

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Versión: 5

Fecha: Bogotá D.C., enero de 2024

TABLA DE CONTENIDO

INTRODUCCIÓN	5
1. OBJETIVOS.....	5
1.1 Objetivo general	5
1.2 Objetivos específicos	5
2. ALCANCE.....	6
3. DEFINICIONES.....	6
4. MARCO NORMATIVO.....	8
5. METODOLOGÍA DE IMPLEMENTACIÓN MODELO DE SEGURIDAD.....	8
5.1 Ciclo de operación	8
5.2 Alineación norma ISO 27001:2013 vs ciclo de operación	9
5.2.1 FASE I: Diagnóstico	11
5.2.2 FASE II: Planificación	12
5.2.3 FASE III: Implementación	14
5.2.4 FASE IV: Evaluación del desempeño	15
5.2.5 FASE V: Mejora continua	16
6. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	16
7. HOJA DE RUTA.....	20
CONTROL DE CAMBIOS.....	25

INDICE DE TABLAS

Tabla 1. Fases Ciclo Operación vs Estructura ISO 27001:2013	10
Tabla 2. Fase Diagnóstico	11
Tabla 3. Fase Planificación	12
Tabla 4. Fase Implementación	14
Tabla 5. Fase Evaluación del Desempeño	15
Tabla 6. Fase Mejora continua.....	16
Tabla 7. Plan de Seguridad y privacidad de la información - Fases	17

INDICE DE ILUSTRACIONES

Ilustración 1. Ciclo de mejora continua - AGN	9
Ilustración 2. Hoja de Ruta	20

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 - MSPI, para ser implementada en el año 2024 en el Archivo General de la Nación y la creación del Plan de Apertura y Uso de Datos Abiertos, el cual debe presentar una guía para la identificación, análisis, priorización, estructuración, publicación, promoción y monitoreo de los Datos Abiertos, para el año 2024.

1. OBJETIVOS

1.1 Objetivo general

Definir la hoja de ruta para la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI - de la política de Gobierno Digital, alineadas con la NTC/IEC ISO 27001, la Política pública de Seguridad Digital y la estrategia del Archivo General de la Nación, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de la información de la entidad.

1.2 Objetivos específicos

- Realizar el plan de trabajo específico conforme a los resultados obtenidos del instrumento MSPI de MINTIC vigencia 2023.
- Alinear el Sistema de Gestión de Seguridad de la Información - SGSI con la Ley de protección de datos personales, transparencia y acceso a la información pública.

2. ALCANCE

La vigencia del presente plan es el año 2024 y aplica al proceso de gestión de las Tecnologías de Información y al 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:** Es un activo de alta validez, que contiene información vital de la empresa y que debe ser protegida.
- **Amenaza:** Es la causa potencial de un daño a un activo de información.
- **Análisis de riesgos:** Es la utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos.
- **Causa:** Factor o evento que pueden provocar un riesgo o que puede desencadenar una situación de peligro o incertidumbre.

- **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.
- **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.
- **Riesgo:** Grado de exposición de un activo que permite la materialización de una amenaza.
- **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 se 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 normatividad aplicable a la entidad, y específicamente, el decreto 612 de 2018, la Política de Gobierno Digital y su Modelo de Seguridad y Privacidad de la Información alineado con la NTC/IEC ISO 27001, y la estrategia de Seguridad Digital del Estado colombiano.

Internamente se tienen como base las políticas, manuales, procedimientos y formatos asociados al sistema de gestión de seguridad de la información que se encuentran publicados en el sistema de gestión de calidad del Archivo General de la Nación.

5. METODOLOGÍA DE IMPLEMENTACIÓN MODELO DE SEGURIDAD

5.1 Ciclo de operación

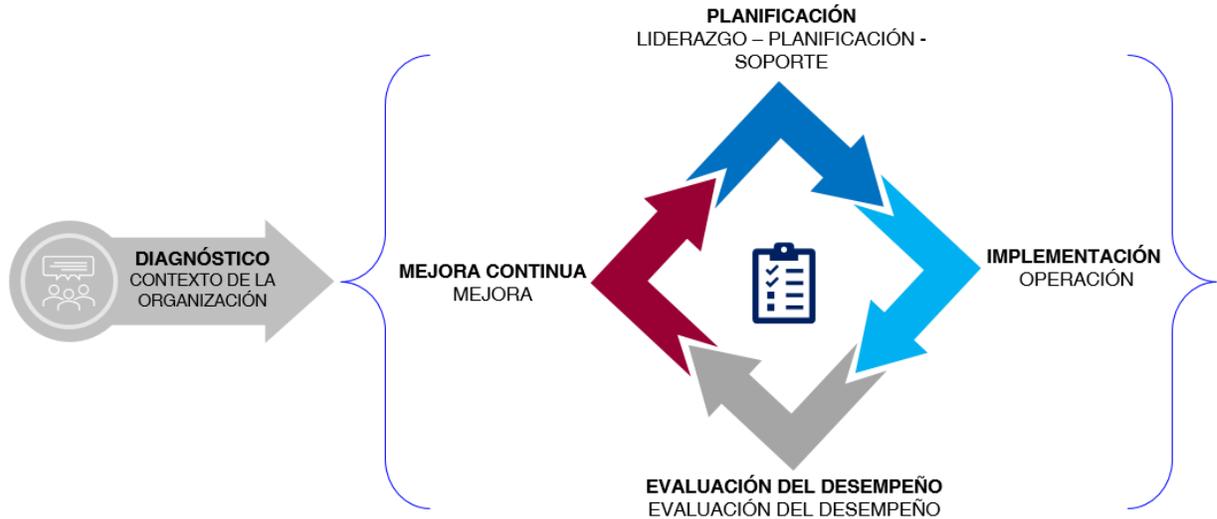
El Modelo de Seguridad y Privacidad de la Información de la Estrategia de Gobierno Digital observa el siguiente ciclo de operación que contempla cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

- **Fase Diagnóstico:** 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 los modelos de gestión de la siguiente forma:

Ilustración 1. Ciclo de mejora continua - AGN



Fuente: <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 (Diagnóstico, 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	Capítulo ISO 27001:2013 ¹
Diagnóstico	Contexto de la Organización
Planificación	Liderazgos Planificación Soporte
Implementación	Operación
Evaluación de desempeño	Evaluación de desempeño
Mejora Continua	Mejora

Fuente: Estructura ISO 27001:2013

5.2.1 FASE I: Diagnóstico

Tabla 2. Fase 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	<p>Diagnóstico de la situación actual de la entidad con relación a la gestión de seguridad de la información.</p> <p>Diagnóstico 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.</p> <p>Valoración estado actual de la gestión de seguridad de la entidad con base en el Instrumento de Evaluación MSPI de MINTIC.</p>
Identificar el nivel de madurez de seguridad de la información en el AGN	<p>Valoración del nivel de estratificación de la entidad frente a la seguridad de la información con base en el método planteado en el documento '<i>ANEXO 3: ESTRATIFICACIÓN DE ENTIDADES</i>' del modelo seguridad de la información para la estrategia de Gobierno en Línea 2.0.</p> <p>Valoración del nivel de madurez de seguridad y privacidad de la información en la entidad de acuerdo con los lineamientos establecidos en el capítulo '<i>MODELO DE MADUREZ</i>' del documento Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea.</p>
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: NTC-ISO-IEC 27001:2013,

Para la recolección de la información, en esta fase se utilizarán mecanismo 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, 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 FASE II: Planificación

Tabla 3. Fase 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 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 para el año 2024.	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.

<p>Actualizar las políticas de seguridad digital de la entidad. la cual debe ser actualizada cada año.</p>	<p>Actualizar la Política General de Seguridad de la Información la cual debe ser aprobada por la Alta Dirección y socializada al interior del AGN.</p> <p>Actualizar el manual Políticas de Seguridad 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.</p>
<p>Elaborar y/o actualizar documentación de operación (formatos de procesos, procedimientos y documentos debidamente definidos y establecidos) del sistema de seguridad de la información</p>	<p>Elaborar y/o Actualizar los documentos de operación del sistema de seguridad de la información, tales como:</p> <ul style="list-style-type: none"> • Manual Sistema de Gestión de seguridad de la información. • Manual Políticas de Seguridad de la información. • Política de Gestión de Incidentes. • Política de seguridad de la información del sitio web. • Política de transferencia de la información. • Política de tratamiento y protección de datos personales. • Política de uso de redes virtuales. • Política General de la Seguridad de la Información. • Procedimiento Elaboración y Administración de Copias de Seguridad. • Procedimiento reporte de Incidentes de Seguridad de la Información. •
<p>Identificar y valorar activos de información</p>	<p>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.</p>
<p>Identificar, valorar y tratar los riesgos de seguridad de la información y ciberseguridad de la entidad</p>	<p>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 selección de los controles, se tomará como base los objetivos de control y los controles</p>

	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 el año 2024 acorde a las recomendaciones dadas por MINTIC

Fuente: ISO 27001:2013

5.2.3 FASE III: Implementación

Tabla 4. Fase 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 de Gestión y Desempeño.
Ejecutar el plan de tratamiento de riesgos	Ejecutar el plan de Tratamiento de Riesgos de Seguridad y Privacidad 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 de 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 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 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 Ingeniería Social (actividad elaborada por terceros)	Ejecutar pruebas semestrales de ingeniería social orientadas a verificar aspectos como: (i) los protocolos 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 FASE IV: Evaluación del desempeño

Tabla 5. Fase Evaluación del 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)	<p>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 auditoría revisado y aprobado por la Alta Dirección.</p> <p>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.</p>
Plan de seguimiento, evaluación y análisis de SGSI	<p>Elaboración documento con el plan de seguimiento, evaluación y análisis del SGSI revisado y aprobado por el Comité de Riesgos.</p>

Fuente: ISO 27001:2013

5.2.5 FASE V: Mejora continua

Tabla 6. Fase Mejora continua

<p>Objetivo</p>	<p>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</p>
<p>Metas</p>	<p>Actividades \ Instrumentos \ Resultados</p>
<p>Diseñar plan de mejoramiento para el año 2024</p>	<p>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.</p>

Fuente: ISO 27001:2013

6. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

A continuación se presenta el análisis de las brechas identificadas en el Archivo General de la Nación respecto con los lineamientos establecidos

Archivo General de la Nación Jorge Palacios Preciado

Dirección: Carrera 6 No.6 - 91, Bogotá D.C., Colombia

Teléfono: (+57) 601 328 2888

en la NTC/IEC ISO 27001 y en el Modelo de Seguridad y Privacidad de la Información – MSPI de la política de Gobierno Digital del Mintic:

Tabla 7. Plan de Seguridad y privacidad de la información - Fases

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 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	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
	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 esta 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	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.	Identificar los activos de información
	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	Alinear los objetivos de la seguridad de la información con los objetivos del negocio.
--	--

<p>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.</p>	<p>Identificar el portafolio de proyectos e iniciativas a priorizar en el PESI con los recursos humanos y financieros aproximados</p>
	<p>Elaborar una matriz con la estimación aproximada de recursos, tiempos de referencia para su implementación, justificación y priorización</p>

FASE VI: ENTRENAMIENTO EN SEGURIDAD DE LA INFORMACIÓN

CHARLAS DE CONCIENCIACIÓN

<p>Realizar las capacitaciones a los funcionarios y contratistas de la entidad.</p>	<p>Establecer las acciones necesarias de socialización y transferencia de conocimientos de seguridad de la información.</p>
	<p>Realizar una evaluación que permita medir el conocimiento asimilado por los funcionarios capacitados en temas de seguridad informática.</p>
	<p>Socializar el informe del proceso de concientización</p>

Fuente: ISO 27001:2013

7. HOJA DE RUTA

Ilustración 2. Hoja de Ruta

FASE	OBJETIVO	ACTIVIDADES	2024											
			Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
Fase I: Análisis De Brecha Análisis Gap ISO 27001 Y MSPI	Elaborar el análisis GAP (análisis de brecha) frente a la norma ISO 27001:2013 y el Modelo de seguridad y privacidad de la información MSPI del AGN	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												

		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 esta 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	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													
	Identificar los activos de	Identificar los activos de información													

Fase III: Análisis De Riesgos Identificación De Activos De Información	información de los procesos de negocio AGN incluidos en el alcance.	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)	Generar plan de remediación del anterior hacking ético realizado en AGN												
		Seguimiento al cumplimiento del plan de remediación del anterior hacking ético del AGN												
		Hacking ético: Recolección de información.												
		Hacking ético: Identificación de sistemas y servicios.												
		Hacking ético: Identificación y verificación de vulnerabilidades.												
		Hacking ético: Presentaciones informes de resultados y generación del plan de remediación												

		Ingeniería Social: Determinar entre las partes el perfil de los funcionarios y contratistas a los cuales se les debe realizar pruebas de ingeniería social											
		Ingeniería Social: Elaboración de los instrumentos y herramientas a utilizar de acuerdo con el perfil de los empleados a evaluar y las pruebas aprobadas											
		Ingeniería Social: Realización de las pruebas de ingeniería social											
		Ingeniería Social: Análisis de resultados y generación del plan de remediación											
Fase V: Plan Estratégico De Seguridad De La Información - PESI	Identificar el conjunto de responsabilidades , prácticas y acciones a ser desarrolladas por el AGN	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											

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
5		Martha Patricia Vargas	Actualización