Plan de Implementación del Sistema de Gestión de Seguridad de la Información (SGSI)

Versión: 1.0

Visado por PUENTE DE LA VEGA CHUMBE Felix Fabian FAU 20552560711 hard
Motivo: Doy V° B°
Fecha: 2025/01/31 17:52:32-0500

Visado por TORREBLANCA GARCIA Miluska Erika FAU 20552560711 hard
Motivo: Doy V° B°
Fecha: 2025/01/30 18:14:55-0500

Visado por SANTOS CABEZAS DE LEON Janet Gisella FAU 20552560711 hard
Motivo: Doy V° B°
Fecha: 2025/01/31 17:12:32-0500

Visado por CHUMPITAZ VILLALOBOS PERCY GASTON FIR 10331014 hard
Motivo: Doy V° B°
Fecha: 2025/01/31 17:18:42-0500

Visado por MILLONES SORIANO Luis Andres FAU 20552560711 hard
Motivo: Doy V° B°
Fecha: 2025/01/31 17:40:52-0500

Ciclo de Aprobación

Rol	Nombre	Firma	Fecha
Creado por:	Sub Unidad de Abastecimiento		2024
Revisado por:	Comité de Gobierno y Transformación Digital		2025
Aprobado por:	Coordinación Ejecutiva		2025

Historia de Cambios

Versión (Estado)	Autor	Descripción del Cambio	Fecha

Contenido

1. INTRODUCCIÓN

El Programa Nacional "A Comer Pescado" (en adelante, PNACP) requiere cumplir con la Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD de la Presidencia del Consejo de Ministros que exige la implementación de un Sistema de Gestión de Seguridad de la Información (en adelante, SGSI) basado en la Norma Técnica Peruana vigente (*NTP ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información*).

En ese sentido, mediante la ejecución del presente plan, el PNACP implementará su SGSI basado en ISO 27001:2022, cumpliendo las disposiciones gubernamentales en materia de gobierno digital y gestionando de manera efectiva la seguridad de la información.

2. OBJETIVOS

2.1 Objetivo General:

Implementar el Sistema de Gestión de Seguridad de la Información del PNACP en conformidad con la norma NTP ISO/IEC 27001:2022.

2.2 Objetivos Específicos:

- Fomentar la cultura de seguridad de la organización en la entidad.
- Cumplir con la normativa vigente en materia de seguridad de la información.
- Gestionar adecuadamente los riesgos de la seguridad de la información.
- Brindar confianza digital a los ciudadanos y administrados.

3. MARCO LEGAL

3.1 Marco normativo

a. Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD que exige la implementación de la NTP ISO/IEC 27001:2022.
b. Oficio N° D001378-2021-PCM-SGD de fecha 24 de marzo de 2021, por medio de la cual la Secretaría de Gobierno y Transformación Digital de la

Presidencia del Consejo de Ministros remite 18 compromisos para que el Programa inicie y continúe el proceso de transformación digital.

c. Decreto Legislativo N° 1412, Ley de Gobierno Digital.

d. Decreto de Urgencia N° 006-2020, que crea el Sistema Nacional de Transformación Digital.

e. Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.

f. Ley Nº 29733, Ley de Protección de Datos Personales.

3.2 Marco de referencia y consulta

a. NTP ISO/IEC 27001:2022, Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información.

Nota: La Norma Técnica Peruana NTP-ISO/IEC 27001:2022 es la adopción nacional del estándar internacional ISO/IEC 27001:2022, por lo que en adelante se les denominará ISO/IEC 27001, indistintamente.

b. NTP ISO/IEC 27002:2022, Tecnología de la información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información. 1ª Edición.

Nota: La Norma Técnica Peruana NTP-ISO/IEC 27002:2022 es la adopción nacional del estándar internacional ISO/IEC 27002:2022, por lo que en adelante se les denominará ISO/IEC 27002, indistintamente.

c. NTP ISO 31000:2018, Gestión del riesgo. Directrices. 2ª Edición.

Nota: La Norma Técnica Peruana NTP-ISO 31000:2018 es la adopción nacional del estándar internacional ISO 31000:2018, por lo que en adelante se les denominará ISO 31000, indistintamente.

4. METODOLOGÍA

En la implementación del SGSI se aplicará implícitamente el modelo PDCA que comprende las fases de Planear, Hacer, Revisar y Actuar, tal como se muestra en la siguiente imagen:

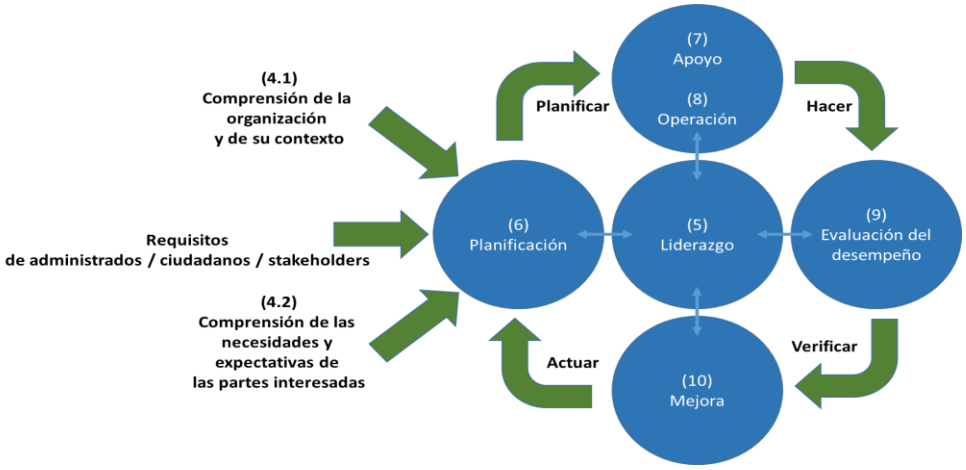

Imagen 1: Ciclo de implementación y operación del SGSI

Al finalizar el proyecto, la operación del SGSI deberá repetir estas fases de manera continua a través del tiempo en ciclos que mínimamente deben ser anuales, de manera que el sistema madure continuamente.

5. CONTEXTO DE LA ENTIDAD

5.1 Contexto externo

El PNACP ha identificado los siguientes asuntos externos que son relevantes para su propósito y que afectan su capacidad para lograr el resultado deseado de su SGSI:

- Datos de ciudadanos/administrados: El PNACP recolecta y trata datos de ciudadanos. Es necesario garantizar la seguridad de dichos datos y asegurar la privacidad de la ciudadanía.
- Cambios en los requisitos legales y reglamentarios: La legislación relativa a la seguridad de la información no deja de evolucionar y, por tanto, el SGSI debe actualizarse para adaptarse a esos cambios a medida que se producen.
- Terceros contratados por el PNACP: Existen terceros que prestan servicios al PNACP para el cumplimiento de sus funciones. El nivel de interacción e intercambio de información con ellos debe ser tomado en consideración al implementar el SGSI.
- Avances tecnológicos: El SGSI se verá afectado por los cambios tecnológicos que puedan producirse en el futuro. Por lo tanto, es

necesario realizar un seguimiento de dichos cambios y evaluar su impacto en el SGSI.

- Cambios sociales, económicos, políticos y culturales: Por ser una entidad gubernamental, el PNACP debe tomar en cuenta los cambios en el entorno relacionados al ámbito político, económico, cultural y social. Estos podrían tener un impacto en el SGSI.
- Eventos imprevistos/sin precedentes: Debido a circunstancias imprevistas, como una catástrofe natural o una pandemia, podría ser necesario realizar cambios en el SGSI.

5.2 Contexto interno

- Requerimientos de información de los empleados: Los servidores civiles que trabajan para el PNACP acceden a información para llevar a cabo sus labores. Sus requisitos juegan un papel importante en el diseño del SGSI.
- Rotación de servidores civiles: La rotación de personal crea la necesidad de una formación adicional y una mayor atención al funcionamiento eficaz del SGSI.
- Cambios en servicios: Los productos y servicios proporcionados por el PNACP a los ciudadanos y administrados pueden sufrir cambios, y estos tienen un impacto directo en el SGSI.
- Cambios en los sistemas y procesos internos: Los sistemas y procesos internos del PNACP pueden sufrir cambios coyunturales, creando así la necesidad de cambiar el SGSI.

6. ALCANCE DEL SGSI

El proceso propuesto es el proceso de soporte: Gestión de Tecnologías de la Información y Comunicaciones. Se justifica por ser el proceso en el que se apoyan todos los procesos misionales de la entidad.

7. ROLES Y RECURSOS NECESARIOS PARA EL PROYECTO

7.1 Roles y responsabilidades para la implementación del SGSI

Para la implementación del SGSI se requieren los siguientes roles:

a. **Comité de Gobierno y Transformación Digital – CGD** (Sponsor del proyecto)

Compuesto por las autoridades del máximo nivel en la entidad. Tiene las siguientes responsabilidades:

- Gestionar la asignación de servidores y recursos necesarios para la implementación del SGSI.
- Promover y gestionar la implementación de estándares y buenas prácticas en seguridad digital en la entidad.
- Elaborar informes anuales que midan el progreso de la implementación del SGSI.
- Vigilar por el cumplimiento de la normatividad relacionada con la seguridad de la información.
- Gestionar, mantener y documentar el SGSI.

b. **Oficial de Seguridad y Confianza Digital** (Líder de proyecto)**.**
Tiene las siguientes responsabilidades:

- Coordinar y reportar al Comité de Gobierno y Transformación Digital institucional la implementación, mantenimiento, y la aplicación de las normas relacionadas a seguridad y confianza digital.
- Coordinar con los dueños de los procesos o, en su defecto, con los responsables de las unidades de organización de la entidad toda iniciativa de mejora relacionada con la seguridad digital bajo su gestión.
- Promover y desarrollar una cultura de seguridad digital en los servidores de la entidad, así como en el ciudadano en general, todo ello de manera coordinada con el Comité de Gobierno y Transformación Digital.
- Formular, articular, supervisar y coordinar la implementación, mantenimiento y mejora del SGSI.
- Asistir, en calidad de miembro del Comité de Gobierno y Transformación Digital, en la correcta orientación, dirección, evaluación, monitoreo, control y mejora continua en temas relacionados a la seguridad digital en la entidad; del mismo modo, en la definición e implementación de acciones, técnicas, estratégicas, coordinación y de respuesta ante incidentes de seguridad digital.
- Preparar los planes de auditoría al SGSI y garantizar el cumplimiento de las acciones correctivas que deriven.

c. **Dueño del proceso de alcance del SGSI (Unidad de Administración y Finanzas)**

Tiene las siguientes responsabilidades:

- Destacar la importancia y la necesidad de la seguridad de la información dentro de las Unidades Orgánicas mediante la ejecución proactiva, la asistencia a reuniones y el fomento de la atención de los empleados al SGSI.
- Responsabilizarse de todos los activos de información que utiliza el proceso a su cargo.
- Tomar las medidas adecuadas en relación con los incidentes de seguridad de la información que se notifican sobre sus activos.
- Atender las cuestiones planteadas por el Oficial de Seguridad y Confianza Digital, y garantizar la resolución de los requerimientos en el momento oportuno.
- Garantizar una presencia adecuada durante las auditorías internas/externas y trabajar con el Oficial de Seguridad y Confianza Digital para abordar los resultados de las auditorías.
- Garantizar la disponibilidad de los recursos adecuados para implementar / mantener el SGSI, según aplique.
- Planificar, ejecutar y medir los controles de seguridad de la información de índole técnico.

7.2 Presupuesto requerido

A continuación, se detalla la inversión requerida para cumplir con el proyecto:

Tabla 01: Fases para la Implementación

N	FASE	MONTO
01	Planificación	S/ 25,000.00
02	Ejecución	S/ 30,000.00
03	Seguimiento y Control	S/ 20,000.00
04	Cierre	

Los mismos que se detallan en la Tabla 02: Detalle de Fases para la Implementación del SGSI.

Tabla 02: Detalle de Fases para la Implementación

FASE	ACTIVIDAD	DETALLE	DOCUMENTO / ENTREGABLE
Planificación	Definición del alcance del SGSI.	Definir con la entidad el alcance del SGSI y documentarlo.	**Alcance del SGSI**
	Reunión de Kick Off	Reunión de inicio con la dirección donde se detalla el plan de trabajo y organización del proyecto.	**Presentación de Kick Off** **Lista de asistentes**
	Elaboración de política del SGSI	Se debe elaborar la política del SGSI considerando los requisitos de la norma.	**Política del SGSI**
	Definición de objetivos de seguridad de la información	Se deben definir los objetivos de seguridad empleando un formato. Se deben definir criterios e indicadores de medición para dichos objetivos.	**Objetivos de Seguridad de la Información**
	Elaborar documento alcance del SGSI	Se debe identificar: Asuntos internos y externos, necesidades y expectativas, partes interesadas, roles / responsabilidades / autoridades. Se define el alcance del SGSI	**Contexto de la Organización**
	Elaboración de procedimiento de gestión de riesgos de seguridad de la información	Se debe definir la metodología para desarrollar el inventario de activos y la evaluación de riesgos	**Procedimiento de gestión de riesgos de seguridad de la información**
	Elaboración de procedimiento de control de documentos	Documento que define la pirámide documental (ej. Reglamento, Manual, Políticas, Procedimientos, Instructivos) y su codificación.	**Procedimiento de control de documentos**
	Elaboración de procedimiento de auditoría interna	Documento que establece los pasos para realizar la auditoría interna del SGSI.	**Procedimiento de auditoría interna**
	Elaboración de procedimiento de revisión por parte de la dirección	Documento que establece los lineamientos de revisión periódica por parte de la dirección de la entidad.	**Procedimiento de revisión por parte de la dirección**
	Charla de concientización	Charla de formación y sensibilización en seguridad para los trabajadores de la entidad (1 hora aproximadamente) donde se explica los conceptos de seguridad y highlights del proyecto SGSI. Implica preparar material y ejecutar la charla.	**Presentación de Concientización** **Lista de asistencia**

FASE	ACTIVIDAD	DETALLE	DOCUMENTO / ENTREGABLE
	Clasificación e inventario de activos de información	Elaboración del inventario de activos de información en base al alcance del SGSI (siguiendo el procedimiento de gestión de riesgos aprobado)	**Inventario de activos de información**
	Evaluación y plan de tratamiento de riesgos	Identificación de riesgos y planificar su tratamiento con los controles de la norma (siguiendo el procedimiento de gestión de riesgos aprobado)	**Matriz de evaluación y tratamiento de riesgos**
Ejecución	Elaboración de política de seguridad de personal	Desarrollar la política de seguridad en recursos humanos según la norma	**Política de seguridad de personal**
	Elaboración de política de seguridad física	Desarrollar la política de seguridad física en base a la norma (controles físicos)	**Política de seguridad física**
	Elaboración de política de seguridad con proveedores	Desarrollar la política de seguridad con proveedores	**Política de seguridad con proveedores**
	Elaboración de política de control de accesos	Implica el desarrollo de la política y procedimientos/formatos para: Altas y bajas, conciliación periódica de accesos, matriz de roles.	**Política de control de accesos**
	Elaboración de política de seguridad de contraseñas	Implica el desarrollo de la política y procedimientos/formatos para: Construcción de contraseñas complejas, concientización en el uso de contraseñas.	**Política de seguridad de contraseñas**
	Elaboración de política de buen uso de activos	Desarrollo de política para lineamientos dirigidos a usuario final.	**Política de buen uso de activos**
	Elaboración de política de seguridad en operaciones	Desarrollo de política dirigida a administración TIC (servicios, red e infraestructura). Implica la documentación de procedimientos operativos (responsabilidad del cliente)	**Política de seguridad en operaciones**
	Elaboración de política de desarrollo seguro	Desarrollo de política con lineamientos de seguridad para el ciclo de desarrollo de software.	**Política de desarrollo seguro**
	Elaboración de política de gestión de incidentes de seguridad	Desarrollo de política y protocolo de gestión de incidentes.	**Política de gestión de incidentes de seguridad de la información**

FASE	ACTIVIDAD	DETALLE	DOCUMENTO / ENTREGABLE
	Elaboración de política de continuidad de seguridad de la información	La entidad no cuenta con un Plan de Continuidad por lo que se deberá elaborar un plan de continuidad básico (drp/contingencia) y luego incorporar la seguridad de la información. Se deben realizar pruebas (como mínimo de escritorio) del plan.	**Política de continuidad de la seguridad de la información** **Plan de continuidad que incluye seguridad** **Informe de pruebas**
	Elaboración de política de BYOD (traiga su propio dispositivo)	Implica, además de la política, definir qué dispositivos personales se emplearán para uso corporativo y llevar un control de ellos.	**Política de BYOD**
	Elaboración de política de cumplimiento	Implica, además de la política, definir una matriz legal/normativa que aplique a la entidad.	**Política de cumplimiento**
	Elaboración de política de respaldo y restauración	Implica, además de la política, establecer una planificación del respaldo y programar pruebas de restauración.	**Política de respaldo y restauración**
	Elaboración de política de seguridad de equipos	Implica, además de la política, establecer un plan de mantenimiento preventivo con los respectivos registros de su ejecución.	**Política de seguridad de equipos**
	Elaboración de política de control de cambios	Implica, además de la política, establecer un flujo de autorización y ejecución de los cambios y un formato de control de éstos.	**Política de control de cambios**
	Elaboración de política de seguridad en la gestión de proyectos	Implica, además de la política, preparar un formato de control de proyectos en el que se incluya los aspectos de seguridad de la información.	**Política de seguridad en la gestión de proyectos**
	Elaboración de Declaración de Aplicabilidad (SOA)	Elaborar el SOA en base a los 93 controles de la versión 2022 de la norma.	**Declaración de aplicabilidad**
	Elaboración de Manual de SGSI	Elaborar el Manual del SGSI que es el compendio de cumplimiento de todas las cláusulas de la norma.	**Manual del SGSI**
	Elaboración del plan de análisis de vulnerabilidades	Elaborar el plan de mitigación de vulnerabilidades identificadas en el ethical hacking/pentesting	**Plan de mitigación de vulnerabilidades**

FASE	ACTIVIDAD	DETALLE	DOCUMENTO / ENTREGABLE
	Seguimiento del Plan de Tratamiento de Riesgo	Informe del seguimiento del plan de tratamiento del riesgo definido en la gestión de riesgos. No se debe culminar todo el plan si no es factible pero debe estar definido en fechas.	**Informe de seguimiento del plan de tratamiento del riesgo**
Evaluación y Control	Revisión interna de toda la documentación	Se realiza una evaluación de todo lo trabajado desde un enfoque de auditor interno. Esto con el propósito de ir con más confianza a la auditoría interna.	**Informe de revisión interna del SGSI**
	Auditoría interna del SGSI	Debe ser realizado por un tercero de preferencia (no casa de certificación) para mayor objetividad.	**Informe de auditoría interna**
	Resolución de no conformidades y observaciones de auditoría interna	Según el informe de auditoría interna se subsanan las No Conformidades y se prepara para auditoría de certificación.	**Informe de resolución de no conformidades**
Cierre	Realizar reunión de cierre de proyecto	Debe de realizarse una reunión con el miembro del Comité de Gobierno y Transformación Digital del Programa.	**Acta de Reunión de cierre de proyecto**
	Suscribir el acta de cierre del proyecto	Se deberá de suscribir el acta de cierre del proyecto.	**Acta de Cierre del Proyecto**

8. MONITOREO Y EVALUACIÓN

El proceso de monitoreo y evaluación del Plan de Implementación del Sistema de Gestión de Seguridad de la Información – SGSI del PNACP, se realiza en el marco de la Norma Técnica Peruana "NTP ISO/IEC 27001".

9. CRONOGRAMA

A continuación, el cronograma de actividades.

	PNACP	Mes 01		Mes 02		Mes 03		Mes 04		Mes 05		Mes 06		Mes 07		Mes 08		Mes 09		Mes 10
		Semana 1-2	Semana 3-4	Semana 1-2	Semana 3-4	Semana 1-2	Semana 3-4	Semana 1-2	Semana 3-4	Semana 1-2	Semana 3-4	Semana 1-2	Semana 3-4	Semana 1-2	Semana 3-4	Semana 1-2	Semana 3-4	Semana 1-2	Semana 3-4	Semana 1-2
	Fases																			
1	**Planificación**																			
1.1	Definición del alcance del SGSI.	■																		
1.2	Elaboración de política de seguridad de la información SGSI		■																	
1.3	Definición de objetivos de seguridad de la información		■																	
1.4	Elaborar documento Contexto de la Organización		■																	
1.5	Elaboración de procedimiento de gestión de riesgos de seguridad de la información		■	■																
1.6	Elaboración de procedimiento de auditoría interna				■															
1.7	Clasificación e inventario de activos de información				■	■	■													
1.8	Evaluación y plan de tratamiento de riesgos						■	■	■											
2	**Ejecución**																			
2.1	Elaboración de políticas específicas de seguridad de la información						■	■	■	■	■	■	■							
2.2	Elaboración de Declaración de Aplicabilidad (SOA)							■	■											
2.3	Desarrollo de Manual de SGSI			■	■	■	■	■	■											
2.4	Seguimiento del Plan de Tratamiento de Riesgo													■	■					
3	**Evaluación y Control**																			
3.1	Revisión interna de toda la documentación															■	■			
3.2	Auditoría interna del SGSI																■			
3.3	Resolución de no conformidades y observaciones de auditoría interna																	■	■	
4	**Cierre**																			
4.1	Reunión con el Comité de Gobierno y Transformación Digital																			■
4.2	Suscripción del Acta de cierre del proyecto																			■