ARCHIVO GENERAL DE LA NACIÓN COLOMBIA

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ARCHIVO GENERAL DE LA NACIÓN JORGE PALACIOS PRECIADO

2021

Archivo General de la Nación Jorge Palacios Preciado.

www.archivogeneral.gov.co / información al ciudadano / sistema de peticiones, quejas y reclamos.

E-mail: contacto@archivogeneral.gov.co - Cr. 6 No. 6-91 Tel: 328 2888 - Fax: 337 2019

Bogotá D.C., Colombia. Fecha: 31-01-2021- V:1

La cultura es de todos Mincultura

Titulo	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN				
Fecha actualización:	Noviembre del 2020				
Sumario	Este documento presenta un Plan de Seguridad y Privacidad de la Información que apoye el establecimiento del Sistema de Gestión de Seguridad y Privacidad de la Información del Archivo General de la Nación, acorde a los requerimientos del modelo de seguridad de la estrategia de Gobierno Digital, los requerimientos del negocio y en cumplimiento de las disposiciones legales vigentes.				
Palabras claves:	Políticas, Buenas prácticas, Controles, Guía				
Formato:	PDF		Lenguaje:		Español
Código:	GIT-M-02	Versión:	3	Estado:	
Categoría:	Documento Técnico				
Autor:	Jaime Alberto Duarte Hoyos				
Revisó:	Omar Villarreal Osorio				
Presentación aprobación					
Aprobó:	Comité Institucional de Gestión del Desempeño				
Información Adicional:					

CONTENIDO

INTRODUCCIÓN

En este plan se hace referencia del habilitador **Seguridad y Privacidad** por lo cual es necesario hablar del **Modelo de Seguridad y Privacidad de la Información** que hace parte de la antigua estrategia Gobierno en Línea – **GEL.** En este modelo se propone un conjunto de guías prácticas que contribuyen a mitigar los riesgos asociados a la seguridad de la información, así como velar por la preservación de la confidencialidad, integridad y disponibilidad de los activos de información con los que cuenta la Entidad. En tal sentido, la seguridad de la información actúa como eje transversal e integral para el desarrollo de objetivos y metas propuestas a través de estructuras de relaciones y procesos organizacionales que velan por la protección de la información de la entidad.

En el presente documento se deja plasmado en forma detallada todas y cada una de las actividades que requiere el Modelo de Seguridad y Privacidad de la Información, para ser implementada en el año 2021 en el Archivo General de la Nación.

1. OBJETIVO

1.1.OBJETIVO GENERAL

Establecer un Plan de Seguridad y Privacidad de la Información que apoye el establecimiento del Sistema de Gestión de Seguridad y Privacidad de la Información del Archivo General de la Nación, acorde a los requerimientos del modelo de seguridad de la estrategia de Gobierno Digital, los requerimientos del negocio y en cumplimiento de las disposiciones legales vigentes.

1.2.OBJETIVO ESPECIFICOS

- Definir las etapas para establecer la estrategia de seguridad de la información de la entidad.
- Apalancar la implementación del Sistema de Gestión de Seguridad de la Información de la entidad de acuerdo con los requerimientos establecidos en el modelo de seguridad de la estrategia de Gobierno Digital.
- Establecer lineamientos para la implementación y/o adopción de mejores prácticas de seguridad en la Institución.
- Optimizar la gestión de la seguridad de la información al interior de la entidad.

2. ALCANCE

El plan comprende las directrices trazadas en Seguridad y Privacidad de la Información, como habilitador transversal de la Política de Gobierno Digital[1] bajo el Modelo de Seguridad y Privacidad de la Información – MSPI, establecidos por el Ministerio de las Tecnologías de la Información y las Comunicaciones – MINTIC, alineado con las buenas prácticas descritas en la norma ISO 27001:13. De igual manera da alcance a la implementación de lo dispuesto en la legislación vigente sobre protección y tratamiento de datos personales[2].

3. DEFINICIONES

Para la adecuada gestión del Plan de Seguridad y privacidad de la Información se debe manejar con propiedad los siguientes términos:

Activo de información: aquello que es de alta validez y que contiene información vital de la empresa que debe ser protegida.

Amenaza: Es la causa potencial de un daño a un activo de información.

Anexo SL: Nuevo esquema definido por International Organization for Standardization - ISO para todos los Sistemas de Gestión acorde al nuevo formato llamado “Anexo SL”, que

[1] Decreto 1008 de 2018 “Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones”
[2] Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”, con sus respectivas modificatorias, reglamentación y vigencia

proporciona una estructura uniforme como el marco de un sistema de gestión genérico.

Análisis de riesgos: Utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos.

Causa: Razón por la cual el riesgo sucede.

Ciclo de Deming: Modelo mejora continua para la implementación de un sistema de mejora continua.

Colaborador: Es toda persona que realiza actividades directa o indirectamente en las instalaciones de la entidad, Trabajadores de Planta, Trabajadores Temporales, Contratistas, Proveedores y Practicantes.

Confidencialidad: Propiedad que determina que la información no esté disponible a personas no autorizados

Controles: Son aquellos mecanismos utilizados para monitorear y controlar acciones que son consideradas sospechosas y que pueden afectar de alguna manera los activos de información.

Disponibilidad: Propiedad de determina que la información sea accesible y utilizable por aquellas personas debidamente autorizadas.

Dueño del riesgo sobre el activo: Persona responsable de gestionar el riesgo.

Impacto: Consecuencias de que la amenaza ocurra. Nivel de afectación en el activo de información que se genera al existir el riesgo.

Incidente de seguridad de la información: Evento no deseado o inesperado, que tiene una probabilidad de amenazar la seguridad de la información.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

Oficial de Seguridad de la Información: Persona encargada de administrar, implementar, actualizar y monitorear el Sistema de Gestión de Seguridad de la Información.

Probabilidad de ocurrencia: Posibilidad de que se presente una situación o evento específico.

Responsables del Activo: Personas responsables del activo de información.

Riesgo: Grado de exposición de un activo que permite la materialización de una amenaza.

Riesgo Inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

Riesgo Residual: Nivel de riesgo remanente como resultado de la aplicación de medidas de seguridad sobre el activo.

PSE: Proveedor de Servicios Electrónicos, es un sistema centralizado por medio del cual las empresas brindan a los usuarios la posibilidad de hacer sus pagos por Internet.

SARC: Siglas del Sistema de Administración de Riesgo Crediticio.

SARL: Siglas del Sistema de Administración de Riesgo de Liquidez.

SARLAFT: Siglas del Sistema de Administración del Riesgo de Lavado de Activos y

Financiación del Terrorismo.

SARO: Siglas del Sistema de Administración de Riesgos Operativos.

Seguridad de la Información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información (ISO 27000:2014).

SGSI: Siglas del Sistema de Gestión de Seguridad de la Información.

Sistema de Gestión de Seguridad de la información SGSI: permite establecer, implementar, mantener y mejorar continuamente la gestión de la seguridad de la información de acuerdo con los requisitos de la norma NTC-ISO-IEC 27001.

Vulnerabilidad: Debilidad de un activo o grupo de activos de información que puede ser aprovechada por una amenaza. La vulnerabilidad de caracteriza por ausencia en controles de seguridad que permite ser explotada.

4. MARCO NORMATIVO

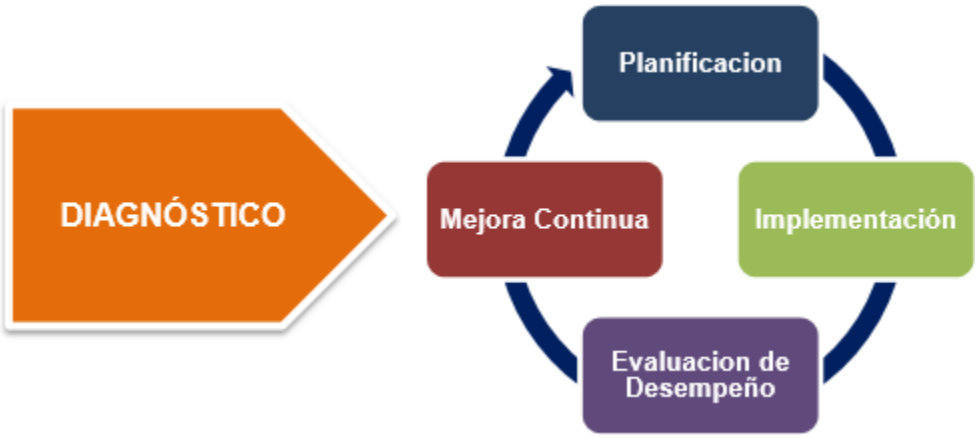
Para la construcción de este manual se tiene como base, la norma ISO – IEC 27001:2013 Sistema de Gestión de la Seguridad de la Información, el modelo de gestión de la seguridad de la información y la política de información del Archivo General de la Nación.

5. METODOLOGIA IMPLEMENTACION MODELO DE SEGURIDAD

5.1. CICLO OPERACIÓN

El Modelo de Seguridad y Privacidad de la Información de la Estrategia de Gobierno Digital observa el siguiente ciclo de operación que contempla cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información[3].

3 Modelo de Seguridad y Privacidad, MINTIC, Pág. 1-2



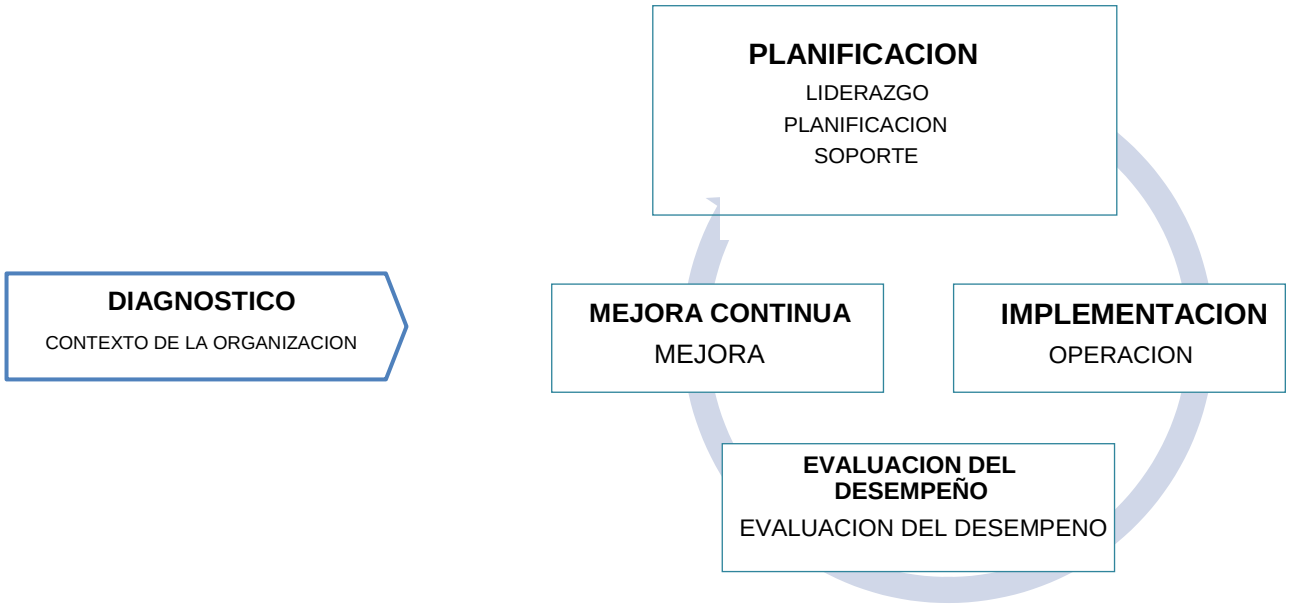
Ciclo de operación Modelo de Seguridad y Privacidad de la Información
Fuente: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

- **Fase Diagnostico**: Permite identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información
- **Fase Planificación (P**lanear**):** En esta fase se establecen los objetivos a alcanzar y las actividades del proceso susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los objetivos.
- **Fase Implementación (H**acer**):** En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.
- **Fase Evaluación de desempeño (V**erificar**):** Una vez implantada la mejora, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas.
- **Fase Mejora Continua (A**ctuar**):** Se analizan los resultados de las acciones implementadas y si estas no se cumplen los objetivos definidos se analizan las causas de las desviaciones y se generan los respectivos planes de acciones.

5.2.ALINEACION NORMA ISO 27001:2013 vs CICLO DE OPERACION

Aunque en la norma ISO 27001:2013 no se determina un modelo de mejora continua (PHVA) como requisito para estructurar los procesos del Sistema de Gestión de Seguridad de la Información, la nueva estructura de esta versión se puede alinear con el ciclo de mejora continua de las modelos de gestión de la siguiente forma:

Norma ISO 27001:2013 alineado al Ciclo de mejora continua



Fuente: Elaborada con base en la información publicada en la página web *http://www.welivesecurity.com/la-es/2013/10/09/publicada-iso-270002013-cambios-en-la- norma-para-gestionar-la-seguridad-de-la-informacion/*

El siguiente cuadro muestra la relación entre las fases del ciclo de operación del Modelo de Seguridad y Privacidad de la Información (Diagnostico, Planificación, Implementación, Evaluación, Mejora Continua) y la estructura de capítulos y numerales de la norma ISO 27001:2013:

Tabla 1. Fases Ciclo Operación vs Estructura ISO 27001:2013

Fase	Capitulo ISO 27001:2013[4]
Diagnostico	Contexto de la Organización
Planificación	Liderazgos Planificación Soporte
Implementación	Operación
Evaluación de desempeño	Evaluación de desempeño
Mejora Continua	Mejora

5.1.1. Fase DIAGNOSTICO en la norma ISO 27001:2013.

En el **capítulo 4** - **Contexto de la organización** de la norma ISO 27001:2013, se

[4] NTC-ISO-IEC 27001:2013, Pág. 1-12

determina la necesidad de realizar un análisis de las cuestionas externas e internas de la organización y de su contexto, con el propósito de incluir las necesidades y expectativas de las partes interesas de la organización en el alcance del SGSI.

5.1.2. Fase PLANEACION en la norma ISO 27001:2013

En el capítulo 5 - Liderazgo, se establece las responsabilidades y compromisos de la Alta Dirección respecto al Sistema de Gestión de Seguridad de la Información y entre otros aspectos, la necesidad de que la Alta Dirección establezca una política de seguridad de la información adecuada al propósito de la organización asegure la asignación de los recursos para el SGSI y que las responsabilidades y roles pertinentes a la seguridad de la información se asignen y comuniquen.

En el capítulo 6 - Planeación, se establece los requerimientos para la valoración y tratamiento de riesgos de seguridad y para la definición de objetivos viables de seguridad de la información y planes específicos para su cumplimiento.

En el capítulo 7 - Soporte se establece que la organización debe asegurar los recursos necesarios para el establecimiento, implementación y mejora continua Sistema de Gestión de Seguridad de la Información.

5.1.3. Fase IMPLEMENTACION en la norma ISO 27001:2013.

En el capítulo 8 - Operación de la norma ISO 27001:2013, se indica que la organización debe planificar, implementar y controlar los procesos necesarios para cumplir los objetivos y requisitos de seguridad y llevar a cabo la valoración y tratamiento de los riesgos de la seguridad de la información.

5.1.4. Fase EVALUACION DEL DESEMPEÑO

En la norma ISO 27001:2013. En el capítulo 9 - Evaluación del desempeño, se define los requerimientos para evaluar periódicamente el desempeño de la seguridad de la información y eficacia del sistema de gestión de seguridad de la información.

5.1.5. Fase MEJORA CONTINUA

En la norma ISO 27001:2013. En el capítulo 10 - Mejora, se establece para el proceso de mejora del Sistema de Gestión de Seguridad de la Información, que a partir de las no-conformidades que ocurran, las organizaciones deben establecer las acciones más efectiva para solucionarlas y evaluar la necesidad de acciones para eliminar las causas de la no conformidad con el objetivo de que no se repitan.

5.3.FASES I: DIAGNOSTICO

Objetivo	Identificar el estado del Archivo General de la Nación con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información

Metas	Actividades \ Instrumentos \ Resultados
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior del AGN.	**Diagnóstico** de la **situación actual** de la entidad con relación a la gestión de seguridad de la información. **Diagnostico nivel de cumplimiento** de la entidad frente a los objetivos de control y controles establecidos en el Anexo A de la **norma ISO 27001:2013**. **Valoración estado actual** de la gestión de seguridad de la entidad con base en el Instrumento de Evaluación MSPI de MINTIC.
Identificar el nivel de madurez de seguridad y privacidad de la información en el AGN	**Valoración** del **nivel de estratificación** de la entidad frente a la seguridad de la información **con base en** el método planteado en el documento '*ANEXO 3: ESTRATIFICACIÓN DE ENTIDADES*' del modelo seguridad de la información para la estrategia de Gobierno en Línea 2.0. **Valoración** del **nivel de madurez** de seguridad y privacidad de la información en la entidad de acuerdo con los lineamientos establecidos en el capítulo '*MODELO DE MADUREZ*' del documento Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea.
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	**Ejecución prueba de vulnerabilidades** con el fin de identificar el nivel de seguridad y protección de los activos de información de la entidad y definición de planes de mitigación.

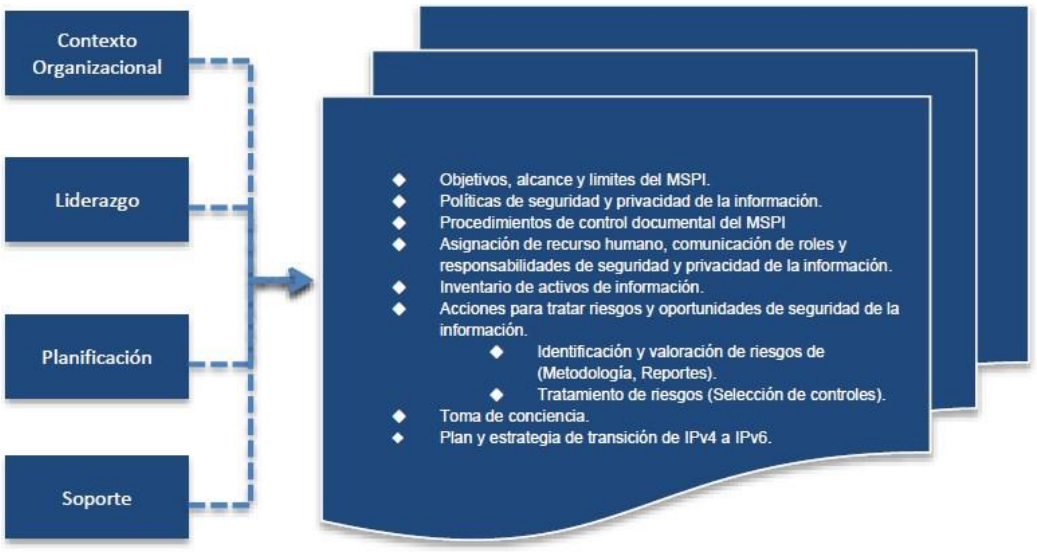
Para la recolección de la información, en esta fase se utilizarán mecanismo como:

- Diligenciamiento de cuestionarios con el objetivo de determinar el nivel de cumplimiento del AGN con relación a los dominios de la norma ISO/IEC 27001:2013.
- Documentación existente en el sistema de calidad de la entidad relacionada con la información de las partes interesadas de la entidad y los roles y funciones asociados a la seguridad de la información.
- Fuentes externas, como las guías de autoevaluación, encuesta y estratificación dispuestas por la estrategia de Gobierno en Línea Ministerio de Tecnologías de la

Información y las Comunicaciones.

5.4.FASES II: PLANIFICACION

Objetivo	Definir la estrategia metodológica, que permita establecer el alcance, objetivos, procesos y procedimientos, pertinentes a la gestión del riesgo y mejora de seguridad de la información, en procura de los resultados que permitan dar cumplimiento con las metas propuestas del SGSI.



Fase de planificación modelo de seguridad

Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno en Línea

Metas	Actividades \ Instrumentos \ Resultados
Realizar un análisis de Contexto y factores externos e internos de la Entidad en torno a la seguridad de la información.	**Realizar** un **Análisis de Contexto** de la entidad entorno a la seguridad de la información teniendo en cuenta el capítulo 4. CONEXTO DE LA ORGANIZACIÓN de la norma ISO 27001:2013, con el fin de poder determinar las cuestiones externas e internas de la organización que son pertinentes para la implementación del Sistema de Gestión de Seguridad de la Información.

Definir el alcance del SGSI de la entidad	**Definir** el **alcance** del **Sistema de Gestión de Seguridad de la Información** 'SGSI' del AGN aprobado por la Alta Dirección y socializado al interior de la Entidad. Definir el alcance del SGSI, en el cual se establece los límites y la aplicabilidad del Sistema de Gestión de Seguridad de la Información.
Definir Roles, Responsables y Funciones de seguridad y privacidad de la información	**Adicionar** las **funciones de seguridad** de la información al **Comité de Riesgos** del AGN y formalizarlas mediante acto administrativo. **Establecer** el **Rol** de **Oficial de Seguridad** de la información. **Definir** un **marco de gestión que contemple roles y responsabilidades** para la implementación, administración, operación y gestión de la seguridad de la información en el AGN. **Definir la estructura organizacional** de la Entidad que contendrá los roles y responsabilidad **pertinentes a la seguridad** de la información.
Definir la metodología de riesgos de seguridad de la información	**Definir Metodología** de Valoración de **Riesgos de Seguridad**. **Integrar** la **metodología** definida con la metodología de riegos operativos del AGN. **Implementar** un **sistema de información** para la administración y gestión de los riesgos de seguridad de la entidad.
Elaborar las políticas de seguridad y privacidad de la información de la entidad	**Elaborar Política General de Seguridad y Privacidad** la cual debe ser aprobada por la Alta Dirección y socializada al interior del AGN. **Elaborar** el **manual de Políticas de Seguridad y Privacidad de la Información**, que corresponde a un documento que contiene las políticas y los lineamientos que se implementaran en el AGN, con el objetivo de proteger la Confidencialidad, Integridad, Disponibilidad, Trazabilidad, Autenticidad de la información. Estas políticas deben ser aprobadas por la Alta Dirección y socializadas al interior del AGN.

Elaborar documentación de operación (formatos de procesos, procedimientos y documentos debidamente definidos y establecidos) del sistema de seguridad de la información	**Elaborar** los **documentos de operación del sistema de seguridad** de la información, tales como: • Declaración de aplicabilidad • Procedimiento y/o guía de identificación y clasificación de activos de información. • Procedimiento Continuidad del Negocio, Procedimientos operativos para gestión de TI • Procedimiento para control de documentos (SGI) • Procedimiento para auditoría interna (SGI) • Procedimiento para medidas correctivas (SGI) • Procedimiento para la gestión de eventos e incidentes de seguridad de la información • Procedimiento para la gestión de vulnerabilidades de seguridad de la información. • Entre otros.
Identificar y valorar activos de información	**Realizar** la **identificación** y **valoración** de los **activos de información** de la entidad de acuerdo con su nivel de criticidad de acuerdo con el alcance del SGSI. Documentar el inventario de activos de información de la entidad.
Identificar, valorar y tratar los riesgos de seguridad de la información de la entidad	**Realizar** la **identificación** y **valoración** de los **riesgos** transversales de **seguridad** de la información y definir los respectivos planes de tratamiento. Realizar la valoración de riesgos de seguridad de la información de acuerdo con el alcance del SGSI. Definir los planes de acción que incluya los controles a implementar con el objetivo de mitigar los riesgos identificados en el proceso de valoración de riesgos. Para la seleccionar de los controles, se tomará como base los objetivos de control y los controles establecidos en el Anexo A de la norma ISO/IEC 27001:2013.
Establecer plan de capacitación, comunicación y sensibilización de seguridad de la información.	**Elaborar plan** anual de **capacitación** y sensibilización anual de seguridad de la información
Establecer Plan de diagnóstico de IPv4 a IPv6	**Realizar** el **diagnóstico** para la **transición** de la entidad de **IPv4 a IPv6**. Documentar el Plan de diagnóstico para la transición de IPv4 a IPv6.

5.5.FASES III: IMPLEMENTACION

Objetivo	Llevar acabo la implementación de la fase de planificación del SGSI, teniendo en cuenta para esto los aspectos más relevantes en los procesos de implementación del Sistema de Gestión de Seguridad de la Información del Archivo General de la Nación.

Fase de implementación modelo de seguridad

Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno en Línea

Metas	Actividades \ Instrumentos \ Resultados
Establecer el plan de implementación de seguridad de la información	**Implementar** el **plan de implementación** del **modelo de seguridad y privacidad** de la información el cual debe ser revisado y aprobado por el comité de riesgos
Ejecutar el plan de tratamiento de riesgos	**Ejecutar** el **plan de tratamiento de los riesgos** transversales de seguridad de la información identificados en la fase de planificación que fue presentado en el comité de riegos.
Ejecutar del plan y estrategia de transición de IPv4 a IPv6.	**Ejecutar plan de transición a IPv6** y elaborar informe de Implementación.
Establecer indicadores de gestión de seguridad	**Definir los indicadores** para medir la gestión del modelo de seguridad y establecer los mecanismos para su medición. Estos indicadores deben permitir verificar la eficacia y efectividad de los controles implementados para mitigar los riesgos de seguridad de la entidad.

Implementar procedimiento de gestión de eventos e incidentes de seguridad	**Implementar** el procedimiento y los mecanismos para la **gestión de los eventos e incidentes de seguridad** de la información**.**
Implementar procedimiento de gestión de vulnerabilidades	**Implementar** el procedimiento y los mecanismos para la **gestión de vulnerabilidades seguridad** de la información**.**
Ejecutar plan de capacitación y sensibilización de seguridad	**Ejecutar** el plan anual de capacitación, socialización y sensibilización de seguridad de la información
Ejecutar pruebas semestrales de vulnerabilidades e intrusión	**Ejecutar** el plan semestral de **pruebas vulnerabilidades** e intrusión con el objetivo de identificar el nivel de protección de los activos de información del AGN. Para tal efecto, se deberá tener en cuenta los respectivos requerimientos de seguridad relacionados con pruebas de vulnerabilidades establecidos por el l Archivo General de la Nación
Ejecutar pruebas de Ethical Hacking	**Ejecutar** pruebas semestrales de **Ethical Hacking** orientadas a poder determinar los niveles de riesgo y exposición de la organización ante atacantes interno o externo que puedan a comprometer activos críticos de la entidad y con esto generar interrupción en los servicios, afectar la continuidad del negocio y/o acceder de forma no autorizada a la información sensible o clasificada de la entidad o de carácter personal de los trabajadores o terceros que laboren para la entidad.
Ejecutar pruebas de Ingeniera Social	**Ejecutar** pruebas semestrales de **ingeniería social** orientadas a verificar aspectos como: (i) los protocoles internos de seguridad, (ii) el nivel de concientización de los funcionarios y terceros que laboren en la entidad sobre temas de seguridad de la información, (iii) el conocimiento y/o cumplimiento de las políticas de seguridad y privacidad de la información de la entidad y (iv) el nivel de exposición de la información publicada en internet del AGN y de sus funcionarios.

5.6.FASES IV: EVALUACION DE DESEMPEÑO

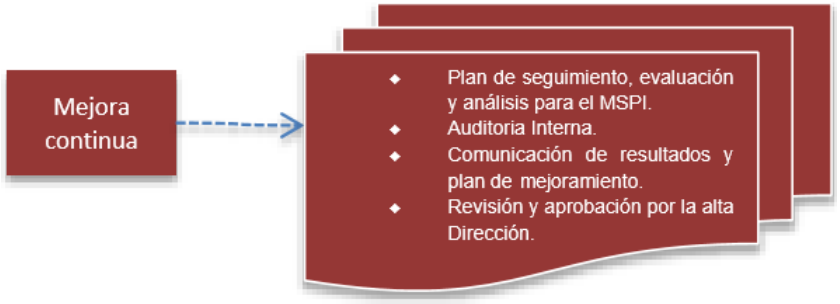
Objetivo	Evaluar el desempeño y la eficacia del SGSI, a través de instrumentos que permita determinar la efectividad de la implantación del SGSI.

Fase Evaluación Desempeño modelo de seguridad
Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno en Línea

Metas	Actividades \ Instrumentos \ Resultados
Ejecución de auditorías de seguridad de la información	**Ejecución de auditorías** del modelo de seguridad y de temas normativos y de cumplimiento de seguridad de la información aplicables a la entidad, de acuerdo con el plan de auditoria revisado y aprobado por la Alta Dirección. Las auditorías internas se deberán llevar a cabo para la revisión del Sistema de Gestión de Seguridad 'SGSI' de la Información implementado en la entidad, con la finalidad de verificar que los objetivos de control, controles, procesos y procedimientos del SGSI cumpla con los requisitos establecidos en la norma ISO 27002:2013 y los del MSPI.
Plan de seguimiento, evaluación y análisis de SGSI	**Elaboración documento** con el **plan de seguimiento, evaluación y análisis del SGSI** revisado y aprobado por el Comité de Riesgos.

5.7.FASES V: MEJORA CONTINUA

Objetivo	Consolidar los resultados obtenidos del componente 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 SGSI



Fase Mejora Continua modelo de seguridad
Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno en Línea

Metas	Actividades \ Instrumentos \ Resultados
Diseñar plan de mejoramiento	**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 Sistema de Gestión de Seguridad de la Información.

6. IMPLEMENTACION MODELO DE SEGURIDAD ALINEADO A RIESGOS

6.1.PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2021

FASE I: ANÁLISIS DE BRECHA																	
ANÁLISIS GAP ISO 27001 y MSPI																	
Objetivo	Actividades	Productos	Responsables	Mes													Total
				Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic		
Elaborar el análisis GAP (análisis de brecha) frente a la norma ISO 27000 y el Modelo de seguridad y privacidad de la información MSPI del AGN	Conocer el negocio del AGN, procesos definidos en el alcance, recursos que soportan los procesos, responsables del SGSI, tecnologías utilizadas y terceras partes involucradas	• Informe de resultados del análisis, evaluación y diagnóstico de la situación actual e Identificación de brechas para cada dominio de ISO/IEC 27001:2013 y MSPI alineado con Gobierno Digital. • Recomendaciones sobre las brechas identificadas en el instrumento de evaluación y nivel de madurez en línea base de seguridad (MPSI).	Oficial de seguridad de la Informacion														
	Identificar y entender el contexto interno y externo del AGN, partes interesadas y factores críticos de éxito																
	Realizar entrevistas y recopilación de documentación con las personas responsables en los procesos de ejecutar las actividades contempladas en los controles, para identificar la forma como se ejecutan actualmente dichos controles					1			1			1			1	4
	Realizar un análisis GAP o de brecha al SGSI, siguiendo como marco de referencia la norma ISO 27001:2013, a fin de establecer el nivel de cumplimiento de la misma de acuerdo con el alcance definido por el AGN y establecer el estado deseado del sistema																
	Estimar el nivel de cumplimiento de las normativas externas aplicables y políticas internas del AGN.																
	Elaborar el plan de recomendaciones para el cierre de las brechas identificadas y lograr un nivel de madurez aceptable para el AGN	Plan de Acción para el cierre de las brechas detectadas	Oficial de seguridad de la Informacion			1			1			1			1	4
	Revisión de autorizaciones, avisos de privacidad, solicitudes, quejas y reclamos, procedimientos de gestión de incidentes y demás relacionados al cumplimiento de la ley de protección de datospersonales desde la perspectiva de responsabilidad demostrada (se deben tener en cuenta la existencia de otras leyes o normativas que tengan relación como la Ley de transparencia).	Informe de diagnóstico de cumplimiento de ley 1581 de 2012 y responsabilidad demostrada	Oficial de seguridad de la Informacion			1			1			1			1	4
	Realizar el diligenciamiento del instrumento de evaluación, identificación y nivel de madurez en línea base de seguridad (MSPI), de acuerdo con lo establecido por Gobierno Digital	Instrumento de evaluación diligenciado, identificación y nivel de madurez en línea base de seguridad (MSPI), de acuerdo con lo establecido com las politicas de Gobierno Digital	Oficial de seguridad de la Informacion			1			1			1			1	4

FASE II: ESTABLECIMIENTO DEL SGSI																	
DISEÑO DE POLITICAS Y PROCEDIMIENTOS DE SEGURIDAD																	
	Construir el manual de políticas y procedimientos respetando la estructura propuesta por la norma ISO 27000, de acuerdo con: Resultados del análisis GAP. Requerimientos y normativas que deba satisfacer al AGN Las buenas prácticas de seguridad,	Documento de la definición de los objetivos del SGSI Documento de la definición del alcance del SGSI. Documento del procedimiento actual de Revisión por la OAP del Sistema Integrado de Gestión de Calidad - SIGC frente a los requisitos del SGSI	Oficial de seguridad de la Informacion						1						1	2
Diseñar políticas y procedimientos de seguridad conforme la estructura propuesta por la norma ISO 27000 alineados al Sistema Integrado de Gestión de la Entidad	Como mínimo se deberá elaborar o actualizar las políticas y procedimientos alineado a lo exigido por la norma ISO 27001:2013 y por MPSI. **Políticas:** 1. BYOD 2. Capacitación y Sensibilización en Seguridad de Información 3. Clasificación de la información 4. Confidencialidad 5. Contraseñas 6. Control de acceso 7. Controles criptográficos 8. Copias de seguridad 9. Disponibilidad 10. Dispositivo sobre dispositivos móviles y teletrabajo 11. Eliminación y destrucción 12. Ética empresarial 13. Gestión de Activos 14. Gestión de cambios 15. Gestión de Incidentes de Seguridad de Información y Datos Personales 16. Integridad 17. No repudio 18. Pantalla y escritorio limpios 19. Registro y Auditoria 20. Seguridad de la información y objetivos 21. Seguridad para proveedores 22. Transferencia de información 23. Tratamiento de Datos Personales 24. Uso aceptable **Procedimientos:** **1.** Adquisición, desarrollo y mantenimiento de sistemas de información 2. Aseguramiento de servicios en la red 3. Capacitación y sensibilización del personal 4. Control de acceso físico 5. Control de software 6. Control para código malicioso 7. Controles criptográficos 8. Gestión de cambios 9. Gestión de capacidad 10. Gestión de llaves criptográficas 11. Gestión de usuarios y contraseñas 12. Identificación y clasificación de activos 13. Ingreso y desvinculación del personal 14. Mantenimiento de equipos 15. Protección de activos 16. Retiro de activos 17. Separación de ambientes 18. Transferencia de información 19. Acciones correctivas 20. Auditoría interna 21. Gestión de incidentes 22. Ingreso seguro a los sistemas de información 23. Continuidad de negocio 24. Operación para gestión de ti 25. Trabajo en áreas seguras	• Definición Indicadores de Gestión • Entrega como mínimo de las 24 políticas y 25 procedimientos anteriormente enunciados de seguridad de la información, considerados en los 14 dominios de la norma ISO 27001:2013 y el MSPI.	Oficial de seguridad de la Informacion												1	1

FASE II: ESTABLECIMIENTO DEL SGSI																
DEFINICION DE LA ESTRUCTURA ORGANIZACIONAL SEGURIDAD DE LA INFORMACION																
Emitir una propuesta con las recomendaciones sobre la estructura y ubicación en el organigrama institucional de la función de seguridad de la información ajustada al contexto interno del AGN y teniendo en cuenta sus necesidades.	Proponer el perfil y competencias necesarias del personal a cargo del SGSI y capacitación necesaria para el mantenimiento de la organización de la seguridad de la información. Realizar reuniones con la alta dirección y definir una propuesta sobre la estructura organizacional, incluyendo los roles y responsabilidades de los interesados. Proponer las funciones y responsabilidades de los perfiles a continuación: • Seguridad Informatica • Analista de Monitoreo e Incidentes • Analista SGSI. • Analista de tecnología de seguridad. • Administración de accesos. • Ingeniero de redes.	•Documento propuesto de la estructura organizacional de SI con las competencias técnicas y organizacionales que debe tener cada uno de los integrantes en la organización de la seguridad, •Propuesta del plan de entrenamiento para lograr las competencias requeridas para el mantenimiento del sistema de gestión de seguridad de la información. •Propuesta de Organigrama del SGSI y MPSI. •Propuesta de Roles y responsabilidades del SGSI y MPSI	Oficial de seguridad de la Informacion			1										1
FASE II: ESTABLECIMIENTO DEL SGSI																
DISEÑO DEL PROCESO DE GESTIÓN DE INCIDENTES DE SEGURIDAD																
Definir y documentar formalmente el proceso de gestión de incidentes del SGSI	Proponer el modelo del proceso para la gestión de incidentes, incorporando los recursos existentes en el AGN, como canales de comunicación, mesas de ayuda, políticas y procedimientos relacionados con la continuidad de negocio: • Revisión del proceso actual de manejo de incidentes •Identificación de mejores prácticas (ITIL, DRII, FIRST) • Desarrollo de procedimientos, instructivos y guías relacionados. • Elaboración del plan de implementación del modelo gestión de incidentes • Aprobación y divulgación	Procedimiento para la gestión de incidentes de seguridad de la información	Oficial de seguridad de la Informacion			1			1			1			1	4

FASE II: ESTABLECIMIENTO DEL SGSI																
DEFINICION E IMPLEMENTACIÓN DEL MODELO DE MEDICIÓN DEL SGSI																
Crear, definir e implementar los indicadores (métricas) adecuados para medir la madurez, eficiencia, eficacia, implantación o impacto de controles de seguridad de la información Se deberá tener como referencia la norma ISO 27004:2016	Identificar cuáles son las métricas e indicadores adecuadas que resulten útiles para el seguimiento de los resultados y la dirección de los recursos y la demostración de evidencia de gestión de riesgos. El modelo deberá contener como mínimo los siguientes elementos • Indicadores para la medición del SGSI y MPSI. • Indicadores de la efectividad de los principales controles de seguridad. • Fichas técnicas de los indicadores (fuentes de datos, responsables, periodicidad, meta, etc.) • Procedimiento de medición. análisis y evaluación de las mediciones (acciones correctivas) • Roles y responsabilidades. • Seguridad de los registros Una vez aprobado el modelo se deberá ejecutar el procedimiento de medición abarcando todos los indicadores, análisis y propuesta de las acciones correctivas a que haya lugar	Definición de indicadores de gestión, como mínimo deberán ser 15 indicadores. • Modelo de medición del SGSI y MPSI. • Informe de la medición.	Oficial de seguridad de la Informacion					1								1
FASE III: ANÁLISIS DE RIESGOS																
IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN																
Identificar los activos de información de los procesos de negocio AGN incluidos en el alcance. Construir la matriz de clasificación de los activos de información de acuerdo con los requerimientos de confidencialidad definidos y establecer los requerimientos exigidos por la norma ISO27001:2013 y normas relacionadas ISO 27002 e ISO 27005	Realizar el levantamiento de las bases de datos de información personal basados en la guía de responsabilidad demostrada y la ley de protección de datos personales, para el reporte ante la Superintendencia de Industria y Comercio (SIC) cumpliendo con los lineamientos para su presentación Identificar los activos de información, según la ISO27005 se clasificación en dos tipos	· Inventario de activos de información. · Inventario de bases de datos personales.	Oficial de seguridad de la Informacion					1								1

FASE III: ANÁLISIS DE RIESGOS																
ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN																
Elaborar el mapa de riesgos de la organización basada en los lineamientos establecidos en la norma ISO 31000 e ISO 27005:2008	En base al levantamiento de los activos de información se deberá proceder a ejecutar el análisis de riesgos, contemplando las siguientes actividades: • Identificación del Nivel de riesgo Aceptable. • Plan de tratamiento de Riesgos. • Presentación y socialización de resultados • Determinar la declaración de aplicabilidad, en concordancia con la cláusula 6.1.3 de ISO 27001 versión 2013	Definición de la metodología de Análisis de riesgos de Seguridad de la Información. Documento de análisis de riesgos que incluya identificación de amenazas y vulnerabilidades, Matriz de Riesgos del proceso. Plan de tratamiento de riesgos de seguridad de la información. Informe de Análisis de riesgos para los procesos definidos en el alcance. Declaración de aplicabilidad (SOA)	Oficial de seguridad de la Informacion						1								1

FASE IV: PRUEBAS DE SEGURIDAD																	
HACKING ÉTICO Y PENETRACIÓN																	
Mediante estas pruebas se busca evidenciar las vulnerabilidades que existen dentro de la configuración física y lógica de los sistemas informáticos de la entidad.	**HACKING ÉTICO**: • Recolección de información. • Identificación de sistemas y servicios. • Identificación y verificación de vulnerabilidades. • Presentación informes de resultados.	Informe final de Hacking Ético y las recomendaciones que se dan a conocer al AGN sobre las pruebas de hacking ético definidas en el alcance Informe Técnico de Pruebas del análisis de vulnerabilidad y test intrusión Informe Ejecutivo de Pruebas del análisis de vulnerabilidad y test intrusión Informe con las posibles soluciones frente a las vulnerabilidades encontradas. Recomendaciones sobre aspectos a mejorar a nivel de cultura de seguridad	Oficial de seguridad de la Informacion				1				1				1	3
FASE IV: PRUEBAS DE SEGURIDAD																	
HACKING ÉTICO Y PENETRACIÓN																	
Mediante estas pruebas se busca evidenciar las vulnerabilidades que existen dentro de la configuración física y lógica de los sistemas informáticos de la entidad.	**HACKING ÉTICO**: • Recolección de información. • Identificación de sistemas y servicios. • Identificación y verificación de vulnerabilidades. • Presentación informes de resultados.	Informe final de Hacking Ético y las recomendaciones que se dan a conocer al AGN sobre las pruebas de hacking ético definidas en el alcance Informe Técnico de Pruebas del análisis de vulnerabilidad y test intrusión Informe Ejecutivo de Pruebas del análisis de vulnerabilidad y test intrusión Informe con las posibles soluciones frente a las vulnerabilidades encontradas. Recomendaciones sobre aspectos a mejorar a nivel de cultura de seguridad	Oficial de seguridad de la Informacion				1				1				1	3
INGENIERÍA SOCIAL																	
Mediante estas pruebas se busca evidenciar las vulnerabilidades que existen dentro del AGN, buscando obtener información de personas y procesos claves del negocio mediante acceso físico a la misma o con información de acceso facilitada por el personal del AGN, el cual ha sido objeto de engaño	**INGENIERÍA SOCIAL:** Presentación de la metodología a utilizar. Determinar entre las partes el perfil de los funcionarios a los cuales se les debe realizar pruebas de ingeniería social (20) Elaboración de los instrumentos y herramientas a utilizar de acuerdo con el perfil de los empleados a evaluar y las pruebas aprobadas Realización de las pruebas de ingeniería social, como mínimo: o Pruebas con correos electrónicos tipo Phishing (mínimo 20 correos). o Pruebas con llamadas telefónicas (mínimo 20 llamadas).	Documento de Ingeniería Social que contenga la descripción de la información conseguida, la forma de conseguirla, la fecha y las personas con las que se consiguió según el alcance para veinte (20) funcionarios de la entidad. Descripción de los problemas encontrados, la forma en que se pueden aprovechar y las recomendaciones para corregir y minimizar los riesgos detectados. Documento con las recomendaciones en base a los resultados obtenidos en las pruebas y su socialización.	Oficial de seguridad de la Informacion				1				1				1	3

FASE V: PLAN ESTRATEGICO DE SEGURIDAD DE LA INFORMACIÓN - PESI																
Identificar el conjunto de responsabilidades, prácticas y acciones a ser desarrolladas porel AGN con miras a propender que los riesgos de la información sean apropiadamente administrados, mediante la definición de un modelo de seguridad de la información, alineado con las mejores prácticas, estándares y objetivos del negocio.	En base al conocimientodel AGN y resultados del diagnóstico de la seguridad de la información y documentación resultante de estas actividades en la etapa de diagnóstico, como también de los resultados obtenidos en el análisis de riesgos y pruebas de seguridad se deberán realizar las actividades complementarias que sirvan de insumo para la elaboración del PESI, como son: • Alinear los Objetivos de la seguridad de la información con los objetivos del negocio. • Identificar el portafolio de proyectos e iniciativas a priorizar en el PESI con los recursos humanos y financieros aproximados • Elaborar una matriz con la estimación aproximada de recursos, tiempos de referencia para su implementación, justificación y priorización	Plan Estratégico de Seguridad de la Información PESI a tres (3) años.	Oficial de seguridad de la Informacion												1	1

7. CONTROL DE CAMBIOS

FECHA	VERSIÓN	PROYECTÓ	REVISÓ	APROBÓ	DESCRIPCIÓN
23-05-2018	1.0	Heilin Guarnizo Rodriguez.	Manuel Gomez Patiño.	Erika Rangel Palencia	Versión inicial
18-02-2019	2.0	Heilin Guarnizo Rodriguez.	Manuel Gomez Patiño.	Manuel Gomez Patiño.	Actualización
30-11-2020	3.0	Jaime Alberto duarte	Omar Villarreal Osorio	Omar Villarreal Osorio	Actualización