceso a la información pública 3. Dar continuidad a la implementación del sistema de Seguridad y Privacidad de la Información (SGSI). 4. Seguimiento y monitoreo al cumplimiento de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública aspectos relacionados con el SG.SPI 5. Participar en las actividades que la oficina asesora de planeación determine en la alineación del MIPG con los requisitos de la norma ISO 27001:2013 6. Elaboración del cronograma vigencia 2019 de mantenimiento y registro en la mesa de servicios 7. Diligenciar y tener actualizado el instrumento de control para la administración de certificados digitales (fecha de emisión, fecha de vencimiento y estados). 	<ol style="list-style-type: none"> 1. Abril 2. Febrero, abril, junio, agosto, octubre, Diciembre 3. Febrero a Diciembre 4. Trimestral 5. Trimestral 6. Marzo 7. Enero a Diciembre
6. Propender por la continuidad, funcionamiento, disponibilidad de los sistemas de información misionales y de apoyo de la Entidad	<ol style="list-style-type: none"> 1. Reportes de monitoreo y registros del estado de los servicios de infraestructura, que incluyan novedades o situaciones que puedan afectar la prestación del servicio. 2. Realizar las actividades de copias de respaldo de la información almacenada en los sistemas de información misionales y de apoyo de la entidad, permitiendo la restauración en caso de ser requerida. 3. Elaboración del cronograma vigencia 2019 de mantenimiento y registro en la mesa de servicios 4. Formulación de proyectos de Tecnologías de Información, sistemas de información, servicios digitales y servicios tecnológicos que permitan la modernización de la gestión 6. Realizar la creación de usuarios y asignación de permisos solicitados a través de la mesa de servicios acorde con el procedimiento establecido 7. Documento actualizado de las cuentas habilitadas y deshabilitadas para el acceso a los recursos TIC 8. Mantener actualizado el inventario de uso de licencias de los sistemas de información de la entidad. 	<ol style="list-style-type: none"> 1. Abril, Julio y Noviembre 2. Marzo, junio, septiembre, Diciembre 3. Febrero a Diciembre 4. Julio 6. Agosto 7. Enero a Diciembre 8. Enero a Diciembre

CONTROL DE CAMBIOS

FECHA	VERSIÓN	PROYECTÓ	REVISÓ	APROBÓ	DESCRIPCIÓN
23-05-2018	1.0	Heilin Guarizo Rodriguez.	Manuel Gomez Patiño.	Erika Rangel Palencia	Versión inicial
18-02-2019	2.0	Heilin Guarizo Rodriguez.	Laura Ruiz Gomez	Laura Ruiz Gomez	Actualización

