

**SUPERINTENDENCIA
NACIONAL DE
BIENES ESTATALES**



RESOLUCIÓN N° 0017-2023/SBN-GG

San Isidro, 15 de febrero de 2023

VISTOS:

El Informe N° 00002-2023/SBN-OSI de fecha 2 de febrero de 2023, del Oficial de Seguridad y Confianza Digital; el Memorándum N° 00002-2023/SBN-STCGTD de fecha 2 de febrero de 2023, del Secretario Técnico del Comité de Gobierno Digital de la Superintendencia Nacional de Bienes Estatales; el Informe N° 000229-2023/SBN-OPP de fecha 6 de febrero de 2023, de la Oficina de Planeamiento y Presupuesto; el Informe N° 0050-2023/SBN-OAJ de fecha 8 de febrero de 2023, de la Oficina de Asesoría Jurídica, y;

CONSIDERANDO:

Que, la Resolución Ministerial N° 004-2016-PCM aprobó el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática, y en los numerales 4.3 y 4.4 de esta Norma Técnica se dispone que la organización debe determinar los límites y la aplicabilidad del sistema de gestión de seguridad de la información para establecer su alcance, así como, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información, respectivamente;

Que, mediante el literal a) del artículo 105 en concordancia con el numeral 109.1 del artículo 109 del Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo, aprobado por el Decreto Supremo N° 029-2021-PCM, se establece que las entidades de la Administración Pública tienen la obligación de implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI), toda vez que

comprende el conjunto de políticas, lineamientos, procedimientos, recursos y actividades asociadas, que gestiona una entidad con el propósito de proteger sus activos de información, de manera independiente del soporte en que estos se encuentren; asimismo, es un sistema que contempla la gestión de riesgos e incidentes de seguridad de la información y seguridad digital, la implementación efectiva de medidas de ciberseguridad, y acciones de colaboración y cooperación;

Que, a través del artículo 111 del Reglamento citado en el considerando precedente, se establece que el Titular de la entidad es responsable de la implementación del SGSI, el Comité de Gobierno Digital es responsable de dirigir, mantener y supervisar el SGSI de la entidad y el Oficial de Seguridad Digital es el responsable de coordinar su implementación y mantenimiento;

Que, con el numeral 112.1 del artículo 112 del citado Reglamento, se dispone que las entidades públicas capacitan e informan a su personal sobre sus derechos y obligaciones en materia de seguridad de la información y seguridad digital, siendo estos últimos responsables de su aplicación en el ejercicio de sus funciones y actividades;

Que, mediante el literal d) del artículo 2 del Decreto de Urgencia N° 006-2020, que crea el Sistema Nacional de Transformación Digital, se dispone que son principios del mencionado Sistema la protección de datos personales y preservación de la seguridad, y las competencias digitales, el mismo que consiste en asegurar la estructura de gobernanza, regulación y liderazgo que facilite el equilibrio entre la apertura de datos y los niveles adecuados de privacidad y seguridad digital; y, en el artículo 3, precisa que la transformación digital es el proceso continuo, disruptivo, estratégico y de cambio cultural que se sustenta en el uso intensivo de las tecnologías digitales, sistematización y análisis de datos para generar efectos económicos, sociales y de valor para las personas;

Que, a través de los literales d) y e) del artículo 3 de la Resolución N° 065-2018/SBN, modificada por las Resoluciones Nros. 0074-2018/SBN, 0092-2018/SBN, 024-2019/SBN y 0014-2022/SBN, se establece que es función del Comité de Gobierno Digital de la Superintendencia Nacional de Bienes Estatales gestionar la asignación de personal y recursos necesarios para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en sus Planes Operativos Institucionales, Plan Anual de Contrataciones y otros; y, promover y gestionar la implementación de estándares y buenas prácticas en gestión y gobierno de tecnologías digitales, interoperabilidad, seguridad digital, identidad digital y datos en la entidad, respectivamente;

Que, la Directiva N° DIR-00001-2022/SBN-OPP denominada “Disposiciones para la gestión de los planes institucionales de la Superintendencia Nacional de Bienes Estatales – SBN”, aprobada con la Resolución N° 0076-2022/SBN-GG, regula la elaboración, aprobación, ejecución, seguimiento, evaluación y modificación de los planes institucionales de la entidad y contribuir de esa manera a mejorar su gestión y el logro de los objetivos institucionales;

Que, mediante el acápite 6.1.1. del numeral 6.1. de las Disposiciones Específicas de la Directiva N° DIR-00001-2022/SBN-OPP, se indica que las unidades de organización pueden proponer el plan de trabajo de acuerdo a sus propias necesidades o en el marco de lo regulado por norma particular, debiendo detallar las actividades para el logro de sus objetivos y metas conforme a las prioridades institucionales, siendo que la Oficina de Planeamiento y Presupuesto valida el plan de trabajo propuesto conforme a los criterios establecidos y, de estar conforme, emite el informe de viabilidad técnica y es quien deriva este informe a la Oficina de Asesoría Jurídica cuando corresponda a los sistemas administrativos;

Que, adicionalmente, en los literales e) y f) del acápite 6.1.2. del numeral 6.2. de las Disposiciones Específicas de la precitada Directiva, se establece que los planes institucionales validados deben encontrarse suscritos por el área proponente de manera digital o física; siendo aprobados mediante acto resolutivo, siendo que en el caso de los planes de trabajo son aprobados por el Despacho de la Superintendencia Nacional de Bienes Estatales, la cual es una facultad delegable en el Gerente General, y cuenta con el visado de las unidades de organización involucradas;

Que, en el marco normativo antes reseñado, con el Informe N° 00002-2023/SBN-OSI de fecha 2 de febrero de 2023, el Oficial de Seguridad y Confianza Digital propone el Plan de Trabajo para la Implementación del Sistema de Gestión de Seguridad de la Información de la Superintendencia Nacional de Bienes Estatales, el mismo que ha sido socializado por los miembros del Comité de Gobierno y Transformación Digital de la Superintendencia Nacional de Bienes Estatales, y es con el cual se pretende efectuar actividades de planificación durante el año 2023 consideradas prioritarias, con la finalidad de implementar de manera secuencial el Sistema de Gestión de la Seguridad y Confianza Digital en la entidad;

Que, con el Informe N° 00229-2023/SBN-OPP de fecha 6 de febrero de 2023, la Oficina de Planeamiento y Presupuesto opina que la propuesta del Plan de Trabajo para la Implementación del Sistema de Gestión de Seguridad de la Información de la Superintendencia Nacional de Bienes Estatales, se justifica en el marco de los lineamientos establecidos en el inciso e) del numeral 6.1. de la Directiva N° DIR-00001-2022/SBN-OPP, su contenido se ajusta al contenido mínimo dispuesto en el Anexo 3 de la precitada Directiva, y de otro lado, la propuesta se encuentra vinculada al Objetivo Estratégico Institucional OEI.04 Mejorar la Gestión Institucional, a la Acción Estratégica Institucional AEI.04.02 Sistemas de Información Implementados bajo un enfoque de procesos y digital para la Gestión Institucional, la AEI.04.05 Gestión de Gobierno Digital desplegado en el marco de la transformación digital en la Superintendencia Nacional de Bienes Estatales y la Actividad Operativa AO.9.1.2 Fortalecimiento del Gobierno Digital; asimismo, precisa que la propuesta de plan no requerirá presupuesto, por lo que concluye que se encuentra conforme con la propuesta, por lo que, emite viabilidad técnica favorable para la continuación del trámite de aprobación correspondiente;

Que, con el Informe N° 0050-2023/SBN-OAJ de fecha 8 de febrero de 2023, la Oficina de Asesoría Jurídica expresa que la propuesta de Plan de Trabajo para la Implementación del Sistema de Gestión de Seguridad de la Información de la Superintendencia Nacional de Bienes Estatales, cumple con las disposiciones para la

elaboración y aprobación de los planes, previstas en el numeral 6.1. de las Disposiciones Específicas de la Directiva N° DIR-00001-2022/SBN-OPP aprobada mediante la Resolución N° 0076-2022/SBN-SG, por lo que emite opinión legal favorable. Asimismo, indica que atendiendo a lo regulado en el artículo 111 del Reglamento del Decreto Legislativo N° 1412, aprobado por el Decreto Supremo N° 029-2021-PCM, se establece que el Titular de la entidad es responsable de la implementación del SGSI, por lo que bajo dicha prerrogativa normativa, puede aprobar el plan propuesto, lo cual es concordante con la Resolución N° 063-2017/SBN a través del cual se delegó en la Gerencia General la facultad para aprobar los planes de trabajo a nivel institucional, delegación de facultad que a su vez, guarda armonía con las funciones previstas en los literales c) y d) del artículo 11 del Texto Integrado del Reglamento de Organización y Funciones de la Superintendencia Nacional de Bienes Estatales, aprobado por la Resolución N° 0066-2022/SBN; en tal sentido, el Gerente General cuenta con la facultad para aprobar el plan propuesto;

Que, bajo el contexto normativo y evaluaciones técnica y legal mencionadas en los considerandos precedentes, el Plan de Trabajo para la Implementación del Sistema de Gestión de Seguridad de la Información de la Superintendencia Nacional de Bienes Estatales, permitirá el despliegue de las actividades para la implementación del Sistema de Gestión de Seguridad de la Información, así como se plantean unidades de medida que permitirá su evaluación y/o reajustes en su implementación, por lo que es necesario aprobarlo mediante el acto resolutorio correspondiente;

Con el visado de la Oficina de Asesoría Jurídica, la Oficina de Planeamiento y Presupuesto, y el Oficial de Seguridad y Confianza Digital de la Superintendencia Nacional de Bienes Estatales, y;

De conformidad con lo dispuesto en la Resolución Ministerial N° 004-2016-PCM; el Reglamento del Decreto Legislativo N° 1412, aprobado por el Decreto Supremo N° 029-2021-PCM; el Decreto de Urgencia N° 006-2020; la Resolución N° 065-2018/SBN y modificatorias; la Directiva N° DIR-00001-2022/SBN-OPP, aprobada con la Resolución N° 0076-2022/SBN-GG; y, conforme a la función prevista en los literales c) y d) del artículo 11 del Texto Integrado del Reglamento de Organización y Funciones de la Superintendencia Nacional de Bienes Estatales, aprobado por la Resolución N° 0066-2022/SBN;

RESUELVE:

Artículo 1.- Aprobar el “Plan de Trabajo para la Implementación del Sistema de Gestión de Seguridad de la Información de la Superintendencia Nacional de Bienes Estatales”, que como anexo forma parte integrante de la presente Resolución.

Artículo 2.- La ejecución del documento aprobado mediante el artículo 1 de la presente Resolución estará a cargo del Oficial de Seguridad y Confianza Digital, y el Comité de Gobierno y Transformación Digital de la Superintendencia Nacional de Bienes Estatales es el encargado de coordinar el avance del plan y garantizar los recursos necesarios para su implementación.

Artículo 3.- Disponer la notificación de la presente Resolución y su anexo al Oficial de Seguridad y Confianza Digital, al Secretario Técnico del Comité de Gobierno y Transformación Digital de la Superintendencia Nacional de Bienes Estatales – SBN y a la Líder de Gobierno y Transformación Digital, para los fines pertinentes.

Artículo 4.- Publicar la presente Resolución y su Anexo en el día de su emisión, en la Sede Digital de la Superintendencia Nacional de Bienes Estatales (www.gob.pe/sbn).

Regístrese y comuníquese.

PAUL ALEX LLAMOJA CABANILLAS
Gerente General
Superintendencia Nacional de Bienes Estatales



TIPO DE DOCUMENTO : PLAN DE TRABAJO

NOMBRE DEL DOCUMENTO : PLAN DE TRABAJO PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA SUPERINTENDENCIA NACIONAL DE BIENES ESTATALES

NÚMERO DE DOCUMENTO : SGSI-PLAN-001-2023/SBN-OTI

NOMBRE DE LA UNIDAD DE ORGANIZACIÓN : OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

San Isidro, febrero de 2023

Versión : No. 1

Índice

Contenido

1. PRESENTACIÓN.....	3
2. ANTECEDENTES	3
3. ESTADO DE IMPLEMENTACIÓN DEL SGSI EN LA SBN	4
4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	4
5. BASE LEGAL.....	4
6. ALCANCE.....	6
7. OBJETIVO	6
7.1. Objetivo del Plan	6
7.2. Vinculación con el PEI y POI	6
8. INDICADOR	7
9. ACTIVIDADES O TAREAS PENDIENTES DE EJECUTAR.....	7
9.1. Actividades o Tareas.....	7
9.2. Vinculación con el POI	8
10. RECURSOS / INSUMOS.....	8
10.1. Personal.....	8
10.1.1.Grupo o Equipo de Trabajo	8
10.1.2.Puestos, Grupos u Órgano Colegiado	9
10.2. Bienes, Servicios y Otros	11
10.2.1. Bienes	11
10.2.2.Servicio(s)	12
11. PRESUPUESTO.....	12
12. SEGUIMIENTO Y EVALUACIÓN.....	12
12.1.Comité de Gobierno y Transformación Digital.....	12
13. CRONOGRAMA DE EJECUCIÓN	13

PLAN DE TRABAJO PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA SUPERINTENDENCIA NACIONAL DE BIENES ESTATALES

1. PRESENTACIÓN

La información es el activo más importante del cual depende el funcionamiento de la institución.

Para alcanzar los objetivos de la SBN, es esencial mantener los principios de confidencialidad, integridad y disponibilidad, motivos por los cuales, la información debe estar siempre protegida.

Un Sistema de Gestión de Seguridad de la Información (SGSI) es un sistema que nos permite tener una herramienta de gestión que nos ayuda a implementar, gestionar y minimizar los posibles riesgos que puedan atentar contra la seguridad de la información en la SBN.

El presente plan de trabajo plantea el establecimiento de las bases para la implementación de un Sistema de Gestión de Seguridad de la Información en la SBN. Su desarrollo contempla la implementación de un solo proceso misional el cual constituye el inicio de la implementación del SGSI en la SBN.

2. ANTECEDENTES

Con Resolución Ministerial N° 004-2016-PCM se aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

A continuación, se indican las fases o etapas de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014, para su implementación.

- a. Contexto de la Organización.
- b. Liderazgo.
- c. Planificación.
- d. Soporte.
- e. Operación.
- f. Evaluación.
- g. Mejora Continua.

3. ESTADO DE IMPLEMENTACIÓN DEL SGSI EN LA SBN

Con Resolución N° 0062-2021/SBN se aprobó el documento SGSI-PLAN-001-2021/SBN-OAF denominado “Plan de gestión para la implementación del proyecto del Sistema de Gestión de Seguridad de la Información de la SBN”.

En dicho documento aprobado, se encuentran los seis (6) componentes de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014", asignadas como fases y descritas a detalle en el Anexo I titulado Cronograma de Actividades del Plan de Trabajo.

De lo descrito en el párrafo anterior, se indica que ya se encuentran implementadas las siguientes fases y sus respectivos subcomponentes:

Fase 1: Elaborar el contexto de la Organización

- Elaborar el Plan del proyecto de implementación de la SGSI.
- Elaborar el Alcance del SGSI.

Fase 2: Determinar el Liderazgo.

- Determinar el compromiso de la Alta Dirección de la SBN dentro del proyecto de implementación del SGSI.

4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Con Resolución N° 0061-2021/SBN se aprobó el documento denominado Política de Seguridad de la Información de la Superintendencia Nacional de Bienes Estatales y es parte de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014" en su fase 2. Por lo tanto, el presente plan de trabajo es complemento y se encuentra alineado a esta política ya adoptada en la SBN.

5. BASE LEGAL

- ✓ Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado y modificatorias.
- ✓ Ley N° 27309, Ley que incorpora los delitos informáticos al Código Penal.
- ✓ Ley N° 28493, Ley que regula el uso del correo electrónico comercial no solicitado (SPAM), modificada por la Ley N° 29246.
- ✓ Ley N° 29733, Ley de Protección de Datos Personales, modificada por el Decreto Legislativo N° 1353.
- ✓ Decreto Supremo N° 003-2013-JUS, que aprueba el Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales.

- ✓ Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
- ✓ Resolución Ministerial N° 166-2017-PCM, que modifican el artículo 5 de la Resolución Ministerial N° 004-2016-PCM, referente al Comité de Gestión de Seguridad de la Información.
- ✓ Decreto Supremo N° 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.
- ✓ Decreto de Urgencia N° 007-2020, que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
- ✓ Norma Técnica Peruana NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición.
- ✓ Norma Técnica Peruana NTP-ISO 31000:2018 Gestión del riesgo. Directrices. 2a Edición.
- ✓ ISO/IEC 27002:2013 Tecnología de la Información. Técnicas de seguridad. Código de Buenas Prácticas para los controles de seguridad de la información.
- ✓ ISO/IEC 27005:2009 Tecnología de la Información. Técnicas de seguridad. Gestión del Riesgo en la seguridad de la información.
- ✓ Resolución N° 0014-2022/SBN, que modifica la Resolución N° 065-2018/SBN, que conforma el Comité de Gobierno Digital de la Superintendencia Nacional de Bienes Estatales – SBN, modificada con las Resoluciones Nros. 074-2018/SBN, 092-2018/SBN, 024-2019/SBN y 0014-2022/SBN.
- ✓ Resolución N° 0061-2021/SBN, que aprueba el documento SGSI-POL-001 denominado "Políticas de la Seguridad de la Información de la Superintendencia Nacional de Bienes Estatales".
- ✓ Resolución N° 0062-2021/SBN, que aprueba el documento SGSI-PLAN-001-2021/SBN-OAF denominado "Plan de Gestión para la Implementación del Proyecto del Sistema de Gestión de Seguridad de la Información de la SBN".

6. ALCANCE

El presente Plan de Trabajo es aplicado al Proceso Misional M01, denominado Gestión de Predios Estatales, para la implementación del Sistema de Gestión de Seguridad de la Información.

7. OBJETIVO

7.1. Objetivo del Plan

Implementar el SGSI que permita realizar la gestión adecuada de los riesgos que comprometan la confidencialidad, integridad y disponibilidad de la información en la Superintendencia Nacional de Bienes Estatales.

7.2. Vinculación con el PEI y POI

Objetivo Estratégico Institucional – PEI	Acción Estratégica Institucional	Objetivo del Plan
OEI.04 Mejorar la Gestión Institucional	AEI.04.02 Sistemas de Información implementados bajo un enfoque de procesos y digital para la gestión institucional.	OBJ.01 Implementar el Sistema de Gestión de Seguridad de la Información (SGSI), que permita realizar la gestión adecuada de los riesgos que comprometan la confidencialidad, integridad y disponibilidad de la información en la Superintendencia Nacional de Bienes Estatales.
	AEI.04.05 Gestión de Gobierno Digital desplegado en el marco de transformación digital en la SBN.	

8. INDICADOR

Objetivo del Plan	Nombre del Indicador	Método de cálculo	Logro esperado
OBJ.01 Implementar el Sistema de Gestión de Seguridad de la Información (SGSI), que permita realizar la gestión adecuada de los riesgos que comprometan la confidencialidad, integridad y disponibilidad de la información en la Superintendencia Nacional de Bienes Estatales.	Porcentaje de Fases Implementadas del SGSI con actos aprobados por el Comité de Gobierno y Transformación Digital, en favor de la SBN.	$\frac{\text{Núm. de Fases Imp.}}{\text{Total, de Fases}} * 100 = R$ Porcentaje de Fases Implementadas	100%

Justificación: El indicador cuantifica la implementación de las fases del SGSI, según el alcance definido al Proceso Misional M01, denominado Gestión de Predios Estatales. Permite medir el Porcentaje de Fases Implementados del SGSI con actos aprobados por el Comité de Gobierno y Transformación Digital, promoviendo la cultura de la seguridad en la SBN.

Responsables del indicador: Alta Dirección, Comité de Gobierno y Transformación Digital y Oficial de Seguridad y Confianza Digital.

9. ACTIVIDADES O TAREAS PENDIENTES DE EJECUTAR

9.1. Actividades o Tareas

FASE Y TAREAS DE LA ACTIVIDAD OPERATIVA:

Fase 3: Act.01 Realizar la Planificación.

- Definir la metodología de evaluación de riesgos de información del SGSI en base al alcance establecido.
- Realizar el inventario de activos correspondiente al Alcance del SGSI.
- Elaborar la evaluación y tratamiento de riesgos.
- Redactar el documento de la declaración de aplicabilidad (SOA).
- Elaborar el plan de tratamiento de riesgos.

Fase 4: Act.02 Implementar el Soporte.

- Concientizar al personal de toda la Organización de la SBN sobre la importancia de la seguridad de la información.

Fase 5: Act.03 Generar la Operación.

- Implantar los controles seleccionados.
- Documentar los procedimientos, políticas y requisitos necesarios del SGSI.
- Implementar el plan de tratamiento de riesgos y documentar los resultados.

Fase 6: Act.04 Realizar la Evaluación.

- Realización de Auditoría Interna del SGSI.

Fase 7: Act.05 Implementar la Mejora Continua.

- Preparar los planes de acción de las no conformidades y las recomendaciones de la auditoría.
- Difusión a los integrantes del Comité de Gobierno Digital para su revisión por la Alta Dirección.
- Aprobación por el Comité de Gobierno Digital referido a la implementación de SGSI.
- Gestionar la aprobación formal institucional (OPP-OAJ-GG-ADIR).

9.2. Vinculación con el POI

Actividad Operativa POI	Actividad o tarea del Plan	
9.1.2 Fortalecimiento del Gobierno Digital.	Fase 3	Act.01 Realizar la planificación
	Fase 4	Act.02 Implementar el soporte
	Fase 5	Act.03 Generar la operación
	Fase 6	Act.04 Realizar la evaluación
	Fase 7	Act.05 Implementar la mejora continua

10. RECURSOS / INSUMOS

10.1. Personal

10.1.1. Grupo o Equipo de Trabajo

La función del grupo o equipo de trabajo es realizar el trabajo operativo de la implementación y realizar tareas establecidas y tomar decisiones sobre diversos temas que requieren un enfoque multidisciplinario.

La Líder de Gobierno Digital es la responsable de reunir al equipo de trabajo para hacer el seguimiento del avance del plan del proyecto de SGSI y en otros casos cuando el Comité de Gobierno Digital lo considere necesario.

El equipo de trabajo estará conformado por:

1. Personal que involucre el alcance del SGSI.
2. Líder de Gobierno Digital.
3. Personal de OTI.
3. Oficial de Seguridad y Confianza Digital (OSyCD).
4. Especialista Técnico de Seguridad de la Información.

10.1.2. Puestos, Grupos u Órgano Colegiado

Las Fases 1 y 2 se encuentran ejecutadas, mientras que el presente Plan corresponde realizar las Fases tres (3) a la Fase siete (7).

Actividad o tarea del Plan		Responsables
Fase 1	Act.01 Contexto de la Organización	
1	Elaborar Plan de Trabajo para la Implementación del Sistema de Gestión de Seguridad de la Información de la Superintendencia Nacional de Bienes Estatales.	- Oficial de Seguridad y Confianza Digital. - Comité de Gobierno y Transformación Digital. - Alta Dirección.
2	Elaborar el Alcance del SGSI	- Oficial de Seguridad y Confianza Digital. - Comité de Gobierno y Transformación Digital. - Alta Dirección.
Fase 2	Act.02 Liderazgo	
1	Determinar el compromiso de la Alta Dirección de la SBN dentro del proyecto de implementación del SGSI.	- Comité de Gobierno Digital. - Alta Dirección.
Fase 3	Act.03 Planificación	
1	Definir la metodología de evaluación de riesgos de información del SGSI en base al alcance establecido.	- Oficial de Seguridad y Confianza Digital. - Comité de Gobierno y Transformación Digital. - Alta Dirección.

2	Realizar el inventario de activos correspondiente al Alcance del SGSI.	- Oficial de Seguridad y Confianza Digital. - Comité de Gobierno y Transformación Digital. - Alta Dirección.
3	Elaborar la evaluación y tratamiento de riesgos.	- Oficial de Seguridad y Confianza Digital. - Comité de Gobierno y Transformación Digital. - Alta Dirección.
4	Redactar el documento de la declaración de aplicabilidad (SOA).	- Oficial de Seguridad y Confianza Digital. - Comité de Gobierno y Transformación Digital. - Alta Dirección.
5	Elaborar el plan de tratamiento de riesgos.	- Oficial de Seguridad y Confianza Digital. - Comité de Gobierno y Transformación Digital. - Alta Dirección.
Fase 4	Act.04 Soporte	
1	Concientizar al personal de toda la organización de la SBN sobre la importancia de la seguridad de la información.	- Oficial de Seguridad y Confianza Digital. - Comité de Gobierno y Transformación Digital. - Alta Dirección.
Fase 5	Act.05 Operación	
1	Implantar los controles seleccionados.	- Oficial de Seguridad y Confianza Digital. - Comité de Gobierno y Transformación Digital. - Alta Dirección.
2	Documentar los procedimientos, políticas y requisitos necesarios del SGSI.	- Oficial de Seguridad y Confianza Digital. - Comité de Gobierno y Transformación Digital. - Alta Dirección.
3	Implementar el plan de tratamiento de riesgos y documentar los resultados.	- Oficial de Seguridad y Confianza Digital. - Comité de Gobierno y Transformación Digital. - Alta Dirección.
Fase 6	Act.06 Evaluación	
1	Realización de Auditoría Interna del SGSI.	- Auditores designados. - Comité de Gobierno y Transformación Digital. - Alta Dirección.

Fase 7	Act.07 Mejora Continua	
1	Preparar los planes de acción de las no conformidades y las recomendaciones de la auditoría.	- Auditores encargados. - Oficial de seguridad y Confianza Digital. - Comité de Gobierno y Transformación Digital. - Alta Dirección.
2	Difusión a los integrantes del Comité de Gobierno Digital para su revisión por la Alta Dirección.	- Oficial de Seguridad y Confianza Digital. - Comité de Gobierno y Transformación Digital. - Alta Dirección.
3	Aprobación por el Comité de Gobierno Digital referido a la implementación de SGSI.	- Comité de Gobierno y Transformación Digital. - Alta Dirección.
4	Gestionar aprobación formal institucional (OPP-OAJ-GG-ADIR).	- Comité de Gobierno Digital. - OPP. - ADIR, GG y OAJ.

10.2. Bienes, Servicios y Otros

10.2.1. Bienes

- NTP-ISO/IEC 27001:2014, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos, 2ª Edición.
- NTP-ISO/IEC 27002:2017, Tecnología de la Información. Técnicas de Seguridad. Código de Prácticas para Controles de Seguridad de la Información. 1ª Edición.
- NTP-ISO/IEC 27004:2018, Tecnología de la Información. Técnicas de Seguridad. Gestión de la Seguridad de la Información. Seguimiento, medición, análisis y evaluación. 2ª Edición.
- NTP-ISO/IEC 27005:2018, Tecnología de la Información. Técnicas de Seguridad. Gestión de Riesgos de la Seguridad de la Información. 2ª Edición.
- NTP-ISO/IEC 27014:2021, Seguridad de la Información, Ciberseguridad y Protección de la Privacidad. Gobernanza de Seguridad de la Información. 1ª Edición.
- NTP-ISO 31000:2018 Gestión del riesgo. Directrices. 2a Edición.
- NTP-ISO/IEC 27035-2:2019, Tecnología de la Información. Técnicas de Seguridad. Gestión de Incidentes de la Seguridad de la Información. Parte 2: Directrices para planificar y Prepararse para la respuesta a incidentes. 1ª Edición.

10.2.2. Servicio(s)

- Auditoría interna.

Objetivo del Plan	Actividad del Plan	Recursos / Insumos	Costo estimado anual
OBJ.01 Implementar el Sistema de Gestión de Seguridad de la Información (SGSI), que permita realizar la gestión adecuada de los riesgos que comprometan la confidencialidad, integridad y disponibilidad de la información en la Superintendencia Nacional de Bienes Estatales.	Act.01 Contexto de la Organización	Actividad Concluida	-----
	Act.02 Liderazgo	Actividad Concluida	-----
	Act.03 Planificación	NTP/ISO 27001:2014	-----
	Act.04 Soporte		
	Act.05 Operación		
	Act.06 Evaluación		
	Act.07 Mejora Continua		

11. PRESUPUESTO

Para el desarrollo del presente plan de trabajo no se requiere de presupuesto alguno.

12. SEGUIMIENTO Y EVALUACIÓN

12.1. Comité de Gobierno y Transformación Digital

Una de las funciones del Comité de Gobierno y Transformación Digital consiste principalmente en vigilar el cumplimiento de la normatividad relacionada con la implementación del Sistema de Gestión de la Seguridad de la Información (SGSI), gestionar, mantener y documentar el SGSI de la SBN.

Además, deberá coordinar el avance del proyecto y garantizar los recursos necesarios para la implementación del plan de gestión, revisar los entregables propuestos por el Oficial de Seguridad y Confianza Digital, promover la difusión y apoyo a la implementación y despliegue de la seguridad de la información dentro de la SBN e informar a la Alta Dirección sobre el progreso del proyecto dentro de los plazos establecidos en el presente plan.

El comité de gobierno y transformación digital está conformado por:

N°	Cargo	Oficina
1	Superintendente, Presidente del CGTD	ADIR
2	Gerente General, Miembro del CGTD	GG
3	Asesor de Alta Dirección, Líder de Gobierno y Transformación Digital	ADIR
4	Supervisor de Tecnologías de la Información, Secretario Técnico del CGTD	TI
5	Supervisor del Sistema Administrativo de Personal, Miembro del CGTD	SAPE
6	Jefe/a de la Unidad de Trámite Documentario, Miembro del CGTD	UTD
7	Oficial de Seguridad y Confianza Digital, Miembro del CGTD	OSyCD
8	Jefe de la Oficina de Asesoría Jurídica, Miembro del CGTD	OAJ
9	Jefe de la Oficina de Planeamiento y Presupuesto, Miembro del CGTD	OPP

Nota: En adelante SAPE es la Unidad de Recursos Humanos (URH) y TI es la Oficina de Tecnologías de la Información (OTI).

13. CRONOGRAMA DE EJECUCIÓN

La Programación de las Acciones del Plan de Trabajo de la Implementación del SGSI, el cual se presenta en el ANEXO 1, adjunto al presente documento.

Nota: La fecha de inicio del presente Plan de Trabajo propuesto en el anexo 1 será al día siguiente después de ser aprobado por el Comité de Gobierno y Transformación Digital.

ANEXO 1 – PROGRAMACIÓN DE LAS ACCIONES DEL PLAN DE TRABAJO DE LA IMPLEMENTACIÓN DEL SGSI

OBJ. 01 Implementar el Sistema de Gestión de Seguridad de la Información (SGSI), que permita realizar la gestión adecuada de los riesgos que comprometan la confidencialidad, integridad y disponibilidad de la información en la Superintendencia Nacional de Bienes Estatales

CÓDIGO	FASES	ACTIVIDADES	UNIDAD DE MEDIDA	Meses																META PROGRAMA	UNIDAD / COLEGIADO RESPONSABLE				
				Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8	Mes 9	Mes 10	Mes 11											
				SEM-1	SEM-2	SEM-3	SEM-4	SEM-1	SEM-2	SEM-3	SEM-4	SEM-1	SEM-2	SEM-3	SEM-4	SEM-1	SEM-2	SEM-3	SEM-4	SEM-1	SEM-2	SEM-3	SEM-4		
ACT.01	CONTEXTO DE LA ORGANIZACIÓN																								
	1	Elaborar el Plan de Gestión del Proyecto de Implementación del SGSI	Plan Aprobado	Subactividad concluido																1	- Oficial de Seguridad y Confianza Digital. - Comité de Gobierno y Transformación Digital. - Alta Dirección.				
		Elaborar el alcance del SGSI	Alcance del SGSI Aprobado	Subactividad concluido																1	- Oficial de Seguridad y Confianza Digital. - Comité de Gobierno y Transformación Digital. - Alta Dirección.				
ACT.02	LIDERAZGO																								
	2	Determinar el compromiso de la Alta Dirección de la SBN dentro del Proyecto de Implementación del SGSI	Actas suscritas con el compromiso de Alta Dirección para implementar el SGSI.	Subactividad concluido																1	- Oficial de Seguridad y Confianza Digital. - Comité de Gobierno y Transformación Digital. - Alta Dirección.				
		Elaborar la Política y Objetivos de Seguridad de la Información	Políticas y objetivos aprobados	Subactividad concluido																1	- Oficial de Seguridad y Confianza Digital. - Comité de Gobierno y Transformación Digital. - Alta Dirección.				
ACT.03	PLANIFICACIÓN																								
	3	Definir la metodología de evaluación y tratamiento de riesgos	Informe sobre la metodología de riesgos definida	[Gantt bar from Mes 1 SEM-1 to Mes 1 SEM-1]																1	- Oficial de Seguridad y Confianza Digital. - Comité de Gobierno y Transformación Digital. - Alta Dirección.				
		Realizar el inventario de activos correspondiente al alcance del SGSI	Inventario elaborado y presentado	[Gantt bar from Mes 1 SEM-1 to Mes 2 SEM-1]																1	- Oficial de Seguridad y Confianza Digital. - Comité de Gobierno y Transformación Digital. - Alta Dirección.				
		Elaborar la evaluación y tratamiento de riesgos	Informe de evaluación realizada y presentada	[Gantt bar from Mes 2 SEM-1 to Mes 3 SEM-1]																1	- Oficial de Seguridad y Confianza Digital. - Comité de Gobierno y Transformación Digital. - Alta Dirección.				
		Redactar el documento de la Declaración de Aplicabilidad (SOA)	Documento de Aplicabilidad aprobado	[Gantt bar from Mes 3 SEM-1 to Mes 4 SEM-1]																1	- Oficial de Seguridad y Confianza Digital. - Comité de Gobierno y Transformación Digital. - Alta Dirección.				
		Elaborar el Plan de Tratamiento de Riesgos	Plan de tratamiento de riesgos aprobado	[Gantt bar from Mes 4 SEM-1 to Mes 6 SEM-1]																1	- Oficial de Seguridad y Confianza Digital. - Comité de Gobierno y Transformación Digital. - Alta Dirección.				
ACT.04	SOPORTE																								
	4	Concientizar a todo el personal de la SBN, sobre la importancia de la Seguridad de la Información	Plan de capacitación sobre la importancia de seguridad de la información	[Gantt bar from Mes 2 SEM-1 to Mes 10 SEM-1]																1	- Oficial de Seguridad y Confianza Digital. - Comité de Gobierno y Transformación Digital. - Alta Dirección.				
ACT.05	OPERACIÓN																								
	5	Implantar los controles seleccionados	Controles implementados	[Gantt bar from Mes 6 SEM-1 to Mes 7 SEM-1]																100%	- Oficial de Seguridad y Confianza Digital. - Comité de Gobierno y Transformación Digital. - Alta Dirección.				
		Documentar los procedimientos, políticas y requisitos necesarios del SGSI	Políticas y Procedimientos del SGSI Documentados	[Gantt bar from Mes 7 SEM-1 to Mes 8 SEM-1]																100%	- Oficial de Seguridad y Confianza Digital. - Comité de Gobierno y Transformación Digital. - Alta Dirección.				
		Implementar el Plan de Tratamiento de Riesgos y documentar los resultados	Implementación del plan de riesgos	[Gantt bar from Mes 8 SEM-1 to Mes 9 SEM-1]																1	- Oficial de Seguridad y Confianza Digital. - Comité de Gobierno y Transformación Digital. - Alta Dirección.				
ACT.06	EVALUACIÓN																								
	6	Realización de Auditoría Interna del SGSI	Auditoría ejecutada	[Gantt bar from Mes 10 SEM-1 to Mes 11 SEM-1]																1	- Auditores designados. - Comité de Gobierno y Transformación Digital. - Alta Dirección.				
ACT.07	MEJORA CONTINUA																								
	7	Preparar los planes de acción de las no conformidades y las recomendaciones de la auditoría	Plan de acción de no conformidades ejecutado y aprobado	[Gantt bar from Mes 10 SEM-1 to Mes 11 SEM-1]																1	- Auditores designados. - Oficial de Seguridad y Confianza Digital. - Comité de Gobierno y Transformación Digital. - Alta Dirección.				
		Difusión a los integrantes del Comité de Gobierno Digital para su revisión por la Alta Dirección	Presentación del proyecto de SGSI implementado al Comité	[Gantt bar from Mes 11 SEM-1 to Mes 11 SEM-1]																1	- Oficial de Seguridad y Confianza Digital. - Comité de Gobierno y Transformación Digital. - Alta Dirección.				
		Aprobación por el Comité de Gobierno Digital referido a la implementación del SGSI	Implementación del proyecto del SGSI aprobado	[Gantt bar from Mes 11 SEM-1 to Mes 11 SEM-1]																1	- Comité de Gobierno y Transformación Digital. - Alta Dirección.				
		Gestionar la aprobación formal institucional (OPP-OAJ-GG-DIR)	Aprobación institucional	[Gantt bar from Mes 11 SEM-1 to Mes 11 SEM-1]																1	- Comité de Gobierno Digital. - OPP. - OAJ. - GG.				