PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Versión: 4

Enero de 2023

Titulo	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN				
Fecha actualización:	Enero del 2022				
Sumario	Este documento establece lineamientos para la implementación de políticas que garanticen la administración, manejo y control de la seguridad y privacidad de la información				
Palabras claves:	Políticas, Buenas prácticas, Controles, Guía				
Formato:	PDF		Lenguaje:		Español
Código:	GIT-M-02	Versión:	4	Estado:	
Categoría:	Documento Técnico				
Autor:	Jaime Alberto Duarte Hoyos				
Revisó:	Omar Villarreal Osorio				
Aprobó:	Comité Institucional de Gestión del Desempeño 19 de enero de 2023				

INTRODUCCIÓN 4
1. OBJETIVOS 5
1.1. OBJETIVO GENERAL 5
1.2. OBJETIVO ESPECÍFICOS 5
2. ALCANCE 5
3. DEFINICIONES 5
4. MARCO NORMATIVO 7
5. METODOLOGÍA IMPLEMENTACIÓN MODELO DE SEGURIDAD 7
5.1. CICLO OPERACIÓN 7
5.2. ALINEACIÓN NORMA ISO 27001:2013 vs CICLO DE OPERACIÓN 8
5.2.1 FASES I: DIAGNÓSTICO 10
5.2.2 FASES II: PLANIFICACIÓN 11
5.2.3 FASES III: IMPLEMENTACIÓN 14
5.2.4 FASES IV: EVALUACIÓN DE DESEMPEÑO 16
5.2.5 FASES V: MEJORA CONTINUA 17
6. IMPLEMENTACIÓN MODELO DE SEGURIDAD ALINEADO A RIESGOS 18
7. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 18
8. HOJA DE RUTA 22
9. CONTROL DE CAMBIOS 24

INTRODUCCIÓN

Este plan define los lineamientos y actividades que contribuyen a mitigar los riesgos asociados a la seguridad de la información y los riesgos de seguridad y privacidad de la información (ISO 27001:2013, ISO 2032:2012), 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 2023 en el Archivo General de la Nación y la creación del Plan de Apertura y Uso de Datos de Abiertos, el cual debe presentar una guía para la identificación, análisis, priorización, estructuración, publicación, promoción y monitoreo de los Datos Abiertos, para el año 2023.

1. OBJETIVOS

1.1. 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.

1.2. OBJETIVO ESPECÍFICOS

- Realizar el plan de trabajo específico, conforme a los resultados obtenidos del instrumento MSPI de MINTIC vigencia 2023.
- Alinear el SGSI con la ley de protección de datos personales, transparencia y acceso a la información pública.
- Realizar la alineación de las políticas del MIPG y el SG-SPI con los objetivos institucionales y la medición del SIPG

2. ALCANCE

La vigencia del presente plan es 2023 y aplica el proceso de gestión de las TI y el gobierno digital

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.
- 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 Plan 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. METODOLOGÍA IMPLEMENTACIÓN 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[1].

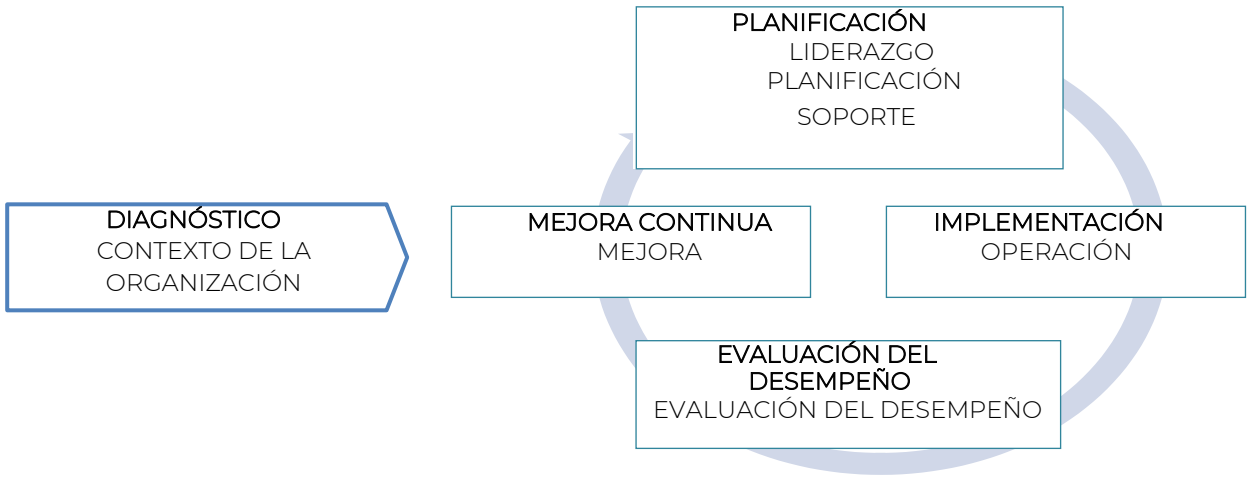
[1] Modelo de Seguridad y Privacidad, MINTIC, Pág. 1-2

- 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 (Planear): 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 (Hacer): En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.
- Fase Evaluación de desempeño (Verificar): Una vez implantada la mejora, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas.
- Fase Mejora Continua (Actuar): 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. ALINEACIÓN NORMA ISO 27001:2013 vs CICLO DE OPERACIÓN

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, 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: información tomada de 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[2]
Diagnostico	Contexto de la Organización
Planificación	Liderazgos Planificación Soporte

[2] NTC-ISO-IEC 27001:2013, Pág. 1-12

Implementación	Operación
Evaluación de desempeño	Evaluación de desempeño
Mejora Continua	Mejora

Fuente: Estructura ISO 27001:2013

5.2.1 FASES I: DIAGNÓSTICO

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 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 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.

Fuente: ISO 27001:2013

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

- Diligenciamiento del instrumento de MINTIC con el objetivo de determinar el nivel de cumplimiento del Modelo de Seguridad y Privacidad de la Información 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.

5.2.2 FASES II: PLANIFICACIÓN

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 y la ciberseguridad, en procura de los resultados que permitan dar cumplimiento con las metas propuestas del SGSI.
Metas	Actividades \ Instrumentos \ Resultados

Realizar un análisis de Contexto y factores externos e internos de la Entidad en torno a la seguridad digital.	**Realizar** un **Análisis de Contexto** de la entidad entorno a la seguridad digital teniendo en cuenta el capítulo 4. CONTEXTO DE LA ORGANIZACIÓN de la norma ISO27001:2013, 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 para el año 2022	**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	**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.
Actualizar las políticas de seguridad digital de la entidad. la cual debe ser actualizada cada año	**Actualizar Política General de Seguridad y Privacidad** la cual debe ser aprobada por la Alta Dirección y socializada al interior del AGN. **Actualizar** 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 y/o actualizar documentación de operación (formatos de procesos, procedimientos y documentos debidamente definidos y establecidos) del sistema de seguridad de la información	**Elaborar y/o Actualizar 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.
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 y ciberseguridad 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 concienciación de seguridad de la información.	Elaborar plan anual de concienciación de seguridad de la información
Realizar el Plan de Apertura y Uso de Datos Abiertos	Elaborar el Plan de Apertura y Uso de Datos Abiertos para los años 2022 -2023 acorde a las recomendaciones dadas por MINTIC

Fuente: ISO 27001:2013

5.2.3 FASES III: IMPLEMENTACIÓN

Objetivo	Llevar a cabo 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.

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
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

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 información de la entidad.
Implementar procedimiento de gestión de eventos e incidentes de seguridad y ciber 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 concienciación de seguridad	**Ejecutar** el plan anual de concienciación de seguridad de la información
Ejecutar el Plan de Apertura y Uso de Datos Abiertos	**Ejecutar** el Plan de Apertura y Uso de Datos Abiertos
Ejecutar pruebas semestrales de vulnerabilidades e intrusión (actividad elaborada por terceros)	**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 (actividad elaborada por terceros)	**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 (actividad elaborada por terceros)	**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.

Fuente: ISO 27001:2013

5.2.4 FASES IV: EVALUACIÓN 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.
Metas	Actividades \ Instrumentos \ Resultados

Ejecución de auditorías de seguridad de la información (actividad elaborada por terceros)	**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.

Fuente: ISO 27001:2013

5.2.5 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

Metas	Actividades \ Instrumentos \ Resultados
Diseñar plan de mejoramiento para el año 2022	**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.

Fuente: ISO 27001:2013

6.IMPLEMENTACIÓN MODELO DE SEGURIDAD ALINEADO A RIESGOS

Fuente: ISO 27001:2013

7.PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

FASE I: ANÁLISIS DE BRECHA	
ANÁLISIS GAP ISO 27001 y MSPI	
Objetivo	Actividades
Elaborar el análisis GAP (análisis de brecha) frente a la norma ISO 27001:2013 y el Modelo de	Conocer el negocio del AGN, procesos definidos en el alcance, recursos que soportan los procesos, responsables del SGSI, tecnologías utilizadas y terceras partes involucradas
	Identificar y entender el contexto interno y externo del AGN, partes interesadas y factores críticos de éxito

seguridad y privacidad de la información MSPI del AGN	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
	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

FASE II: ESTABLECIMIENTO DEL SGSI	
DISEÑO DE POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD	
Diseñar y/o actualizar políticas y procedimientos de seguridad conforme la estructura propuesta por la norma ISO 27001:2013 alineados al Sistema Integrado de Gestión de la Entidad	Actualizar el manual de políticas y procedimientos respetando la estructura propuesta por la norma ISO 27000, de acuerdo con:
	Elaborar y actualizar las políticas y procedimientos alineado a lo exigido por la norma ISO 27001:2013 y por MPSI.
	Definir y documentar formalmente el proceso de gestión de incidentes 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

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.	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
	Actualización de matriz de riesgos.
	Realizar el Registro Nacional de Base de Datos

FASE IV: PRUEBAS DE SEGURIDAD	
HACKING ÉTICO Y PENETRACIÓN	
Identificar las vulnerabilidades que existen dentro de la configuración física y lógica de los sistemas informáticos de la entidad. (esta actividad se requiere ser elaborada por terceros)	HACKING ÉTICO:
	Recolección de información.
	Identificación de sistemas y servicios.
	Identificación y verificación de vulnerabilidades.
	Presentaciones informes de resultados.
	INGENIERÍA SOCIAL:
	Determinar entre las partes el perfil de los funcionarios y contratistas a los cuales se les debe realizar pruebas de ingeniería social
	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
	Análisis de resultados

FASE V: PLAN ESTRATEGICO DE SEGURIDAD DE LA INFORMACIÓN - PESI	
Identificar el conjunto de responsabilidades, prácticas y acciones a ser desarrolladas por el 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 conocimiento del 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

FASE VI: ENTRENAMIENTO EN SEGURIDAD DE LA INFORMACIÓN
CHARLAS DE CONCIENCIACIÓN

Realizar las capacitaciones a los funcionarios y contratistas de la entidad.	Establecer las acciones necesarias para dimensionar e implementar el programa de entrenamiento requerido por el AGN en lo referente a seguridad de la información tomando como insumo los resultados de las pruebas de ingeniería social.
	Realizar una evaluación que permita medir el conocimiento asimilado por los funcionarios capacitados en temas de seguridad informática.
	Socializar el informe del proceso de concientización

FASE VI: SENSIBILIZACIÓN Y ENTRENAMIENTO EN SEGURIDAD DE LA INFORMACIÓN	
AUDITORIA INTERNA SGSI	
Realizar las auditorias de SGSI acorde a las políticas definidas en la entidad.	Desarrollar actividades preparatorias que busquen orientar al AGN para afrontar el proceso de auditoría.
	Realizar la recolección de evidencia suficiente y probatoria sobre el cumplimiento de los requisitos que exige la norma ISO 27001:2013.
	Desarrollar el informe y recomendaciones del proceso.

8. HOJA DE RUTA

Proyectos	2023											
	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
FASE V												

Elaboración PESI												
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												
Elaborar una matriz con la estimación aproximada de recursos, tiempos de referencia para su implementación												
elaboración de guía Datos Abiertos												
FASE VI Sensibilización Y Entrenamiento En Seguridad De La Información												

9.CONTROL DE CAMBIOS

	FECHA APROBACIÓN	RESPONSABLE	DESCRIPCIÓN
1	23-05-2018	Manuel Gómez Patiño.	Versión inicial
2	18-02-2019	Manuel Gómez Patiño.	Actualización
3	30/03/2021	Omar Villarreal Osorio	Actualización
4	23/12/2022	Omar Villarreal Osorio	Actualización