PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

SUBDIRECCIÓN DE GESTIÓN Y MANEJO DE ARREAS PROTEGIDAS
GRUPO DE SISTEMAS DE INFORMACIÓN Y RADIO COMUNICACIONES
2021

SUBDIRECCION DE GESTION Y MANEJO DE AREAS PROTEGIDAS
Calle 74 No. 11 - 81 Piso 3 Bogotá, D.C., Colombia
Teléfono: 353 2400 Ext.: 3141
www.parquesnacionales.gov.co

Tabla de contenido

SUBDIRECCION DE GESTION Y MANEJO DE AREAS PROTEGIDAS
Calle 74 No. 11 - 81 Piso 3 Bogotá, D.C., Colombia
Teléfono: 353 2400 Ext.: 3141
www.parquesnacionales.gov.co

CONTROL DE VERSIONES

Versión	Fecha Actualización	Elaborado /Modificado	Revisado	Fecha Ultima Revisión	Numero total de Paginas	Comentario
01	06/10/2020	Fernando Bolivar			8	Creación Documento
02	28/04/2021	Fernando Bolivar			25	Actualización Documento
03	31/05/2021	Fernando Bolivar			24	Actualización Documento

SUBDIRECCION DE GESTION Y MANEJO DE AREAS PROTEGIDAS
Calle 74 No. 11 - 81 Piso 3 Bogotá, D.C., Colombia
Teléfono: 353 2400 Ext.: 3141
www.parquesnacionales.gov.co

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

SUBDIRECCION DE GESTION Y MANEJO DE AREAS PROTEGIDAS
Calle 74 No. 11 - 81 Piso 3 Bogotá, D.C., Colombia
Teléfono: 353 2400 Ext.: 3141
www.parquesnacionales.gov.co

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 en Línea 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.

OBJETIVOS

2.1. OBJETIVO GENERAL

Dar continuidad a la estrategia de Seguridad de la información, para garantizar la gestión y mejora continua del Subsistema de Gestión de Seguridad de la Información – SGSI de Parques Nacionales Naturales de Colombia, respondiendo así a las necesidades de preservar la confidencialidad, integridad y disponibilidad de los activos de información de la entidad, la cual está acorde a los requerimientos del modelo de seguridad de la estrategia de gobierno en línea, los requerimientos del negocio y en cumplimiento de las disposiciones legales vigentes.

2.2. OBJETIVOS ESPECIFICOS

- Establecer actividades, responsables y tiempo de ejecución para continuar con la implementación y mejora del Sistema de Seguridad de la Información de Parques Nacionales Naturales de Colombia, el cual se encuentra bajo los requisitos del Modelo de Seguridad y Privacidad de la Información MPSI del MINTIC, establecido como habilitador transversal de seguridad de la información en la Política de Gobierno Digital.

SUBDIRECCION DE GESTION Y MANEJO DE AREAS PROTEGIDAS
Calle 74 No. 11 - 81 Piso 3 Bogotá, D.C., Colombia
Teléfono: 353 2400 Ext.: 3141
www.parquesnacionales.gov.co

- Desarrollar el plan de Comunicación para la implementación de la estrategia de Seguridad de la Información del SGSI que tiene diseñada la entidad para su ejecución en la vigencia 2021.

- Continuar con la implementación y gestión del Subsistema de Seguridad de la Información en Parques Nacionales Naturales de Colombia mediante el desarrollo de las actividades planteadas en el presente plan, en el control operacional y la estrategia de divulgación.

2.3. DERECHOS DEL DOCUMENTO

Documento de uso interno y exclusivo de Parques Nacionales Naturales de Colombia este contiene información confidencial de la Dirección Central de Parques Nacionales Naturales de Colombia y para lo cual el lector de este documento se compromete a resguardar y no divulgar la información contenida en el mismo.

Así mismo, este documento se considera propiedad de Parques Nacionales Naturales de Colombia y su divulgación parcial o total a terceros, no está permitida sin el consentimiento previo y explícito por escrito de la Entidad.

ALCANCE

Conforme en el alcance definido para el Sistema de Gestión de Seguridad de la Información de Parques Nacionales Naturales de Colombia, se define que el alcance del Plan de Seguridad de la Información involucra los procesos de direccionamiento, misionales y de apoyo, así como las sedes de la entidad a nivel nacional. De igual manera Parques Nacionales Naturales de Colombia, acorde con su misionalidad y naturaleza declara aplicables todos los requisitos de la NTC/ISO 27001:2013 y todos los controles del Anexo A, sin excepción alguna.

SUBDIRECCION DE GESTION Y MANEJO DE AREAS PROTEGIDAS
Calle 74 No. 11 - 81 Piso 3 Bogotá, D.C., Colombia
Teléfono: 353 2400 Ext.: 3141
www.parquesnacionales.gov.co

REQUERIMIENTOS LEGALES

NORMA	FECHA	DESCRIPCION
Ley 527 de 1999	18/08/1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones
Ley 1266 de 2008	31/12/2008	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
Ley 1341 de 2009	30/07/2009	Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
Ley 1581 de 2012	17/10/2012	Por la cual se dictan disposiciones generales para la protección de datos personales
Ley 1712 de 2014	03/06/2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones
Ley 1753 de 2015	9/06/2015	Por medio de la cual se expide el PND 2014-2018 “Todos por un nuevo país” en el Art. 45 establece “Estándares, modelos y lineamientos de tecnologías de la información y las comunicaciones para los servicios al ciudadano”.
Ley 1955 de 2019	25/05/2019	Por la cual se expide el Plan Nacional de Desarrollo 2018-2022. “Pacto por Colombia, Pacto por la Equidad”.
Decreto 2573 de 2014	12/12/2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Decreto 1078 de 2015	26/05/2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Decreto 415 de 2016	07/03/2016	Por el cual se adiciona el Decreto Único reglamentario del sector de la Función Pública, Decreto 1083 de 2015, en lo

SUBDIRECCION DE GESTION Y MANEJO DE AREAS PROTEGIDAS
Calle 74 No. 11 - 81 Piso 3 Bogotá, D.C., Colombia
Teléfono: 353 2400 Ext.: 3141
www.parquesnacionales.gov.co

		relacionado con la definición de lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.
CONPES 3701 de 2011	14/07/2011	Lineamientos de Política para Ciberseguridad y Ciberdefensa
CONPES 3854 de 2016	11/04/2016	Política nacional de seguridad digital

METODOLOGIA PARA LA IMPLEMENETACIÓN DEL MODLEO DE SEGURIDAD Y PRIVACIDAD

3.1. CICLO DE OPERACIÓN

El Modelo de Seguridad y Privacidad de la Información de la Estrategia de Gobierno en Línea 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].

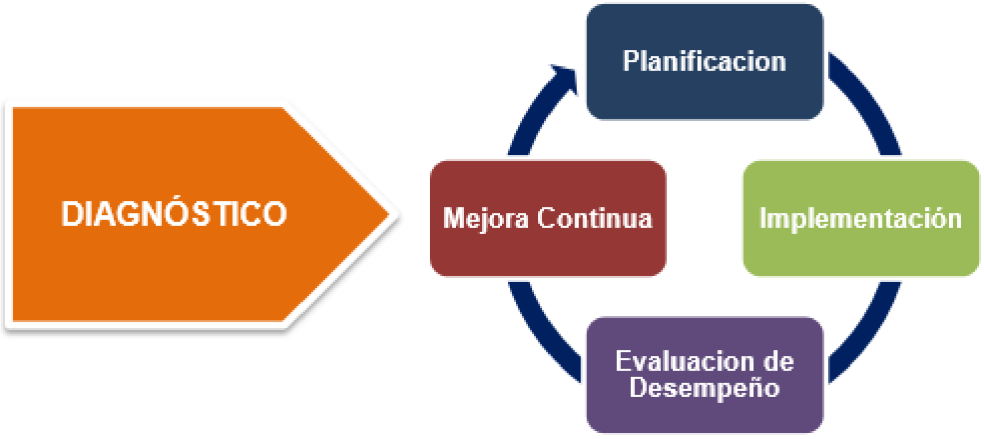


Figura 1: Ciclo de Operación Modelo de Seguridad y Privacidad de la Información
Fuente: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

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

SUBDIRECCION DE GESTION Y MANEJO DE AREAS PROTEGIDAS
Calle 74 No. 11 - 81 Piso 3 Bogotá, D.C., Colombia
Teléfono: 353 2400 Ext.: 3141
www.parquesnacionales.gov.co

- **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

3.2. 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, la nueva estructura de esta versión se puede alinear con el ciclo de mejora continua de las modelos de gestión de la siguiente forma:

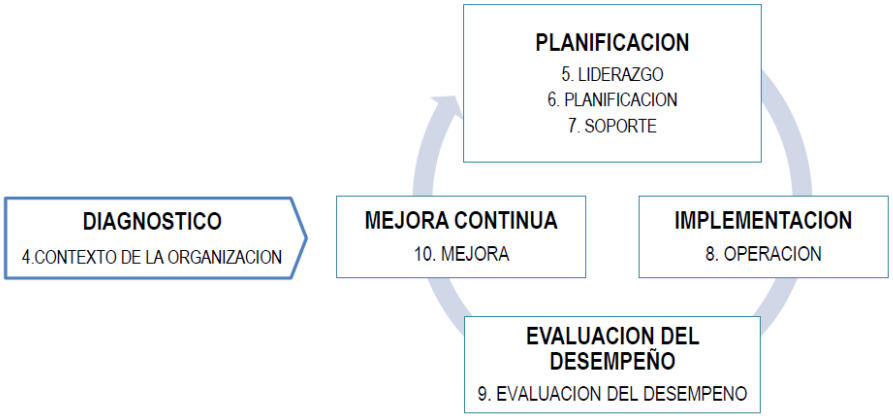


Figura 2: Norma ISO 27001:2013 alineada a la mejora continua
Fuente: Elaborada con base en la información publicada en la página web http://www.welivesecurity.com/la-es/2013/10/09/publicada-iso-270002013-cambios-en-la-norma-para-gestionar-la-seguridad-de-la-informacion/

SUBDIRECCION DE GESTION Y MANEJO DE AREAS PROTEGIDAS
Calle 74 No. 11 - 81 Piso 3 Bogotá, D.C., Colombia
Teléfono: 353 2400 Ext.: 3141
www.parquesnacionales.gov.co

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

- **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.

[2] NTC-ISO-IEC 27001:2013, Pág. 1-12

SUBDIRECCION DE GESTION Y MANEJO DE AREAS PROTEGIDAS
Calle 74 No. 11 - 81 Piso 3 Bogotá, D.C., Colombia
Teléfono: 353 2400 Ext.: 3141
www.parquesnacionales.gov.co

- **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.

- 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.

- 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.

3.3. FASE 1: DIAGNOSTICO

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 27001:2013**. **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 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 en Línea. **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

SUBDIRECCION DE GESTION Y MANEJO DE AREAS PROTEGIDAS
Calle 74 No. 11 - 81 Piso 3 Bogotá, D.C., Colombia
Teléfono: 353 2400 Ext.: 3141
www.parquesnacionales.gov.co

	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 de le entidad 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

3.4. 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

SUBDIRECCION DE GESTION Y MANEJO DE AREAS PROTEGIDAS
Calle 74 No. 11 - 81 Piso 3 Bogotá, D.C., Colombia
Teléfono: 353 2400 Ext.: 3141
www.parquesnacionales.gov.co

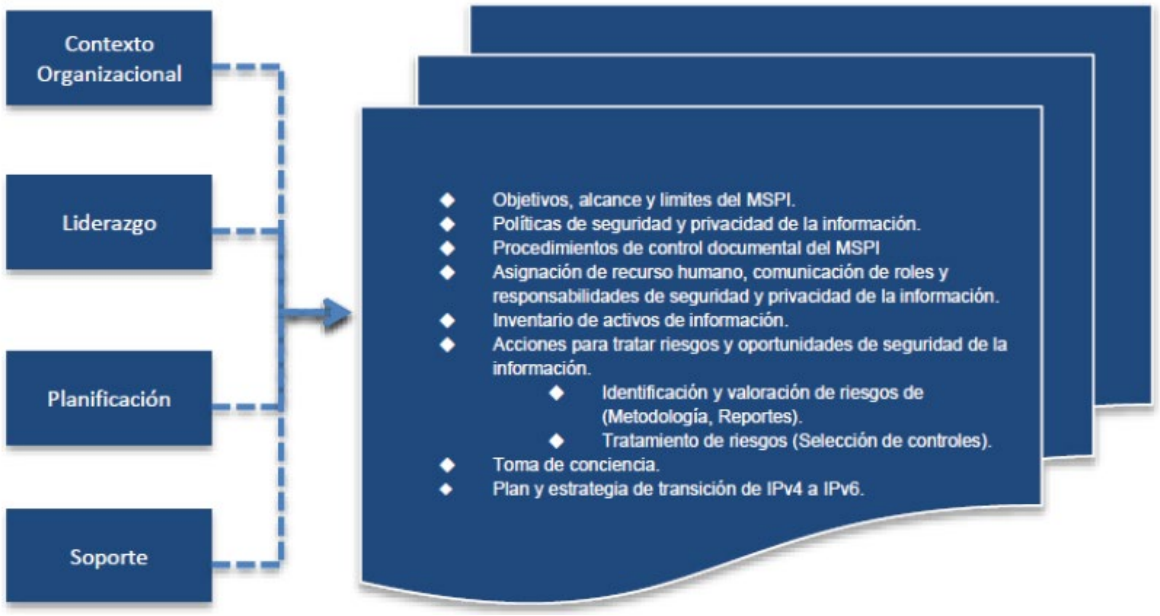


Figura 3: Fase de Planificación Modelo de Seguridad
Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno en Línea

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' 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.

SUBDIRECCION DE GESTION Y MANEJO DE AREAS PROTEGIDAS
Calle 74 No. 11 - 81 Piso 3 Bogotá, D.C., Colombia
Teléfono: 353 2400 Ext.: 3141
www.parquesnacionales.gov.co

	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.
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 27001:2013.
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.

SUBDIRECCION DE GESTION Y MANEJO DE AREAS PROTEGIDAS
Calle 74 No. 11 - 81 Piso 3 Bogotá, D.C., Colombia
Teléfono: 353 2400 Ext.: 3141
www.parquesnacionales.gov.co

3.5. FASE 3: IMPLEME NTACIÓN

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 de la entidad.

Figura 4: 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	**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

SUBDIRECCION DE GESTION Y MANEJO DE AREAS PROTEGIDAS
Calle 74 No. 11 - 81 Piso 3 Bogotá, D.C., Colombia
Teléfono: 353 2400 Ext.: 3141
www.parquesnacionales.gov.co

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.

SUBDIRECCION DE GESTION Y MANEJO DE AREAS PROTEGIDAS
Calle 74 No. 11 - 81 Piso 3 Bogotá, D.C., Colombia
Teléfono: 353 2400 Ext.: 3141
www.parquesnacionales.gov.co

3.6. 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 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.

SUBDIRECCION DE GESTION Y MANEJO DE AREAS PROTEGIDAS
Calle 74 No. 11 - 81 Piso 3 Bogotá, D.C., Colombia
Teléfono: 353 2400 Ext.: 3141
www.parquesnacionales.gov.co

3.7. 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

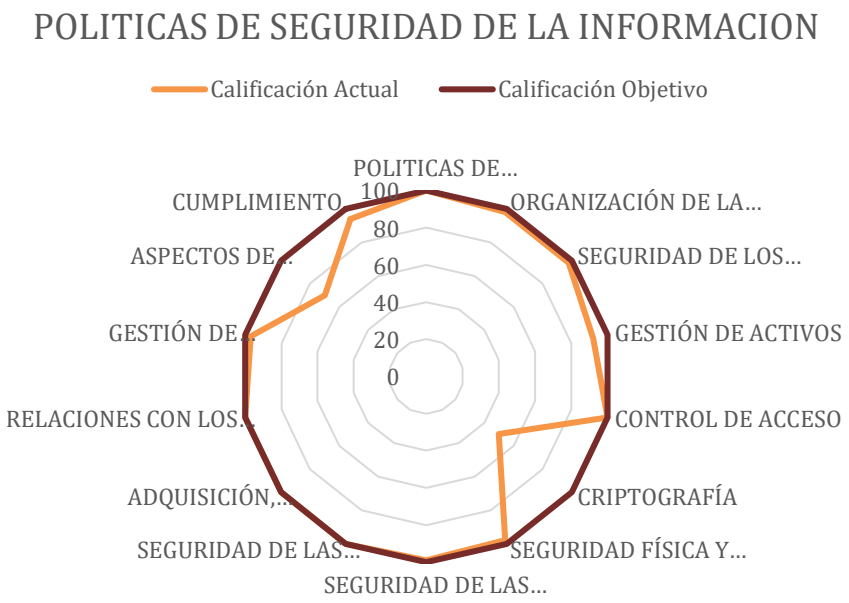
Figura 6: Fase Mejora Continua Modelo de Seguridad
Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno en Línea

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

SUBDIRECCION DE GESTION Y MANEJO DE AREAS PROTEGIDAS
Calle 74 No. 11 - 81 Piso 3 Bogotá, D.C., Colombia
Teléfono: 353 2400 Ext.: 3141
www.parquesnacionales.gov.co

RESULTADOS PARA LA VIGENCIA 2020

A continuación, se presentan los resultados de la vigencia 2020 así como los avances que ha logrado la entidad en la implementación del SGSI.



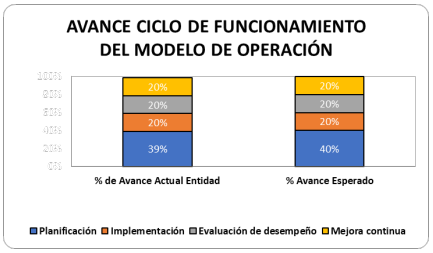
Brechas Anexo A ISO 27001:2013

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación	Calificación	EVALUACIÓN DE
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	98	100	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	98	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	92	100	OPTIMIZADO
A.9	CONTROL DE ACCESO	100	100	OPTIMIZADO
A.10	CRIPTOGRAFÍA	50	100	EFECTIVO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	98	100	OPTIMIZADO
A.12	SEGURIDAD DE LAS OPERACIONES	99	100	OPTIMIZADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	100	100	OPTIMIZADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	100	100	OPTIMIZADO
A.15	RELACIONES CON LOS PROVEEDORES	100	100	OPTIMIZADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	97	100	OPTIMIZADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	70	100	GESTIONADO
A.18	CUMPLIMIENTO	94	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		**93**	**100**	OPTIMIZADO

SUBDIRECCION DE GESTION Y MANEJO DE AREAS PROTEGIDAS
Calle 74 No. 11 - 81 Piso 3 Bogotá, D.C., Colombia
Teléfono: 353 2400 Ext.: 3141
www.parquesnacionales.gov.co

Como se observa en los datos anteriores, se concluye que la entidad, avanzó significativamente en la implementación de los controles del SGSI, obteniendo un promedio general de 93%, logrando una ubicación general del SGSI en un nivel de madurez "*Administrado*"; donde de los 14 dominios, 12 se encuentran en "Optimizado", 1 en el nivel "Efectivo" y 1 en el nivel "Definido".

En este mismo sentido y con relación al cumplimiento de la norma ISO27001:2013, visto desde la perspectiva del ciclo PHVA, se obtuvieron los siguientes resultados:



AVANCE PHVA		
COMPONENTE	% de	% Avance
Planificación	39%	40%
Implementación	20%	20%
Evaluación de desempeño	20%	20%
Mejora continua	20%	20%
TOTAL	99%	100%

Instrumento de identificación de la Línea Base de Seguridad para PNNC

ALINEACION CON EL PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION

Continuando con la ejecución de los proyectos descritos en el PETI y teniendo en cuenta los resultados y avances obtenidos anteriormente, para la vigencia 2021, se dará continuidad al desarrollo de actividades de implementación, fortalecimiento y mejoramiento al Subsistema de Gestión de Seguridad de la Información, a continuación, se presenta la ficha del proyecto:

Objetivo del Proyecto	Continuidad del desarrollo del Subsistema de Seguridad de la Información para Parques nacionales Naturales de Colombia. Realizar las actividades del plan de Seguridad de la Información para dar continuidad a la implementación, gestión, verificación y mejora continua del Sistema de Gestión de Seguridad de la Información – SGSI. con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los activos de información.

SUBDIRECCION DE GESTION Y MANEJO DE AREAS PROTEGIDAS
Calle 74 No. 11 - 81 Piso 3 Bogotá, D.C., Colombia
Teléfono: 353 2400 Ext.: 3141
www.parquesnacionales.gov.co

Iniciativas Asociadas			
Codigo	Nombre	Detalle	Estrategia de TI
	Desarrollo de las Fases de implementación y Mejora del SGSI	Continuar con la actualización de Control operacional; actualización de indicadores de gestión; Implementación de Plan de tratamiento de los riesgos; Implementar los controles (Definidos en la Declaración de aplicabilidad) y Ejecución de plan de comunicaciones y capacitación SGSI, así como desarrollar campañas de sensibilización de TI. Definir y desarrollar las estrategias para la implementación del plan de continuidad de Negocio	POLITICA DE GOBIERNO DIGITAL SUBSISTEMA DE SEGURIDAD DE LA INFORMACION PLAN DE COMUNICACIONES BCP / DRP
LINEA DE TIEMPO Y COSTOS			
Tiempo Aproximado de Implementación		Prioridad	Costo
11 Meses		Alta	Renovación Software Gestión SGSI: $150.000000 Actualización Centro de Computo Nivel Central y Direcciones Territoriales $1.800.000.000 Ampliación Capacidades DRP Google Cloud Platform $300.000.000
Descripción			
Con la ejecución de este proyecto, se continuará con la implementación y mejora del Subsistema de Gestión de Seguridad de la Información SGSI, el cual se encuentra articulado con la Política de Gobierno Digital y el Modelo Integrado de Planeación y Gestión – MIPG.			

SUBDIRECCION DE GESTION Y MANEJO DE AREAS PROTEGIDAS
Calle 74 No. 11 - 81 Piso 3 Bogotá, D.C., Colombia
Teléfono: 353 2400 Ext.: 3141
www.parquesnacionales.gov.co

PLANIFICACION VIGENCIA 2021

FASE	ACTIVIDADES	RESPPONSABLE	PERIODO DE EJECUCION	**Entregable**
Planificación	Determinar acciones a desarrollar de acuerdo con los resultados de la Auditoria al SGSI 2020	GSIR	Enero – Marzo 2021	Plan de Trabajo acciones de Mejora 2021
	Actualizar y publicar la Estrategia de Sensibilización y Divulgación del SGSI	GSIR	Abril 2021	Plan de Comunicaciones 2021
	Revisar y Actualizar los indicadores de gestión de SGSI	GSIR	Enero – Marzo 2021	Indicadores de Gestión 2021
	Elaborar el plan de trabajo para el SGSI para la vigencia 2021	GSIR	Marzo 2021	Plan de trabajo Vigencia 2021
Implementación	Consolidar información y generar documento de planeación del ejercicio de Análisis de Impacto al Negocio – BIA	GSIR	Abril – Junio 2021	Análisis de Brechas BIA
	Documentar y/o actualizar procedimientos del SGSI	GSIR	Abril – Diciembre 2021	Hoja metodológica 2021 MSPI
	Desarrollar las acciones para el dominio de Gestión de activos de información	GSIR	Abril – Diciembre 2021	Matriz Activos de Información e Inventario de activos tecnológicos 2021
	Ejecutar la Estrategia de divulgación y	GSIR	Abril – Diciembre 2021	Plan de Comunicaciones 2021

SUBDIRECCION DE GESTION Y MANEJO DE AREAS PROTEGIDAS
Calle 74 No. 11 - 81 Piso 3 Bogotá, D.C., Colombia
Teléfono: 353 2400 Ext.: 3141
www.parquesnacionales.gov.co

	sensibilización del SGSI.			
Evaluación y Desempeño	Revisar y hacer seguimiento, a la implementación del GSI (Monitoreo, medición, análisis y evaluación de indicadores).	GSIR COMITÉ INTERINSTITUCIONAL	Abril – Diciembre 2021	Hoja metodológica 2021 MSPI
	Realizar el Autodiagnóstico de la implementación del SGSI con la nueva herramienta de Gobierno Digital	GSIR	Abril – Noviembre 2021	Instrumento de Autodiagnóstico MSPI 2021
	Realizar Análisis de Vulnerabilidades a la infraestructura de TI	GSIR	Enero – Diciembre 2021	Informe de análisis de Vulnerabilidades y plan de mitigación
Mejora Continua	Revisar y ejecutar las acciones definidas en el plan de trabajo del SGSI como mejoramiento continuo del subsistema.	GSIR	Abril – Diciembre 2021	Hoja metodológica 2021 MSPI
	Comunicar resultados de auditoria	Control Interno	Diciembre 2021	Informe Acciones Correctivas Auditoria

SUBDIRECCION DE GESTION Y MANEJO DE AREAS PROTEGIDAS
Calle 74 No. 11 - 81 Piso 3 Bogotá, D.C., Colombia
Teléfono: 353 2400 Ext.: 3141
www.parquesnacionales.gov.co