PARQUES NACIONALES
NATURALES DE COLOMBIA

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

GRUPO DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES
2024-2025

TABLA DE CONTENIDO

1. DECLARACIÓN DE ALCANCE

El presente documento es la base para la definición del Modelo de Seguridad y Privacidad de la Información - MSPI definido por el gobierno nacional, así mismo representa el Dominio de Arquitectura de Seguridad de acuerdo con el Modelo de Arquitectura Empresarial – MAE correspondiente al Marco de Arquitectura Empresarial del Estado Colombiano – MRAE.

2. INTRODUCCIÓN

Hoy día, la información está definida como uno de los activos más valiosos e importantes para cualquier tipo de organización, información que sólo tiene sentido cuando está disponible y es utilizada de forma adecuada, actividad que implica, que es necesario que las organizaciones tengan una adecuada gestión sobre sus recursos y activos de información con único fin de asegurar y controlar el debido acceso, tratamiento y uso de la información.

El aseguramiento y la protección de la seguridad de la información de las organizaciones y de los datos de carácter personal de los usuarios, representan un reto al momento de pretender garantizar su confidencialidad, integridad, disponibilidad y privacidad, razón por la cual, la seguridad de la información se ha convertido en uno de los aspectos de mayor preocupación a nivel mundial.

Cualquier tipo de organización independiente de su tamaño y naturaleza, debe ser consecuente que la diversidad de amenazas existentes que actualmente atentan contra la seguridad y privacidad de la información, representan un riesgo que al materializarse no solo les puede acarrear costos económicos, sanciónales legales, afectación de su imagen y reputación, sino que pueden afectar la continuidad y supervivencia del negocio. Lo anterior, sumado a un entorno tecnológico en donde cada día se hace más complejo de administrar y asegurar, genera que cada vez más la seguridad de la información forme parte de los objetivos y planes estratégicos de las organizaciones. Por lo tanto, es indispensable que los responsables dentro de las organizaciones encargados de velar por la protección y seguridad de sus recursos, infraestructura e información, periódicamente estén adoptando, implementando y mejorando medidas de seguridad orientadas a prevenir y/o detectar los riesgos que pueden llegar a comprometer la disponibilidad, integridad y confidencialidad de los activos de información a través de los cuales se gestiona la información del negocio, independientemente si está es de carácter pública o privada.

En la medida que las organizaciones tengan una visión general de los riesgos que pueden afectar la seguridad y privacidad de la información, podrán establecer controles y medidas efectivas, viables y transversales con el propósito de salvaguardar la disponibilidad, integridad y confidencialidad tanto de la información del negocio como los datos de carácter personal de sus empleados, usuarios y partes interesadas. Es indispensable que las organizaciones realicen una adecuada identificación, clasificación, valoración, gestión y tratamiento de los riegos que pueden afectar su seguridad, con el propósito de implementar medidas y controles efectivos que les permitan estar preparados ante situaciones adversas que puedan comprometer tanto la seguridad física y lógica de sus instalaciones, personas, recursos y sistemas, como la seguridad de su información.

Las entidades del sector público están en la obligación de garantizar la debida seguridad, protección y privacidad de la información de sus usuarios y terceros que residen en sus bases de datos, lo que implica, que deben contar con los más altos estándares y niveles de seguridad con el propósito de asegurar la debida recolección, almacenamiento, respaldo, tratamiento, uso, intercambio y distribución de esta información.
Una de las preocupaciones permanentes de este tipo de entidades, es la de poder garantizar la seguridad de las operaciones que realizan con sus usuarios y terceros, lo cual, cada día es más complejo de conseguir debido a la evolución de las tecnologías y la apertura de nuevos canales de comunicación que generan retos significativos con el propósito de prevenir los fraudes en general.

Debido a los múltiples riesgos y amenazas que hoy en día atentan contra la seguridad de la información y la protección y privacidad de los datos, es fundamental que las organizaciones establezcan, implementen, mantengan y mejoren continuamente un sistema de gestión de seguridad de la información basado en los riesgos y a su vez, alineado con los objetivos estratégicos y necesidades tanto del negocio como de sus partes interesadas.

PARQUES NACIONALES NATURALES DE COLOMBIA es consciente que la protección y aseguramiento de su información es fundamental para garantizar su debida gestión administrativa y operativa, razón por la cual debe establecer un marco normativo de Seguridad de la Información que contemple políticas, límites, responsabilidades y obligaciones frente a la seguridad y privacidad de la información de la entidad.

El presente documento contiene el plan de seguridad y privacidad de la información para el establecimiento del Sistema de Gestión de Seguridad y Privacidad de la información de PARQUES NACIONALES NATURALES DE COLOMBIA, el cual tomará como referencia el Modelo de Seguridad y Privacidad de la estrategia de Gobierno Digital y la norma ISO 27001 [1], los cuales proporcionan un marco metodológico basado en buenas prácticas para llevar a cabo la implementación de un modelo de Gestión de Seguridad y Privacidad de la información en cualquier tipo de organización, lo cual, permite garantizar su efectiva implementación y asegurar su debida permanecía y evolución en el tiempo.

Así mismo, este documento constituye la base para la definición del Dominio de Arquitectura de Seguridad, conforme a lo establecido por el MRAE. Su enfoque se dirige a asegurar la alineación con los objetivos estratégicos de PNNC, así como a integrar y fortalecer los demás dominios del MAE, asegurando la implementación de la seguridad de la información a nivel nacional.

3. OBJETIVOS

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 de PARQUES NACIONALES NATURALES DE COLOMBIA, acorde a los requerimientos del Dominio de Gestión de Seguridad de MRAE V3.0, los requerimientos del negocio y en cumplimiento de las disposiciones legales vigentes.

3.1. OBJETIVOS ESPECÍFICOS

- Definir las etapas para establecer la estrategia del Dominio de Seguridad de la Información de la entidad y el Modelo de Seguridad de la Información.
- Definir la Hoja de Ruta Estratégica para apalancar el cumplimiento del Dominio de Seguridad de la Información.
- 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 entidad
- Optimizar la gestión de la seguridad de la información al interior de la entidad

4. METODOLOGÍA PARA LA IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD

4.1. CICLO DE OPERACIÓN

El Modelo de Seguridad y Privacidad de la Información de la Estrategia de Gobierno Digital contempla 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].

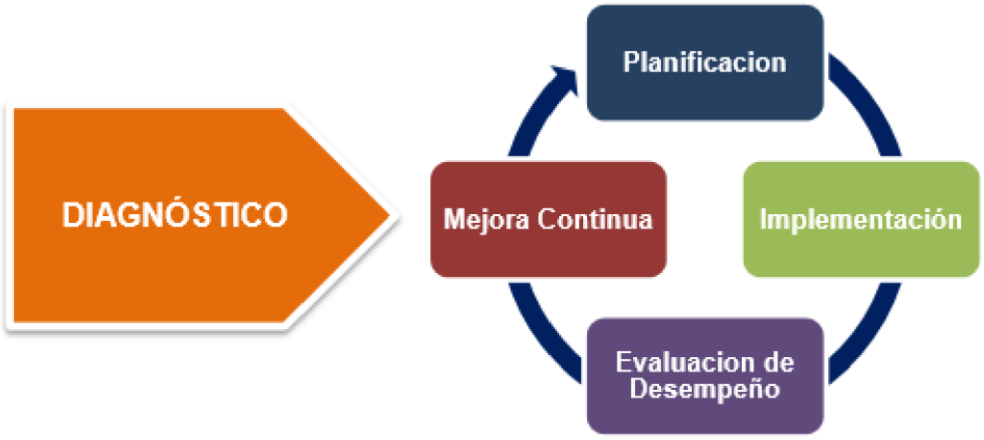

Figura 1: Ciclo de Operación Modelo de Seguridad y Privacidad de la Información
Fuente: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

- ✓ **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

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

4.2. ALINEACIÓN NORMA ISO 27001:2022 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, la nueva estructura de esta versión se puede alinear con el ciclo de mejora continua de las modelos de gestión de la siguiente forma:

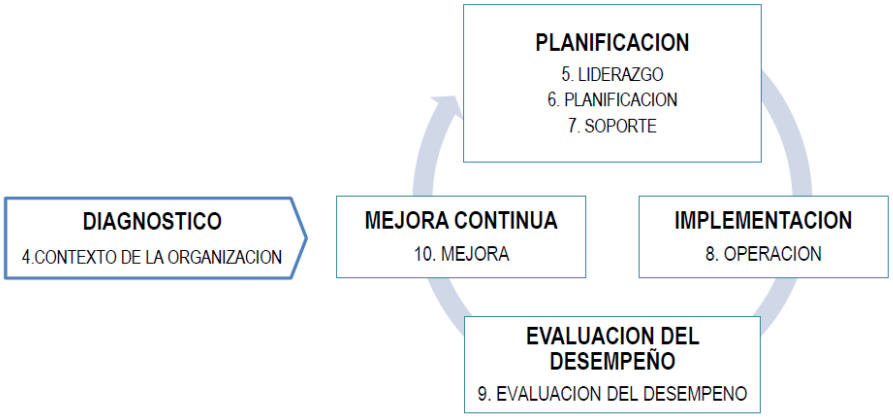

Figura 2: Norma ISO 27001:2022 alineada a la mejora continua
Fuente: Elaborada con base en la información publicada en la página web

https://www.escuelaeuropeaexcelencia.com/2022/12/norma-iso-270012022-todo-lo-que-debes-saber-sobre-el-nuevo-estandar-de-seguridad-de-la-informacion/#:~:text=%C2%BFQu%C3%A9%20es%20la%20norma%20ISO,periodicidad%20media%20de%20cinco%20a%C3%B1os.

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 27001:2022:

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

FASE	Capitulo ISO 27001:2013[2]
Diagnostico	1. Contexto de la Organización
Planificación	2. Liderazgo 3. Planificación 4. Soporte
Implementación	5. Operación
Evaluación de Desempeño	6. Evaluación de Desempeño
Mejora Continua	7. Mejora

- ✓ **Fase DIAGNOSTICO en la norma ISO 27001:2022.** En el **capítulo 4** - **Contexto de la organización** de la norma ISO 27001:2022, se determina la necesidad de realizar un análisis de las cuestiones 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.

[2] NTC-ISO-IEC 27001:2013, Pág. 1-12

- ✓ **Fase PLANEACION en la norma ISO 27001:2022** 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.

- ✓ **Fase IMPLEMENTACION en la norma ISO 27001:2022.** En el **capítulo 8 - Operación** de la norma ISO 27001:2022, 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.

- ✓ Fase **EVALUACION DEL DESEMPEÑO en la norma ISO 27001:2022.** 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.

- ✓ Fase **MEJORA CONTINUA en la norma ISO 27001:2022.** 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.

4.3. FASE 1: DIAGNÓSTICO

Objetivo	Identificar el estado de la Entidad 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 de la Entidad	**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 27001:2022**. **Valoración estado actual** de la gestión de seguridad de la entidad con base en el Instrumento de Evaluación MSPI de MINTIC.

GRUPO DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES
Calle 74 No. 11 - 81 Piso 8 Bogotá, D.C., Colombia
Teléfono: 353 2400 Ext.: 3119

Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad	**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 Digital. **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 Digital.
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 de le entidad con relación a los dominios de la norma ISO/IEC 27001:2022
- ✓ 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 Digital Ministerio de Tecnologías de la Información y las Comunicaciones

4.4. FASE 2: 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, en procura de los resultados que permitan dar cumplimiento con las metas propuestas del SGSI.

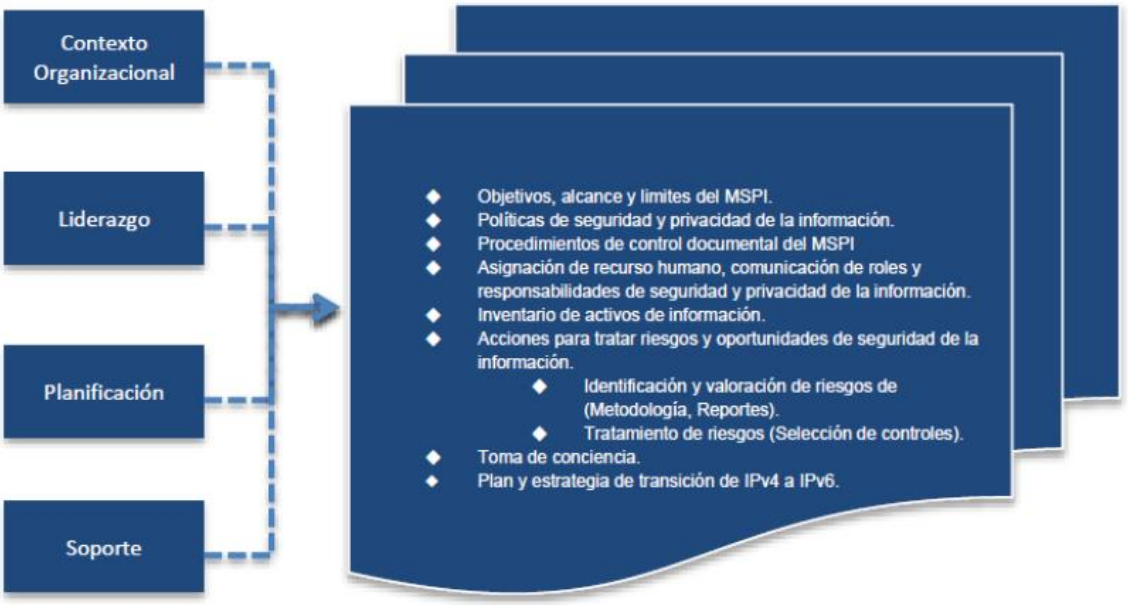

Figura 3: Fase de Planificación Modelo de Seguridad
Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno Digital

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 27001:2022, 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' de la entidad 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** de la entidad 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 la entidad. **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 de la entidad. **Implementar** un **sistema de información** para la administración y gestión de los riesgos de seguridad de la entidad.

METAS	ACTIVIDADES / INSTRUMENTOS / RESULTADOS
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 de la Entidad. **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 la Entidad con el objetivo de proteger la disponibilidad, integridad y confidencialidad de la información. Estas políticas deben ser aprobadas por la Alta Dirección y socializadas al interior de la Entidad.
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 27001:2022.
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.

GRUPO DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES
Calle 74 No. 11 - 81 Piso 8 Bogotá, D.C., Colombia
Teléfono: 353 2400 Ext.: 3119

4.5. FASE 3: 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 de la entidad.

Figura 4: Fase de Implementación Modelo de Seguridad
Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno Digital

METAS	ACTIVIDADES / INSTRUMENTOS / RESULTADOS
Establecer el plan de implementación de seguridad de la información	**Desarrollar** 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 anuales de vulnerabilidades e intrusión	**Ejecutar** el plan anual de **pruebas vulnerabilidades** e intrusión con el objetivo de identificar el nivel de protección de los activos de información

	de la entidad. Para tal efecto, se deberá tener en cuenta los respectivos requerimientos de seguridad relacionados con pruebas de vulnerabilidades establecidos por la entidad o la circular que las reemplacen.
Ejecutar pruebas de Ethical Hacking	**Ejecutar** pruebas anuales 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 anuales 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 de la entidad y de sus empleados.

4.6. FASE 4: 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

Figura 5: Fase Evaluación de Desempeño Modelo de Seguridad
Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno Digital

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.

GRUPO DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES
Calle 74 No. 11 - 81 Piso 8 Bogotá, D.C., Colombia
Teléfono: 353 2400 Ext.: 3119

4.7. FASE 5: 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.

Figura 6: Fase Mejora Continua Modelo de Seguridad
Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno Digital

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

GRUPO DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES
Calle 74 No. 11 - 81 Piso 8 Bogotá, D.C., Colombia
Teléfono: 353 2400 Ext.: 3119

4.8. HOJA DE RUTA DEL DOMINIO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La siguiente Hoja de Ruta está alineada con el Plan de Implementación del Modelo de Seguridad de la Información en sus fases y da un cumplimiento estratégico al Dominio, de acuerdo con el MRAE V3.0 y los lineamientos en materia de Seguridad. Las fases de evaluación y mejora continua están alineadas con los procesos institucionales dictados en la materia, por lo cual hacen parte del ciclo y no se mencionan en la Hoja de Ruta.

COMPONENTE	ACTIVIDAD FASE DIAGNÓSTICO	2024-2025							
		2024				2025			
Trimestre		I	II	III	IV	I	II	III	IV
ACTUALIZACIÓN	Actualización de la evaluación de la situación actual de la entidad en términos de la Seguridad de la Información y la Ciberseguridad								
FASE DE PLANIFICACIÓN									
ACTUALIZACIÓN	Análisis de la estrategia para el cumplimiento de seguridad de la información								
FASE DE IMPLEMENETACIÓN									
ACTUALIZACIÓN	Definición de compromisos objetivo de la Seguridad de la Información								

4.9. PLAN DE IMPLEMENTACIÓN MODELO DE SEGURIDAD

COMPONENTE	ACTIVIDAD FASE DIAGNÓSTICO	2024-2025			
		2024		2025	
ACTUALIZACION	Actualizar el Estado de la Gestión de Seguridad en la Entidad	SEMESTRE 1		SEMESTRE 1	
	Actualizar el Nivel de madurez de seguridad en la entidad	SEMESTRE 1		SEMESTRE 1	
	Identificar Vulnerabilidades Técnicas	SEMESTRE 1	SEMESTRE 2	SEMESTRE 1	SEMESTRE 2
FASE DE PLANIFICACIÓN					
ACTUALIZACION	Actualizar análisis del Contexto de la Entidad entorno a la seguridad	SEMESTRE 1		SEMESTRE 1	
	Actualizar el Alcance del SGSI en la Entidad	SEMESTRE 1		SEMESTRE 1	

COMPONENTE	ACTIVIDAD FASE DIAGNÓSTICO	2024-2025			
		2024		2025	
	Actualizar Roles y Responsabilidades de Seguridad de la Información	SEMESTRE 1		SEMESTRE 1	
	Actualizar la metodología de Riesgos de Seguridad de la Información	SEMESTRE 1		SEMESTRE 1	
	Actualizar políticas de Seguridad y Privacidad de la Información	SEMESTRE 1		SEMESTRE 1	
	Documento Operación del Sistema de Seguridad	SEMESTRE 1		SEMESTRE 1	
	Actualizar Activos de Información	SEMESTRE 1		SEMESTRE 1	
	Actualizar y aplicar plan de Sensibilización	SEMESTRE 1		SEMESTRE 1	
	Actualizar Plan IPv4/IPv6	SEMESTRE 1		SEMESTRE 1	
FASE DE IMPLEMENETACIÓN					
ACTUALIZACION	Actualizar de Controles del Anexo A		SEMESTRE 2		SEMESTRE 2
	Implementación de plan de acción derivados de auditorias		SEMESTRE 2		SEMESTRE 2
	Ejecutar plan de tratamiento de Riesgos		SEMESTRE 2		SEMESTRE 2
	Actualizar transición IPv4/IPv6		SEMESTRE 2		SEMESTRE 2
	Actualizar la gestión de Incidentes de Seguridad		SEMESTRE 2		SEMESTRE 2
	Implementar Gestion de Incidentes de Seguridad		SEMESTRE 2		SEMESTRE 2
	Ejecutar Plan de Sensibilización		SEMESTRE 2		

GRUPO DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES
Calle 74 No. 11 - 81 Piso 8 Bogotá, D.C., Colombia
Teléfono: 353 2400 Ext.: 3119

COMPONENTE	ACTIVIDAD FASE DIAGNÓSTICO	2024-2025			
		2024		2025	
	Ejecutar Plan de Pruebas de Vulnerabilidades		SEMESTRE 2	SEMESTRE 1	SEMESTRE 2
FASE EVALUACIÓN DEL DESEMPENO					
	Auditoria de Seguridad	SEMESTRE 1			SEMESTRE 2
FASE DE MEJORA CONTINUA					
	Plan de Mejoramiento			SEMESTRE 1	

5. CONTROL DE CAMBIOS

FECHA DE VIGENCIA VERSIÓN ANTERIOR	VERSIÓN ANTERIOR	MOTIVO DE LA ACTUALIZACIÓN

CRÉDITOS		
Elaboró	Nombre	Fernando Bolívar Buitrago Emerson Cruz Aldana
	Cargo	Profesionales Contratistas Grupo Tecnologías de la Información y las Comunicaciones
	Fecha	10/12/2024
Revisó	Nombre	Adriana Lorena Beltrán Carlos Arturo Sáenz Barón
	Cargo	Profesional Contratista Grupo Tecnologías de la Información y las Comunicaciones Profesional Especializado Grado 15 Grupo Tecnologías de la Información y las Comunicaciones
	Fecha:	10/12/2024
Aprobó	Nombre	Gipsy Vivian Arenas Hernández
	Cargo	Coordinadora Grupo Tecnologías de la Información y las Comunicaciones
	Fecha:	10/12/2024

GRUPO DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES
Calle 74 No. 11 - 81 Piso 8 Bogotá, D.C., Colombia
Teléfono: 353 2400 Ext.: 3119