

Código: S01.01.02.01

Versión: 01

Nombre del procedimiento:

**Implementación del sistema de gestión de la seguridad de la información**

	<b>Unidad de organización</b>	<b>Firma y sello</b>
Elaborado por:	Oficina de Tecnologías de la Información (OTI)	 Firmado digitalmente por: FAU HORNA Pedro Alberto FAU 20131057823 hard Fecha: 04/10/2023 14:56:20-0500
Revisado por:	Oficina de Planeamiento y Presupuesto (OPP)	 Firmado digitalmente por: ALFARO CONDE Jorge Antonio FAU 20131057823 hard Fecha: 04/10/2023 12:04:58-0500
Aprobado por:	Gerencia General (GG)	

**Control de cambios**

Versión	Sección del procedimiento	Descripción del cambio
01	Total	Adecuación a Norma Técnica N° 001-2018-PCM/SGP

**Objetivo del procedimiento:**

Preservar la confidencialidad, integridad y disponibilidad de la información aplicando un proceso de gestión de riesgos, que proporcione confianza a las partes interesadas en el sentido en que los riesgos se manejan adecuadamente, al instituir mecanismos para reducir sus posibles consecuencias, alineándolas con los objetivos de la SBN y las disposiciones legales y técnicas vigentes.

**Alcance del procedimiento:**

Es de alcance obligatorio para OTI, OPP, ADIR y demás unidades de organización de la SBN.

**Base normativa:**

- 1) Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.
- 2) Decreto Legislativo N° 1412 que aprueba la Ley de Gobierno Digital.
- 3) Decreto Supremo N° 157-2021-PCM, que aprueba el Reglamento del Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.
- 4) Decreto Supremo N° 011-2022-VIVIENDA, que aprueba la Sección Primera del Reglamento de Organización y Funciones de la Superintendencia Nacional de Bienes Estatales - SBN.
- 5) Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 EDI. Tecnología de la Información. Técnicas de Seguridad".

- Sistemas de Gestión de Seguridad de la Información. Requisitos. 2da. Edición”, en todas las entidades integrantes del Sistema Nacional de Transformación Digital y modificaciones.
- 6) Decreto Supremo N° 050-2018-PCM, que establece la definición de Seguridad Digital en el ámbito nacional.
  - 7) Resolución N° 0064-2022/SBN, que aprueba la Sección Segunda del Reglamento de Organización y Funciones de la Superintendencia Nacional de Bienes Estatales – SBN.
  - 8) Resolución N° 0065-2018/SBN, que conforma el Comité de Gobierno y Transformación Digital de la SBN, modificada por: Resolución N° 074-2018/SBN, Resolución N° 024-2019/SBN y Resolución N° 014-2022/SBN.

#### **Siglas y definiciones:**

Siglas:

1	ADIR	Alta Dirección de la SBN
2	CGTD	Comité de Gobierno de Transformación Digital
3	ISO/IEC	ISO Organización Internacional de Normalización, (International Organization for Standardization), IEC hace referencia a Comisión Electrotécnica Internacional (International Electrotechnical Commission).
4	NTP	Norma Técnica Peruana
5	OAJ	Oficina de Asesoría Jurídica
6	OSCD	Oficial de Seguridad y Confianza Digital
7	PCM	Presidencia del Consejo de Ministros
8	PNMGP	Política Nacional de Modernización de la Gestión Pública
9	SBN	Superintendencia Nacional de Bienes Nacionales
10	SGP	Secretaría de Gestión Pública
11	SGSI	Sistema de Gestión de la Seguridad de la Información
12	SOA	Declaración de Aplicabilidad (Statement of Applicability)
13	ST	Secretario Técnico
14	UO	Unidades de organización / Área usuaria

Definiciones:

1	Acta	Documento que certifica y registra todo lo acontecido o pactado durante la reunión de los miembros del CGTD.
2	Resolución	Documento de carácter oficial que contiene la decisión o declaración decisiva sobre un asunto de su competencia.
3	Sistema de Gestión de Seguridad de la información	Es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una entidad y lograr sus objetivos institucionales.

#### **Requisitos para iniciar el procedimiento:**

Descripción del requisito	Fuente
Normativa sobre el SGSI en el Estado Peruano y NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª. Edición”.	Diario Oficial El Peruano
Decisión de implementar una política o normativa sobre el SGSI.	ADIR

N. <sup>º</sup>	Descripción de la actividad	Unidad de organización	Responsable
1	Coordinar agenda y efectuar convocatoria.	ST	Supervisor/a TI
2	Participar en reunión y tomar acuerdos	CGTD	Miembros del CGTD
3	Elaborar acta de reunión	ST	Supervisor/a TI
4	Suscribir el acta con los acuerdos y/o disposiciones: - Implementar el SGSI en la SBN - Ampliar o modificar los alcances de la implementación del SGSI Nota: La conformación del Comité de Gobierno y Transformación Digital se ilustra en el <b>Anexo 4</b>	CGTD	Miembros del CGTD
5	Elaborar el Plan de Gestión de Proyecto de Implementación del SGSI.	OTI	Supervisor/a
6	Coordinar agenda y efectuar convocatoria.	ST	Supervisor/a TI
7	Participar en reunión y tomar acuerdo de aprobación del Plan de Proyecto de Implementación del SGSI	CGTD	Miembros del CGTD
8	Elaborar acta de reunión	ST	Supervisor/a TI
9	Suscribir el acta con los acuerdos adoptados	CGTD	Miembros del CGTD
10	Gestionar aprobación del plan por Titular de la entidad, elaborar informe técnico sustentatorio	ST	Supervisor/a TI
11	Emitir opinión técnica	OPP	
12	Emitir opinión legal y elaborar proyecto de resolución	OAJ	
13	Aprobar plan de Gestión de Proyecto de Implementación del SGSI (suscribir resolución)	Despacho de la Superintendencia	Superintendente/a
14	Elaborar documento en el que se señale la política y objetivos de seguridad de la información.	OTI	Oficial de Confianza y Seguridad Digital
15	Revisar documento, coordinar agenda y efectuar convocatoria.	ST	Supervisor/a TI

16	Participar en reunión y tomar acuerdo de aprobación del documento en el que se señale la política y objetivos de seguridad de la información	CGTD	Miembros del CGTD
17	Elaborar acta de reunión	ST	Supervisor/a TI
18	Suscribir el acta con los acuerdos adoptados	CGTD	Miembros del CGTD
19	Establecer el contexto de la entidad (elaborar matrices). Definir la Metodología de Evaluación y Tratamiento de Riesgos. Planificar definiendo el alcance, la política y metodología. Identificar activos, amenazas y vulnerabilidades. Analizar riesgos y coste/beneficio. Decidir el tratamiento de riesgos	OTI UO	Oficial de Confianza y Seguridad Digital Representantes de UO
20	Elaborar documento Evaluación y Tratamiento de Riesgos. Elaborar Plan de Tratamiento de Riesgos.	OTI UO	Oficial de Confianza y Seguridad Digital Representantes de UO
21	Revisar documento, coordinar agenda y efectuar convocatoria.	ST	Supervisor/a TI
22	Participar en reunión y tomar acuerdo de aprobación del Plan de Tratamiento de Riesgos.	CGTD	Miembros del CGTD
23	Elaborar acta de reunión	ST	Supervisor/a TI
24	Suscribir el acta con los acuerdos adoptados	CGTD	Miembros del CGTD
25	Redactar el documento de la Declaración de Aplicabilidad (SOA). Se consideran los controles señalados en el ISO 27001.	OTI	Oficial de Confianza y Seguridad Digital
26	Revisar documento, coordinar agenda y efectuar convocatoria.	ST	Supervisor/a TI
27	Participar en reunión y tomar acuerdo de aprobación del Documento de la Declaración de Aplicabilidad (SOA).	CGTD	Miembros del CGTD
28	Elaborar acta de reunión	ST	Supervisor/a TI
29	Suscribir el acta con los acuerdos adoptados	CGTD	Miembros del CGTD
30	Elaborar planes de capacitación y concientización sobre la importancia de la seguridad de la información, dirigidos a todo el personal de la SBN.	OTI	Oficial de Confianza y Seguridad Digital

31	Revisar los planes de capacitación y concientización, coordinar agenda y efectuar convocatoria.	ST	Supervisor/a TI
32	Participar en reunión y tomar acuerdo de aprobación de los planes de capacitación y concientización.	CGTD	Miembros del CGTD
33	Elaborar acta de reunión	ST	Supervisor/a TI
34	Suscribir el acta con los acuerdos adoptados	CGTD	Miembros del CGTD
35	Capacitar al personal de la SBN en seguridad de la información.	OTI	Oficial de Confianza y Seguridad Digital
36	Implementar y aplicar los controles seleccionados en el SOA. (ISO 27001). Documentar los procedimientos, políticas y requisitos necesarios del SGSI en coordinación con las unidades de organización involucradas.	OTI UO	Oficial de Confianza y Seguridad Digital Representantes de UO
37	Implementar el Plan de Tratamiento de Riesgos y documentar los resultados. Coordinar y supervisar que se cumpla el Plan de Tratamiento de Riesgos. Elaborar informe sobre el cumplimiento del Plan de Tratamiento de Riesgos.	OTI UO	Oficial de Confianza y Seguridad Digital Representantes de UO
38	Revisar el informe sobre el cumplimiento del Plan de Tratamiento de Riesgos, coordinar agenda y efectuar convocatoria.	ST	Supervisor/a TI
39	Participar en reunión y revisar el cumplimiento del Plan de Tratamiento de Riesgos.	CGTD	Miembros del CGTD
40	Elaborar acta de reunión	ST	Supervisor/a TI
41	Suscribir el acta con los acuerdos adoptados	CGTD	Miembros del CGTD
42	Elaborar documento poniendo en conocimiento la próxima realización de la auditoría interna. Al menos 3 meses antes.	OTI	Oficial de Confianza y Seguridad Digital
43	Realizar auditoría interna (evaluación del desempeño). Supervisar sistemas, controles, etc. y extraer evidencias. Elaborar informe con los hallazgos y el cumplimiento de la auditoría.	OTI	Oficial de Confianza y Seguridad Digital
44	Revisar el informe con los hallazgos y cumplimientos de la auditoría, coordinar agenda y efectuar convocatoria.	OTI	Supervisor/a

45	Participar en reunión y revisar el informe con los hallazgos y cumplimientos de la auditoría.	CGTD	Miembros del CGTD
46	Elaborar acta de reunión	ST	Supervisor/a TI
47	Suscribir el acta con los acuerdos adoptados	CGTD	Miembros del CGTD
48	Elaborar documento los planes de acción de las No Conformidades y recomendaciones de auditoría.	OTI	Oficial de Confianza y Seguridad Digital
49	Revisar documento con los planes de acción, coordinar agenda y efectuar convocatoria.	OTI	Supervisor/a
50	Participar en reunión y revisar y aprobar los planes de acción de las No Conformidades y recomendaciones.	CGTD	Miembros del CGTD
51	Elaborar acta de reunión	ST	Supervisor/a TI
52	Suscribir el acta con los acuerdos adoptados	CGTD	Miembros del CGTD
53	Gestionar aprobación de los planes de acción por Titular de la entidad y elaborar informe técnico sustentatorio.	ST	Supervisor/a TI
54	Emitir opinión técnica	OPP	
55	Emitir opinión legal y elaborar proyecto de resolución	OAJ	
56	Aprobar los planes de acción de las No Conformidades y recomendaciones (suscribir resolución).	Despacho de la Superintendencia	Superintendente/a
57	Difundir los planes de acción de las No Conformidades y recomendaciones	ST	Supervisor/a OTI Oficial de Confianza y Seguridad Digital
58	Implementar los planes de acción de las No Conformidades y recomendaciones, según competencias. Nota: Mejora continua, continúa en actividad 42.	UO	Responsables de UO
<b>Fin del procedimiento</b>			



**MANUAL DE PROCEDIMIENTOS DEL PROCESO S01  
TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES DE  
LA SUPERINTENDENCIA NACIONAL DE BIENES ESTATALES**

CÓDIGO	MAPRO-01-2023/SBN-OTI
VERSIÓN	1.00

**Documentos que se generan:**

- Resolución con el Plan de Gestión de Proyecto de Implementación del SGSI.
- Actas de compromiso de la Alta Dirección de la SBN.
- Documentos varios que aprueban las políticas y objetivos de la seguridad de la información, Plan de Tratamiento de Riesgos, Aprobación de Aplicabilidad (SOA), Planes de Capacitación y Concientización, Informe de hallazgos y cumplimientos de la auditoría.
- Resolución con los planes de acción de las No Conformidades y Recomendaciones (posterior a la auditoría).

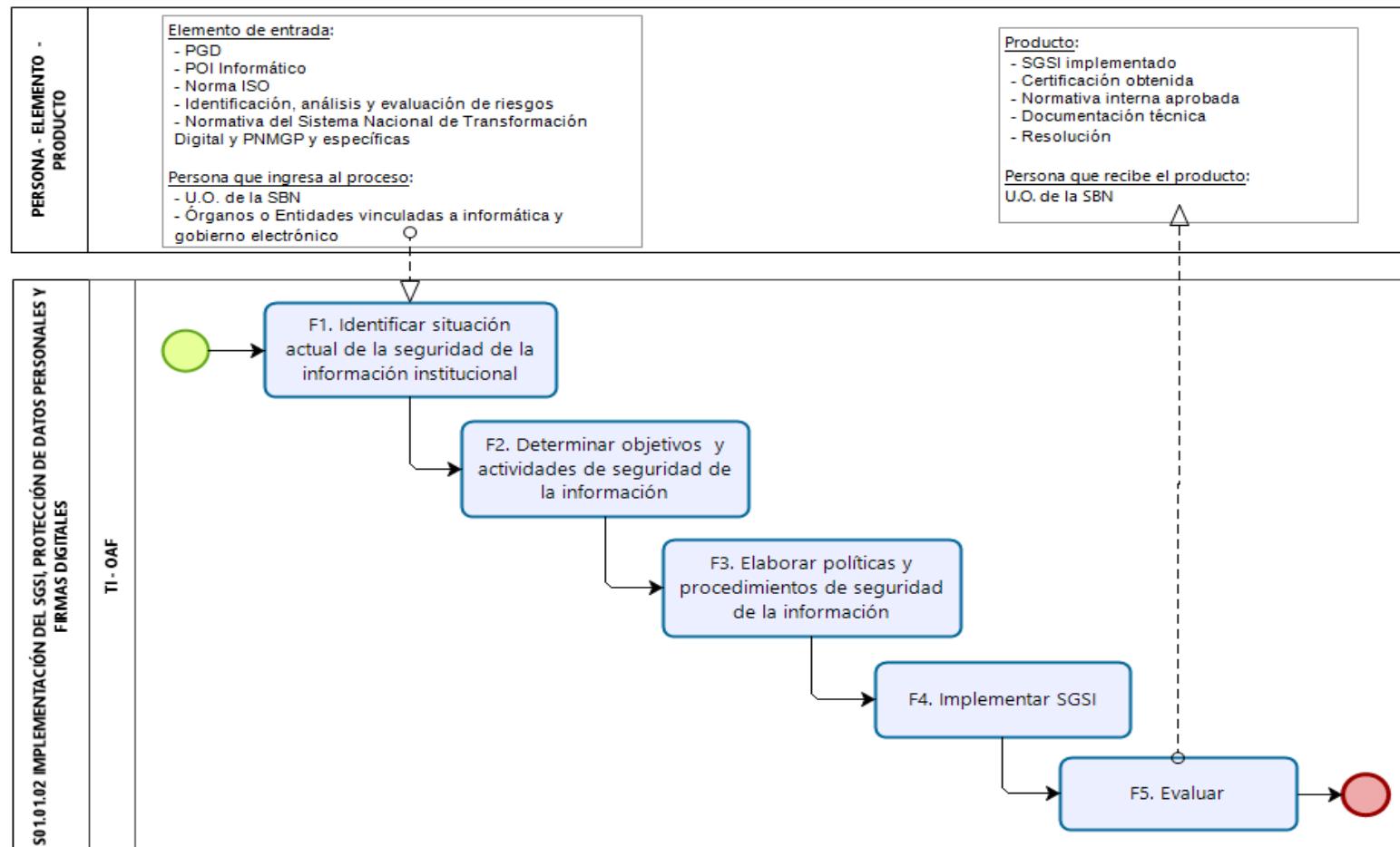
**Proceso relacionado:**

S01.01.02 Implementación del SGSI, protección de datos personales y firmas digitales

Diagrama de proceso (*anexar el diagrama del proceso relacionado*)

## DIAGRAMA DEL PROCESO Nivel 2:

### S01.01.02 IMPLEMENTACIÓN DEL SGSI, PROTECCIÓN DE DATOS PERSONALES Y FIRMAS DIGITALES.



## DIAGRAMA DEL PROCEDIMIENTO

### S01.01.02.01 IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

