PLAN DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 2023-2025

Plan N° PAIS.GTI.PLA.03

Versión N° 01

Etapa	Responsable	Cargo	Visto Bueno y sello:
Formulado por:	José Lorenzo Mori Vargas	Oficial de Seguridad y Confianza Digital	Firmado digitalmente por MORI VARGAS Jose Lorenzo FAU 20601993181 hard Motivo: Soy el autor del documento Fecha: 09.06.2023 08:38:47 -05:00
Revisado por:	Jorge Luis Távara Vallejos	Ejecutivo de la Unidad de Tecnologías de la Información	Firmado digitalmente por TAVARA VALLEJOS Jorge Luis FAU 20601993181 soft Motivo: Soy el autor del documento Fecha: 09.06.2023 09:11:43 -05:00
	Irma Jennypher Cuba Araoz	Ejecutiva de la Unidad de Planeamiento y Presupuesto	Firmado digitalmente por CUBA ARAOZ Irma Jennypher FAU 20601993181 hard Motivo: Soy el autor del documento Fecha: 09.06.2023 09:23:05 -05:00
	Igor Elías Mejía Verástegui	Ejecutivo de la Unidad de Asesoría Jurídica	Firmado digitalmente por MEJIA VERASTEGUI Igor Elias FAU 20601993181 soft Motivo: Soy el autor del documento Fecha: 09.06.2023 12:53:45 -05:00
	Lenin Bernardo Gutiérrez Roncal	Especialista de Gestión de Calidad	Firmado digitalmente por GUTIERREZ RONCAL Lenin Bernardo FAU 20601993181 soft Motivo: Soy el autor del documento Fecha: 09.06.2023 10:43:04 -05:00
Aprobado por:	Justo Alejandro Pozo Zárate	Director Ejecutivo	Firmado digitalmente por POZO ZARATE Justo Alejandro FAU 20601993181 hard Motivo: Soy el autor del documento Fecha: 26.06.2023 17:18:49 -05:00

PLAN DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

ÍNDICE

1. INTRODUCCIÓN

Los Directivos, funcionarios y trabajadores de la Administración Pública, hoy más que nunca deben tomar conciencia sobre la importancia de cuidar los activos de información que producen y tratan durante la ejecución de sus actividades, donde la prevención de riesgos es vital para su protección y conservación en el marco de la seguridad de la información.

Proteger la información de una entidad pública o de cualquier organización en general, no significa cerrar o restringir de forma totalitaria los accesos hacia los activos de información que pudiera tener la entidad, sino, tener implementado controles adecuados y eficientes (procedimientos, mecanismos, protocolos y buenas prácticas) que permitan garantizar la confidencialidad, la integridad y la disponibilidad (CID) de la información.

La necesidad de proteger la información que se produce y trata en la entidad, más que necesidad es y debe ser un compromiso de todas las personas que conforman el Programa Nacional "Plataformas de Acción para la Inclusión Social – PAIS", compromiso que no sólo se limitaría a identificar o inventariar los activos de información de la que se dispone, sino también en conocer con cierto grado de madurez, todo lo que abarca o puede abarcar un Sistema de Gestión de Seguridad de la Información (SGSI).

Es así que, en el Programa Nacional "Plataformas de Acción para la Inclusión Social – PAIS" se requiere implementar el Sistema de Gestión de Seguridad de la Información (SGSI), por ser esta una herramienta de gestión de riesgos que se deriva no sólo de una necesidad, sino, de la obligación que como entidad pública se tiene ante el órgano rector de conformidad con las normas de Gobierno y Transformación Digital.

Lo descrito nos lleva a formular el presente plan, en cuyo contenido se plasman aspectos esenciales que permitirán al Programa Nacional "Plataformas de Acción para la Inclusión Social – PAIS" implementar su respectivo Sistema de Gestión de Seguridad de la Información según sus fases, tal como lo contempla la Norma Técnica Peruana NTP ISO/IEC 27001:2014:

2. MARCO NORMATIVO

2.1	Decreto Legislativo N° 1412:	Decreto Legislativo que aprueba la Ley de Gobierno Digital.
2.2	Decreto de Urgencia N° 006-2020:	Crea el Sistema Nacional de Transformación Digital.
2.3	Decreto de Urgencia N° 007-2020:	Aprueba el marco de Confianza Digital y establece medidas para su fortalecimiento.
2.4	Decreto Supremo N° 029-2021-PCM:	Aprueba el reglamento de la Ley de Gobierno Digital.
2.5	Decreto Supremo N° 157-2021-PCM:	Aprueba el reglamento del Sistema Nacional de Transformación Digital.
2.6	Resolución Ministerial N° 004-2016-PCM:	Aprueba el uso obligatorio de la Norma Técnica Peruana NTP ISO/IEC 27001:2014.
2.7	Resolución Ministerial N° 041-2017-PCM:	Aprueba el uso obligatorio de la Norma Técnica Peruana NTP ISO/IEC 12207:2016.
2.8	Resolución Ministerial N° 263-2017-MIDIS:	Aprueba el Manual de Operaciones del PNPAIS.
2.9	Resolución Ministerial N° 087-2019-PCM:	Aprueba disposiciones para la conformación y funciones del Comité de Gobierno Digital, modificando en parte a la RM. N° 119-2018-PCM.
2.10	Resolución Ministerial N° 002-2021-MIDIS:	Aprueba las políticas de seguridad de la información del MIDIS.

2.11	Resolución Ministerial N° 049-2021-MIDIS:	Aprueba el Plan de Gobierno Digital 2021-2023 del MIDIS.
2.12	Resolución Ministerial N° 111-2021-MIDIS:	Aprueba el Plan de Continuidad Operativa del MIDIS.
2.13	Resolución Ministerial N° 121-2021-MIDIS:	Aprueba directiva de procedimientos del ciclo de vida del software del MIDIS y PPSS.
2.14	Resolución Ministerial N° 138-2021-MIDIS:	Aprueba el Manual para la Gestión de Riesgos de Procesos del MIDIS y PPSS.
2.15	Resolución Ministerial N° 100-2023-MIDIS:	Aprueba el Plan Estratégico Institucional 2021 – 2026 Ampliado del MIDIS.
2.16	Resolución Ministerial N° 159-2022-MIDIS	Aprueba Directiva N° 003-2022-MIDIS, denominada “Catálogo de documentos oficiales del MIDIS”
2.17	Resolución Directoral N° 028-2020-MIDIS/PNPAIS-DE	Aprueba procedimiento denominado requerimiento e implementación de Sistemas Informáticos en el marco del ciclo de vida del software del PNPAIS.
2.18	Resolución Directoral N° 138-2020-MIDIS/PNPAIS-DE	Aprueba la versión 3 de la Política del Sistema de Gestión Integrado del PNPAIS.
2.19	Resolución Directoral N° 213-2020-MIDIS/PNPAIS-DE	Aprueba directiva sobre normas para el acceso a la red interna, servicios digitales y uso del internet en el PNPAIS.
2.20	Resolución Directoral N° 144-2021-MIDIS/PNPAIS-DE	Actualiza la conformación del Comité de Gobierno y Transformación Digital del PNPAIS.

3. ALCANCE

3.1. ÁMBITO DE APLICACIÓN

El presente plan aplica para los procesos misionales de las siguientes Unidades de Organización:

	UNIDAD	PROCESO
1	Unidad de Articulación y Gestión de Servicios - UAGS	M02: Gestión de Articulación de Servicios
2	Unidad de Plataformas de Servicios - UPS	MI.01.3: Operatividad y mantenimiento de las plataformas de servicio

3.2. ACTORES INVOLUCRADOS

Los principales actores involucrados en el Plan de Implementación del Sistema de Gestión de Seguridad de la Información del PNPAIS son:

3.3.1 Ministerio de Desarrollo e Inclusión Social – MIDIS
3.3.2 Presidencia del Consejo de Ministros - PCM

4. DIAGNÓSTICO

4.1) REALIDAD PROBLEMÁTICA

El PNPAIS no cuenta con su respectivo SGSI aprobado, tal cual lo establece el marco normativo de la Ley de Gobierno Digital y la Norma Técnica Peruana NTP ISO/IEC 27001:2014, el cual es de uso obligatorio para las entidades de la Administración Pública.

El no tener aprobado el respectivo SGSI implica el no cumplimiento de uno de los compromisos de Gobierno Digital, sobre la que ejerce supervisión y control la PCM en su calidad de ente rector, tarea que lo ejecuta a través del CNSD de la SGTD.

El SGSI como herramienta de gestión y sub sistema del SGI, facilita la gestión de riesgos de seguridad digital, específicamente los de seguridad de la información, como tal, su no implementación dificulta la administración de riesgos que son propios del entorno digital del PNPAIS, así como de toda infraestructura tecnológica de la que se sirve o con la que interactúan los diferentes procesos de la entidad.

En el PNPAIS se produce y se gestiona información inherente a la misión institucional, los cuales se guardan en distintos medios y formatos, de los que no se tiene el control respectivo a nivel de activo y su grado de sensibilidad (criticidad).

4.2) ANÁLISIS CONTEXTUAL

4.2.1) Según las normas de Gobierno Digital, el Comité de Gobierno y Transformación Digital de la entidad, tiene entre otras las funciones siguientes:

a) Gestionar la asignación de personal y recursos necesarios para la implementación del Plan de Gobierno Digital, Modelo de Gestión Documental (MGD), Modelo de Datos Abiertos Gubernamentales y Sistema de Gestión de Seguridad de la Información (SGSI) en sus planes operativos institucionales, Plan Anual de Contrataciones y otros.

b) 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.

c) Elaborar informes anuales que midan el progreso de la implementación del Plan de Gobierno Digital y evalúen el desempeño del Modelo de Gestión Documental (MGD), Modelo de Datos Abiertos Gubernamentales y Sistema de Gestión de Seguridad de la Información (SGSI).

d) Vigilar el cumplimiento de la normatividad relacionada con la implementación del Gobierno Digital, Interoperabilidad, Seguridad de la Información y Datos Abiertos en las entidades públicas.

e) Gestionar, mantener y documentar el Modelo de Gestión Documental (MGD), Modelo de Datos Abiertos Gubernamentales y Sistema de Gestión de Seguridad de la Información (SGSI) en la entidad.

4.2.2) En el marco normativo de Gobierno Digital, para la implementación del SGSI del PNPAIS, en uso de las buenas prácticas de gestión se conforma el grupo de trabajo de acuerdo a lo siguiente:

N°	ROL	RESPONSABILIDAD
1	Representante de la Unidad de Organización comprendida en el ámbito de aplicación.	✓ Implementa el SGSI para los procesos identificados y comprendidos en el ámbito de aplicación.
2	Oficial de Seguridad y Confianza Digital de la entidad.	✓ Coordina la implementación y el mantenimiento del SGSI
3	Oficial de Gobierno de Datos	✓ Brinda apoyo y soporte en el marco de sus funciones y competencias
4	Oficial de Datos Personales	

N°	ROL	RESPONSABILIDAD
5	Coordinador y/o Encargado del SGI (Sistema de Gestión Integrado)	

4.2.3) De conformidad con la Norma Técnica Peruana NTP ISO/IEC 27001:2014 y el estándar ISO 27001:2022, la implementación del SGSI tiene dos contextos o fases; en la primera se formula y aprueba toda la documentación requisitos del sistema, según se muestra en el detalle de la tabla N° 01 siguiente. En la segunda fase se ejecutan las reglas, disposiciones, procedimientos y controles que se establecen para asegurar el mantenimiento del SGSI.

TABLA N° 01: ETAPAS / REQUISITOS DEL SGSI

N°	ETAPA	DOCUMENTOS REQUISITOS
1	CONTEXTO DE LA ORGANIZACIÓN Y LIDERAZAGO	6.1.1) **CONTEXTO DE LA ORGANIZACIÓN** - Comprender la organización y su contexto, - Comprender las necesidades y expectativas de las partes interesadas - Determinar el alcance del SGSI - Sistema de Gestión de Seguridad de la Información 6.1.2) **LIDERAZGO** - Liderazgo y compromiso - Política - Roles, responsabilidades y autoridades organizacionales
2	PLANIFICACIÓN Y SOPORTE	6.1.3) **PLANIFICACIÓN** - Acciones para tratar los riesgos y las oportunidades - Objetivos de Seguridad de la Información y planificación para conseguirlos 6.1.4) **SOPORTE** - Recursos - Competencia - Concientización - Comunicación - Información documentada
3	OPERACIÓN	6.1.5) **OPERACIÓN** - Planificación y control operacional - Evaluación de riesgos de Seguridad de la Información - Tratamiento de riesgos de seguridad de la información
4	EVALUACIÓN DEL DESEMPEÑO Y MEJORAS	6.1.6) **EVALUACIÓN DEL DESEMPEÑO** - Monitoreo, medición, análisis y evaluación - Auditoría interna - Revisión por la Dirección 6.1.7) **MEJORAS** - No conformidades y acción correctiva - Mejora continua

4.2.4) Los documentos requisitos del SGSI que se formularán y aprobarán en la primera fase según la Norma Técnica Peruana ISO/IEC 27001:2014 y el estándar ISO 27001:2022, son los que se muestran a continuación según sus etapas, para lo

cual previamente se debe contar con los formatos de análisis situacional y otros, según las listas siguientes:

a) ANÁLISIS SITUACIONAL DEL SGSI

N°	COD	DOCUMENTO / PRODUCTO
1	PNPAIS-SGSI-001	ANALISIS DE BRECHAS INICIAL
2	PNPAIS-SGSI-002	EVALUACION DE CONTROLES
3	PNPAIS-SGSI-003	EVALUACION DE REQUISITOS Y CONTROLES-ISO-27001

b) CONTEXTO DE LA ORGANIZACIÓN Y LIDERAZGO

En esta etapa, como requisito de su SGSI, el PNPAIS dispondrá de los documentos siguientes, lo que permitirá comprender la organización y su contexto interno y externo, así como conocer de las necesidades y expectativas de las partes interesadas, y establecer las políticas de liderazgo respectivas.

N°	COD	DOCUMENTO / PRODUCTO
1	PNPAIS-SGSI-004	ANALISIS DE CONTEXTO EXTERNO
2	PNPAIS-SGSI-005	ANALISIS DE CONTEXTO INTERNO
3	PNPAIS-SGSI-006	REQUERIMIENTO DE PARTES INTERESADAS
4	PNPAIS-SGSI-007	POLITICA DE SEGURIDAD DE LA INFORMACIÓN
5	PNPAIS-SGSI-008	ROLES Y RESPONSABILIDADES

c) PLANIFICACIÓN Y SOPORTE

El PNPAIS, para implementar y/o mantener su SGSI, tiene establecido sus objetivos de seguridad, en función de los cuales gestiona sus riesgos y oportunidades de mejora de forma sistemática y planificada, con orientación a resultados:

En esta etapa, como requisito del SGSI el PNPAIS dispondrá de los documentos siguientes:

N°	COD	DOCUMENTO / PRODUCTO
1	PNPAIS-SGSI-009	METODOLOGIA PARA LA GESTION DE RIESGOS DE SEGURIDAD DIGITAL
2	PNPAIS-SGSI-010	FORMATO INVENTARIO DE ACTIVOS
3	PNPAIS-SGSI-011	MATRIZ DE RIESGO
4	PNPAIS-SGSI-012	PLAN DE TRATAMIENTO DE RIESGOS
5	PNPAIS-SGSI-013	MATRIZ DE APLICABILIDAD
6	PNPAIS-SGSI-014	PLAN DE FORMACIÓN Y CONCIENCIACIÓN

d) OPERACIÓN

El PNPAIS administra, supervisa y controla su SGSI, asegurando la sostenibilidad del mismo en el tiempo en base a la gestión de riesgos al que están expuestos los activos de información de la entidad.

En esta etapa, se formularán controles que ayuden y a aporten a la administración del SGSI del PNPAIS, tales como:

N°	COD	DOCUMENTO / PRODUCTO
1	PNPAIS-SGSI-015	PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DIGITAL

e) EVALUACIÓN DEL DESEMPEÑO Y MEJORAS

El PNPAIS monitorea, mide, analiza y evalúa de forma progresiva su SGSI, para lo cual se apoya en los controles (políticas, normativas, procedimientos, programas, planes) de auditoría establecidos para la gestión de riesgos y oportunidades de seguridad de la entidad, así como de otros recursos de información (revisión por la Dirección, no conformidades y acciones correctivas) que permitirán aplicar la mejora continua al SGSI

En esta etapa, como requisito del SGSI, el PNPAIS dispondrá de los documentos siguientes:

N°	COD	DOCUMENTO / PRODUCTO
1	PNPAIS-SGSI-016	PROGRAMA DE AUDITORIAS
2	PNPAIS-SGSI-017	PROCEDIMIENTO DE AUDITORIA INTERNA
3	PNPAIS-SGSI-018	PLAN DE AUDITORIA
4	PNPAIS-SGSI-019	INFORME DE AUDITORIA INTERNA
5	PNPAIS-SGSI-020	RESULTADO DE LA EVALUACION POR LA DIRECCION
6	PNPAIS-SGSI-021	INFORME DE EVALUACIÓN POR LA DIRECCIÓN
7	PNPAIS-SGSI-022	PROCEDIMIENTO PARA LAS ACCIONES CORRECTIVAS
8	PNPAIS-SGSI-023	POLÍTICA DE CIFRADO DE DISPOSITIVOS
9	PNPAIS-SGSI-024	POLÍTICA DE COMUNICACIÓN INALÁMBRICA
10	PNPAIS-SGSI-025	POLÍTICA DE DISPOSITIVOS MÓVILES
11	PNPAIS-SGSI-026	POLÍTICA DE SEGURIDAD DE COMPUTACIÓN EN LA NUBE
12	PNPAIS-SGSI-027	POLÍTICA DE SEGURIDAD DE RECURSOS HUMANOS
13	PNPAIS-SGSI-028	POLITICA DE ACTIVIDAD DE SEGUIMIENTO
14	PNPAIS-SGSI-029	POLITICA DE CODIFICACIÓN SEGURA
15	PNPAIS-SGSI-030	POLITICA DE CONTROL DE ACCESOS
16	PNPAIS-SGSI-031	POLITICA DE ELIMINACIÓN DE LA INFORMACIÓN
17	PNPAIS-SGSI-032	POLITICA DE ENMASCARAMIENTO DE DATOS
18	PNPAIS-SGSI-033	POLITICA DE FILTRADO WEB

N°	COD	DOCUMENTO / PRODUCTO
19	PNPAIS-SGSI-034	POLITICA DE GESTION DE LA CONFIGURACIÓN
20	PNPAIS-SGSI-035	POLITICA DE INTELIGENCIA DE AMENAZAS
21	PNPAIS-SGSI-036	POLITICA DE MONITOREO DE LA SEGURIDAD FISICA
22	PNPAIS-SGSI-037	POLITICA DE PREPARACIÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO
23	PNPAIS-SGSI-038	POLITICA DE PREVENCION DE FUGAS DE DATOS
24	PNPAIS-SGSI-039	POLITICA DE SEGURIDAD DE LA INFORMACIÓN PARA EL USO DEL SERVICIO DE LA NUBE
25	PNPAIS-SGSI-040	POLITICA SEGURIDAD DE LA INFORMACION EN GESTION DE PROYECTOS
26	PNPAIS-SGSI-041	POLITICA DE SEGURIDAD PARA PROVEEDORES
27	PNPAIS-SGSI-042	POLITICA DE USO ACEPTABLE DE LOS ACTIVOS

4.2.5) En adición a los documentos listados en cada una de las etapas de la implementación y/o mantenimiento del SGSI del PNPAIS, se podrán emplear documentos complementarios como los que se indican a continuación, en la medida que estos sean relevantes y tengan vinculación con en el SGI del PNPAIS, cuidando en todo momento que, todo lo actuado en materia de seguridad de la información se mantenga como información documentada:

a) Informe Técnico sobre Gestión de la Seguridad de la Información
b) Informe Técnico en materia de Gobierno y Transformación Digital
c) Actas de sesión de trabajo relativos a la seguridad digital
d) Reportes de no conformidades y acciones correctivas
e) Otros documentos afines a la gestión de la seguridad digital

4.3) CONCLUSIONES Y RECOMENDACIONES

4.3.1) El SGSI se implementa como un sub-sistema del SGI del PNPAIS, cuyo plan debe estar alineado al marco de la Ley de Gobierno Digital, específicamente en lo que corresponde al ámbito de la Seguridad y Confianza Digital.

4.3.2) El CGTD-PNPAIS será quien vise cada uno de los documentos requisitos del SGSI según sus fases.

5. MARCO ESTRATÉGICO

5.1) OBJETIVO ESTRATÉGICO INSTITUCIONAL / ACCIÓN ESTRATÉGICA INSTITUCIONAL

Los objetivos estratégicos y las acciones estratégicas están definidos en el Plan Estratégico Institucional (PEI) del MIDIS como sector, el mismo que alcanza a los Programas Sociales, siendo estos los siguientes:

OBJETIVO ESTRATÉGICO INSTITUCUIONAL	ACCIÓN ESTRATÉGICA INSTITUCIONAL
OEI.O5 Fortalecer la Gestión Institucional	AEI.05.01 Soporte digital para la prestación de servicios implementado en el MIDIS
	AEI.05.02 Sistema de Gestión de Calidad Implementado

OEI.06 Fortalecer la Gestión de Riesgos de Desastres	AEI.06.02 Riesgos identificados y difundidos
	AEI.06.03 Continuidad Operativa implementada en el MIDIS

Fuente: Plan Estratégico Institucional del MIDIS.

5.2) OBJETIVO GENERAL Y ESPECÍFICO DEL SGSI

Para el SGSI del PNPAIS, se establecen los siguientes objetivos de seguridad de la información, todos con sus respectivos indicadores:

COD	OBJETIVO	INDICADOR	META ANUAL
		GENERAL	
O.1)	Preservar la CONFIDENCIALIDAD, la INTEGRIDAD y la DISPONIBILIDAD de la información.	1.1) (N° total de Servidores/as certificados en Fundamentos de Seguridad de la Información en Aula Digital PCM / N° Total de Servidores del PNPAIS) * 100	2023: 05% 2024: 10% 2025: 20%
		1.2) (N° total de procesos N-1 comprendidos en el alcance del SGSI / N° total de procesos del PNPAIS) * 100	2023: 05% 2024: 10% 2025: 15%
		ESPECÍFICO	
O.2)	Impulsar el fortalecimiento de capacidades de los servidores y servidoras del PNPAIS en el marco de la Seguridad Digital	1.3) (N° total de servidores/as del PNPAIS capacitados en el marco de la Seguridad Digital del PNPAIS / N° total de servidores y servidores del PNPAIS) * 100	2023: 05% 2024: 10% 2024: 15%
		1.4) (N° total de servidores y servidoras del PNPAIS capacitados en el Seguridad de Datos Personales / N° total de servidores y servidores de del PNPAIS) * 100	2024: 10% 2025: 15%
O.3)	Minimizar los riesgos de Seguridad de la Información en el ámbito laboral de los trabajadores del PNPAIS	1.5) (N° total de controles implementados / N° total de controles comprendidos en la ISO 27001:2022) * 100	2023: 25% 2024: 50% 2025: 100%
		1.6) (N° total de riesgos de Seguridad de la Información valorados como medios y bajos / N° total de riesgos de Seguridad de la Información valorados como Muy altos y altos) * 100	2023: 10% 2024: 15% 2025: 30%
O.4)	Mejorar la gestión institucional a través de procedimientos de Gestión de Incidentes de Seguridad Digital	1.7) (N° total de incidentes de Seguridad Digital reportados / N° total de incidentes de Seguridad Digital controlados y cerrados) * 100	2023: 25% 2024:50% 2025: 100%

Para alcanzar la meta planificada, los propietarios de los procesos comprendidos en el alcance, en coordinación con la Unidad de Tecnologías de la Información gestionarán ante la Unidad de Recursos Humanos, se impulse el fortalecimiento de capacidades del personal en las materias que correspondan.

6. PROGRAMACIÓN DE ACTIVIDADES

Las actividades que se ejecutarán para la implementación del SGSI del PNPAIS, se detallan en el anexo N° 01 del presente plan.

7. SEGUIMIENTO Y EVALUACIÓN

7.1) El Oficial de Seguridad y Confianza Digital, una vez de aprobado el presente plan, formulará un informe trimestral indicando el avance de la implementación del SGSI al Líder del CGTD-PNPAIS, quien a su vez dará cuenta del estado de avance de la implementación del SGSI a la Dirección Ejecutiva, el que se efectuará en y durante la reunión de coordinación del CGTD-PNPAIS.

7.2) El CGTD-PNPAIS, una vez de finalizada la 1ra. Fase de la implementación del SGSI, informará a través de la Dirección Ejecutiva, de todo lo actuado a la Secretaría de Gobierno y Transformación Digital de la PCM, a fin que la PCM en su condición de ente rector, disponga lo conveniente para la revisión o auditoría interna según corresponda, en aras de lograr la certificación correspondiente.

8. ANEXOS

8.1) CRONOGRAMA DE ACTIVIDADES PARA LA IMPLEMENTACIÓN DEL SGSI
8.2) GLOSARIO DE TÉRMINOS (Definiciones y Abreviaturas)

ANEXO N° 01 (8.1)
CRONOGRAMA DE ACTIVIDADES PARA LA ELABORACIÓN DE LOS DOCUMENTOS REQUISITOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) DEL PNPAIS

N°	ACTIVIDAD / TAREA	RESPONSABLE	PRODUCTO (MEDIO DE VERIFICACIÓN)	AÑO							
				2023			2024				
				TRIMESTRE			TRIMESTRE				
				2	3	4	1	2	3	4	
1	**ACCIONES PREVIAS A LA FORMULACIÓN DE LOS DOCUMENTOS REQUISITOS DEL SGSI**										
1.1	Reunión de coordinación del CGTD-PNPAIS, para tomar conocimiento del plan de implementación del SGSI, de las acciones y obligaciones que se desplegarán para la ejecución del plan.	LÍDER GOB. DIGITAL Y OFICIAL DE SEGURIDAD Y CONFIANZA DIGITAL	Memorando de convocatoria y Acta de Reunión	X							
2.1	Designación de los representantes de los procesos involucrados en el alcance del Plan, así como de los procesos que apoyarán en su ejecución.	Unidades de Organización involucradas	Memorando de designación	X							
2.2	Preparación e inducción al personal involucrado en el proceso de ejecución del Plan del SGSI - PNPAIS	UTI	Acta de Trabajo	X							
2	**APROBAR LOS DOCUMENTOS REQUISITOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN**										
2.1	Elaboración y aprobación de los documentos requisitos siguientes en el marco del SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) **1) ANÁLISIS SITUACIONAL** ✓ (PNPAIS-SGSI-001) ANALISIS DE BRECHAS INICIAL ✓ (PNPAIS-SGSI-002) EVALUACION DE CONTROLES ✓ (PNPAIS-SGSI-003) EVALUACION DE REQUISITOS Y CONTROLES-ISO-27001	UAGS / UPS / UTI / UPP / UAJ CGTD-PNPAIS.	Resolución Directoral		X						
2.2	**2) CONTEXTO DE LA ORGANIZACIÓN Y LIDERAZGO** ✓ (PNPAIS-SGSI-004) ANÁLISIS DE CONTEXTO EXTERNO ✓ (PNPAIS-SGSI-005) ANÁLISIS DE CONTEXTO INTERNO ✓ (PNPAIS-SGSI-006) REQURIMIENTO DE PARTES INTERESADAS ✓ (PNPAIS-SGSI-007) POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN ✓ (PNPAIS-SGSI-008) ROLES Y RESPONSABILIDADES	UAGS / UPS / UTI / UPP / UAJ CGTD-PNPAIS.	Resolución Directoral			X					
2.3	**3) PLANIFICACIÓN Y SOPORTE** ✓ (PNPAIS-SGSI-009) METODOLOGÍA PARA LA GESTION DE RIESGOS DE SEGURIDAD DIGITAL ✓ (PNPAIS-SGSI-010) FORMATO DE INVENTARIO DE ACTIVOS ✓ (PNPAIS-SGSI-011) MATRIZ DE RIESGOS ✓ (PNPAIS-SGSI-012) PLAN DE TRATAMIENTO DE RIESGOS ✓ (PNPAIS-SGSI-013) MATRIZ DE APLICABILIDAD ✓ (PNPAIS-SGSI-014) PLAN DE FORMACIÓN Y CONCIENCIACIÓN	UAGS / UPS / UTI / UPP / UAJ CGTD-PNPAIS.	Resolución Directoral				X				
2.4	**4) OPERACIÓN** ✓ (PNPAIS-SGSI-015) PROCEDIMIENTO DE GESTION DE INCIDENTES DE SEGURIDAD DIGITAL	UAGS / UPS / UTI / UPP / UAJ CGTD-PNPAIS.	Resolución Directoral					X			
2.5	**5) EVALUACIÓN DEL DESEMPEÑO Y MEJORAS** ✓ (PNPAIS-SGSI-016) PROGRAMA DE AUDITORÍAS ✓ (PNPAIS-SGSI-017) PROCEDIMIENTO DE AUDITORÍA INTERNA ✓ (PNPAIS-SGSI-018) PLAN DE AUDITORÍA	UAGS / UPS / UTI / UPP / UAJ CGTD-PNPAIS.	Resolución Directoral						X		

N°	ACTIVIDAD / TAREA	RESPONSABLE	PRODUCTO (MEDIO DE VERIFICACIÓN)	AÑO							
				2023			2024				
				TRIMESTRE			TRIMESTRE				
				2	3	4	1	2	3	4	
	✓ (PNPAIS-SGSI-019) INFORME DE AUDITORÍA ✓ (PNPAIS-SGSI-020) RESULTADO DE LA EVALUACIÓN POR LA DIRECCIÓN ✓ (PNPAIS-SGSI-021) INFORME DE EVALUACIÓN POR LA DIRECCIÓN ✓ (PNPAIS-SGSI-022) PROCEDIMIENTO PARA LAS ACCIONES CORRECTIVAS										
2.6	✓ (PNPAIS-SGSI-023) POLÍTICA DE CIFRADO DE DISPOSITIVOS ✓ (PNPAIS-SGSI-024) POLÍTICA DE COMUNICACIÓN INHALÁMBRICA ✓ (PNPAIS-SGSI-025) POLÍTICA DE DISPOSITIVOS MÓVILES ✓ (PNPAIS-SGSI-026) POLÍTICA DE SEGURIDAD DE COMPUTACIÓN EN LA NUBE ✓ (PNPAIS-SGSI-027) POLÍTICA DE SEGURIDAD DE RECURSOS HUMANOS ✓ (PNPAIS-SGSI-028) POLÍTICA DE ACTIVIDAD DE SEGUIMIENTO ✓ (PNPAIS-SGSI-029) POLÍTICA DE CODIFICACIÓN SEGURA ✓ (PNPAIS-SGSI-030) POLÍTICA DE CONTROL DE ACCESOS ✓ (PNPAIS-SGSI-031) POLÍTICA DE ELIMINACIÓN DE LA INFORMACIÓN ✓ (PNPAIS-SGSI-032) POLÍTICA DE ENMASCARAMIENTO DE DATOS ✓ (PNPAIS-SGSI-033) POLÍTICA DE FILTRADO WEB ✓ (PNPAIS-SGSI-034) POLÍTICA DE GGESTIÓN DE LA CONFIGURACIÓN ✓ (PNPAIS-SGSI-035) POLÍTICA DE INTELIGENCIA DE AMENAZAS ✓ (PNPAIS-SGSI-036) POLÍTICA DE MONITOREO DE LA SEGURIDAD FÍSICA ✓ (PNPAIS-SGSI-037) POLÍTICA DE PREPARACÍÓN DE LAS TIC PARA LA CONTINUIDAD DEL NEGOCIO ✓ (PNPAIS-SGSI-038) POLÍTICA DE PREVENCIÓN DE FUGA DE DATOS ✓ (PNPAIS-SGSI-039) POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA EL USO DEL SERVICIO DE LA NUBE ✓ (PNPAIS-SGSI-040) POLÍTICA DE SEGURIDAD DE INFORMACIÓN EN GESTIÓN DE PROYECTOS ✓ (PNPAIS-SGSI-041) POLÍTICA DE SEGURIDAD PARA PROVEEDORES ✓ (PNPAIS-SGSI-042) POLÍTICA DE USO ACEPTABLE DE LOS ACTIVOS	UAGS / UPS / UTI / UPP / UAJ CGTD-PNPAIS.	Resolución Directoral							X	
2.7	Organizar expediente e informar de situación actual del SGSI – PNPAIS al CGTD-PNPAIS	Oficial de Seguridad y Confianza Digital	Informe Técnico								X
2.8	Informar del estado de avance de la implementación del SGSI a la alta Dirección a través del CGTD-PNPAIS	Líder del Comité de Gobierno y Transformación Digital	Informe Técnico								X
2.9	Remisión de expediente del SGSI al ente RECTOR	Comité de Gobierno y Transformación Digital PNPAIS	Oficio								X
2.10	Seguimiento, monitoreo y vigilancia del SGSI - PNPAIS	Comité de Gobierno y Transformación Digital PNPAIS	Acta de Trabajo								X

Nota: La denominación de los documentos requisitos del SGSI, podrá ser variado en su denominación cuando corresponda y sea necesario de acuerdo a la realidad de la entidad.

ANEXO N° 02 (8.2)

DEFINICIONES Y ABREVIATURAS

1) DEFINICIONES

1.1) Aceptación de riesgo[1]: Decisión de aceptar el riesgo.

1.2) Activo de Información[2]: Información que tiene valor para el MIDIS, pudiendo además ser aquel recurso (humano, tecnológico, etc.) que efectúa el tratamiento directo o indirecto de la información que soporta uno o más procesos del MIDIS. Hace referencia a la información y a los activos asociados a la información.

1.3) Control[3]: En seguridad de la información hace referencia a un mecanismo o forma de ejercer vigilancia y supervisión en un ambiente operacional administrable, pudiendo estos ser los siguientes:

a) Las configuraciones de los sistemas
b) Documentos normativos (directivas, procedimientos, protocolos, etc.)
c) Mecanismos de seguridad y protección (Firewall o cortafuegos, etc.)
d) Registros, bitácoras, etc.

1.4) Confianza digital[4]: Es el estado que emerge como resultado de cuan veraces, predecibles, éticas, proactivas, transparentes, seguras, inclusivas y confiables son las interacciones digitales que se generan entre personas, empresas, entidades públicas o cosas en el entorno digital, con el propósito de impulsar el desarrollo de la economía digital y la transformación digital. Es un componente de la transformación digital y tiene como ámbitos la protección de datos personales, la ética, la transparencia, la seguridad digital y la protección del consumidor en el entorno digital.

1.5) Comité de Gobierno y Transformación Digital[5]: Es el mecanismo de gobernanza a nivel institucional para el gobierno y transformación digital en las entidades de la administración pública, responsable de liderar y dirigir el proceso de transformación digital en la entidad.

1.6) Confidencialidad[6]**:** Garantizar que la información sea accesible únicamente para quienes tengan acceso autorizado.

1.7) Disponibilidad[7]**:** Garantizar que los usuarios autorizados tengan acceso a la información y activos asociados cuando sea necesario.

1.8) Ciberseguridad[8]: Capacidad tecnológica de preservar el adecuado funcionamiento de las redes, activos y sistemas informáticos y protegerlos ante amenazas y vulnerabilidades en el entorno digital. Comprende la perspectiva técnica de la Seguridad Digital y es un ámbito del Marco de Seguridad Digital del país.

---

[1] ISO/IEC 27001:2008
[2] Anexo 1 de la RM. N° 138-2021-MIDIS
[3] Anexo A, NTP ISO/IEC 27001:2014
[4] Art. 3 del D.U. N° 007-2020
[5] Art. 13 D.S. N° 157-2021-PCM
[6] ISO/IEC 27001:2018
[7] ISO/IEC 27001:2018
[8] Literal “h”, art. 3, D.U. N° 007-2020

1.9) **Evaluación del riesgo**[9]: Proceso de comparación del riesgo estimado frente al criterio de riesgo para determinar el significado del riesgo.

1.10) **Equipo de Respuesta ante Incidentes de Seguridad Digital (CSIRT)**[10]**:** Es aquel equipo responsable de la gestión de incidentes de seguridad digital que afectan los activos de una entidad pública o una red de confianza.

1.11) **Evento de la Seguridad de la Información**[11]**:** Ocurrencia identificada en un sistema, servicio o red indicando una posible brecha de política de seguridad de la información o falla de las salvaguardas o una situación desconocida previa que puede ser relevante.

1.12) **Estimación del riesgo**[12]**:** Proceso total de análisis y evaluación del riesgo.

1.13) **Entorno Digital**[13]**:** es el dominio o ámbito habilitado por las tecnologías y dispositivos digitales, generalmente interconectados a través de redes e infraestructuras de datos o comunicación, incluyendo el internet, que soportan los procesos, servicios, plataformas que sirven como base para la interacción entre personas, empresas, entidades públicas o dispositivos.

1.14) **Ente rector**[14]**:** La Presidencia del Consejo de Ministros, a través de su Secretaría de Gobierno y Transformación, es quien tiene la rectoría de Gobierno y Transformación Digital.

1.15) **Gestión de riesgos**[15]: La gestión de riesgos de seguridad en el entorno digital está integrada en la toma de decisiones, diseño de controles de seguridad en los servicios digitales y procesos de la entidad. Es responsabilidad de la alta dirección dirigirla, mantenerla e incorporarla en la gestión integral de riesgos de la entidad.

1.16) **Gestión de incidentes de seguridad digital**[16]**:** Proceso formal que tiene por finalidad planificar, preparar, identificar, analizar, contener, investigar incidentes de seguridad digital, así como la recuperación y la determinación de acciones correctivas para prevenir incidentes similares.

1.17) **Gobierno Digital**[17]**:** Es el uso estratégico de las tecnologías digitales y datos en la Administración Pública para la creación de valor público. Se sustenta en un ecosistema compuesto por actores del sector público, ciudadanos y otros interesados, quienes apoyan en la implementación de iniciativas y acciones de diseño, creación de servicios digitales y contenidos, asegurando el pleno respeto de los derechos de los ciudadanos y personas en general en el entorno digital.

---

[9] ISO/IEC 27001:2008
[10] Art. 104, D.S. N° 029-2021-PCM
[11] ISO/IEC 27001:2008
[12] ISO/IEC 27001:2008
[13] Literal “c”, art. 3, D.U. N° 007-2020
[14] Art. 8 D. Leg. N° 1412, Art. 2 del D.S. N° 029-2021-PCM y Art. 5 del D.S. N° 157-2021-PCM.
[15] Art. 95, D.S. N° 029-2021-PCM
[16] Literal “f”, art. 3, D.U. N° 007-2020
[17] Art. 6, D.S. N° D. Leg. N° 1412

1.18) Integridad[18]: En seguridad de la información, es salvaguardar la exactitud e integridad de la información y activos asociados.

1.19) Incidente de Seguridad Digital[19]: Es un evento o serie de eventos que pueden comprometer la confianza, la prosperidad económica, la protección de las personas y sus datos personales, la información, entre otros activos de la organización, a través de tecnologías digitales.

1.20) Matriz de riesgo[20]: Instrumento que permite consolidar la información referente a los riesgos identificados, lo cual incluye el tipo, causas, consecuencias y nivel de riesgo, así como las medidas de control identificados para afrontarlos.

1.21) Norma Técnica[21]: Para los efectos del presente plan, se refiere a la Norma Técnica Peruana NTP ISO/IEC 27001:2014 y demás estándares que conforman la familia ISO 27000.

1.22) Oficial de Seguridad y Confianza Digital[22]: Para los efectos del presente plan, se refiere al rol y responsabilidad que tiene el servidor designado como Oficial de Seguridad y Confianza Digital de la entidad, para coordinar la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información – SGSI del PNPAIS.

1.23) Oficial de Datos Personales[23]**:** Es el rol responsable de velar por el cumplimiento de las normas en materia de protección de datos personales en su entidad. Dicho rol es ejercido por un funcionario o servidor público designado por la máxima autoridad administrativa de la entidad, el mismo que puede recaer en el titular de la oficina de asesoría jurídica de la entidad o en el titular de la oficina de tecnologías de la información de la misma, o quienes hagan sus veces.

1.24) Oficial de Gobierno de Datos[24]**:** Es el rol responsable de asegurar el uso ético de las tecnologías digitales y datos en la entidad pública, proponer iniciativas de innovación basadas en datos, fomentar una cultura basada en datos, articular y gestionar el uso de datos gubernamentales, y asegurar la calidad e integridad de datos que contribuya a la creación de valor público. Asimismo, es responsable de impulsar y coordinar el modelamiento, procesamiento, análisis y desarrollo de servicios de información de datos gubernamentales y datos abiertos con los responsables de los procesos correspondientes, así como de coordinar la implementación del Modelo de Referencia de Datos de la entidad.

1.25) Parte interesada[25]: Persona u organización que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad.

1.26) Probabilidad[26]: Posibilidad de que un evento determinado ocurra en un periodo de tiempo dado.

---

[18] ISO/IEC 27001:2008
[19] Art. 3 del D.U. N° 007-2020
[20] RM. N° 138-2021-MIDIS
[21] NTP ISO/IEC 27001:2014
[22] Art. 111, D.S. N° 029-2021-PCM
[23] Art. 68.6, D.S. N° 029-2021-PCM
[24] Art. 68.2, D.S. N° 029-2021-PCM
[25] Tomado del art. 109.2) del D.S. N° 029-2021-PCM y de la NTP ISO/IEC 27001:2014
[26] R.M. N° 138-2021-PCM

1.27) Riesgo[27]: Posibilidad de que suceda algún evento adverso que afecta el logro de los objetivos de la entidad.

1.28) Riesgo residual[28]: Es aquel riesgo que subsiste, después de haber implementado las medidas de control.

1.29) Riesgo de seguridad digital[29]; Efecto de la incertidumbre relacionada con el uso, desarrollo y gestión de las tecnologías digitales y datos, en el curso de cualquier actividad. Resulta de la combinación de amenazas y vulnerabilidades en el entorno digital y es de naturaleza dinámica. Puede socavar el logro de los objetivos económicos y sociales al alterar la confidencialidad, integridad y disponibilidad de las actividades o el entorno, así como poner en riesgo la protección de la vida privada de las personas. Incluye aspectos relacionados con los entornos físicos y digitales, las actividades críticas, las personas y organizaciones involucradas en la actividad y los procesos organizacionales que la respaldan.

1.30) Seguridad Digital[30]: Es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas.

1.31) Secretaría de Gobierno y Transformación Digital (SGTDI)[31]: Unidad Organizacional de la Presidencia del Consejo de Ministros que, ejerce la rectoría del Sistema Nacional de Transformación Digital en el país y en las materias de Gobierno, Confianza y Transformación Digital, siendo la autoridad técnico-normativa a nivel nacional en dichas materias. Asimismo, es el Líder Nacional de Gobierno Digital responsable del proceso de transformación digital en el país y dirección estratégica del Gobierno Digital en el Estado Peruano.

1.32) Sistema de Gestión de Seguridad de la Información (SGSI)[32]**:** 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,

1.33) Sistema de Gestión Integrado (SGI)[33]**:** Incluye los requisitos del Sistema de Gestión de Calidad (SGC), Sistema de Gestión Anti soborno (SGAS), Sistema de Control Interno (SCI) y Gestión de la Seguridad de la Información (SGSI).

1.34) Seguridad de la Información (SI)[34]**:** Es preservar la confidencialidad, la integridad y la disponibilidad de la información; además, también pueden ser involucradas otras características como la autenticación, responsabilidad, no-repudio y fiabilidad.

---

[27] R.M. N° 138-2021-PCM
[28] R.M. N° 138-2021-PCM
[29] Literal "g", art. 3, D.U. N° 007-2020
[30] Art. 30, D. Leg. N° 1412
[31] Art. 68) del ROF aprobado con RM. N° 156-2021-PCM y Art. 5 del D.S. N° 157-2021-PCM
[32] Art. 109, D.S. N° 029-2021-PCM
[33] RD. N° 080-2022-MIDIS/PNPAIS-DE
[34] ISO/IEC 27001:2008

1.35) Servicio Digital[35]; Es aquel servicio provisto de forma total o parcial a través de internet u otras redes equivalentes, que se caracteriza por ser parcial o totalmente automatizado y utilizar de manera intensiva las tecnologías digitales y datos, permitiendo al menos una de las siguientes prestaciones; i) Adquirir un bien, servicio, información o contenido, ii) Buscar, compartir, usar y acceder a datos, contenido o información sobre productos, servicios o personas, iii) Pagar un servicio o bien (tangible o intangible) y, iv) El relacionamiento entre personas.

1.36) Tratamiento del riesgo[36]: Proceso de selección e implementación de controles para minimizar o mitigar el riesgo.

1.37) Transformación Digital[37]**:** Es el proceso continuo, disruptivo, estratégico y de cambio cultural que se sustenta en el uso intenso de las tecnologías digitales, sistematización y análisis de datos para generar efectos económicos, sociales y de valor para las personas.

1.38) Vulnerabilidad[38]: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos.

2) ABREVIATURAS

2.1) CCA: Comité de Control de Calidad
2.2) CSIRT: Equipo de Respuesta a Incidentes de Seguridad Digital
2.3) CCP: Coordinación de Control Patrimonial
2.4) CGTD-PNPAIS: Comité de Gobierno y Transformación Digital del PNPAIS
2.5) DE: Dirección Ejecutiva
2.6) PNPAIS: Programa Nacional "Plataformas de Acción para la Inclusión Social - PNPAIS"
2.7) SGSI-PNPAIS: Sistema de Gestión de Seguridad de la Información del PNPAIS
2.8) SGI: Sistema de Gestión Integrado
2.9) UTI: Unidad de Tecnologías de la Información
2.10) URRHH: Unidad de Recursos Humanos
2.11) UAGS: Unidad de Articulación y Gestión de Servicios
2.12) UPS: Unidad de Plataforma de Servicios
2.13) UCI: Unidad de Comunicación e Imagen
2.14) UA: Unidad de Administración
2.15) UAJ: Unidad de Asesoría Jurídica
2.16) UPP: Unidad de Planeamiento y Presupuesto
2.17) UO: Unidades de Organización

[35] Literal "i", art. 3, D.U. N° 007-2020
[36] ISO/IEC 27001:2008
[37] Art. 3, D.U. N° 006-2020
[38] https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf