SUPERINTENDENCIA NACIONAL DE BIENES ESTATALES

RESOLUCIÓN Nº 0066-2024/SBN-GG

San Isidro, 25 de julio de 2024

VISTOS:

El Acta de Reunión Nº 44-2024-CGTD de fecha 31 de mayo de 2024, del Comité de Gobierno y Transformación Digital (CGTD); los Memorándums Nros. 00026 y 00454-2024/SBN-OTI de fechas 21 de mayo y 24 de junio de 2024, respectivamente, de la Oficina de Tecnologías de la Información; el Informe N° 00732-2024/SBN-OPP de fecha 21 de mayo de 2024, de la Oficina de Planeamiento y Presupuesto; y el Informe N° 00258-2024/SBN-OAJ de fecha 24 de julio de 2024, de la Oficina de Asesoría Jurídica, y;

CONSIDERANDO:

Que, el Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, establece un marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno;

Que, el Reglamento del Decreto Legislativo N° 1412, aprobado por Decreto Supremo N° 029-2021-PCM, señala en el numeral 109.1 del artículo 109, que el Sistema de Gestión de Seguridad de la Información (SGSI), 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, 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, el citado Reglamento del Decreto Legislativo N° 1412, establece en el numeral 109.3 del artículo 109, que las entidades de la administración pública deben implementar un Sistema de Gestión de Seguridad de la Información (SGSI), teniendo como alcance mínimo sus procesos misionales y aquellos que son relevantes para su operación;

Que, la Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD, dispone en el numeral 3.1 del artículo 3 que el Plan de implementación del Sistema de Gestión de Seguridad de la Información - Plan SGSI, es el instrumento que establece, como mínimo, los objetivos, actividades, recursos, responsables y plazos para implementar un Sistema de Gestión de Seguridad de la Información, en un periodo máximo de tres (03) años. Es aprobado por la máxima autoridad administrativa o la que haga sus veces en la entidad pública;

Que, asimismo, indica en el numeral 3.2 del artículo 3 de la precitada Resolución, que las entidades públicas deben formular y aprobar el Plan de implementación del Sistema de Gestión de Seguridad de la Información - Plan SGSI y registrarlo en la Plataforma Facilita Perú para conocimiento y evaluación del Centro Nacional de Seguridad;

Que, mediante el Acta de Reunión Nº 44-2024-CGTD de fecha 31 de mayo de 2024, del Comité de Gobierno y Transformación Digital (CGTD) aprueba por unanimidad la propuesta de Plan de implementación del Sistema de Gestión de Seguridad de la Información de la Superintendencia Nacional de Bienes Estatales;

Que, la Oficina de Tecnologías de la Información, a través del Memorándum N° 00026-2024/SBN-OTI remite a la Oficina de Planeamiento y Presupuesto el sustento de la propuesta del “Plan de implementación del sistema de gestión de seguridad de la información de la Superintendencia Nacional de Bienes Estatales” y solicita la opinión técnica pertinente para continuar con el trámite correspondiente;

Que, con el Informe N° 00732-2024/SBN-OPP, la Oficina de Planeamiento y Presupuesto opina que la propuesta del Plan de Implementación del Sistema de Gestión de Seguridad de la Información de la Superintendencia Nacional de Bienes Estatales, se encuentra vinculada al Objetivo Estratégico Institucional OEI.04 Mejorar la Gestión Institucional del Plan Estratégico Institucional PEI 2024-2028 de la SBN y con la actividad operativa AO00020400052 Fortalecimiento del Gobierno digital del POI 2014 Modificado versión 1. Asimismo, precisa que la propuesta de plan no requerirá presupuesto, por lo que, emite viabilidad técnica favorable para la continuación del trámite de aprobación correspondiente;

Que, mediante Memorándum N° 00529-2024/SBN-OTI, la Oficina de Tecnologías de la Información remite a la Oficina de Asesoría Jurídica la propuesta final del documento denominado "Plan de Implementación del Sistema de Gestión de Seguridad de la Información- SGSI", a fin de continuar con el trámite correspondiente;

Que, en mérito a las consideraciones expuestas, la Oficina de Asesoría Jurídica mediante Informe N° 00258-2024/SBN-OAJ emite opinión legal favorable señalando que la propuesta de Plan SGSI presentado, cumple con las disposiciones para la elaboración y aprobación de los planes prevista en el numeral 6.1 de las Disposiciones Específicas de la Directiva N° DIR-00001-2022/SBN-OPP “Disposiciones para la gestión de los planes institucionales de la Superintendencia Nacional de Bienes Estatales-SBN", aprobada mediante Resolución N° 0076-2022/SBN-GG. Asimismo, señala que el precitado Plan se ajusta al contenido mínimo dispuesto en el numeral 3.5 del artículo 3. Plan de implementación del Sistema de Gestión de Seguridad de la Información de la Resolución de Secretaría de Gobierno y Transformación Digital Nº 003-2023-PCM/SGTD;

Que, si bien, la Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD, establece que el Plan SGSI es aprobado por la máxima autoridad administrativa, esta prerrogativa normativa, es concordante con la Resolución N° 063-2017/SBN que delegó en la Gerencia General la facultad para aprobar los planes de trabajo a nivel institucional;

Con el visado de la Oficina de Asesoría Jurídica, la Oficina de Planeamiento y Presupuesto, y la Oficina de Tecnologías de la Información;

RESUELVE:

Artículo 1.- Aprobar el "Plan de 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.- Encargar a la Oficina de Tecnologías de la Información el registro del "Plan de Implementación del Sistema de Gestión de Seguridad de la Información de la Superintendencia Nacional de Bienes Estatales" en la Plataforma Facilita Perú, para conocimiento y evaluación del Centro Nacional de Seguridad Digital.

Artículo 3.- Disponer la publicación de la presente resolución y su anexo en la Sede Digital de la Superintendencia Nacional de Bienes Estatales (www.gob.pe/sbn).

Regístrese y comuníquese.

Firmado digitalmente por:
LARREA SANCHEZ Manuel Eduardo FAU
20131057823 hard
Motivo: Firma
Fecha: 25/07/2024 14:57:35-0500

MANUEL EUDARDO LARREA SÁNCHEZ
Gerente General
Superintendencia Nacional de Bienes Estatales

Firmado digitalmente por:
RAMIREZ GARRO Jose Aurelio FAU
20131057823 hard
Fecha: 25/07/2024 10:25:07-0500

Firmado digitalmente por:
LLAMOJA CABANILLAS Paul Alex FAU
20131057823 hard
Motivo: Visto bueno
Fecha: 25/07/2024 10:56:34-0500

Firmado digitalmente por:
FARJE HORNA Pedro Alberto FAU
20131057823 hard
Motivo: Visto bueno
Fecha: 25/07/2024 12:08:17-0500

TIPO DE DOCUMENTO : PLAN DE TRABAJO

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

NÚMERO DE DOCUMENTO : SGSI-PLAN-001-2024/SBN

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

San Isidro, julio de 2024

Versión : No. 1

Índice

1. INTRODUCCIÓN 3
2. OBJETIVOS DEL PLAN SGSI 3
   2.1. Objetivos 3
   2.2. Indicador 4
   2.3. Articulación con el PEI y POI 4
3. MARCO LEGAL 5
   3.1. Marco Legal 5
   3.2. Norma Técnica 6
4. TÉRMINOS, DEFINICIONES Y SIGLAS 6
   4.1. Términos y definiciones 6
   4.2. Siglas 8
5. CONTEXTO DE LA ENTIDAD 8
   5.1. Misión 8
   5.2. Política Institucional 8
   5.3. Objetivos estratégicos institucionales 9
   5.4. Valores institucionales 9
   5.5. Funciones institucionales 9
   5.6. Partes Interesadas 9
   5.7. Requisitos de las partes interesadas 10
   5.8. FODA 11
6. MAPA DE PROCESOS DE LA ENTIDAD 11
7. ALCANCE DEL SGSI 12
8. ACTIVIDADES 12
   8.1. Estado de Implementación del SGSI en la SBN 12
   8.2. Fases y actividad operativa 12
9. CRONOGRAMA 14
10. RECURSOS Y PRESUPUESTO / INSUMOS 14
   10.1. Personal 14
      10.1.1. Grupo o equipo de trabajo 14
      10.1.2. Puestos, grupos o comité 15
   10.2. Recursos documentales, servicios y otros 19
      10.2.1. Recursos documentales 19
      10.2.2. Servicios 19
      10.2.3. Otros 19
   10.3. Presupuesto 20
11. MONITOREO Y EVALUACIÓN 20
12. ANEXOS 20
   Anexo 1 – Programación de las actividades del plan de implementación del SGSI de la SBN 21
   Anexo 2 – Mapa de procesos de la SBN 22

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

1. INTRODUCCIÓN

La información es el activo más importante del cual depende el correcto funcionamiento de la institución, es necesario reconocer su valor, juega un papel muy importante en la toma de decisiones operativas y estratégicas.

Para alcanzar los objetivos de la Superintendencia Nacional de Bienes Estatales, de aquí en adelante 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 en lo sucesivo SGSI, es un sistema que permite tener una herramienta de gestión que ayude a implementar, gestionar y minimizar los posibles riesgos que puedan atentar contra la seguridad de la información en la SBN.

Según la Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD Resolución que establece la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las entidades públicas, propone el uso obligatorio de la Norma Técnica Peruana NTP ISO/IEC 27001:2022 vigente para el análisis, diseño implementación, operación, mantenimiento y mejora continua de SGSI, asimismo establece los responsables y roles que deben cumplir en dicha implementación, y para la elaboración del plan plantea la estructura mínima que debe contener. En tal sentido se procederá a su implementación siguiendo los lineamientos expuestos y el modelo.

El presente plan de implementación establece las bases para un SGSI en la SBN y su desarrollo contempla la implementación de un solo proceso misional el cual constituye el inicio del SGSI en la SBN.

2. OBJETIVOS DEL PLAN SGSI

2.1. Objetivos

Definir los componentes para implementar, operar, monitorear, mantener y mejorar el SGSI con la finalidad de contribuir con el Objetivo Estratégico Institucional OEI.04 Mejorar la Gestión Institucional.

Implementar el SGSI que permita realizar la gestión adecuada de los riesgos que comprometan la confidencialidad, integridad y disponibilidad de la información en la SBN, estableciendo controles para minimizar los riesgos significativos y de alto impacto para el negocio, como el robo o fuga de información, accesos no autorizados, mal uso y/o cualquier otro daño que afecte la divulgación indebida de la información confidencial, la alteración o modificación de la misma, y en general la continuidad de las operaciones.

Desarrollar y mantener una cultura en Seguridad de la Información orientada a la identificación y análisis de riesgos, a través de la sensibilización de los servidores civiles de la SBN.

Objetivo del Plan	Nombre del Indicador	Método de cálculo	Logro esperado
OBJ.01 Implementar el SGSI, que permita realizar la gestión adecuada de los riesgos que comprometan la confidencialidad, integridad y disponibilidad de la información en la SBN.	Porcentaje de Fases Implementadas del SGSI con actos aprobados por el CGTD, en favor de la SBN.	Núm. de Fases Imp. ---------- * 100 = R Total, de Fases Porcentaje de Fases Implementadas	100%

2.2. Indicador

El indicador cuantifica la implementación de las fases del SGSI, según el alcance definido al Proceso Misional M01, denominado Gestión de Predios Estatales, lo cual permite medir el porcentaje de fases implementadas del SGSI con actos aprobados por el Comité de Gobierno y Transformación Digital, en adelante CGTD, de tal manera, promueve la cultura de la seguridad en la SBN.

Responsables del indicador: Despacho de la Superintendencia, el CGTD y el Oficial de Seguridad y Confianza Digital, en lo sucesivo OSCD.

2.3. Articulación con el PEI y POI

Objetivo Estratégico Institucional – PEI	Acción Estratégica Institucional	Actividad operativa POI anual 2024	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.	AO00020400052 Fortalecimiento del Gobierno digital	OBJ.01 Implementar el SGSI, que permita realizar la gestión adecuada de los riesgos que comprometan la confidencialidad, integridad y disponibilidad de la información en la SBN.
	AEI.04.05 Gestión de Gobierno Digital desplegado en el marco de transformación digital en la SBN.		

Actividad Operativa POI	Actividad o tarea del Plan	
AOI00020400052 Fortalecimientodel Gobierno Digital.	Fase 1	**Act.01** Contexto de la Organización (actualizar)
	Fase 2	**Act.02** Liderazgo (actualizar)
	Fase 3	**Act.03** Realizar la planificación
	Fase 4	**Act.04** Implementar el soporte
	Fase 5	**Act.05** Generar la operación
	Fase 6	**Act.06** Realizar la evaluación
	Fase 7	**Act.07** Implementar la mejora continua

3. MARCO LEGAL

3.1. Marco Legal

3.1.1. Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado y modificatorias.
3.1.2. Ley N° 27309, Ley que incorpora los delitos informáticos al Código Penal.
3.1.3. Ley N° 28493, Ley que regula el uso del correo electrónico comercial no solicitado (SPAM), y modificatoria.
3.1.4. Ley N° 29733, Ley de Protección de Datos Personales, y modificatoria.
3.1.5. Resolución Directoral N° 022-2022-INACAL/DN que aprueba la actualización y el uso de la NormaTécnica Peruana NTP.
3.1.6. Decreto de Urgencia N° 007-2020, que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
3.1.7. Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley del Gobierno Digital, se establece el marco de gobernanza del Gobierno Digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital, datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales, en la digitalización de procesos y prestación de los servicios digitales, por parte de las entidades de la administración pública, en los tres niveles de gobierno.
3.1.8. Decreto Supremo N° 003-2013-JUS, que aprueba el Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales.
3.1.9. 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.
3.1.10. 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.
3.1.11. Resolución de Secretaría de Gobierno y Transformación Digital Nº 003-2023-PCM/SGTD, que establece la implementación y mantenimiento del sistema de gestión de seguridad de la información en las entidades públicas.

3.1.12. Resolución N° 065-2018/SBN, que conforma el Comité de Gobierno Digital de la Superintendencia Nacional de Bienes Estatales, modificada por las Resoluciones Nros. 0074-2018/SBN, 0092-2018/SBN, 0024-2019/SBN y 0014-2022/SBN.

3.2. Norma Técnica

Con Resolución Directoral N° 022-2022-INACAL/DN se aprueba la actualización y el uso de la NormaTécnica Peruana **NTP ISO/IEC 27001:2022** Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3ª Edición Reemplaza a la 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 27002:2022** Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información. 2ª Edición Reemplaza a la NTP-ISO/IEC 27002:2017; **NTP ISO/IEC 27005:2022** Seguridad de la información, ciberseguridad y protección de la privacidad. Orientación sobre la gestión de los riesgos de seguridad de la información. 3ª Edición Reemplaza a la NTP-ISO/IEC 27005:2018, así como otras NTPs conexas.

Norma Técnica Peruana **NTP-ISO 31000:2018** Gestión del riesgo. Directrices. 2a Edición.

A continuación, se indican las fases de la "NTP ISO/IEC 27001:2022", para su implementación:

- Contexto de la Organización.
- Liderazgo.
- Planificación.
- Soporte.
- Operación.
- Evaluación.
- Mejora Continua.

4. TÉRMINOS, DEFINICIONES Y SIGLAS

4.1. Términos y definiciones

4.1.1. **Activo de Información:** Cualquier información que tiene valor para la Entidad y para el Sistema de Gestión de Seguridad de la Información. Se consideran también los recursos humanos, tecnológicos que intervienen en el tratamiento directo o indirecto de la información, así como sus procesos y actividades.

4.1.2. **Análisis de Riesgo:** Proceso de comprender la naturaleza del riesgo y determinar el nivel de riesgo.

- **Nota 1:** El análisis de riesgos proporciona las bases para la evaluación del riesgo y para tomar las decisiones sobre el tratamiento del riesgo.
- **Nota 2:** El análisis de riesgo incluye la estimación del riesgo.

4.1.3. **Confidencialidad:** Propiedad de la información que hace que no esté disponible o que sea revelada a individuos o entidades no autorizados.

4.1.4. **Disponibilidad:** Propiedad de ser accesible y utilizable ante la demanda de una entidad autorizada.

4.1.5. **Gestión de Riesgo:** Aplicación sistemática de políticas de gestión procedimientos y prácticas a las actividades de comunicación, consulta, establecimiento del contexto e identificación, análisis, evaluación, tratamiento, seguimiento y revisión de riesgos.

4.1.6. **Incidente de Seguridad de la Información:** Suceso inesperado en el que se transgrede un determinado control de la información y que genera un impacto negativo en la entidad.

4.1.7. **Integridad:** Propiedad de precisión y completitud de la información.

4.1.8. **Oficial de Seguridad de la Información**: El Oficial de Seguridad de la Información es el responsable del Sistema de Gestión de la Seguridad de la Información (SGSI) y reporta al CGTD, es designado por la institución.

4.1.9. **Propietario del activo:** Es el funcionario asignado de garantizar que el activo asignado bajo su responsabilidad esté protegido con los controles definidos en el SGSI y que le apliquen a dicho activo; es el responsable por la afectación de la confidencialidad, integridad y disponibilidad del mismo, en cualquiera de los procesos que se encuentre involucrado.

4.1.10. **Riesgo de Seguridad de la Información:** Posibilidad de que una amenaza dada explote vulnerabilidades de un activo o de un grupo de activos y por lo tanto cause daño a la institución.

4.1.11. **Seguridad de la Información:** Todas las acciones orientadas a preservar la integridad, confidencialidad y disponibilidad de la información y los activos asociados a su tratamiento independiente de la forma en la que la información se encuentre.

4.1.12. **Sistema de Gestión de la Seguridad de la Información (SGSI):** Es un componente del sistema de gestión de una organización, con base en un enfoque de riesgos, que tiene como función establecer, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. El SGSI está conformado por políticas, procedimientos, directrices, recursos y actividades asociadas, gestionadas por la organización, en la búsqueda de la protección de sus activos de información.

4.2. Siglas

CGTD	:	Comité de Gobierno y Transformación Digital
DS	:	Despacho de la Superintendencia
GG	:	Gerencia General
IEC	:	Comisión Electrónica Internacional - siglas en inglés (International Electrotechnical Commission)
INACAL	:	Instituto Nacional de Calidad
ISO	:	Organización Internacional de Normalización - siglas en inglés (International Organization for Standardization)
NTP	:	Norma Técnica Peruana
OAF	:	Oficina de Administración y Finanzas
OAJ	:	Oficina de Asesoría Jurídica
OPP	:	Oficina de Planeamiento y Presupuesto
OSCD	:	Oficial de Seguridad y Confianza Digital
OTI	:	Oficina de Tecnologías de la Información
PCM	:	Presidencia del Consejo de Ministros
PEI	:	Plan Estratégico Institucional
POI	:	Plan Operativo Institucional
SBN	:	Superintendencia Nacional de Bienes Estatales
SGSI	:	Sistema de Gestión de Seguridad de la Información
SoA	:	Declaración de Aplicabilidad - siglas en inglés (Statement of Applicability)
URH	:	Unidad de Recursos Humanos
UTD	:	Unidad de Tramite Documentario

5. CONTEXTO DE LA ENTIDAD

5.1. Misión

Gestionar y supervisar los predios estatales en beneficio de las entidades públicas, privadas y ciudadanía, de manera transparente y eficiente (fuente: www.sbn.gob.pe).

5.2. Política Institucional

Promover y priorizar el saneamiento y la defensa de predios estatales para su entrega a los proyectos de inversión pública e inversión privada, bajo un enfoque de servicios públicos digitalizados (fuente: www.sbn.gob.pe).

5.3. Objetivos Estratégicos institucionales

OEI.01 : Fortalecer el Sistema de Información nacional de los predios e inmuebles estatales en beneficio del país.

OEI.02 : Incrementar la supervisión de predios estatales a fin de que se cumplan de manera efectiva la finalidad a favor de la sociedad.

OEI.03 : Mejorar la gestión integral de los predios estatales a favor de la sociedad.

OEI.04 : Fortalecer la gestión institucional.

OEI.05 : Fortalecer la Gestión de Riesgos de Desastres (GRD).

5.4. Valores institucionales

- Ética
- Profesionalismo
- Compromiso
- Probidad
- Neutralidad
- Transparencia

5.5. Funciones Institucionales

- **Normar** : Fortalecemos el Sistema Nacional de Bienes Estatales.
- **Capacitar** : Desarrollamos las competencias técnicas de los servidores de los tres niveles de gobierno.
- **Supervisar** : Los bienes y actos que las entidades del sistema realizan en función de sus competencias.
- **Gestionar** : Administramos, adquirimos y disponemos los bienes garantizando su buen uso.

Normar los actos de adquisición, disposición, administración y supervisión de los bienes estatales, así de como de ejecutar dichos actos respecto de los bienes cuya administración está a su cargo, de acuerdo con la normatividad vigente, gozando de autonomía económica, presupuestal, financiera, técnica y funcional, con representación judicial propia.

Proponer y promover la aprobación de normas legales destinadas al fortalecimiento del Sistema Nacional de Bienes Estatales, priorizando la modernización de la gestión del Estado y el proceso de descentralización.

5.6. Partes interesadas

Para el desarrollo del SGSI se pueden considerar las siguientes partes interesadas:

a. Los administrados; que corresponde a todo ciudadano, empresa o institución que de manera directa o indirecta requiera interactuar con la SBN.

b. El Gobierno en sus tres niveles:

i. Gobiernos Locales.
ii. Gobiernos Regionales.
iii. Gobierno Central: Ministerio de Vivienda, Construcción y Saneamiento, Presidencia del Consejo de Ministros y el Despacho Presidencial.

c. Unidades de Organización de la SBN con los colaboradores contratados bajo cualquier tipo de modalidad.

5.7. Requisitos de las Partes interesadas

Para el desarrollo del SGSI se pueden considerar los siguientes requisitos de seguridad de la información de las partes interesadas:

a. Los administrados:

- Confidencialidad de la Información.
- Disponibilidad de la Información.
- Integridad de la Información.
- Protección de la información personal.
- Operatividad de las plataformas tecnológicas.

b. El Gobierno:

- Confidencialidad de la Información.
- Disponibilidad de la Información.
- Integridad de la Información.
- Cumplimiento de la legislación y regulación en temas relacionados a seguridad de la información.

c. Unidades de Organización:

- Confidencialidad de la Información.
- Disponibilidad de la Información.
- Integridad de la Información.
- Contar con las condiciones de seguridad física y lógica en el desarrollo de sus funciones dentro de la SBN.

5.8. FODA

	FORTALEZAS		DEBILIDADES	
FACTORES INTERNOS	**F1**	Alto nivel de compromiso del Despacho de la Superintendencia en su Rol de Líder en la implementación del SGSI.	**D1**	Personal insuficiente para atender aumentos de carga laboral.
	F2	Alto nivel de involucramiento del Gerente General para implementar el SGSI en base a la NTP 27001:2022.	**D2**	Falta de compromiso del personal para participar en actividades de capacitación y/o asistencia técnica.
	F3	Capacidad técnica y de trabajo en equipo por parte del personal de la SBN.	**D3**	Nivel medio en la madurez institucional para la gestión de riesgos.
	F4	Transparencia en la información y puesta a disposición de la población de los resultados de la gestión.	**D4**	Limitada optimización de los sistemas informáticos institucionales.
	F5	Alto compromiso institucional para la mitigación de riesgos de la Seguridad de la Información.	**D5**	Infraestructura tecnológica en proceso de obsolescencia
	F6	Alto compromiso del personal en la simplificación y mejora permanente de los procesos y procedimientos institucionales.	**D6**	Marco normativo interno en materia de Seguridad de la información, desactualizado o inexistente.

	F7	Alto sentido de vocación y de servicio a la ciudadanía.	**D7**	Inexistencia de un entorno de contingencia ante incidentes que afecten la infraestructura física del datacenter.
	F8	Sólida trayectoria institucional evidenciados en la amplia experiencia y en la alta especialización en la administración de predios estatales.	**D8**	Falta de medición de los controles de seguridad implementados.
	F9	Marco normativo del Sistema Nacional de Bienes Estatales (SNBE) garantiza la transparencia de la administración de predios estatales.	**D9**	Procedimiento de desarrollo de software poco maduros.

	OPORTUNIDADES		**AMENAZAS**	
FACTORES EXTERNOS	**O1**	Marco normativo estatal en materia de SGSI garantiza cumplimiento obligatorio de las entidades públicas.	**A1**	Limitado conocimiento de los grupos de interés sobre lalabor del SBN.
	O2	Alta aceptación de la sociedad e instituciones públicas y privadas respecto a la implementación del SGSI del estándar internacional ISO 27001:2022.	**A2**	Percepción negativa de la ciudadanía sobre las entidades públicas.
	O3	Creciente demanda de infraestructura pública por terrenos para proyectos de desarrollo.	**A3**	Eventos mediáticos afectan en forma negativa la imagen institucional.
	O4	La pandemia incrementó de uso de tecnologías de la información y comunicaciones, por motivos laborales, educativos, personales y de otra índole.	**A4**	Cambios en las leyes y regulaciones pueden impactar la forma en la que opera y en toman decisiones respecto a los procesos misionales.
	O5	Políticas institucionales y normativa vigente que regula los sistemas administrativos, desarrolladas bajo el enfoque de integridad y lucha contra la corrupción.	**A5**	Limitado presupuesto institucional y bajas remuneraciones del personal respecto al mercado laboral.
	O6	Apoyo y colaboración de la Secretaría de Gobierno y Transformación Digital (SEGTDI) y el Centro Nacional de Seguridad Digital (CNSD) de la PCM para el desarrollo e implementación de nuevas soluciones tecnológicas, así como seguridad digital.	**A6**	Usurpación/invasión de predios estatales administrados por la SBN.

6. MAPA DE PROCESOS DE LA ENTIDAD

Mediante Resolución Nº 0047-2020/SBN-GG, de fecha 14 de agosto de 2020, se resuelve aprobar el "Mapa de Procesos Niveles 0, 1 y 2 de la Superintendencia Nacional de Bienes Estatales", actualmente vigente y en aplicación (https://www.sbn.gob.pe/instrumentos-de-gestion-manual-de-procedimientos-mapro). El Anexo N° 02 ilustra el mapa de procesos nivel 0.

7. ALCANCE DEL SGSI

La SBN teniendo en consideración los factores internos y externos, además de la normatividad vigente, las partes interesadas y sus expectativas ha definido el alcance del SGSI:

El Alcance del SGSI será establecido para el Proceso Misional M01 denominado Gestión de predios estatales, que incluye la planificación, gobierno, investigación, gestión, desarrollo, mantenimiento y operatividad, proceso que debe ser continuo, viable seguro, basado de las tecnologías de la información; y la gestión de la seguridad de la información y la infraestructura tecnológica contemplados dentro de la Sede principal y sedes anexos de la SBN, así de como de las áreas físicas externas donde se ejecuta parte del proceso.

8. ACTIVIDADES

8.1. Estado de implementación del SGSI en la SBN.

A partir del 1 de mayo de 2024, todas las certificaciones iniciales deberán realizarse en función a la NTP ISO/IEC 27001:2022, en tal sentido es necesario la adecuación de lo avanzado; como, por ejemplo: la Resolución N° 0061-2021/SBN, que aprueba el documento denominado "Política de la Seguridad de la Información de la Superintendencia Nacional de Bienes Estatales".
Es de precisar, que todo el avance efectuado por el CGTD en lo relacionado a la implementación del SGSI debe ser actualizado y adecuado a lo que indica la NTP ISO/IEC 27001:2022, y en tal sentido estas fases y sus respectivos subcomponentes deben ser revisados.

8.2. Fases y actividad operativa

Fase 1: Act.01 Elaborar el contexto de la Organización

- Elaborar el Plan de Implementación de la SGSI de la SBN (presente documento).
- Elaborar el Alcance del SGSI.

Fase 2: Act.02 Determinar el Liderazgo.

- Determinar el liderazgo y compromiso del Despacho de la Superintendencia de la SBN dentro del Plan de implementación del SGSI.
- Adecuación y actualización de la Política de Seguridad de la Información, a lo que establece la NTP ISO/IEC 27001:2022.

Fase 3: Act.03 Realizar la Planificación.

- Definir la metodología de evaluación y tratamiento de riesgos.
- Realizar el inventario de activos correspondiente al alcance del SGSI.
- Elaborar el instructivo análisis de amenazas y vulnerabilidades.
- Elaborar la metodología para la evaluación y tratamiento de riesgos.
- Consolidar el inventario de activos de información y la matriz de riesgo y oportunidad de mejora.
- Validar la Matriz de riesgos de seguridad de la información.
- Elaborar la directiva para empleo de estándares y desarrollo de sistemas de información.

- Elaborar el documento procedimiento para el acceso físico al centro de datos.
- Elaborar el procedimiento de gestión de usuarios.
- Elaborar el documento procedimiento para la gestión de cambios de aplicaciones informáticas.
- Elaborar el documento procedimiento de administración de bases de datos.
- Elaborar el documento procedimiento para la gestión de copias de respaldo y resguardo de la información.
- Elaborar el documento procedimiento de atención a las/los usuarias/os internos a través de mesa de ayuda de la OTI.
- Elaborar el procedimiento técnico del SGSI.
- Elaborar procedimiento de gestión de incidentes de seguridad de la información.
- Actualizar la directiva de uso de correo electrónico institucional.
- Elaborar el documento de gestión de la capacidad de infraestructura tecnológica.
- Elaborar el documento procedimiento de gestión de cambios en la infraestructura tecnológica.
- Redactar el documento de la Declaración de Aplicabilidad (SoA).
- Elaborar los lineamientos de seguridad de la información.
- Elaborar directiva para la seguridad de la información en la Gestión de Proveedores.
- Elaborar el Plan de contingencia de Tecnologías de Información.
- Elaborar el Plan de Tratamiento de Riesgos.

Fase 4: Act.04 Implementar el Soporte.

- Concientizar al personal de la SBN sobre la importancia de la seguridad de la información.
- Evaluar el conocimiento adquirido por las/los servidoras/es civiles sobre seguridad de la información.
- Difundir la política y objetivos de seguridad de la información.
- Realizar el taller Semana de la seguridad de la información.
- Implementación del portal del Sistema de Gestión de Seguridad de la Información del Programa.

Fase 5: Act.05 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.06 Realizar la Evaluación.

Auditoría Interna:

- Coordinar con el Centro Nacional de Seguridad Digital la realización de una auditoria.
- Elaborar el plan de auditoría.
- Realización de Auditoría Interna del SGSI.
- Elaborar el informe de auditoría.
- Presentar el informe de auditoría y definir acciones correctivas y oportunidades de mejora.

Auditoría de Certificación:

- Gestionar los recursos para la auditoria de certificación.
- Realizar la auditoria de certificación.
- Revisar el Informe de auditoría.
- Presentar el informe de auditoría y definir acciones correctivas y oportunidades de mejora.

Revisar y medir desempeño del SGSI:

- Realizar la medición de desempeño del SGSI.
- Revisar y presentar el estado de implementación del SGSI al CGTD y al Despacho de la Superintendencia.

Fase 7: Act.07 Implementar la Mejora Continua.

- Realizar el seguimiento y monitoreo a los resultados de la auditoria para la mejora continua.
- Preparar los planes de acción de las no conformidades y las recomendaciones de la auditoría.
- Difusión a los integrantes del CGTD para su revisión y presentación al Despacho de la Superintendencia.
- Aprobación por el CGTD referido a la implementación de SGSI.
- Gestionar la aprobación formal institucional (OPP-OAJ-GG-DS).

9. CRONOGRAMA

El cronograma de ejecución del presente plan se encuentra en el Anexo N° 01 “Programación de las actividades del plan de implementación del SGSI de la SBN”. La fecha de inicio será al día siguiente de su aprobación mediante acto resolutivo.

10. RECURSOS Y PRESUPUESTO / 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.

Líder de Gobierno Digital es 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 CGTD lo considere necesario.

El equipo de trabajo estará conformado por:

a) Despacho de la Superintendencia.
b) Líder de Gobierno Digital.
c) Comité de Gobierno y Transformación Digital (CGTD).
d) Oficial de Seguridad y Confianza Digital (OSCD).
e) Personal de OTI.
f) Personal de las unidades de organización que involucre el alcance del SGSI.
g) Especialista Técnico de Seguridad de la Información.

10.1.2. Puestos, Grupos o Comité

Las Fases 1 y 2 se encuentran con un grado de avance, pero requieren necesariamente actualizarlas, así también corresponde en el presente Plan realizar la implementación de las actividades o tareas consideradas en todas sus fases.

Actividad o tarea del Plan		Responsables
Fase 1	**Act.01 Contexto de la Organización**	
1	Elaborar Plan de Trabajo para la Implementación delSistema de Gestión de Seguridad de la Informaciónde la SBN	- OSCD - CGTD - DS
2	Elaborar el Alcance del SGSI	- OSCD - CGTD - DS
Fase 2	**Act.02 Liderazgo**	
1	Determinar el compromiso del Despacho de la Superintendencia de la SBN dentro del proyecto de implementación del SGSI	- CGTD - DS
2	Elaborar la Política y Objetivos de Seguridad de la Información	- OSCD - CGTD - DS
Fase 3	**Act.03 Planificación**	
1	Definir la metodología de evaluación de riesgos de información del SGSI en base al alcance establecido	- OSCD - CGTD - DS
2	Realizar el inventario de activos correspondiente al Alcance del SGSI	- OSCD - CGTD - DS
3	Elaborar el documento Instructivo análisis de amenazas y vulnerabilidades	- OSCD - CGTD - DS
4	Consolidar el inventario de activos de información y la matriz de riesgo y oportunidad de mejora	- OSCD - CGTD - DS
5	Validar la Matriz de riesgos de seguridad de la información	- OSCD - CGTD - DS

6	Directiva para empleo de estándares y desarrollo de sistemas de información	- OSCD - CGTD - DS
7	Elaborar el documento Procedimiento para el acceso físico al centro de datos	- OSCD - CGTD - DS
8	Elaborar el procedimiento de gestión de usuarios	- OSCD - CGTD - DS
9	Elaborar el documento Procedimiento para la gestión de cambios de aplicaciones informáticas	- OSCD - CGTD - DS
10	Elaborar el documento Procedimiento para la gestión de cambios de aplicaciones informáticas	- OSCD - CGTD - DS
11	Elaborar el documento Procedimiento de administración de bases de datos	- OSCD - CGTD - DS
12	Elaborar el documento Procedimiento para la Gestión de Copias de Respaldo y Resguardo de la Información	- OSCD - CGTD - DS
13	Elaborar documento procedimiento de atención a las/los usuarias/os internos a través de mesa de ayuda de la OTI	- OSCD - CGTD - DS
14	Elaborar el Procedimiento técnico del Sistema de Gestión de Seguridad de la Información	- OSCD - CGTD - DS
15	Elaborar procedimiento de Gestión de incidentes de seguridad de la información	- OSCD - CGTD - DS
16	Actualizar Directiva de uso de correo electrónico institucional	- OSCD - CGTD - DS
17	Elaborar el documento de gestión de la capacidad de infraestructura tecnológica	- OSCD - CGTD - DS
18	Elaborar el documento Procedimiento de gestión de cambios en la infraestructura tecnológica	- OSCD - CGTD - DS
19	Redactar el documento de la declaración de aplicabilidad (SoA)	- OSCD - CGTD - DS
20	Lineamientos de seguridad de la información	- OSCD - CGTD - DS

21	Directiva para la seguridad de la información en la Gestión de Proveedores	- OSCD. - CGTD. - DS
22	Elaborar el documento Plan de contingencia de TI	- OSCD - CGTD - DS
23	Elaborar el plan de tratamiento de riesgos	- OSCD - CGTD - DS
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	- OSCD - CGTD - DS
2	Evaluar el conocimiento adquirido por los servidores civiles sobre seguridad de la información	- OSCD - CGTD - DS
3	Difundir la política y objetivos de seguridad de la información	- OSCD - CGTD - DS
4	Semana de la seguridad de la información	- OSCD - CGTD - DS.
5	Implementación del portal del Sistema de Gestión de Seguridad de la Información del Programa	- OSCD. - CGTD - DS
Fase 5	**Act.05 Operación**	
1	Implantar los controles seleccionados	- OSCD - CGTD - DS
2	Documentar los procedimientos, políticas y requisitos necesarios del SGSI	- OSCD - CGTD - DS
3	Implementar el plan de tratamiento de riesgos y documentar los resultados	- OSCD - CGTD - DS
Fase 6	**Act.06 Evaluación**	
	Auditoría Interna	
1	Coordinar con el CNSD la realización de una auditoria	- OSCD - CGTD - DS

2	Elaborar el Plan de Auditoria	- OSCD - CGTD - DS
3	Realización de Auditoría Interna del SGSI	- Auditores designados - CGTD - DS
4	Elaborar el Informe de auditoria	- Auditores designados - CGTD - DS
5	Presentar el Informe de Auditoría y definir acciones correctivas y oportunidades de mejora	- Auditores designados - CGTD - DS
	Auditoría de Certificación	
1	Gestionar los recursos para la auditoria de certificación	- OSCD - CGTD - DS
2	Realizar la auditoria de certificación	- Auditores designados - CGTD - DS
3	Revisar el Informe de auditoria	- Auditores designados - CGTD - DS
4	Presentar el Informe de Auditoría y definir acciones correctivas y oportunidades de mejora	- OSCD - CGTD - DS
	Revisar y Medir Desempeño del SGSI	
1	Realizar la medición de desempeño del SGSI	- OSCD
2	Revisar y presentar el estado de implementación del SGSI al Comité de Gobierno Digital y al Despacho de la Superintendencia	- OSCD
Fase 7	**Act.07 Mejora Continua**	
1	Preparar los planes de acción de las noconformidades y las recomendaciones de la auditoria	- Auditores encargados - OSCD - CGTD -DS
2	Difusión a los integrantes del Comité de GobiernoDigital para su revisión por el Despacho de la Superintendencia	- OSCD - CGTD - DS
3	Aprobación por el Comité de Gobierno Digital referido a la implementación de SGSI	- CGTD. - DS
4	Gestionar aprobación formal institucional (DS, GG, OAJ, OPP)	- CGTD. - DS, GG, OAJ, OPP

10.2. Recursos documentales, servicios y otros

10.2.1. Recursos Documentales

- NTP-ISO/IEC 27001:2022, Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3ª Edición Reemplaza a la NTP-ISO/IEC 27001:2014.
- NTP-ISO/IEC 27002:2022, Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información. 2ª Edición Reemplaza a la NTP-ISO/IEC 27002:2017.
- NTP-ISO/IEC 27005:2022, Seguridad de la información, ciberseguridad y protección de la privacidad. Orientación sobre la gestión de los riesgos de seguridad de la información. 3ª Edición Reemplaza a la NTP-ISO/IEC 27005:2018.
- NTP-ISO 31000:2018 Gestión del riesgo. Directrices. 2a Edición.
- Normativa conexa vigente y normativa interna de la SBN.

10.2.2. Servicio(s)

- Servicio de acompañamiento para la implementación del SGSI.

  Mediante consultores que guíen el desarrollo de la implementación del SGSI y que permita alcanzar los niveles de eficiencia y mejora requeridos, de esta manera trabajar en estrecha colaboración con el personal de las unidades de organización que involucre el alcance del SGSI, proporcionando el acompañamiento técnico y proporcionando orientación experta en la aplicación de los estándares adecuados, como la NTP ISO/IEC 27001:2022 y el apoyo para implementar políticas, procedimientos, y para establecer indicadores de rendimiento.

- Auditoría interna en todas las Fases del Plan de implementación del SGSI.

  El servicio y el informe debe contener como mínimo los siguientes puntos:

  - Áreas y alcance auditado, así como la fecha de auditoría.
  - No conformidades y observaciones encontradas, acordadas con los auditados.
  - Valoración de los puntos fuertes y las áreas susceptibles de mejora del SGSI.
  - Acciones correctivas propuestas para las salvedades o no conformidades identificadas, destinadas a garantizar el cumplimiento de una determinada desviación existente actualmente.
  - Recomendaciones, que no se traten de acciones correctivas de una determinada salvedad, si no de oportunidades de mejora o acciones que podrían suponer una evolución o mayor madurez del proceso auditado en cuestión, pero que en la actualidad no constituye una salvedad o no conformidad.
  - Documentación auditada.
  - Firma del Auditor/Auditores.

10.2.3. Otros

Recursos requeridos para la evaluación y certificación por parte de la entidad certificadora.

10.3. Presupuesto

Para el desarrollo del presente plan de trabajo no se requiere de presupuesto adicional al asignado en el presupuesto anual.

11. MONITOREO Y EVALUACIÓN

El Comité de Gobierno y Transformación Digital, es responsable de dirigir, mantener y supervisar el SGSI de la SBN, para lo cual, debe monitorear el avance del proyecto, garantizar los recursos necesarios para la implementación del presente plan, 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 institución e informar al Despacho de la Superintendencia sobre el progreso del proyecto dentro de los plazos establecidos en el presente plan.

La OTI, en calidad de secretaría técnica del Comité, elabora y gestiona, la documentación pertinente, así como, informa mensualmente al Comité sobre los avances implementados; a su vez de manera semestral (enero y julio, con cortes al mes anterior) comunica mediante informe detallado a la Oficina de Planeamiento y Presupuesto.

El Comité de Gobierno y Transformación Digital está conformado por:

N°	Cargo	Oficina
1	Superintendente/a Nacional de Bienes Estatales, presidente del CGTD	DS
2	Gerente/a General, Miembro del CGTD	GG
3	Líder de Gobierno y Transformación Digital	DS
4	Supervisor/a de Tecnologías de la Información de la OTI, secretario técnico del CGTD	OTI
5	Supervisor/a de Personal de la Unidad de Recursos Humanos	URH
6	Jefe/a de la Unidad de Trámite Documentario, Miembro del CGTD	UTD
7	Oficial de Seguridad de la Información (OSCD), Miembro del CGTD	OSCD
8	Jefe/a de la Oficina de Asesoría Jurídica, Miembro del CGTD	OAJ
9	Jefe/a de la Oficina de Planeamiento y Presupuesto, Miembro del CGTD	OPP

12. ANEXOS

Anexo N° 01 – PROGRAMACIÓN DE LAS ACTIVIDADES DEL PLAN DE IMPLEMENTACIÓN DEL SGSI DE LA SBN

Anexo N° 02 – MAPA DE PROCESOS DE LA SBN

ANEXO 1 – PROGRAMACIÓN DE LAS ACTIVIDADES DEL PLAN DE IMPLEMENTACIÓN DEL SGSI DE LA SBN

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	Mes 1				Mes 2				Mes 3				Mes 4				Mes 5				Mes 6				Mes 7				Mes 8				Mes 9				Mes 10				Mes 11				Mes 12				META PROGRAMADA	UNIDAD / COLEGIADO RESPONSABLE
				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	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	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 Implementación del SGSI en la SBN	Plan Aprobado	X	X	X	X	X	X																																											1	OSCD - CGTD - DS
		Elaborar el alcance del SGSI	Alcance del SGSI Aprobado	X	X	X	X	X	X																																											1	OSCD - CGTD - DS
ACT.02		LIDERAZGO																																																			
	2	Determinar el liderazgo y compromiso de la Alta Dirección de la SBN dentro del Plan de Implementción del SGSI	Actas suscritas con el compromiso de Alta Dirección para implementar el SGSI	X	X																																															1	OSCD - CGTD - DS
		Adecuación y actualización de la Política de Seguridad de la Información a lo que establece la NTP ISO/IEC 27001:2022	Política actualizada y aprobada	X	X	X	X	X	X																																											1	OSCD - CGTD - DS
ACT.03		PLANIFICACIÓN																																																			
		Definir la metodología de evaluación y tratamiento de riesgos	Informe sobre la metodología de riegos definida	X	X	X	X																																													1	OSCD - CGTD - DS
		Realizar el inventario de activos correspondiente al alcance del SGSI	Inventario elaborado y presentado	X	X	X	X	X	X	X	X																																									1	OSCD - CGTD - DS
		Elaborar el Instructivo análisis de amenazas y vulnerabilidades	Documento	X	X	X	X	X	X	X	X																																									1	OSCD - CGTD - DS
		Consolidar el inventario de activos de información y la matriz de riesgo y oportunidad de mejora	Matriz Riesgos/Oportunidad - Inventario de activos					X	X	X	X	X	X	X	X																																					1	OSCD - CGTD - DS
		Validar la Matriz de riesgos de seguridad de la información.	Matriz Riesgos/Oportunidad					X	X	X	X	X	X	X	X																																					1	OSCD - CGTD - DS

		Elaborar la directiva para el empleo de estandares y desarrollo de sistemas de información y gestionar su aprobación	Documento aprobado					X	X	X	X	X	X	X	X																																					1	OSCD - CGTD - DS
		Elaborar el documento procedimiento para el acceso fisico al centro de datos	Directiva de Control de acceso al centro de datos					X	X	X	X	X	X	X	X																																					1	OSCD - CGTD - DS
		Elaborar el procedimiento de gestion de usuarios	Directiva de administracion de base de datos e incorporara al MAPRO					X	X	X	X	X	X	X	X																																					1	OSCD - CGTD - DS
		Elaborar el documento procedimiento para la gestión de cambios de aplicaciones informáticas	Documento					X	X	X	X	X	X	X	X																																					1	OSCD - CGTD - DS
		Elaborar el documento procedimiento de administración de bases de datos	Directiva de administracion de base de datos e incorporara al MAPRO					X	X	X	X	X	X	X	X																																					1	OSCD - CGTD - DS
	3	Elaborar el documento procedimiento para la Gestion de Copias de Respaldo y Resguardo de la Información	Directiva de Gestion de Backups e incorporrar al MAPRO					X	X	X	X	X	X	X	X																																					1	OSCD - CGTD - DS
		Elaborar el documento procedimiento de atencion a las/los usuarias/os internos a traves de mesa de ayuda de la OTI	Documento aprobado por resolucion,					X	X	X	X	X	X	X	X																																					1	OSCD - CGTD - DS
		Elaborar el procedimiento técnico del Sistema de Gestión de Seguridad de la Información	Elaborar procedimiento e incorporrar al MAPRO					X	X	X	X	X	X	X	X																																					1	OSCD - CGTD - DS
		Elaborar procedimiento de Gestión de incidentes de seguridad de la información	Elaborar procedimiento e incorporrar al MAPRO					X	X	X	X	X	X	X	X																																					1	OSCD - CGTD - DS
		Actualizar directiva de uso de correo electrónico institucional	Documento aprobado por resolucion					X	X	X	X	X	X	X	X																																					1	OSCD - CGTD - DS
		Elaborar el documento de gestión de la capacidad de infraestructura tecnológica	Documento					X	X	X	X	X	X	X	X																																					1	OSCD - CGTD - DS

		Elaborar el documento procedimiento de gestión de cambios en la infraestructura tecnológica	Documento					X	X	X	X	X	X	X	X																																			1	OSCD - CGTD - DS
		Redactar el documento de la Declaración de Aplicabilidad (SOA)	Documento de Aplicabilidad aprobado													X	X	X	X																																	1	OSCD - CGTD - DS
		Elaborar los lineamientos de seguridad de la información	Documento													X	X	X	X																																	1	OSCD - CGTD - DS
		Elaborar directiva para la seguridad de la información en la Gestión de Proveedores	Documento													X	X	X	X																																	1	OSCD - CGTD - DS
		Elaborar el documento Plan de contingencia de TI	Documento aprobado por resolucion,													X	X	X	X																																	1	OSCD - CGTD - DS
		Elaborar el Plan de Tratamiento de Riesgos	Plan de tratamiento de riesgos aprobado																	X	X	X	X	X	X	X	X																									1	OSCD - CGTD - DS
ACT.04		**SOPORTE**																																																			
		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					X	X							X	X							X	X							X	X																			4	OSCD - CGTD - DS
		Evaluar el conocimiento adquirido por las/los servidoras/es civiles sobre seguridad de la información.	Aplicación de formulario							X								X								X								X																		4	OSCD - CGTD - DS
	4	Difundir la política y objetivos de seguridad de la información	Medios de comunicación de la SBN							X								X								X								X								X							X			6	OSCD - CGTD - DS
		Realizar el taller Semana de la seguridad de la información.	Registro de participantes					X								X								X								X																				4	OSCD - CGTD - DS
		Implementación del portal del Sistema de Gestion de Seguridad de la Información	Portal en operatividad																					X	X	X	X																									1	OSCD - CGTD - DS
ACT.05		**OPERACIÓN**																																																			

		Implantar los controles seleccionados	Controles implementados																									X	X	X	X	X	X																			100%	OSCD - CGTD - DS
	5	Documentar los procedimientos, políticas y requisitos necesarios del SGSI	Políticas y Procedimientos del SGSI Documentados																													X	X	X	X	X	X															100%	OSCD - CGTD - DS
		Implementar el Plan de Tratamiento de Riesgos y documentar los resultados	Implementación del plan de riesgos																															X	X	X	X	X	X													1	OSCD - CGTD - DS
ACT.06		EVALUACIÓN																																																					
		Coordinar con el CNSD la realización de una auditoria	Solicitud dirigida al CNSD																																			X	X													1	OSCD - CGTD - DS
		Elaborar el plan auditoria	Plan de Auditoria																																			X	X													1	OSCD - CGTD - DS
		Realización de Auditoría Interna del SGSI	Auditoría ejecutada																																					X	X											1	Auditores designados - CGTD - DS
		Elaborar el Informe de auditoria	informe																																							X										1	Auditores designados - CGTD - DS
		Presentar el informe de auditoria y definir acciones correctivas y oportunidades de mejora	informe																																							X										1	Auditores designados - CGTD - DS
		AUDITORIA DE CERTIFICACION																																																			
	6	Gestionar los recursos para la auditoria de certificación	Requerimiento																																							X										1	OSCD - CGTD - DS
		Realizar la auditoria de certificación	Memorandum																																								X	X								1	OSCD - CGTD - DS
		Revisar el Informe de auditoria	Informe																																										X							1	OSCD - CGTD - DS

		Presentar el informe de auditoria y definir acciones correctivas y oportunidades de mejora	Informe																																									X						1	OSCD - CGTD - DS
		REVISAR Y MEDIR DESEMPEÑO DEL SGSI																																																		
		Realizar la medición de desempeño del SGSI	Fichas de indicadores del SGSI																																										X					1	OSCD - CGTD - DS
		Revisar y presentar el estado de implementación del SGSI al Comité de Gobierno Digital y a la Dirección.	Formatos e informe																																											X				1	OSCD - CGTD - DS
ACT.07		MEJORA CONTINUA																																																	
		Realizar el seguimiento y monitoreo a los resultados de la auditoria para la mejora continua	Informe																																												X			1	OSCD - CGTD - DS
		Preparar los planes de acción de las no conformidades y las recomendaciones de la auditoría	Plan de acción de no conformidades ejecutado y aprobado																																												X	X		1	Auditores designados - OSCD - CGTD - DS
	7	Difusión a los integrantes del Comité de Gobierno Digital para su revisión por la Alta Dirección	Proyecto de SGSI implementado al Comité																																														X	1	OSCD - CGTD - DS
		Aprobación por el Comité de Gobierno Digital referido a la implementación del SGSI	Implementación del proyecto del SGSI aprobado																																														X	1	CGTD - DS
		Gestionar la aprobación formal institucional (OPP-OAJ-GG-DIR)	Aprobación institucional																																														X	1	CGTD - OPP - OAJ - GG

ANEXO 2

Mapa de Procesos – Nivel 0

Mapa de Procesos – Nivel 1