PLAN N° 002 -2024-PRONIS

PLAN DE IMPLEMENTACIÓN DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN DEL PROGRAMA NACIONAL DE INVERSIONES EN SALUD – PRONIS 2024 – 2025

ÍNDICE

PROGRAMA NACIONAL DE INVERSIONES EN SALUD – JEFE DE LA UNIDAD DE ADMINISTRACIÓN Y FINANZAS – PRONIS

PROGRAMA NACIONAL DE INVERSIONES EN SALUD – JEFE DE LA UNIDAD DE ASESORÍA JURÍDICA – PRONIS

PROGRAMA NACIONAL DE INVERSIONES EN SALUD – JEFE DE LA UNIDAD DE PLANEAMIENTO PRESUPUESTO Y MODERNIZACIÓN – PRONIS

1. PRESENTACIÓN

El presente documento describe en forma detallada el Plan de Sistema de Gestión de Seguridad de la Información (SGSI) del Programa Nacional de Inversiones en Salud – PRONIS, con el fin de preservar la confidencialidad, integridad y disponibilidad de esta, mediante la implementación de controles que permitan hacer frente a amenazas de ataque o intromisión, error, actos de la naturaleza (inundación, incendio, etc.) o vulnerabilidades inherentes a su uso, en cumplimiento de la Ley de Gobierno Digital y la Norma Técnica Peruana "NTP ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3a Edición".

El Programa Nacional de Inversiones en Salud – PRONIS, tiene como objeto formular, evaluar y ejecutar los proyectos de inversión mediana y alta complejidad de los órganos del Ministerio de Salud que tienen competencia sobre esa materia, considerando los enfoques de género, interculturalidad y derechos humanos. Asimismo, formula, evalúa y ejecuta proyectos de inversión en salud, bajo cualquier fuente de financiamiento, para todos los niveles de complejidad a nivel nacional, en el marco de convenios suscritos y conforme a la normatividad vigente. Gestiona y supervisa el cumplimiento de las obligaciones contractuales en el marco de los proyectos de inversión ejecutados bajo las modalidades de asociación publico privado y obras por impuestos, conforme a la normatividad vigente.

El PRONIS, gestiona, mantiene, monitorea, documenta y efectúa el mejoramiento continuo del SGSI a través de su Comité de Gobierno y Transformación Digital (CGTD) promueve el cumplimiento de normas técnicas, estándares internacionales y de las mejores prácticas de seguridad de la información, a fin de garantizar la confidencialidad, integridad y disponibilidad de la información.

Por otro lado, el artículo 3 de la Resolución Ministerial N° 166-2017-PCM que modifica la Resolución Ministerial N° 004-2016-PCM, dispone que las entidades deben asegurar la implementación del Sistema de Gestión de Seguridad de la Información, priorizando en el alcance los procesos misionales y aquellos que sean relevantes para su operatividad; el artículo 105 del Reglamento del Decreto Legislativo N° 1412 que aprueba la Ley de Gobierno Digital, dispone que las entidades públicas tienen como una de sus obligaciones en seguridad digital, el implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI), por lo cual dispuso implementar un Plan de Sistema de Gestión de Seguridad de la Información, basada en la Norma Técnica Peruana NTP ISO/IEC 27001:2022.

El Equipo de Trabajo de Tecnologías de la Información y Comunicación (ETTIC) del Programa Nacional de Inversiones en Salud – PRONIS, adopta medidas de identificar, analizar, evaluar y dar tratamiento a los riesgos de seguridad de la información según el alcance del Sistema de Gestión de Seguridad de la Información – SGSI, en cumplimiento con la normativa vigente para garantizar razonablemente el logro de los objetivos estratégicos y operativos de la Entidad.

2. BASE LEGAL

2.1. Ley N° 27269, Ley de Firmas y Certificados Digitales, y modificatoria.
2.2. Ley N° 27291, Ley que modifica el Código Civil permitiendo la utilización de los medios electrónicos para la comunicación de la manifestación de voluntad y la utilización de la firma electrónica.
2.3. Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado, y sus modificatorias.
2.4. Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública, y sus modificatorias.

2.5. Ley N° 28493, Ley que regula el uso del correo electrónico comercial no solicitado (SPAM) y modificatoria.
2.6. Ley N° 28530, Ley de promoción de acceso a internet para personas con discapacidad y de adecuación del espacio físico en cabinas públicas de internet, y modificatoria.
2.7. Ley N° 29158, Ley Orgánica del Poder Ejecutivo, y sus modificatorias.
2.8. Ley N° 29733, Ley de protección de datos personales, y sus modificatorias.
2.9. Ley N° 30096, Ley de Delitos Informáticos, y sus modificatorias.
2.10. Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital, y modificatoria.
2.11. Decreto Legislativo N° 1161, que aprueba la Ley de Organización y Funciones del Ministerio de Salud, y sus modificatorias.
2.12. Decreto Legislativo N° 1353, que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el Régimen de Protección de Datos Personales y la regulación de la gestión de intereses, y modificatoria.
2.13. Decreto de Urgencia N° 007-2020, que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, y modificatoria.
2.14. Decreto Supremo N° 003-2013-JUS, que aprueba el Reglamento de la Ley Nº 29733, Ley de Protección de Datos Personales.
2.15. Decreto Supremo N° 035-2014-SA, se crea el Programa Nacional de Inversiones en Salud, y modificatoria.
2.16. Decreto Supremo N° 010-2019-RE, que ratifica el "Convenio sobre la Ciberdelincuencia".
2.17. Decreto Supremo N° 021-2019-JUS, que aprueba el Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública, y modificatoria.
2.18. Decreto Supremo N° 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N°1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las Tecnologías y medios electrónicos en el procedimiento administrativo, y modificatoria.
2.19. Decreto Supremo N° 157-2021-PCM, que aprueba el Reglamento del Decreto de Urgencia Nº 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.
2.20. Decreto Supremo N° 103-2022-PCM, que aprueba la Política Nacional de Modernización de la Gestión Pública al 2030.
2.21. Resolución de Secretaria 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.
2.22. Resolución Ministerial N° 246-2007-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2a. Edición" en todas las entidades integrantes del Sistema Nacional de Informática.
2.23. Resolución Ministerial N° 119-2018-PCM, que dispone la creación de un Comité de Gobierno Digital en cada entidad de la Administración Pública, y su modificatoria.
2.24. Resolución Ministerial N° 1151-2018-MINSA, que aprueba el Manual de Operaciones del Programa Nacional de Inversiones en Salud-PRONIS, y su modificatoria
2.25. Resolución Ministerial N° 358-2023/MINSA, que aprueba el Plan Estratégico Institucional (PEI) 2019 – 2026 ampliado del Ministerio de Salud.
2.26. Resolución Directoral N° 019-2013-JUS/DGPDP, que aprueba la Directiva de Seguridad de la información administrada por los Bancos de Datos Personales.
2.27. Resolución Directoral N° 022-2022-INACAL/DN, que aprueba entre otros la Norma Técnica Peruana NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3a Edición. Reemplaza a la NTP-ISO/IEC 27001:2014.

2.28. Resolución de Coordinación General N° 004-2018-PRONIS-CG en el numeral 1.1 del artículo 1 aprueba la constitución del Equipo de Trabajo de Tecnologías de Información y Comunicación en la Unidad de Administración y Finanzas.

2.29. Resolución de Coordinación General N° 09-2020-PRONIS-CG, que aprueba la Directiva N° 001-2020-PRONIS denominada: "Disposiciones para la elaboración, aprobación y modificación de los documentos normativos de gestión interna del Programa Nacional de Inversiones en Salud.

2.30. Resolución de Coordinación General N° 01-2022-PRONIS-CG, que constituye el Comité de Gobierno Digital del Programa Nacional de Inversiones en Salud.

2.31. Resolución de Coordinación General N° 71-2023-PRONIS-CG, se designa al Oficial de Seguridad y Confianza Digital del Programa Nacional de Inversiones en Salud - PRONIS.

3. OBJETIVO DEL PLAN DE IMPLEMENTACIÓN

Establecer lineamientos para Implementar un Sistema de Gestión de Seguridad de la Información – SGSI, bajo los requisitos de la Norma Técnica Peruana NTP ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3a Edición.

4. RESULTADOS ESPERADOS

Identificar oportunamente las vulnerabilidades y amenazas que ponen en riesgo la confidencialidad, integridad y disponibilidad de la información en el PRONIS frente a amenazas, internas o externas, deliberadas o accidentales con el fin de mitigar los riesgos a través de controles de seguridad de la información.

5. ALCANCE

El Plan de implementación del Sistema de Gestión de Seguridad de la Información (SGSI) del Programa Nacional de Inversiones en Salud – PRONIS, es de aplicación obligatoria para todo el personal bajo las distintas modalidades de contratación (Cas, Locadores, Proveedores de Servicios), que se encuentren involucrados en los procesos de implementación del SGSI.

6. SIGLAS Y DEFINICIONES

6.1. Siglas y Acrónimos.

- **PRONIS:** Programa Nacional de Inversiones en Salud.
- **ETTIC:** Equipo de Trabajo de Tecnologías de Información y Comunicación.
- **POI:** Plan Operativo Institucional.
- **PEI:** Plan Estratégico Institucional.
- **OEI:** Objetivos Estratégicos Institucionales.
- **AEI:** Acción Estratégica Institucional.
- **SGTD:** Secretaría de Gobierno y Transformación Digital.
- **CGTD:** Comité de Gobierno y Transformación Digital.
- **OSCD:** Oficial de Seguridad y Confianza Digital.
- **NTP:** Norma Técnica Peruana.
- **SGSI:** Sistemas de Gestión de la Seguridad de la Información.

6.2. Definiciones.

6.2.1. Activos de Información: Es el bien o servicio tangible o intangible, que genera, procesa o almacena información, en el cual se le atribuye un grado de valor según su criticidad o asociación con los procesos misionales.

6.2.2. Amenaza: Es cualquier factor que tiene el potencial para explotar una debilidad y dar lugar a algún tipo de daño a la información o a la institución.

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

6.2.4. Control de acceso: Medios o mecanismo para garantizar que el acceso a los activos sea de manera autorizada y restringida, basado en los requerimientos de negocios y los requisitos de seguridad.

6.2.5. Comité de Gobierno y Transformación Digital (CGTD): Responsable de la gobernanza y uso estratégico de los datos de la entidad, estableciendo las políticas y directrices institucionales en la materia, en cumplimiento de los lineamientos y normas emitidas por la Secretaria de Gobierno y Transformación Digital; debiendo impulsar una cultura basada en datos e iniciativas que aseguren la calidad, uso adecuado e interoperabilidad de los datos.

El Comité de Gobierno y Transformación Digital es responsable de dirigir, mantener y supervisar el SGSI.

6.2.6. Evento: Un suceso puede ser interno o externo a la Entidad, que ocurre en un momento determinado y es originado por una causa especifica.

6.2.7. Incidente: Circunstancia o suceso que se presenta de manera inesperada y que puede afectar al desarrollo de una actividad, aunque no forme parte de él. En nuestro contexto, es una interrupción de las condiciones normales de operación en cualquier proceso informático en PRONIS.

6.2.8. Incidente de seguridad de la información: Evento no deseado que genera amenaza a la seguridad de la información y que tiene una probabilidad significativa de comprometer a la operatividad de la Entidad.

6.2.9. Información: Cualquier forma de registro de contenidos susceptibles a ser procesados, distribuidos y almacenados, pudiendo estar en formato electrónico, óptico, magnéticos u otro medio de almacenamiento.

6.2.10. Oficial de Seguridad y Confianza Digital: Es el rol responsable de coordinar la implementación y mantenimiento del SGSI en la entidad, atendiendo las normas en materia de seguridad digital, confianza digital y gobierno digital; y reporta al CGTD.

6.2.11. Riesgo: Es la posibilidad que ocurra un evento adverso que afecte el logro de los objetivos de la entidad / dependencia.

6.2.12. Seguridad de la información: Permite la definición, implementación y la gestión adecuada de la confidencialidad, integridad y disponibilidad de los activos de información independientemente del soporte que los contenga.

6.2.13. Sistema de Gestión de Seguridad de la Información: Es un componente del sistema de gestión de una organización, con base en un enfoque de riesgos, que tiene como función establecer, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. El SGSI 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.

6.2.14. Vulnerabilidad: Debilidad identificada sobre un activo y que puede ser aprovechado por una amenaza para causar una afectación sobre la confidencialidad, integridad o disponibilidad de dicho activo.

7. CONTEXTO DE LA ENTIDAD

El Programa Nacional de Inversiones en Salud – PRONIS fue creado mediante Decreto Supremo N° 035-2014-SA y su modificatoria, bajo el ámbito del Viceministerio de Prestaciones y Aseguramiento en Salud del Ministerio de Salud, con la finalidad de ampliar y mejorar la capacidad resolutiva de los establecimientos de salud y coadyuvar a cerrar las brechas en infraestructura y oferta de servicios para obtener las mejoras sanitaras, en cumplimiento de los lineamientos de la política nacional y sectorial.

PRONIS, tiene como objeto formular, evaluar y ejecutar los proyectos de inversión de mediana y alta complejidad de los órganos del Ministerio de Salud que tienen competencia sobre esa materia, considerando los enfoques de género, interculturalidad y derechos humanos. Asimismo, formula, evalúa y ejecuta proyectos de inversión en salud, bajo cualquier fuente de financiamiento, para todos los niveles de complejidad a nivel nacional, en el marco de los convenios suscritos y conforme a la normatividad vigente. Gestiona y supervisa el cumplimiento de las obligaciones contractuales en el marco de los proyectos de inversión ejecutados bajo las modalidades de asociación publico privado y obras por impuestos, conforme a la normatividad vigente.

Las funciones del PRONIS son reguladas de acuerdo a lo establecido en el Manual de Operaciones (MOP), aprobado con Resolución Ministerial N° 1151-2018/MINSA, modificada por Resolución Ministerial N° 1141-2019/MINSA, el cual detalla las funciones de los órganos de línea, de asesoramiento y de apoyo, así como la estructura orgánica del PRONIS.

7.1. Alineamiento con el Plan Estratégico Institucional / Plan Operativo Institucional.

El PRONIS por ser una Unidad Ejecutora del Ministerio de Salud (MINSA), utiliza el Plan Estratégico Institucional (PEI) del MINSA, como herramienta de gestión. Cabe indicar, que el PEI es un documento de gestión estratégico que articula el ejercicio de las funciones y competencias de los órganos y unidades ejecutoras del MINSA para la implementación de las políticas nacionales en el sector salud, con la finalidad de mejorar el estado de salud de la población.

En dicho marco, el Plan Estratégico Institucional (PEI) 2019 – 2026 Ampliado del Ministerio de Salud establece la declaración de política institucional, la misión, los objetivos y las acciones estratégicas institucionales, los respectivos indicadores y metas, la ruta estratégica y responsables, para el plazo de tres (03) años; concordantes con las prioridades y estrategias establecidas por la Alta Dirección del Ministerio de Salud, los objetivos estratégicos del Plan Estratégico Sectorial Multianual del MINSA, la Política General de Gobierno al 2026, el Decreto Legislativo que aprueba la Ley de Gobierno Digital y su Reglamento, y a nivel internacional con los objetivos de desarrollo sostenible (ODS)

El Plan Operativo Institucional (POI) comprende la programación multianual de las actividades operativas e inversiones necesarias para ejecutar las acciones estratégicas institucionales definidas en el PEI por un periodo no menor a tres años, respetando la vigencia del PEI y estableciendo los recursos financieros y las metas físicas mensuales para cada periodo anual, en relación con los logros esperados de los objetivos del PEI. Con la implementación del POI, la entidad busca reducir las brechas de atención en cuanto a cobertura, calidad y satisfacción de los usuarios de los bienes y servicios que entrega.

El POI multianual 2024-2026 del PRONIS se articula con el PEI del MINSA a través del cuarto (4) objetivo estratégico Institucional (OEI).

De lo expuesto, el Plan de Implementación del SGSI del PRONIS, se encuentra alineado con el PEI del MINSA y el POI del PRONIS de la siguiente manera:

Tabla N°01: PEI y POI en relación al Plan de Implementación del SGSI

Plan Estratégico Institucional (PEI) 2019 – 2026, ampliado – Ministerio de Salud.	**OEI.04** *"Fortalecer la rectoría y la gobernanza sobre el sistema de salud, y la gestión institucional; para el desempeño eficiente, ético e íntegro, en el marco de la modernización de la gestión pública".*
	AEI. 04.06 *"Planificación y Gestión Sectorial de Inversiones y Mantenimiento en Salud Eficiente".*
Plan Operativo Institucional del PRONIS 2024 (consistente con el PIA)	**Actividad Operativa AOI00165500031** *"Gestión de la Infraestructura Tecnológica y Redes de Comunicación del Centro de Datos".*

7.2. Alineamiento con la Ley Gobierno Digital y su Reglamento.

Implementar y mantener un Sistema de Gestión de Seguridad de la Información es una obligación mínima de una Entidad Pública; tal cual lo indica el literal a) del artículo 105 del Reglamento del DS N° 029-2021-PCM.

Asimismo, en la Ley de Gobierno Digital, el literal d) del artículo 32 indica que las Entidades de la Administración Pública, debe de establecer, mantener y documentar un SGSI.

Por lo tanto, PRONIS por ser una Programa adscrito al Ministerio de Salud, elabora lineamientos de implementación para el SGSI a través del Plan de SGSI; debido a que el Sistema de Gestión de Seguridad de la Información, comprende un conjunto de políticas, lineamientos, procedimientos, recursos y actividades asociadas, que nos permitirá proteger los activos de información, gestionar riesgos e incidentes de seguridad de la información y

seguridad digital, implementar medidas de ciberseguridad, y acciones de colaboración y cooperación.

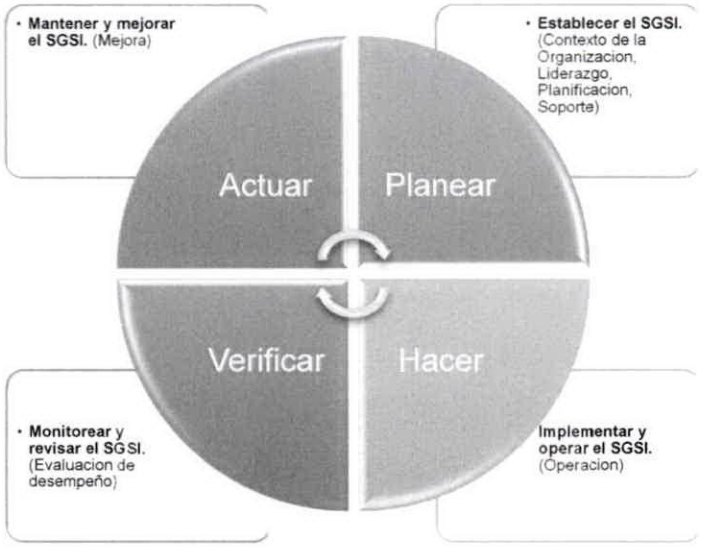
8. LINEAMIENTOS PARA LA IMPLEMENTACIÓN DEL SGSI

8.1. Metodología.

Para la implementación del SGSI, se usará la metodología denominada el ciclo de Deming o – Ciclo de Mejora Continua de Deming, donde se establece las fases de Planificar, Hacer, Verificar y Actuar del SGSI, dichas fases están relacionadas a la "NTP ISO/IEC 27001".

Esta metodología describe los cuatro pasos esenciales que se deben llevar a cabo de forma sistemática para lograr la mejora continua, entendiendo como tal, al mejoramiento continuo del SGSI como disminución de incidentes, aumento de la eficacia, solución de problemas, previsión y disminución de riesgos potenciales, entre otros.

Figura N° 01: Fases del ciclo Deming en el SGSI



Definiciones de las Fases:

- **Planear (PLAN):** Reconocer una oportunidad y planificar el cambio.
  El SGSI tiene que planificarse, de acuerdo al contexto de la entidad, las necesidades y expectativas de las partes interesadas. En esta etapa se planea el alcance, la identificación y definición de los procesos necesarios para conseguir los resultados, entre otros.
- **Hacer (DO):** Probar el cambio.
  Todo lo planeado en la etapa anterior se ejecuta de acuerdo al Plan, se recogen datos de manera correcta para que sean comparados con las metas propuestas.
- **Verificar (CHECK):** Revisar la prueba, analizar los resultados e identificar lo aprendido.
  En esta etapa se analiza todo lo que fue planeado con lo que se realizó. Es probable que todo lo que fue planeado no se haya alcanzado, pues durante la ejecución de las actividades, surgen adversidades que no fueron previstas en la planificación.
- **Actuar (ACT):** tomar acción basada en las lecciones aprendidas. Si el cambio fue exitoso, incorporar lo aprendido, de lo contrario intentar un plan diferente.

Esta fase se centra en lo que pudo incidir para no alcanzar la meta u objetivo propuesto, y definir acciones que permitan solucionar el problema asegurando que no se presente nuevamente. Para esto existen diversos métodos cuantitativos y cualitativos para solucionar problemas.

8.2. Alcance del SGSI

El Programa Nacional de Inversiones en Salud – PRONIS, implementará un sistema integrado de gestión según la Norma Técnica Peruana ISO/IEC 27001:2022, para lo cual se ha establecido el siguiente alcance:

Los sistemas de información que dan soporte a los Procesos de Gestión de Proyectos de Inversión en Salud, Gestión de Seguimiento y Supervisión al cumplimiento de los Contratos y/o Convenios, gestionado desde la sede central del PRONIS.

8.3. Organización para la Implementación del SGSI.

En concordancia con el marco normativo que establece la Implementación y Mantenimiento del SGSI en las Entidades Públicas, y en uso de las buenas prácticas de gestión se conforma el equipo de trabajo:

Tabla N°02: Organización para la Implementación del SGSI

N°	ROL	RESPONSABILIDAD
1	**Coordinador General.**	Máxima autoridad administrativa del PRONIS que proveerá los recursos necesarios para la ejecución del proyecto y aprobará las propuestas de documentos correspondientes al SGSI.
2	**Comité de Gobierno y Transformación Digital (CGTD).**	Es el responsable de la dirección, mantenimiento y supervisión estratégica de los recursos del SGSI, siendo uno de sus objetivos, el promover la implementación del SGSI en el PRONIS, a fin de fortalecer la seguridad e integridad de la información en el PRONIS. Asimismo, cumplirá las funciones que corresponda para este plan, según Resolución de Coordinación General N°01-2022-PRONIS-CG.
3	**Oficial de Seguridad y Confianza Digital (OSCD).**	Gestiona las acciones necesarias para la implementación del SGSI y realiza las coordinaciones con los equipos de trabajo respectivos para la adopción de las medidas aprobadas. Asimismo, cumplirá las funciones que corresponda para este plan, según Resolución de Coordinación General N°71-2023-PRONIS-CG.
4	**Equipo de Trabajo de Tecnologías de Información y Comunicación (ETTIC).**	Conformado por el Coordinador de ETTIC, especialistas y técnicos de los diferentes equipos internos de trabajo, quienes coordinaran con el Oficial de Seguridad y Confianza Digital a fin de implementar controles relacionados a la organización, personal, físico, tecnológicos, desarrollo y mantenimiento de sistemas, entre otros temas propios de su función.
5	**Equipo de Trabajo.**	Equipo conformado por los responsables de las Unidades Funcionales, quienes coordinaran y apoyaran en los diversos

N°	ROL	RESPONSABILIDAD
		aspectos de la implementación del SGSI, a fin de tomar decisiones sobre diversos temas que requieran un enfoque multidisciplinario y a la realización de tareas preestablecidas.

8.4. Matriz de Roles y Responsabilidades para la Formulación y Ejecución del Plan de Implementación del SGSI.

Tabla N° 03: Matriz de Roles y Responsabilidades

ACTIVIDADES	COORDINADOR GENERAL	CGTD	OSCD	ETTIC	EQUIPO DE TRABAJO
Elaboración y/o actualización de los documentos normativos exigidos por la NTP 27001:2022.	I	C, I	R	C, I	C , I
Gestión en la aprobación de los documentos del SGSI	A, R	C	R	-	-
Implementar los controles de Seguridad de la Información.	I	C, I	R, I	R	I
Gestión de Riesgos del SGSI.	I	C, I	R, I	R	R
Supervisión a la Implementación del SGSI.	I	R	R	-	-
Participación de las actividades del SGSI.	I	C, I	R	R	R

Responsable: R; Aprobar: A; Consultar: C; Informar: I.

8.5. Riesgos del Plan de Implementación del SGSI.

La implementación del SGSI implica un cambio de cultura organizacional en todos los niveles de la institución, por ende, es relevante el compromiso integral de todo el personal y de las unidades funcionales involucradas en el plan.

En ese sentido, se detallan algunos riesgos que se pueden presentar durante la implementación del SGSI, y cuáles serían sus acciones de mitigación para reducir el riesgo.

Tabla N° 04: Matriz de Riesgos del Plan

N°	RIESGO	ACCIONES DE MITIGACION
1	Falta de respaldo y compromiso de la Coordinación General y Comité de Gobierno y Transformación Digital	Hacer de conocimiento los reglamentos establecidos por la Secretaria de Gobierno y Transformación Digital. La Coordinación General dará continuidad a la ejecución de los planes aprobados.
2	Falta de compromiso del personal y de las Unidades del PRONIS implicadas en el alcance.	Se debe planificar y realizar actividades de concientización relacionados a seguridad de la información, a través de reuniones de socialización y comunicados por los diferentes medios de comunicación del Programa.

Nº	RIESGO	ACCIONES DE MITIGACION
3	Ausencia de los procesos mapeados de las Unidades del PRONIS comprendidas en el alcance del SGSI.	Se debe socializar con la Alta Dirección y unidades usuarias inmersas en el alcance del proyecto, a través de reuniones y comunicados por los diferentes medios de comunicación. Se debe realizar levantamiento de información de procesos de las unidades inmersas en el alcance del SGSI
4	Falta de capacitación del personal que implementa los controles (gestión de procesos, desarrollo seguro, seguridad informática, atención de servicios, entre otros.)	Se debe realizar reuniones de socialización con el personal de las unidades implicadas en el alcance del proyecto, haciendo hincapié en los beneficios de la implementación del proyecto, y en la obligatoriedad de la implementación por parte de la Secretaría de Gobierno Digital.

8.6. Acciones para la Implementación del SGSI

Para el inicio de la implementación del SGSI se requiere:

- Compromiso de la Coordinación General y el Comité de Gobierno y Transformación Digital.
- Análisis de brechas de seguridad de la información, con la finalidad de determinar la situación actual del PRONIS con respecto al cumplimiento de la NTP ISO/IEC 27001:2022.
- Identificación de procesos y procedimientos del ETTIC.
- Fortalecimiento de las capacidades del Oficial de Seguridad y Confianza Digital y el Equipo de Trabajo en las normas técnicas de ISO 27001 y sus derivados.

Durante la implementación del SGSI se debe realizar:

- Fortalecimiento de capacidades de los equipos de trabajo integrantes de la implementación de SGSI, en los temas: Fundamentos de Seguridad de la Información y Protección de Datos Personales.
- Acompañamiento a los equipos de trabajo en el proceso de implementación.

8.7. Documentos del SGSI

Durante la implementación del SGSI, se elaborará la siguiente información documentada, sin perjuicio de otros que consideren pertinentes:

- **Contexto de la Organización**

  Información documentada donde PRONIS determine las cuestiones externas e internas y las partes interesadas que son pertinentes para su propósito y que afectan su capacidad de lograr el (los) resultado(s) previsto de su SGSI.

- **Alcance del SGSI**

  Información documentada donde PRONIS determina los límites y la aplicabilidad del sistema de gestión de seguridad de la información para establecer su alcance.

- **Liderazgo y Compromiso**

Información documentada donde la Alta Dirección debe demostrar liderazgo y compromiso respecto del sistema de gestión de seguridad de la información.

- **Política de seguridad de la información.**

  Información documentada donde la Alta Dirección establece una política de seguridad de la información, el cual es apropiado al propósito del PRONIS, e incluye los objetivos del sistema de seguridad, los compromisos de satisfacer los requisitos aplicables a la seguridad de la información, así como los compromisos de mejora del sistema de seguridad de la información.

- **Roles, responsabilidades y autoridades organizacionales**

  Información documenta donde la Alta Dirección asigne las responsabilidades y roles para las autoridades pertinentes a la seguridad de la información.

- **Gestión de Riesgos de Seguridad de la Información.**

  Información documentada que describe los métodos y procedimientos que se deben emplear para identificar, analizar, evaluar y tratar los riesgos de seguridad de la información

- **Objetivos de Seguridad de la Información**

  Información documentada que establece los objetivos y su planificación de seguridad de la información, en los niveles y funciones pertinente.

- **Creación, actualización, control y distribución de documentos del SGSI.**

  Información documentada que establece reglas de redacción, aprobación, control, distribución y actualización de documentos.

- **Auditoría interna.**

  Información documentada que define la forma de realizar los programas de auditoría, la forma de realizar las auditorías, informe de resultados, entre otros.

- **Revisión por la dirección**

  Información documentada que define la forma que la Alta Dirección debe de revisar el SGSI de PRONIS a intervalos planificados para asegurar su idoneidad, adecuación y eficacia continua.

- **Mejora continua y acciones correctivas**

  Información documentada que defina las mejoras continuas y las acciones correctivas en el PRONIS.

- **Controles de Seguridad de la Información**

  Información documentada que detalla los controles de seguridad de la información listadas en el Anexo A de la Norma ISO/IEC 27001:2022.

La información documentada en mención, es requerida por la Norma Técnica - ISO/IEC 27001:2022, el cual se encuentra en el cronograma de actividades de este Plan.

8.8. Herramientas de Apoyo al SGSI.

Todos los documentos que se elaboren y/o actualicen se realizarán empleando herramientas ofimáticas, dado que no se cuenta con una aplicación que automatice el SGSI.

Para el resguardo de la información generada (contenedor de información) se utilizará un espacio de almacenamiento que será asignado por el ETTIC, por lo que el Oficial de Seguridad y Confianza Digital administrará la carpeta compartida (colaborativa) y brindará los accesos correspondientes en coordinación con el ETTIC, para todos los integrantes de la implementación del SGSI.

9. MAPA DE PROCESOS DE LA ENTIDAD

El Programa Nacional de Inversiones en Salud – PRONIS, cuenta con un Mapa de Procesos enfocado en la Política Nacional de la Gestión de Modernización y la Política Sectorial del Ministerio de Salud; el mismo que se encuentra articulado al proceso estratégico PE01- Gestión Estratégica, PE01.03 - Planeamiento de Programas de Inversión Pública del Sector y PE01.07 – Gestión de Proyectos de Inversión, que se encuentra en el Mapa de Procesos Institucional del Ministerio de Salud, aprobada con Resolución Ministerial N° 945-2016/MINSA.

El Mapa de Procesos del Programa Nacional de Inversiones en Salud – PRONIS comprende lo siguiente:

- Representación gráfica de los procesos del Programa Nacional de Inversiones en Salud, el cual se visualizan los macro procesos estratégicos, misionales y de soporte, así como su interrelación.
- Descripción del Mapa de Procesos, el cual definirá el detalle de cada macro proceso y servirá de macro referencia para su correspondiente desintegración a través de los Manuales de Procesos y Procedimientos.

El Mapa de Procesos del PRONIS, se detalla en el **Anexo N° 01** del presente Plan.

10. CRONOGRAMA DE ACTIVIDADES

Las actividades que se ejecutarán para la implementación del SGSI del PRONIS, se detallan en el **Anexo N° 02** del presente Plan.

11. PRESUPUESTO

El Plan de Implementación del SGSI del PRONIS, contiene actividades que serán desarrolladas por el personal del ETTIC de acuerdo con sus competencias.

De requerirse presupuesto para la ejecución de actividades del presente plan, se coordinará con la UPPM para la evaluación correspondiente.

12. SEGUIMIENTO Y EVALUACIÓN

La implementación del SGSI será monitoreada y evaluada por el Oficial de Seguridad y Confianza Digital a través del cumplimiento de los entregables definidos:

Tabla N°05: Entregables del Plan de Implementación del SGSI

Entregables	Requisitos de la NTP ISO/IEC 27001:2022	Descripción de los requisitos
Entregable N°1	4	Contexto de la Organización
Entregable N°2	5 y 6	Liderazgo y Planificación
Entregable N°3	7 y 8	Apoyo y Operación
Entregable N°4	9	Evaluación de Desempeño
Entregable N°5	10	Mejora

Estos entregables están relacionados a los hitos que están definidos en el cronograma del Plan de Implementación del SGSI.

La evaluación del Plan de Implementación de SGSI se basa en un indicador de cumplimiento por entregable; a continuación, se detalla los criterios de evaluación:

Tabla N°06: Criterios de Evaluación

Criterio de Cumplimiento		Criterio de Atraso	
Cumplimiento (C)	**Valor**	**Atraso (A)**	**Valor**
Cumplimiento	3	Con atraso	1
En Proceso	2	Sin atraso	2
Iniciando	1		
Sin iniciar	0		

El indicador de cumplimiento por entregable es: Cumplimiento x Atraso

Tabla N°07: Resultado de Evaluación

I = C x A		Con atraso	Sin atraso
		1	2
Cumplimiento	3	**3**	**6**
En Proceso	2	**2**	**4**
Iniciando	1	**1**	**2**
Sin iniciar	0	**0**	**0**

Los resultados del indicador y las acciones de control se detallan a continuación:

Tabla N°08: Resultado del Indicador de Cumplimiento por Entregable

Resultado del Indicador		Acciones de Control
3,4,6	**Aceptable**	No es necesario tomar acciones, ya que se está cumpliendo el plan de implementación del SGSI.

Resultado del Indicador		Acciones de Control
2	Aceptable Condicional	Si es necesario tomar acciones, ya que no se está cumpliendo el plan de implementación del SGSI de manera eficiente.
0,1	Inaceptable	Si es necesario tomar acciones, ya que se corre un alto riesgo de no cumplir con el plan de implementación del SGSI.

El Oficial de Seguridad y Confianza Digital realizará trimestralmente un informe sobre el monitoreo y evaluación del Plan de implementación del SGSI, el cual será reportado a Jefe/a de Administración y Finanzas; y este, a su vez informará semestralmente al/la Coordinador/a General sobre los avances y dificultades de la implementación del SGSI.

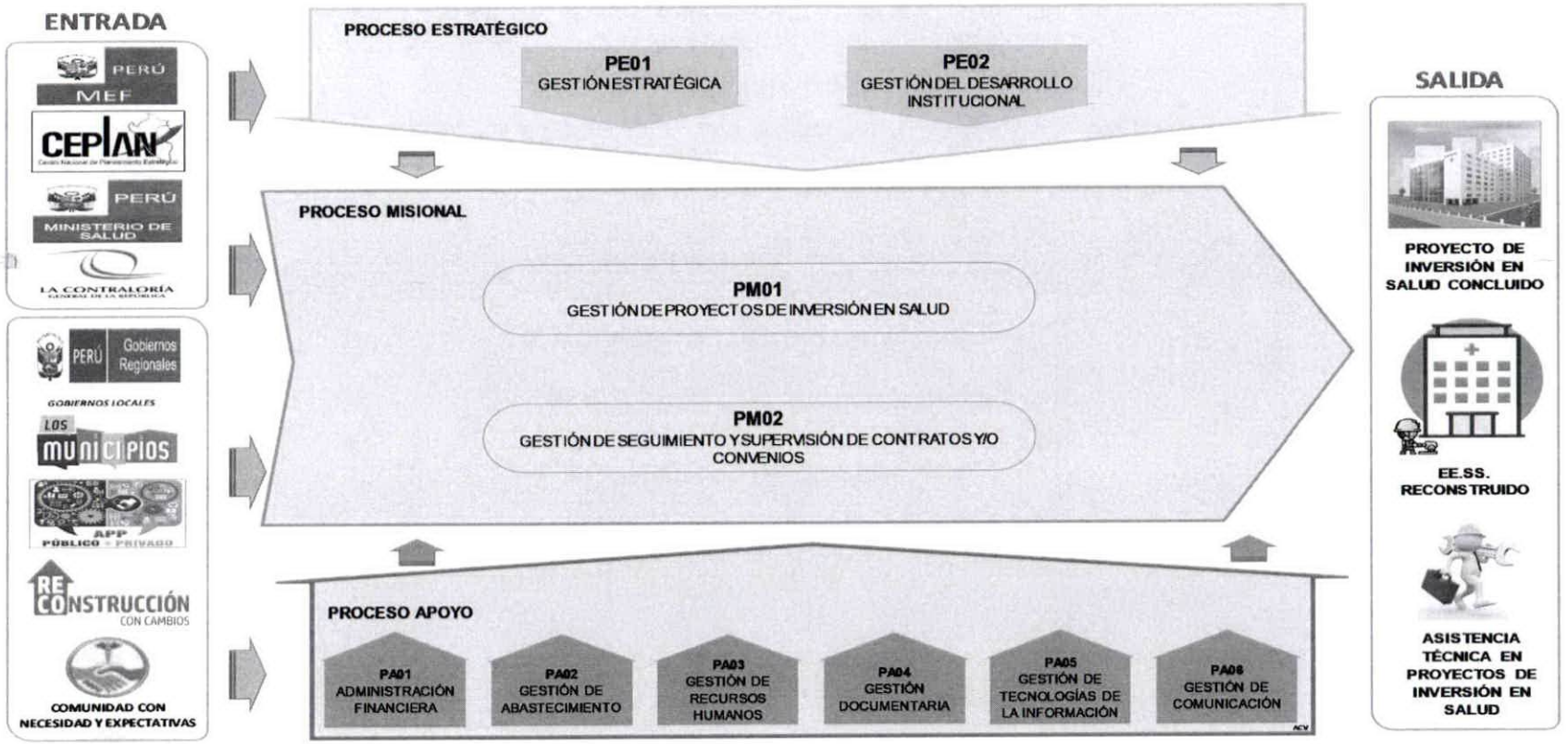
13. ANEXOS

13.1 Anexo N° 01: Mapa de Procesos del Programa Nacional de Inversiones en Salud – PRONIS.

13.2 Anexo N° 02: Cronograma de Actividades del Plan de Implementación del Sistema de Gestión de Seguridad de la Información periodo 2024 – 2025.

ANEXO N° 01

Mapa de Procesos del Programa Nacional de Inversiones en Salud – PRONIS



Fuente: Aprobado con Resolución Ministerial N°1141-2019/MINSA

ANEXO N° 02

Cronograma de Actividades del Plan de Implementación del Sistema de Gestión de Seguridad de la Información periodo 2024 – 2025

Entregable	Requisito de la NT-ISO/IEC 27001:2022	Actividades Principales [1]	AÑO 1				AÑO 2			
			TRIMESTRAL				TRIMESTRAL			
			I	II	III	IV	I	II	III	IV
Fase Previa										
–	–	Asegurar el compromiso de la Coordinación General y del Comité de Gobierno y Transformación Digital para la implementación del SGSI	x							
–	–	Elaborar el diagnóstico del SGSI en el PRONIS y reportar sus resultados	x							
–	–	Fortalecer las capacidades sobre temas relacionada a Seguridad de la Información, a los integrantes de la Implementación de SGSI	x							
–	–	Comunicar el inicio de la implementación del SGSI	x							
Fase I: Planear										
Entregable N°1	**4. Contexto de la Organización**	**a)** Comprender la Organización y su Contexto.		x						
		b) Comprender las Necesidades y Expectativas de las Partes Interesadas.		x						
		c) Determinar y documentar el alcance del sistema de gestión de seguridad de la información.		x						
		d) Establecer, implementar, mantener y mejorar continuamente el sistema de gestión de seguridad de la información, incluyendo los procesos necesarios y sus interacciones.		x						
Entregable N°2	**5. Liderazgo**	**a)** Establecer los compromisos para el SGSI			x					
		b) Documentar la Política de Seguridad de información			x					
		c) Asignar y comunicar los roles y responsabilidades de la seguridad de la información			x					
	Anexo A: Controles Organizacionales	Implementar 37 controles organizacionales (12 o 13 controles por cada trimestre).		x	x	x				
	6. Planificación	**a)** Determinar y documentar las acciones para abordar los riesgos y las oportunidades (metodología para la evaluación y tratamiento de riesgos)				x				
		b) Establecer y documentar los objetivos de seguridad de información y la planificación para conseguirlos				x				

[1] Las actividades principales esta relacionadas a cada requisito de la Norma Técnica Peruana ISO/IEC 27001:2022; por lo tanto, se tendrá que ejecutar tal como lo establece la normativa en mención.

Entregable	Requisito de la NT-ISO/IEC 27001:2022	Actividades Principales [1]	AÑO 1				AÑO 2			
			TRIMESTRAL				TRIMESTRAL			
			I	II	III	IV	I	II	III	IV
		c) Determinar y documentar la planificación de cambios en el SGSI				x				
	Anexo A: Controles de Personal	Implementar 8 controles de personal (4 controles por cada trimestre).			x	x				
Entregable N°3	7. Apoyo	a) Determinar y asignar recursos necesarios para el establecimiento, implementación, mantenimiento y mejora del SGSI					x			
		b) Determinar y asegurar las competencias necesarias de las personas que realizan trabajos que afectan al desempeño de la seguridad de la información.					x			
		c) Determinar las necesidad de comunicación internas y externas pertinente al SGSI					x			
		d) Elaborar y aprobar la información documentada para el SGSI					x			
		e) Determinar estrategias para asegurarse que el personal que trabaja bajo control de PRONIS tome conciencia de la implementación del SGSI, así como la información documentadas.					x			
	Anexo A: Controles Físicos	Implementar 14 controles físicos (4 o 5 controles por cada trimestre).					x	x	x	
Fase II: Hacer										
Entregable N°3	8. Operación	a) Planificar e implementar procesos del SGSI						x		
		b) Evaluar y documentar riesgos de seguridad de la información						x	x	
		c) Implementar el plan de Tratamiento de riesgos de seguridad de la información y documentar.						x	x	
	Anexo A: Controles Tecnológicos	Implementar 34 controles tecnológico (10 o 12 controles por cada trimestre).					x	x	x	
Fase III: Verificar										
Entregable N°4	9. Evaluación de Desempeño	a) Realizar el seguimiento, medición, análisis y evaluación al SGSI						x	x	
		b) Realizar a intervalos planificados la revisión por la dirección							x	
		c) Programar y ejecutar auditoria interna al SGSI								x
Fase IV: Actuar										
Entregable N°5	10. Mejora	a) Atender las no conformidades y acciones correctivas								x
		b) Mejorar continuamente el SGSI								x