PLAN DE IMPLEMENTACIÓN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN 2025-2027

Plan N° 02- 2025-MIDIS/PNPDS-DE

Versión N° 01

Plan aprobado mediante Resolución de Dirección Ejecutiva N° D000004-2025-MIDIS/PNPDS-DE

Etapa	Responsable	Cargo	Visto Bueno y sello:
Formulado por:	Saúl Mateo Pérez Vega	Oficial de Seguridad y Confianza Digital	Firma Digital Programa CONTIGO Firmado digitalmente por PEREZ VEGA Saul Mateo FAU 20605733281 hard Motivo: Soy el autor del documento Fecha: 23.01.2025 18:28:23 -05:00 Fecha:
Revisado por:	Rocio Marisol Rengifo Nakama	Jefa de la Unidad de Planeamiento, Presupuesto y Modernización	Firma Digital Programa CONTIGO Firmado digitalmente por RENGIFO NAKAMA Rocio Marisol FAU 20605733281 hard Motivo: Doy V° B° Fecha: 23.01.2025 18:30:57 -05:00 Fecha:
	Rosa Esther García More	Jefe de la Unidad de Asesoría Jurídica	Firma Digital Programa CONTIGO Firmado digitalmente por GARCIA MORE Rosa Esther FAU 20605733281 hard Motivo: Doy V° B° Fecha: 23.01.2025 18:32:59 -05:00 Fecha:
Aprobado por:	Orfelina Arpasi Quispe	Directora Ejecutiva	Firma Digital Programa CONTIGO Firmado digitalmente por ARPASI QUISPE Orfelina FAU 20605733281 soft Motivo: Doy V° B° Fecha: 23.01.2025 18:39:06 -05:00 Fecha:

HOJA DE CONTROL DE CAMBIOS

Versión	Fecha	Documento sustento [1]	Textos modificados [2]	Responsable[3]
01	21/01/2025	Informe N° D0001-2025-MIDIS/PNPDS-GTD	Documento inicial	Comité de Gobierno Digital

[1] Señalar el informe que sustenta la formulación del documento normativo y/o el informe que sustenta la modificación de la nueva versión del documento.
[2] Señalar los artículos, numerales, literales, anexos, etc. que genera la modificación del documento.
[3] Señalar la unidad de organización que formula la nueva versión del documento.

ÍNDICE

1. INTRODUCCION

El Programa Nacional CONTIGO fue creado el 11 de agosto de 2015, mediante el Decreto Supremo N° 004-2015-MIMP, como parte del Ministerio de la Mujer y Poblaciones Vulnerables bajo la denominación de "Programa de entrega de la pensión no contributiva a personas con discapacidad severa en situación de pobreza", y el 12 de marzo de 2017, fue transferido al Ministerio de Desarrollo e Inclusión Social mediante Decreto Supremo N° 008-2017-MIDIS, modificándose su denominación a "Programa Nacional de entrega de la pensión no contributiva a personas con discapacidad severa en situación de pobreza – CONTIGO".

El Programa Nacional de entrega de la pensión no contributiva a personas con discapacidad severa en situación de pobreza – CONTIGO inicio su cobertura con 411 usuarios, personas con discapacidad severa en situación de pobreza, de las regiones Tumbes y Ayacucho.

En su segundo año de funcionamiento, logró beneficiar a 4,304 usuarios de las regiones Amazonas, Apurímac, Cajamarca, Huánuco, Loreto, Pasco y Huancavelica. A mediados del 2016, brindó la pensión no contributiva a 7,852 beneficiarios de 9 regiones. Al cierre del citado año, alcanzó los 14,625 usuarios, sumando las regiones de Áncash, Lambayeque, La Libertad, Piura y Puno.

En septiembre de 2019, a través del Decreto Supremo N° 303-2019-EF, se aprobó la transferencia de recursos presupuestales que permitió duplicar el número de usuarios a 39,890 para finales de año. Esto también permitió la cobertura del programa en todo el país, llegando a las regiones de Madre de Dios, Ucayali, Ica y Tacna.

El Programa Nacional CONTIGO en el año 2024 amplió su cobertura a 142,771 usuarios con discapacidad severa en situación de pobreza y pobreza extrema a nivel nacional, que son beneficiarios de la pensión no contributiva del Programa.

De acuerdo al artículo 4 del Manual de Operaciones[4] el Programa Nacional CONTIGO cuenta con las siguientes funciones generales:

a) Evaluar las solicitudes para el otorgamiento de la pensión no contributiva.
b) Aprobar la relación de beneficiarios del Programa.
c) Gestionar y monitorear la entrega de la pensión no contributiva.
d) Solicitar información a entidades públicas y privadas para verificar el cumplimiento de los requisitos de acceso al Programa.
e) Coordinar con las entidades públicas y privadas las acciones necesarias para el cumplimiento del objetivo del Programa.
f) Solicitar la inscripción de los beneficiarios del Programa en el Registro Nacional de Personas con Discapacidad.
g) Las demás funciones que se establezcan en el Manual de Operaciones o se deleguen en la normativa vigente.

En dicho contexto, el Programa Nacional CONTIGO se orienta en garantizar la entrega de la pensión no contributiva a personas con discapacidad severa en situación de pobreza, en todo el territorio nacional de manera progresiva, con la finalidad de contribuir en la mejora de la calidad de vida, para ello el Programa ha implementado el Sistema Integrado CONTIGO, el cual permite **a los aliados estratégicos y a los ciudadanos** registrar su solicitud de afiliación, actualización y acceder en tiempo real a la información del estado de los trámites realizados, para el acceso a la pensión no contributiva de los usuarios de su jurisdicción.

[4] Aprobado mediante Resolución Ministerial N° 012-2020-MIDIS de fecha 07ENE2020

A partir del uso de las tecnologías de la información surge una serie de desafíos vinculados a la seguridad de la información, tales como amenazas y vulnerabilidades que pueden llegar a afectar la disponibilidad, integridad y confidencialidad de la información de una organización.

Mediante la Resolución Ministerial N° 004-2016-PCM, dispone el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC-27001:2014. Tecnologías de la Información. Técnicas de Seguridad. Sistema de Gestión de Seguridad de la Información. Requisitos. 2da Edición, en todas las entidades integrantes del Sistema Nacional de Informática.

Asimismo, en el Decreto Supremo N° 029-2021-PCM, reglamento de la Ley de Gobierno Digital, en su Título VII, Seguridad Digital, Capítulo IV, Sistema de Gestión de Seguridad de la Información, artículo109 establece 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 se encuentre, además de que las entidades de la Administración Pública implementan un SGSI en su institución, teniendo como alcance mínimo sus procesos misionales y aquellos que son relevantes para su operación*

El Instituto Nacional de Calidad - Inacal mediante Resolución Directoral N° 022-2022-INACAL/DN publicada el 29/12/2022, Artículo 1: aprueba la Norma Técnica Peruana 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. Mediante el Artículo 2 se deja sin efecto la Norma Técnica Peruana 27001:2014.

2. MARCO NORMATIVO

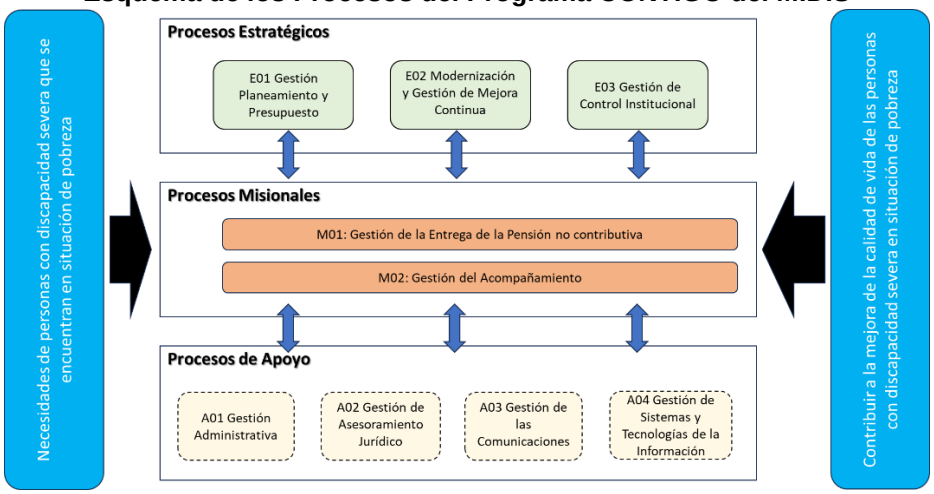
2.1. Ley N° 27658, Ley del Marco de Modernización de la Gestión del Estado.
2.2. Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública y sus modificatorias.
2.3. Ley N° 29733, Ley de Protección de Datos Personales y sus modificaciones.
2.4. Ley N° 30096, Ley de Delitos Informáticos y sus modificaciones.
2.5. Decreto de Urgencia N° 006-2020 que crea el Sistema Nacional de Transformación Digital.
2.6. Decreto de Urgencia N° 007-2020, que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
2.7. Decreto Supremo N° 109-2012-PCM, que aprueba la Estrategia para la Modernización de la Gestión Pública.
2.8. Decreto Supremo N° 003-2013-JUS, Reglamento de la Ley de Protección de Datos Personales.
2.9. Decreto Supremo Nº 004-2015-MIMP, que crea el Programa de entrega de la pensión no contributiva a personas con discapacidad severa en situación de pobreza y su modificatoria.
2.10. Decreto Supremo Nº 008-2017-MIDIS, que aprueba la transferencia del Programa de entrega de la pensión no contributiva a personas con discapacidad severa en situación de pobreza del Ministerio de la Mujer y Poblaciones Vulnerables (MIMP) al Ministerio de Desarrollo e Inclusión Social (MIDIS) y modifica su denominación a “Programa Nacional de entrega de la pensión no contributiva a personas con discapacidad severa en situación de pobreza - CONTIGO”.
2.11. Decreto Supremo Nº 021-2019-JUS, Texto Único Ordenado de la Ley de Transparencia y Acceso a la Información Pública. Decreto Supremo N° 029-2021-PCM, Reglamento del Decreto Legislativo n° 1412, Decreto Legislativo que aprueba la ley de Gobierno Digital.
2.12. Decreto Supremo n° 007-2024-JUS, Reglamento de la Ley de Transparencia y Acceso a la Información Pública
2.13. Resolución Ministerial N° 119-2018-PCM que crea el Comité de Gobierno Digital en cada entidad y su modificatoria

2.14. Resolución Ministerial N° 100-2023-MIDIS, que aprueba el Plan Estratégico Institucional 2021-2026 Ampliado del Ministerio de Desarrollo e Inclusión Social.
2.15. Resolución de Dirección Ejecutiva N° 131-2020-MIDIS/PNPDS-DE, conformar el comité de Gobierno Digital del Programa CONTIGO y sus modificaciones.
2.16. Resolución de Secretaría de Gobierno Digital N° 004-2018-PCM/SEGDI, que aprueba los "Lineamientos del Líder de Gobierno Digital" en la Administración Pública.
2.17. Resolución de Secretaría de Gobierno Digital N° 005-2018-PCM/SEGDI, que aprueba los Lineamientos para la Formulación del Plan de Gobierno Digital en la Administración Pública
2.18. Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD, que establece la implementación y mantenimiento del sistema de gestión de seguridad de la información en las entidades públicas.
2.19. Resolución de Dirección Ejecutiva N° 094-2020-MIDIS/PNPDS-DE, que oficializa la aprobación del Manual de Gestión de Procesos y procedimientos del proceso M1: Gestión de la Afiliación, Autorización de Cobro y Transferencia Monetaria y su modificatoria.

3. MAPA DE PROCESOS DE LA ENTIDAD

Se adjunta esquema de los procesos identificados en el Manual de Operaciones - MOP del Programa Nacional CONTIGO del Ministerio de Desarrollo e Inclusión Social - Midis.

Esquema de los Procesos del Programa CONTIGO del MIDIS



Fuente: Manual de Operaciones del Programa CONTIGO – Resolución Ministerial N° 012-2020/MIDIS

El proceso misional M01 Gestión de la Entrega de la Pensión no contributiva, cuenta con la aprobación del MAPRO M01, mediante Resolución de Dirección Ejecutiva N° D000140-2024-MIDIS/PNPDS-DE de fecha 30OCT2024.

4. ALCANCE DEL SGSI

4.1. AMBITO DE LA APLICACIÓN

El alcance de la implementación del SGSI se alinea a la Norma Técnica Peruana NTP-ISO/IEC 27001:2022 vigente y en el marco regulatorio de gobierno digital y transformación digital, seguridad de la información, seguridad digital y ciberseguridad.

El alcance de la implementación del SGSI comprenderá los activos de información del siguiente proceso misional:

M01 Gestión de la entrega de la pensión no contributiva

- M1.1 Gestión de la afiliación a la pensión no contributiva.
- M1.2 Gestión de la transferencia monetaria en cuenta
- M1.3 Gestión del cobro de la pensión no contributiva

4.2. ACTORES INVOLUCRADOS

a) Los servidores civiles encargados de la coordinación del Sistema de Gestión de Seguridad de la Información designados por las unidades orgánicas que se encuentran dentro del alcance del SGSI.
b) El personal de la Unidad de Tecnologías de la Información.
c) El personal de la Unidad de Operaciones y Transferencias.
d) Integrantes del comité de Gobierno y Transformación Digital.
e) Propietarios del riesgo.

5. DIAGNÓSTICO

El Programa CONTIGO actualmente no dispone de un Sistema de Gestión de Seguridad de la Información (SGSI), el cual es esencial para regular y controlar las políticas y procedimientos de seguridad de la información dentro de la institución. Aunque recientemente se ha adquirido equipos para la infraestructura tecnológica, como un servidor de datos, equipos de seguridad, almacenamiento y herramientas de monitoreo para el centro de datos, la ausencia del SGSI limita la capacidad de establecer un marco integral para la protección y gestión de los activos de información. Esto resalta la necesidad de implementar un SGSI que permita garantizar la alineación con mejores prácticas y estándares de seguridad.

El principal problema es que, a pesar de contar con equipamiento tecnológico, la falta de un SGSI debilita la capacidad para gestionar los riesgos de seguridad de forma sistemática y coherente. Esto deja a la infraestructura tecnológica expuesta a amenazas que podrían comprometer la confidencialidad, integridad y disponibilidad de la información. Además, la creciente dependencia de un entorno digital y la cantidad de usuarios que acceden a los sistemas, incrementa el riesgo de ciberataques, vulnerabilidades y errores humanos no gestionados de manera eficiente.

5.1. CONTEXTO DE LA ENTIDAD

La Unidad de Tecnologías de la Información enfrenta una limitación significativa de personal, operando actualmente con solo dos colaboradores contratados bajo el régimen CAS. Para cubrir esta brecha, se recurre a la contratación de personal mediante órdenes de servicio, lo que permite atender necesidades inmediatas. No obstante, resulta esencial contar con la asistencia técnica del Centro Nacional de Seguridad Digital (CNSD) de la Presidencia del Consejo de Ministros (PCM) y el respaldo estratégico de la Dirección Ejecutiva, a fin de fortalecer la capacidad operativa del área y garantizar el cumplimiento de los objetivos institucionales en materia de seguridad digital.

Por lo tanto, la implementación del SGSI permitirá proteger los activos de información y minimizar los riesgos, esto implica en mantener la continuidad de sus servicios y mejorar la confianza de las partes interesadas implementando controles organizacionales, de personas, físicos y tecnológicos que permitan mitigar los riesgos a un nivel aceptable.

6. MARCO ESTRATÉGICO

6.1. OBJETIVO ESTRATÉGICO INSTITUCIONAL / ACCIÓN ESTRATÉGICA INSTITUCIONAL

Los objetivos y acciones estratégicas del MIDIS, como entidad rectora, están establecidos en su Plan Estratégico Institucional (PEI). Este documento guía también a los programas sociales bajo su competencia, asegurando un enfoque integral y coordinado. A continuación, se detallan:

Objetivo Estratégico Institucional	
OEI.08. Fortalecer la gestión institucional bajo un enfoque de eficiencia	
Acción Estratégica Institucional	
AEI.08.02	Transformación Digital implementada en el MIDIS.

6.2. OBJETIVO GENERAL

- Preservar la confidencialidad, integridad y disponibilidad de la información de la entidad pública.
- Fortalecer la cultura de seguridad de la información en los servidores, funcionarios y colaboradores de la entidad pública.
- Asegurar el cumplimiento normativo en materia de seguridad y confianza digital.
- Gestionar de manera eficaz los riesgos, eventos e incidentes de seguridad de la información.

7. PROGRAMACIÓN DE ACTIVIDADES

Las actividades a realizar para la implementación del sistema de gestión de seguridad de la información - SGSI, se encuentra detallada en el numeral 12, Anexo 01 del presente documento.

Es importante señalar que, después de culminar con la implementación del sistema de seguridad de la información - SGSI, cada año se debe realizar como mínimo una auditoría interna, el cual se tendrá que realizar de acuerdo a lo planificado para luego realizar las acciones correctivas correspondientes a las no conformidades, de tal forma que, se cumpla con mejora continua del SGSI hasta el año 2027.

8. SEGUIMIENTO Y EVALUACIÓN

El Comité de Gobierno y Transformación Digital realizará el seguimiento y evaluación del Plan de Implementación del Sistema de Gestión de Seguridad de la Información del Proceso **M1: Gestión de la entrega de la pensión no contributiva.**

El Oficial de Seguridad y Confianza Digital es responsable de informar los avances de la implementación del sistema de gestión de seguridad de la información al Comité de Gobierno y Transformación Digital del Programa Nacional CONTIGO.

El Comité de Gobierno y Transformación Digital del Programa Nacional CONTIGO supervisa y evalúa el cumplimiento y estado de implementación del Sistema de Gestión de Seguridad de la Información – SGSI.

El proceso de seguimiento y evaluación de la implementación del SGSI en el Programa Nacional CONTIGO, se realiza en el marco de la Norma Técnica Peruana NTP ISO/IEC 27001:2022 y el Anexo “A” de la referida norma (controles de seguridad de la información).

9. ANEXOS

Anexo 01: Programación de actividades

Anexo 02: Términos y definiciones

Anexo 03: Recursos y presupuestos

Anexo 04: Riesgos y acciones de contingencia

ANEXO 01: PROGRAMACIÓN DE ACTIVIDADES

	Tareas / Actividades	2025											2026							RESPONSABLE
		2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	
ETAPA 1: INICIO																				
1	Aprobación del Plan de implementación del SGSI por el CGTD																			CGTD, DE
2	Análisis de brechas del SGSI, permite identificar las diferencias entre el estado actual de seguridad de la información y los requisitos establecidos por estándares en la ISO/IEC 27001.																			OSCD, UTI
ETAPA 2: PLANIFICACION DEL SGSI																				
3	Alcance del SGSI, se debe determinar los límites y la aplicabilidad del sistema de gestión de seguridad de la información.																			OSCD, CGTD
4	Documento de Contexto, se debe determinar los problemas externos e internos que sean relevantes para su propósito y que afecten su capacidad para lograr los resultados esperados																			OSCD, CGTD
5	Política de Seguridad de la Información ISO/IEC 27001:2022																			OSCD, CGTD
6	Asignar roles y responsabilidades para la gestión del SGSI, deben ser claramente definidos y asignados a los empleados para garantizar la adecuada gestión de los riesgos y la protección de la información.																			OSCD, CGTD
7	Programa de Sensibilización y capacitación con temas del Sistema de Gestión de Seguridad de la Información.																			OSCD, CGTD
8	Metodología de Gestión de Riesgos, permite identificar, analizar, evaluar y tratar los riesgos relacionados con la seguridad de la información.																			OSCD, CGTD
9	Manual del SGSI - procedimientos generales del SGSI, es un documento clave que describe los procedimientos generales y las prácticas que guiarán la implementación, operación y mantenimiento del SGSI dentro de una organización.																			OSCD, UTI
10	Inventario de Activos de Información, Consiste en la identificación, clasificación y evaluación de todos los activos de información que se utilizan en la organización, para asegurar que se gestionan adecuadamente y se protegen frente a riesgos.																			OSCD, UTI

	Tareas / Actividades	2025											2026							RESPONSABLE
		2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	
11	Matriz de análisis, evaluación y tratamiento de Riesgos, Su propósito es facilitar la identificación, evaluación y tratamiento de los riesgos que afectan a la seguridad de la información dentro de una organización, ayudando a priorizar las acciones a tomar en función del impacto y la probabilidad de ocurrencia de los riesgos.							■	■											OSCD, CGTD
12	Declaración de Aplicabilidad - SoA, debe identificar y justificar la implementación de los controles de seguridad que se aplican en su SGSI, basados en los riesgos identificados y el contexto específico de la organización.								■	■										OSCD, UTI
13	Aceptación de Riesgos, Este proceso implica reconocer que ciertos riesgos, después de ser evaluados y tratados, pueden ser aceptados por la organización debido a que sus impactos o probabilidades de ocurrencia son bajos, o porque los costos para mitigar esos riesgos exceden los beneficios de la mitigación.									■										OSCD, CGTD
ETAPA 3: IMPLEMENTACIÓN DEL SGSI																				
14	Seguimiento del Plan de Tratamiento de Riesgos, asegura que las acciones identificadas para mitigar, transferir, aceptar o evitar riesgos se implementen correctamente y dentro de los plazos establecidos.									■										OSCD, CGTD
15	Implementación de controles de seguridad, busca proteger la confidencialidad, integridad y disponibilidad de la información										■	■	■	■						OSCD, UTI
16	Seguimiento de la implementación del SGSI, es un proceso continuo que garantiza que las políticas, procedimientos, controles y objetivos del SGSI se lleven a cabo de manera eficaz, alineados con los requisitos de la norma ISO/IEC 27001:2022.													■						CGTD
17	Implementación del Programa de Sensibilización del SGSI, busca generar una cultura de seguridad entre los empleados y partes interesadas, garantizando que comprendan su rol en la protección de la información y apoyen los objetivos del SGSI.													■						CGTD

	Tareas / Actividades	2025											2026							RESPONSABLE
		2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	
ETAPA 4: MONITOREO Y REVISIÓN DEL SGSI																				
18	Monitoreo del SGSI, asegura que el sistema de gestión sea efectivo, se mantenga alineado con los objetivos de la organización y responda a los cambios en el entorno de riesgo																			CGTD, OSCD
19	Programa / Plan de Auditoría Interna, está diseñado para evaluar la eficacia del sistema, verificar el cumplimiento de los controles y garantizar la mejora continua.																			OSCD, UTI
20	Informe de Auditoría Interna presenta los hallazgos, análisis y conclusiones sobre el cumplimiento y la eficacia del SGSI frente a los requisitos de la norma ISO/IEC 27001:2022.																			CGTD, UTI
21	Seguimiento y revisión del SGSI, tiene como objetivo documentar el proceso de identificación, implementación y seguimiento de las medidas correctivas tomadas para resolver no conformidades o deficiencias en el Sistema de Gestión de Seguridad de la Información (SGSI), conforme a los requisitos de la norma ISO/IEC 27001:2022.																			CGTD
ETAPA 5: MANTENER Y MEJORAR EL SGSI																				
22	Informe de atención de Acciones Correctivas, Este informe describe las acciones tomadas para corregir no conformidades identificadas durante auditorías internas, evaluaciones de riesgos, o por otras fuentes dentro de la organización.																			CGTD
23	Informe final de cierre de la implementación, Este informe debe ser exhaustivo, reflejando las actividades realizadas, el cumplimiento de los requisitos de la norma, las mejoras alcanzadas, y la evaluación de la efectividad del sistema implementado.																			CGTD

Leyenda:

- DE: Dirección Ejecutiva
- CGTD: Comité de Gobierno y Transformación Digital.
- OSCD: Oficial de Seguridad y Confianza Digital

ANEXO 02: TERMINOS Y DEFINICIONES

- **Activo de Información**: Cualquier elemento físico, tecnológico o intangible que genera, almacena o procesa Información y tiene valor para la organización, como base de datos, archivos, programas, manuales, equipos de comunicaciones, la imagen de la entidad, la Información como activo corporativo, puede existir de muchas formas (impresa, almacenada electrónicamente, transmitida por medios electrónicos, mostrada en videos, suministrada en una conversación, conocimiento de las personas).
- **Amenazas:** Fuentes generadoras de eventos en las que se originan las pérdidas por riesgos de seguridad de la información.
- **Análisis de riesgo:** Método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias que, al evaluarse de manera objetiva, permite determinar la extensión en que se cumplen los criterios definidos para la auditoría interna.
- **Auditor en seguridad de la información**: Persona con la competencia para efectuar auditorías internas de seguridad de la información.
- **Comité de Gobierno y Transformación Digital**: Es el mecanismo de gobernanza a nivel institucional para el gobierno y transformación digital en las entidades de la ad-ministración pública, responsable de liderar y dirigir el proceso de transformación digital en la entidad.
- **Confidencialidad:** Garantizar que la información sea accesible únicamente para quienes tengan acceso autorizado.
- **Control:** Acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de la organización.
- **Ciberseguridad:** 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.
- **Declaración de aplicabilidad:** Documento que describe los objetivos de control y los controles pertinentes y aplicables para el sistema de gestión de seguridad de la información de la entidad.
- **Disponibilidad:** La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para el uso; la no disponibilidad de la información puede resultar en pérdidas financieras de imagen y/o credibilidad ante los clientes y/o ciudadanos.
- **Dueño del proceso**: Es quien tiene la responsabilidad y autoridad para participar en el proceso de gestión de riesgos de seguridad de la información.
- **Efectividad:** Medida de impacto de la gestión tanto en el logro de los resultados planificados, como en el manejo de los recursos utilizados y disponibles.
- **Eficacia:** Grado en que se realizan las actividades planificadas y se alcanzan los resultados planificados.
- **Estimación de riesgo:** Proceso de asignación de valores a la probabilidad e impacto de un riesgo.
- **Evento de seguridad de la información:** Presencia identificada de una condición de un bien o recurso (sistema, servicio, red, etc), asociada a una posible vulneración de la política de seguridad de la información.
- **Evidencia de auditoria:** Registro, declaración de hechos o cualquier otra información que son relevantes para los criterios de auditoría y que son verificables. La evidencia de la auditoria puede ser cuantitativa o cualitativa.
- **Gestión de riesgo:** Actividades coordinadas para dirigir y controlar los aspectos asociados al riesgo dentro de una organización.

- **Identificación del riesgo:** Proceso para encontrar, numerar y caracterizar los elementos de riesgo asociadas a la seguridad de la información.
- **Impacto:** se establece como la consecuencia directa o indirecta de la materialización de los escenarios de riesgo generando cambios adversos en los objetivos de la organización.
- **Incidente de seguridad de la información:** Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tiene una probabilidad significativa de comprometer las operaciones de la organización y amenazar la seguridad de la información.
- **Información:** Datos relacionados que tienen significado para la organización. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la organización y, en consecuencia, necesita una protección adecuada.
- **Integridad:** La información del Programa Nacional CONTIGO del Midis debe ser clara y completa y solo podrá ser modificada por las personas expresamente autorizadas para ello. La falta de integridad de la información puede exponer a la entidad a toma de decisiones incorrectas, lo cual puede ocasionar pérdida de imagen del Programa Nacional CONTIGO del Midis.
- **Probabilidad:** Es la posibilidad de que la amenaza aproveche la vulnerabilidad para materializar el riesgo.
- **Proceso:** Conjunto de actividades relacionadas mutuamente o que interactúan para generar valor y cuales transforman elementos de entrada en resultados.
- **Riesgo:** Consecuencias que pueden ser generadas por las amenazas asociadas a la seguridad de la Información en los activos del Programa Nacional CONTIGO del Midis.
- **Riesgo en seguridad de la Información:** Es la probabilidad de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando daño al Programa CONTIGO del MIDIS.
- **Riesgo residual:** Es el riesgo que permanece después que se han hecho todos los esfuerzos para identificar y eliminar el riesgo.
- **Seguridad de la información:** Preservación de la integridad, la confidencialidad, y la disponibilidad de la Información; además puede involucrar otras propiedades tales como autenticidad, trazabilidad, no repudio y fiabilidad. (Fuente: NTP ISO/IEC 270001:2014).
- **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
- **Tratamiento de la Información:** Desarrollo de las siguientes actividades sobre la Información, sin limitarse a ellas: creación, acceso, inclusión, exclusión, corrección, comunicación, divulgación, publicación, cesión, eliminación y certificación; por cualquier medio oral, digital y/o escrito, conocido o por conocer.
- **Tratamiento del riesgo:** Proceso de selección e implementación de medidas para modificar el riesgo.
- **Usuario:** Cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice Información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de Información del Programa Nacional CONTIGO del Midis, para propósitos propios de su labor y que tendrá el derecho manifiesto de uso dentro del inventario de información.
- **Vulnerabilidades:** Debilidad de un activo de información frente a una amenaza.
- **Conformidad:** Cumplimiento de un requisito.

ANEXO 03: RECURSOS Y PRESUPUESTOS

De acuerdo a lo indicado en el artículo 4 de la Resolución de Secretaría de Gobierno y Transformación Digital n° 003-2023-PCM/SGTD, los responsables de la gestión de la gestión de la seguridad digital institucional son:

- Titular de la Institución (4.1)
- Jefe(a) de Administración (4.2)
- Comité de Gobierno y Transformación Digital (4.3)
- Oficial de Seguridad y Confianza Digital (4.4)
- Equipo de respuestas ante incidentes de seguridad digital – CSIRT (4.5)
- Jefe(a) de Tecnologías de la Información (4.6)
- Jefe(a) de la Unidad de Planeamiento, Presupuesto y Modernización (4.7)
- Dueños de procesos y responsables de la unidad organizacional (4.8)

Asimismo, para la implementación y mantenimiento del SGSI en la entidad, se conformará un Equipo de Trabajo técnico multidisciplinario y un analista en seguridad de la información, el cual estará liderado por el Oficial de Seguridad y Confianza Digital.

La implementación del SGSI estará a cargo del personal y servicios considerados en el presupuesto de la Unidad de Tecnologías de la Información.

Después de implementado el SGSI en el Programa CONTIGO, debe realizarse como mínimo una vez al año el análisis de vulnerabilidades, según el Decreto Supremo N° 029-2021-PCM, Decreto Supremo que aprueba el Reglamento de la Ley de Gobierno Digital, Artículo 115.

El presupuesto para la ejecución del plan de implementación del Sistema de Gestión de Seguridad de la Información – SGSI, será con cargo al presupuesto asignado a la meta presupuestal 05: Unidad de Tecnologías de la Información, Acción Estratégica Institucional AEI 05.01: Soporte digital para la prestación de servicios implementado en el MIDIS.

ANEXO 04: RIESGOS Y ACCIONES DE CONTINGENCIA

a) LISTA DE RIESGOS IDENTIFICADOS

A continuación, se presentan la lista de riesgos identificados, que podrían alterar o retrasar los objetivos planteados en el presente Plan de Trabajo para la Implementación del SGSI.

CODIGO	RIESGOS
R001	Demoras entre el tránsito administrativos por excesiva burocracia.
R002	Resistencia al cambio tanto de los colaboradores como los responsables de los Órganos, Unidades Orgánicas y Programas.
R003	Delegación de todas las responsabilidades a áreas técnicas.
R004	No asumir que la seguridad de la información es inherente a los procesos de negocio.
R005	Alta tasa de inasistencia del personal a las capacitaciones, charlas o talleres.

b) ACCIONES DE CONTINGENCIA O MITIGACIÓN

A continuación, se listan las acciones correspondientes a realizar ante los riesgos identificados.

CODIGO	RIESGOS	ACCIONES DE CONTINGENCIA
R001	Demoras entre el tránsito administrativo por excesiva burocracia.	Evitar documentación que no aporte valor, realizar procedimientos trabajados en conjunto con quien lo realizará.
R002	Resistencia al cambio tanto de los colaboradores como los responsables de los Órganos, Unidades Orgánicas y Programas.	Identificar al personal clave del Programa CONTIGO con quien iniciar la concientización de Seguridad de la Información.
R003	Delegación de todas las responsabilidades a áreas técnicas.	Dar responsabilidad a la Alta Dirección para que se ejecute a nivel institucional
R004	No asumir que la seguridad de la información es inherente a los procesos de negocio.	Talleres de concientización de gestión de seguridad de la información en los procesos de la institución
R005	Inasistencia del personal a las capacitaciones, charlas o talleres	Envío de correo electrónico y/o avisos en el intranet con información de las capacitaciones, charlas y talleres