

PI-SGSI/OSIN-0001-GCTIC

PLAN PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 2025



Firmado digitalmente por RIEGA RIEGA Larry Edwin Anibal FAU 20131257750 soft

Motivo: Doy V° B°

Fecha: 05.03.2025 17:19:28 -05:00

CONTENIDO

1. [INTRODUCCIÓN 3](#_bookmark0)
2. [OBJETIVOS DEL PLAN SGSI 4](#_bookmark1)
3. [MARCO LEGAL 4](#_bookmark2)
4. [TÉRMINOS Y DEFINICIONES 6](#_bookmark3)
5. [CONTEXTO DE LA ENTIDAD 8](#_bookmark4)
6. [MAPA DE PROCESOS DE LA ENTIDAD 9](#_bookmark5)
7. [ALCANCE DEL SGSI 11](#_bookmark6)
8. [CRONOGRAMA DE ACTIVIDADES 15](#_bookmark7)
9. [RECURSOS Y PRESUPUESTO 15](#_bookmark8)
10. [MONITOREO Y EVALUACIÓN 15](#_bookmark9)
11. [ANEXOS 15](#_bookmark10)

# INTRODUCCIÓN

Las entidades del Estado que administran sus datos como un activo estratégico están orientadas a garantizar que estos se recopilen, procesen, publiquen, almacenen y pongan a disposición durante el tiempo que sea necesario y cuando sea apropiado; considerando las necesidades de información de sus usuarios, beneficiarios y grupos de interés.

Asimismo, EsSalud reconoce la información como un activo de vital importancia para el correcto funcionamiento de los procesos de negocio; ergo, los criterios de integridad, confidencialidad y disponibilidad de la información son esenciales en su tratamiento y la implementación de medidas de seguridad de la información para proteger los precitados criterios.

Para gestionar adecuadamente la seguridad de la información institucional, es necesario establecer, implementar, operar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI).

Un Sistema de Gestión de la Seguridad de la Información (SGSI) consiste en el conjunto de políticas, procedimientos, directrices y actividades que son administrados colectivamente por una organización, que busca proteger los activos de información contra amenazas internas y externas, a través de implementación de controles técnicos, legales y organizativos, procurando garantizar la confidencialidad, integridad y disponibilidad de la información, y asegurar el cumplimiento de los requisitos legales y normativos, en materia de seguridad y confianza digital en el marco del Sistema Nacional de Transformación Digital

En ese sentido, EsSalud busca que la adopción de un Sistema de Gestión de Seguridad de la Información, (en adelante SGSI) integre, escale y actualice de acuerdo con las necesidades de ésta, los procesos, asegurando la confidencialidad, integridad y disponibilidad de los activos de información. Además, busca dar cumplimiento a las disposiciones de la Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD de la Presidencia de Consejo de Ministros, el cual establece que las entidades públicas deben formular y aprobar el Plan SGSI, y registrarlo en la Plataforma Facilita Perú para conocimiento y evaluación del Centro Nacional de Seguridad Digital. Asimismo, en su artículo 1 se precisa que las entidades públicas usan obligatoriamente la Norma Técnica Peruana NTP ISO/IEC 27001 vigente para el análisis, diseño, implementación, operación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información.

De lo precedente, se precisa que, con Resolución Ministerial N° 004-2016-PCM, se aprueba el uso de la Norma Técnica Peruana "ISO NTP/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2a. Edición", posteriormente con Resolución Directoral N° 022-2022-INACAL/DN se aprueba la 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)

Asimismo, en cumplimiento de la Gestión del Marco de Seguridad Digital del Estado Peruano1, el Seguro Social de Salud – EsSalud, debe establecer, mantener y documentar un SGSI, que garantice que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la Entidad, asegurando la confidencialidad, integridad y disponibilidad de los activos de información, minimizando los riesgos y vulnerabilidades del entorno y las tecnologías, promoviendo la continuidad y mejora en sus procesos críticos, adoptando como referencia el enfoque propuesto en la NTP-ISO/IEC 27001:2022.

1 Artículo N° 32 del Decreto Legislativo Nº 1412

Además, con Resolución de Presidencia Ejecutiva N° 1040-PE-ESSALUD-2023, se designa al Oficial de Seguridad y Confianza Digital de EsSalud. Asimismo, con Resolución de Gerencia General N° 1341-GG-ESSALUD-2021, se designa como Oficial de Datos Personales del Seguro Social de Salud al Jefe de la Oficina de Seguridad Informática de la Gerencia Central de Tecnologías de Información y Comunicaciones de EsSalud.

Así también, con Resolución de Presidencia Ejecutiva N° 986-PE-ESSALUD-2018 se crea el Comité de Gobierno Digital del Seguro Social de Salud – EsSalud y con Resolución de Presidencia Ejecutiva N°48-PE-ESSALUD-2023 se actualiza la denominación y conformación del Comité de Gobierno y Transformación Digital del Seguro Social de Salud – EsSalud (en adelante CTGD).

Cabe precisar que la implementación de un Sistema de Gestión de Seguridad de la Información, contribuye a implementar los controles de seguridad requeridos en la Ley 29733 - Ley de Protección de Datos Personales y su Reglamento.

En ese marco, se ha elaborado el Plan para la Implementación del Sistema de Gestión de Seguridad de la Información 2025, en adelante el Plan SGSI, el cual contiene la información requerida para la implementación y gestión eficiente del SGSI en la Entidad.

# OBJETIVOS DEL PLAN SGSI

Implementar el Sistema de Gestión de Seguridad de la Información en la Institución, con el objetivo de:

* Establecer etapas, actividades y recursos necesarios para implementar el Sistema de Gestión de Seguridad de la Información – SGSI.
* Definir los entregables necesarios en cada etapa de implementación del SGSI.
* Implementar el SGSI con un nivel de madurez que permita acceder a la certificación de la norma internacional ISO/IEC 27001:2022.

Los objetivos precedentes se alinean al Plan Estratégico Institucional 2025-2030 del Seguro Social de Salud- EsSalud2, considerando que se orientan a cumplir con el Objetivo Estratégico Institucional: OEI.06: Impulsar la transformación digital, la disrupción y las decisiones basadas en evidencia.

# MARCO LEGAL

* 1. Legislación Nacional
     1. Ley N° 27056: Ley de Creación del Seguro Social de Salud (EsSalud); la cual en su literal e) del artículo 2° establece como una de las funciones de EsSalud, formular y aprobar sus reglamentos internos, así como otras normas que le permitan ofrecer sus servicios de manera ética, eficiente y competitiva.
     2. Ley N° 27658: Ley Marco de Modernización de la Gestión del Estado.
     3. Ley N° 27815: Ley del Código de Ética de la Función Pública y sus modificatorias.
     4. Ley N° 29733: Ley de Protección de Datos Personales.
     5. Decreto Legislativo Nº 1444: que modifica la Ley Nº 30255 Ley de Contrataciones del Estado (vigente desde el 30 de enero de 2019). Derogado por el Literal c) de la Única Disposición Complementaria de la Ley Nº 32069, publicada el 24 de junio de 2024.
     6. Decreto Legislativo N°1412: que aprueba la Ley de Gobierno Digital.
     7. Decreto Supremo que aprueba el Texto Único Ordenado de la Ley Nº 27444 - Ley del Procedimiento Administrativo General Decreto Supremo Nº 004-2019-JUS.

2 Mediante Acuerdo N°019-12E-ESSALUD-2024 del Consejo Directivo de EsSalud, de Fecha 27.12.2024, se aprueba el Plan Estratégico Institucional 2025-2030 de EsSalud.

* + 1. Decreto Supremo N° 003-2013-JUS: que aprueba el Reglamento de la Ley N° 29733, Ley de Protección de Datos personales, y sus modificatorias.
    2. Decreto Supremo Nº 050-2018-PCM: Decreto que aprueba la definición de Seguridad Digital en el Ámbito Nacional.
    3. Decreto de Urgencia N° 006-2020: que crea el Sistema Nacional de Transformación Digital.
    4. Resolución de Secretaría de Gobierno Digital N° 004-2018-PCM/SEGDI, que aprueba los lineamientos del Líder de Gobierno Digital
    5. Resolución Ministerial N° 004-2016-PCM: que aprueba el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2a. Edición, en todas las entidades integrantes del Sistema Nacional de Informática.
    6. Resolución Directoral N° 022-2022- INACAL/DN Aprueban Normas Técnicas Peruanas sobre turismo, acuicultura y otros.
    7. Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD, establece la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las entidades públicas.
    8. Resolución Ministerial Nº119-2018-PCM, dispone la creación de un Comité de Gobierno Digital en cada entidad de la Administración Pública.
    9. Resolución Ministerial Nº 087-2019-PCM, aprueban disposiciones sobre la conformación y funciones del Comité de Gobierno Digital.
    10. Texto Actualizado y Concordado del Reglamento de Organización y Funciones del Seguro Social de Salud

– EsSalud, aprobado por Resolución de Presidencia Ejecutiva Nº 686-PE-ESSALUD-2024 y sus modificatorias.

* + 1. Resolución de Presidencia Ejecutiva N° 1040-PE-ESSALUD-2023, que designa a un Oficial de Seguridad y Confianza Digital de EsSalud.
    2. Resolución de Presidencia Ejecutiva N° 986-PE-ESSALUD-2018, que crea el Comité de Gobierno Digital del Seguro Social de Salud – EsSalud.
    3. Resolución de Gerencia General N° 1341-GG-ESSALUD-2021, que designa como Oficial de Datos Personales del Seguro Social de Salud (EsSalud) al Jefe (a) de la Oficina de Seguridad Informática de la Gerencia Central de Tecnologías de Información y Comunicaciones de EsSalud.
    4. Resolución de Presidencia Ejecutiva N° 48-PE-ESSALUD-2023, que deja sin efecto la Resolución de Presidencia Ejecutiva N°578-PE-ESSALUD-2019 y actualiza la denominación y la conformación del Comité de Gobierno y Transformación Digital del Seguro Social de Salud - EsSalud.
  1. Normas Técnicas Peruanas en materia de seguridad de la información.
     1. 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.
     2. NTP-ISO/IEC 27002:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información. 2ª Edición.
     3. NTP-ISO/IEC 27003:2019 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Orientación. 2ª Edición.
     4. NTP-ISO/IEC 27004:2018: Tecnología de la información. Técnicas de seguridad. Gestión de la seguridad de la información. Seguimiento, medición, análisis y evaluación. 2ª Edición.
     5. NTP-ISO/IEC 27005:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Orientación sobre la gestión de los riesgos de seguridad de la información. 3ª Edición.
     6. NTP ISO/IEC 27006:2009: Tecnología de la información. Técnicas de seguridad. Requisitos para los organismos que realizan auditorías y certificaciones de los sistemas de gestión de la seguridad de la información.
     7. NTP-ISO/IEC 27007:2019: Tecnología de la información. Técnicas de seguridad. Directrices para la auditoría de los sistemas de gestión de la seguridad de la información.
     8. ETP-ISO/IEC TS 27008:2021 Tecnología de la información. Técnicas de seguridad. Lineamientos para la evaluación de los controles de seguridad de la información. 1ª Edición.
     9. NTP-ISO 27799:2021 Informática en la salud. Gestión de la seguridad de la información en salud utilizando la ISO/IEC 27002. 2ª Edición.
     10. NTP-ISO/IEC 27701:2020 Técnicas de seguridad. Extensión de ISO/IEC 27001 e ISO/IEC 27002 para la gestión de la información sobre privacidad. Requisitos y directrices.
     11. NTP-ISO/IEC 27017:2018: Tecnología de la información. Técnicas de seguridad. Código de prácticas para controles de la seguridad de la información/en base a ISO/IEC 27002 para los servicios de nube.
     12. ETP-ISO/IEC TS 27022:2022 Tecnología de la información. Orientación sobre procesos del sistema de gestión de seguridad de la información. 1a Edición.
     13. NTP-ISO/IEC 29100:2021 Tecnología de la información. Técnicas de seguridad. Marco de referencia sobre privacidad. 1ª Edición.
     14. NTP-ISO/IEC 27014:2021 Seguridad de la información, ciberseguridad y protección de la privacidad. Gobernanza de seguridad de la información. 1ª Edición.
     15. NTP- ISO/IEC 31000:2018: Gestión del Riesgo. Directrices. 2a Edición.

# TÉRMINOS Y DEFINICIONES

* 1. Activo de Información: Cualquier dato, información o elemento que tiene valor para la Entidad (software, equipos de cómputo y telecomunicaciones, servicio de correo electrónico, servicio de internet, archivadores, entre otros) y que por lo tanto requiere protección.3
  2. Amenazas: Causa potencial de un incidente no deseado, que puede causar daños a un sistema u organización.4
  3. Análisis de riesgo: Proceso para comprender la naturaleza del riesgo y para determinar el nivel de riesgo.5
  4. Auditoría: Proceso sistemático, independiente y documentado para obtener evidencia de auditoría y evaluarla objetivamente para determinar en qué medida se cumplen los criterios de auditoría.6
  5. Control: Medida que está modificando el riesgo.7
  6. 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.8
  7. Confianza digital: Es el estado que emerge como resultado de cuán 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.9
  8. Conformidad: Cumplimiento de un requisito10.
  9. 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.

1. Numeral 7.1. de la Política Institucional de Seguridad de la Información de ESSALUD,
2. Numeral 3.74 Amenaza, de la NTP ISO/IEC 27000:2018
3. Numeral 3.63 análisis de riesgo, de la NTP ISO/IEC 27000:2018,
4. Numeral 3.3 Auditoria de la NTP ISO/IEC 27000:2018
5. Numeral 3.14 Control de la NTP ISO/IEC 27000:2018,
6. Directiva N° 001-2023-PCM/SGTD Directiva Perfil y responsabilidades del Oficial de Seguridad y Confianza Digital
7. Directiva N° 001-2023-PCM/SGTD Directiva Perfil y responsabilidades del Oficial de Seguridad y Confianza Digital
8. Numeral , 3.11 Conformidad de la NTP ISO/IEC 27000:2018
   1. Dueño del proceso: Es quien tiene la responsabilidad y autoridad para participar en el proceso de gestión de riesgos de seguridad de la información.
   2. Disponibilidad: Propiedad de ser accesible y utilizable bajo demanda por una entidad autorizada.11
   3. Efectividad: Medida en que se realizan las actividades planificadas y se logran los resultados previstos.12
   4. Eficacia: Grado en que se realizan las actividades planificadas y se alcanzan los resultados planificados.
   5. Estimación de riesgo: Proceso de asignación de valores a la probabilidad e impacto de un riesgo.
   6. Expectativas internas y externas: Son aquellos deseos de la parte interesada que no son comunicados de manera explícita pero que influyen en la percepción del desempeño del SGSI.
   7. Evento de seguridad de la información: Ocurrencia identificada de un estado del sistema, servicio o red que indica una posible violación de la política de seguridad de la información o falla de controles, o una situación previamente desconocida que puede ser relevante para la seguridad.13
   8. Evidencia de auditoría: Registros, declaraciones de hechos u otra información que sean pertinentes para los criterios de auditoría y verificables.14
   9. Gestión de riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo15.
   10. Identificación del riesgo: Proceso de encontrar, reconocer y describir riesgos.16
   11. Incidente de seguridad de la información: Un evento o una serie de eventos de seguridad de la información, no deseados o inesperados, que tienen una probabilidad significativa de comprometer los procesos, operaciones o la prestación de servicios de la entidad y de amenazar la seguridad de la información de la entidad pública17
   12. 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.
   13. Incidente de seguridad de la información: Eventos de seguridad de la información únicos o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información18.
   14. 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.
   15. Integridad: Propiedad de exactitud e integridad.19
   16. Partes Interesadas: Todos los clientes, empleados, socios, propietarios, proveedores, sindicatos, organismos reguladores; o incluso grupos de ciudadanos que de una forma u otra pueden verse afectadas por la actividad de la entidad o cuyas decisiones pueden afectar el sistema de gestión.
9. Numeral 3.7 Disponibilidad de la NTP ISO/IEC 27000:2018,

12Numeral 3.20 Efectividad NTP ISO/IEC 27000:2018, 3.20 Efectividad

1. Numeral 3.30 Evento de seguridad de la información de la NTP ISO/IEC 27000:2018.
2. Numeral 3.13.8 Evidencia de auditoría de la NTP ISO/IEC 9000:2015,
3. Numeral 3.69 Gestión de riesgo de la NTP ISO/IEC 27000:2018,
4. Numeral 3.68 Identificación de riesgos de la NTP ISO/IEC 27000:2018,
5. Directiva N°001-2023-PCM/SGTD Directiva Perfil y responsabilidades del Oficial de Seguridad y Confianza Digital
6. Numeral 3.31 Incidente de seguridad de la información NTP ISO/IEC 27000:2018,
7. Numeral 3.36 Integridad de la NTP ISO/IEC 27000:2018,
   1. Proceso: Conjunto de actividades interrelacionadas o interactivas que transforman las entradas en salidas.20
   2. Propietario de información: Los propietarios de la información son los titulares de los órganos Centrales y Desconcentrados del Seguro Social de Salud-EsSalud, y que tienen la responsabilidad de definir el tratamiento y los niveles de seguridad que se implementaran para el uso de la información que corresponde al ámbito de su competencia.21
   3. Responsabilidades: Compromisos u obligaciones del personal o grupo de trabajo.
   4. Riesgo: Combinación de la probabilidad de ocurrencia de un evento y sus consecuencias.22
   5. Riesgos de seguridad de la información: Efecto de la incertidumbre sobre los objetivos de seguridad de la información de la entidad pública.23
   6. Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información24.
   7. Sistema de Gestión de Seguridad de la Información: Es un componente del sistema de gestión de una entidad, 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 sistema de seguridad de la información está conformado por políticas, procedimientos, directrices, recursos y actividades asociadas, gestionadas por la entidad, en búsqueda de la protección de sus activos de información.25
   8. Tratamiento de riesgos: Proceso para modificar el riesgo.26
   9. Usuario: Personas que utilizan o tienen acceso a la información por medios automatizados o manuales. Los usuarios son responsables de conocer y cumplir las políticas, procedimientos y normas establecidas por la Entidad.27
   10. Vulnerabilidades: Debilidad de un activo o control que puede ser explotada por una o más amenazas.28.

# CONTEXTO DE LA ENTIDAD

El Plan Estratégico Institucional (PEI) 2025-2030 del Seguro Social de Salud – EsSalud es el principal documento estratégico de la organización, representando el direccionamiento estratégico y las principales acciones que orientan el proceso de creación de valor en la institución, posibilitando su transformación y la mejora de la calidad de los servicios que brinda a sus asegurados.

1. Numeral 3.54 Proceso de la NTP ISO/IEC 27000:2018
2. Política Institucional de Seguridad de la Información de EsSalud.
3. Política Institucional de Seguridad de la Información de EsSalud.
4. Directiva N° 001-2023-PCM/SGTD Directiva Perfil y responsabilidades del Oficial de Seguridad y Confianza Digital
5. NTP ISO/IEC 27000:2018, 3.28 Seguridad de la Información
6. Política Institucional de Seguridad de la Información de EsSalud.
7. Numeral 3.72 Tratamiento de riesgos de la NTP ISO/IEC 27000:2018,
8. Política Institucional de Seguridad de la Información de EsSalud.
9. Política Institucional de Seguridad de la Información de EsSalud.

|  |  |
| --- | --- |
| Objetivo Estratégico Institucional | Acciones Estratégicas Institucionales |
| Objetivo Estratégico Institucional 6 (OEI 6) Impulsar la transformación digital, la disrupción y las decisiones basadas en evidencia. | AEI 6.2: Ciberseguridad implementada en los sistemas de información de EsSalud. |

En esta línea, para la implementación de controles de ciberseguridad que busca proteger de los Sistemas administrativos y asistenciales a nivel institucional, se debe implementar el Sistema de Gestión de Seguridad de la Información (SGSI) bajo la norma NTP ISO/IEC 27001:2022, estándar internacional que establece los requisitos para la gestión de la seguridad de la información en una organización. Asimismo, para la implementación de los controles de seguridad se tomará en cuenta la norma NTP ISO/IEC 27002:2022: Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de Seguridad de la Información. 2 a edición.

* 1. Análisis situacional de la seguridad de la información en EsSalud

Actualmente EsSalud, busca implementar un Sistema de Gestión de Seguridad de la Información y dar cumplimiento a la Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023- PCM/SGTD, el cual dispone que las entidades públicas usan obligatoriamente la Norma Técnica Peruana NTP ISO/IEC 27001 vigente, para el análisis, diseño, implementación, operación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información.

* 1. Comprender las necesidades y expectativas de las partes interesadas

EsSalud deberá determinar las partes interesadas relevantes para el Sistema de Gestión de Seguridad de la Información (SGSI) y sus requisitos frente a la seguridad de la información.

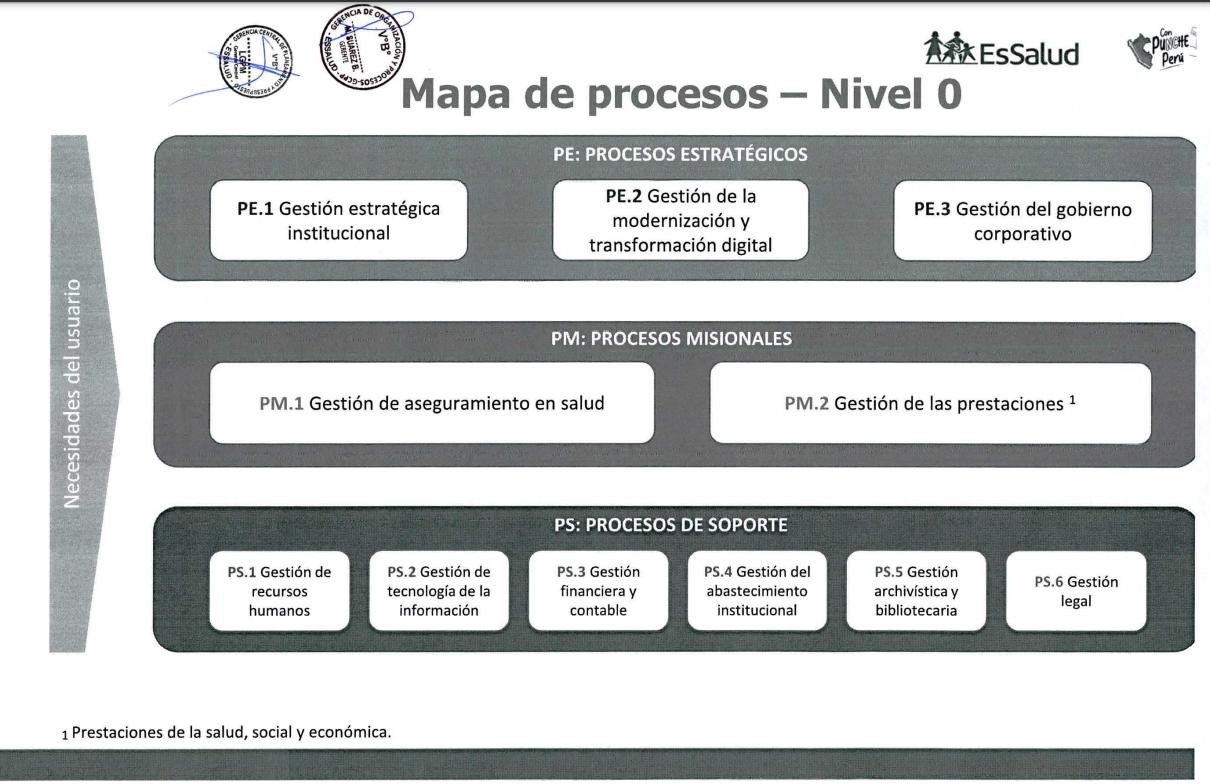
# MAPA DE PROCESOS DE LA ENTIDAD

* 1. Mapa de procesos de EsSalud

Con el fin de identificar el o los procesos a implementar en el Sistema de Gestión de Seguridad de la Información (SGSI), es necesario contemplar a través de una representación gráfica la secuencia e interacción de los diferentes procesos que tienen lugar en la Entidad.

Por consiguiente, a continuación, se muestra los Macroprocesos estratégicos, misionales y de soporte, (ver figura N°1)

*Figura N° 1*: Mapa de procesos -Nivel O EsSalud.



*Fuente: Resolución de Gerencia General Nº 500-GG-ESSALUD-2024*

* 1. PM: Procesos Misionales

Son los que se derivan directamente de la misión de EsSalud, impactan directamente sobre la satisfacción de las necesidades y expectativas de los asegurados, sus derechos habientes y otros clientes; o cualquier aspecto de la misión institucional, referidos principalmente a la gestión del aseguramiento/financiamiento y a la prestación de servicios de salud, económicas y sociales29 (ver cuadro N° 1).

*Cuadro Nº 1:* Procesos Misionales de EsSalud

|  |  |  |
| --- | --- | --- |
| Identificador | Nombre del Macroproceso | Descripción |
| PM. 1 Gestión de aseguramiento en salud | Nombre | Gestión de aseguramiento en salud |
| Código | PM.1 |
| Tipo de proceso | Operativo |
| Objetivo | Asegurar el derecho de toda persona a la seguridad social en salud mediante la recepción, captación y/o gestión de los recursos destinados a la cobertura de las atenciones de salud o cobertura de riesgos de salud. |
| Dueño del | Gerencia Central de Seguros y Prestaciones Económicas (GCSPE), Gerencia |

29 Manual de procesos y procedimientos para la formulación y seguimiento del plan de gobierno digital de EsSalud-2020

|  |  |  |
| --- | --- | --- |
|  | Proceso | Central de Operaciones (GCOP), Gerencia central de Gestión Financiera (GCGF) y Gerencia Central de Atención al asegurado (GCAA) |
| Alcance | Gerencia Central de Seguros y Prestaciones Económicas (GCSPE), Oficina de Seguros y Prestaciones Económicas (OSPE), Gerencia Central de Operaciones (GCOP), Gerencia Central de Atención al asegurado (GCAA), Gerencia central de Gestión Financiera (GCGF), Oficina de Relaciones Institucionales (ORI), Órganos desconcentrados, IPRESS propias. IPRESS tercera. |
| PM.2 Gestión de las prestaciones | Nombre | Gestión de las prestaciones |
| Código | PM.2 |
| Tipo de proceso | Operativo |
| Objetivo | Planificar, programar, operativizar y controlar los servicios de prestación de salud en los diferentes niveles de atención y tipo de complejidad, con el fin de satisfacer la demanda de la población asegurada . |
| Dueño del Proceso | Gerencia Central de Prestaciones de salud (GCPS), Gerencia Central de Seguros y Prestaciones Económicas (GCSPE), Gerencia Central de la Persona adulta mayor y Persona con Discapacidad (GCPAMyPCD) y Gerencia Central de Operaciones (GCOP) |
| Alcance | Gerencia Central de Prestaciones de salud (GCPS), Gerencia Central de Seguros y Prestaciones Económicas (GCSPE), Gerencia Central de la Persona adulta mayor y Persona con Discapacidad (GCPAMyPCD), Gerencia Central de Operaciones (GCOP), Oficina de Relaciones Institucionales (ORI), Oficina de Seguros y Prestaciones Económicas (OSPE), Órganos. unidades Orgánicas (O/UO), Órganos Desconcentrados (OODD) y Órganos Prestadores Nacionales (OPN). |

Se precisa que la Gerencia Central de Planeamiento y Presupuesto, se encuentra realizando un mapeo de procesos en las diferentes unidades orgánicas, de lo cual se analizará la inclusión de los nuevos procesos o sus actualizaciones en el alcance del SGSI, después de su aprobación.

# ALCANCE DEL SGSI

Para la implementación del SGSI, se establece como estrategia la implementación por etapas, según lo descrito en el numeral 7.1. permitiendo la implementación, en primera instancia30, de los procesos que conlleven al cumplimiento de la misión institucional, en este caso, los procesos misionales de EsSalud.

En ese sentido, el alcance del SGSI de EsSalud contempla el siguiente proceso misional: Proceso PM.1.6 Gestión de Asegurados del PM. 1 Gestión de Aseguramiento en Salud, esto en cumplimiento a la Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD que en su numeral 1.1 señala que: “Las entidades públicas usan obligatoriamente la Norma Técnica Peruana NTP ISO/IEC 27001 vigente para el análisis, diseño, implementación, operación, mantenimiento y mejora continua del Sistema de Gestión de

30 Posteriormente podrá implementarse otros procesos de EsSalud.

Seguridad de la Información. Asimismo, aseguran que el SGSI establezca como alcance mínimo a los procesos misionales y aquellos relevantes para la operación y funcionamiento de la entidad pública”

El alcance se ha determinado considerando que el precitado proceso permite atender los reclamos, requerimientos y sugerencias canalizados por los asegurados en las plataformas de atención presencial y medios no presenciales, así como la supervisión de la atención del asegurado y la medición de su satisfacción.

Las Unidades orgánicas comprendidas dentro del alcance del SGSI son:

* GERENCIA CENTRAL DE SEGUROS Y PRESTACIONES ECONÓMICAS (GCSPE)
* OFICINA DE SEGUROS Y PRESTACIONES ECONÓMICAS (OSPE)
* GERENCIA CENTRAL DE OPERACIONES (GCOP)
* GERENCIA CENTRAL DE ATENCIÓN AL ASEGURADO (GCAA)
* GERENCIA CENTRAL DE GESTIÓN FINANCIERA (GCGF)
* OFICINA DE RELACIONES INSTITUCIONALES (ORI)
* IPRESS propias.
* IPRESS tercera.

EsSalud deberá establecer, documentar, implementar, mantener y efectuar la mejora continua del SGSI, utilizando como estrategia la metodología del ciclo de Deming PHVA31 y acorde a los establecido en la NTP- ISO/IEC 27001:2022.

**Planear**

**Hacer**

**Verificar**

**Actuar**

* + Contexto de la organización
  + Liderazgo
  + Planificación
  + Soporte
  + Operación  Evaluación del

desempeño

* + Mejoras

*Gráfico N° 1*: Ciclo Deming – PHVA

Con el fin de mantener ordenado el proyecto de implementación del SGSI, para el presente Plan SGSI se deberá considerar la estructura de la NTP-ISO/IEC 27001:2022 dentro de las siguientes etapas.

* 1. Etapas de Plan SGSI
     1. Etapa 0: Inicial

Permitirá que el CTGD de EsSalud pueda disponer la participación de los órganos y unidades orgánicas para efectuar la implementación del SGSI.

* + 1. Etapa 1: Planificación del SGSI

En esta etapa se efectuará la identificación de activos de información, seguido de un proceso de gestión de riesgos en base a la normativa Institucional y procedimiento vigente, en donde se realizaran tratamiento a los riesgos identificados de nivel muy alto, alto y medio, y se establecerán las políticas,

31 El ciclo PHVA (Planear-Hacer-Verificar-Actuar), también conocido como Ciclo de Deming, es una herramienta gerencial utilizada en la gestión de los sistemas de calidad, que impulsa el mejoramiento continuo de procesos.

objetivos, procesos y procedimientos del SGSI relevantes para la atención de los riesgos, la implementación de los requisitos exigidos por la NTP ISO/IEC 27001:2022 y para mejorar la seguridad de la información, para la identificación de controles aplicables se realiza a través del documento de aplicabilidad.

* + 1. Etapa 2: Implementación del SGSI

Se realiza la implementación (aplicación) de la política, controles, procesos y procedimientos SGSI. Esta etapa también es conocida como la operación de lo definido en la etapa de planificación del SGSI.

* + 1. Etapa 3: Monitoreo y Revisión del SGSI

Se evaluará, donde sea aplicable, el desempeño del SGSI en comparación con la NTP ISO/IEC 27001:2022. Además, se efectuará la revisión del cumplimiento de la política, objetivos y controles de seguridad de la información. Los resultados de esta medición del desempeño son reportados al CGTD.

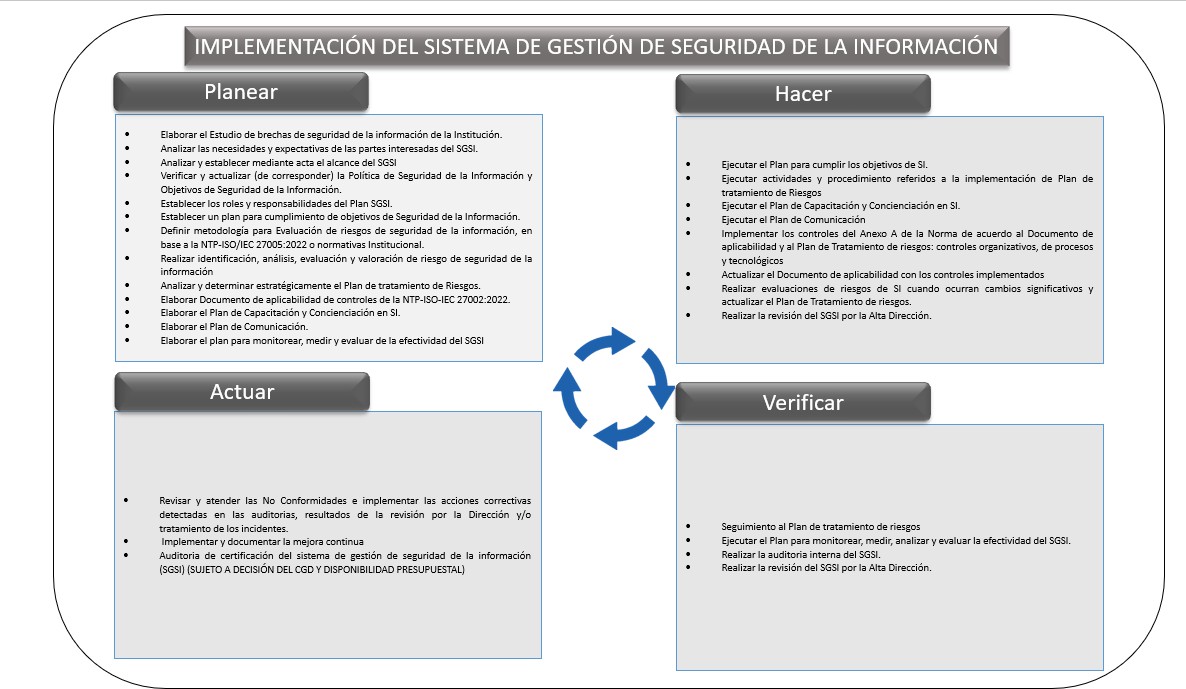
* + 1. Etapa 4: Mantener y Mejorar el SGSI

Tomar acciones correctivas basadas en los resultados de la auditoría interna SGSI, la revisión del CGTD, la revisión a la implementación de los controles de seguridad, los resultados de la efectividad en la atención de los riesgos, eventos e incidentes de seguridad u otra información relevante, para lograr el mejoramiento continuo del SGSI. Terminada la etapa 4 se podrá realizar la auditoría de certificación del SGSI mediante un servicio contratado. Cada etapa de la implementación del SGSI se realizará siguiendo el Ciclo de Mejora Continua (PHVA – Planear / Hacer/Verificar/Actuar).

En esta etapa también se realizará la auditoría interna y la revisión del SGSI por el CGTD



PI-SGSI/OSIN-0001-GCTIC



# CRONOGRAMA DE ACTIVIDADES

PI-SGSI/OSIN-0001-GCTIC

Para la implementación del Sistema de Gestión de Seguridad de la información se presenta el cronograma de actividades (ver Anexo N° 1), donde se establece un periodo de 8 meses (ejercicio 2025). Debe considerarse que este periodo pudiera variar por actividades no previstas en el cronograma, información no disponible según lo programado o evento no previsto.

# RECURSOS Y PRESUPUESTO

Para la implementación del presente Plan SGSI se cuenta con la Previsión Presupuestal N° 2024085783-2025, en la que se precisa que para la implementación del Sistema de Gestión de Seguridad de Información – SGSI, corresponde el monto aproximado de S/ 317,000.00.

# MONITOREO Y EVALUACIÓN

El Seguro Social de Salud, a través del Oficial de Seguridad y Confianza Digital, monitorea, mide, analiza y evalúa de forma progresiva el SGSI, de conformidad con lo establecido en la 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 y la NTP-ISO/IEC 27002:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información. 2ª Edición

En esta etapa, se debe considerar lo siguiente:

* 1. El Oficial de Seguridad y Confianza Digital, una vez aprobado el presente Plan, formulará un informe trimestral indicando el avance de la implementación del SGSI al Líder del Comité de Gobierno y Transformación Digital, quien a su vez dará cuenta del estado de avance de la implementación del SGSI a la Gerencia General.
  2. El Comité de Gobierno y Transformación Digital de EsSalud, una vez finalizada la implementación del SGSI, informará a través de la Presidencia Ejecutiva, de todo lo actuado a la Secretaría de Gobierno y Transformación Digital de la PCM, a fin de que la PCM en su condición de ente rector tenga conocimiento del cumplimiento de la Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023- PCM/SGTD.
  3. La Gerencia Central de Tecnologías de Información y Comunicaciones prevé el inicio del Plan SGSI en el mes de abril 2025.

# 

# ANEXOS

Anexo N°1 : Cronograma de actividades para la implementación del SGSI 2025.

Anexo N°1 Cronograma de actividades para la implementación del SGSI 2025.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Cod. | Actividades | Unidad de Medida | Programación de Metas Físicas 2025 | | | | Medio de verificación | Programación de Metas Financiadas 2025 | | | | Responsable |
| IIT | IIIT | IVT | Total | IIT | IIIT | IVT | Total |  |
| Etapa 0: Inicial | | | | | | | | | | | | |
| 1 | Elaborar el Estudio de brechas de seguridad de la información de la  Institución | Informe de estudio de brechas. | 1 |  |  | 1 | Revisión y conformidad de informe. | S/ 10,000.00 |  |  | S/ 10,000.00 | Gerencia de Tecnologías de Información y Comunicaciones |
| Etapa 1: Planificación del SGSI | | | | | | | | | | | | |
| 1 | Analizar las necesidades y expectativas de las partes interesadas del SGSI. | Informe de necesidades de partes interesadas. | 1 |  |  | 1 | Revisión y conformidad de informe. | S/ 10,000.00 |  |  | S/ 10,000.00 | Gerencia de Tecnologías de Información y Comunicaciones |
| 2 | Analizar y establecer mediante acta el alcance del SGSI | Informe de alcance. | 1 |  |  | 1 | Revisión y conformidad de informe. | S/ 10,000.00 |  |  | S/ 10,000.00 | Gerencia de Tecnologías de Información y Comunicaciones |
| 3 | Verificar y actualizar (de corresponder) la Política de Seguridad de la Información y Objetivos de Seguridad de la  Información. | Informe de política de seguridad de la información | 1 |  |  | 1 | Revisión y conformidad de informe. | S/ 10,000.00 |  |  | S/ 10,000.00 | Gerencia de Tecnologías de Información y Comunicaciones |
| 4 | Establecer los roles y responsabilidades del Plan SGSI. | Informe de roles y responsabilidades | 1 |  |  | 1 | Revisión y conformidad de informe. | S/ 10,000.00 |  |  | S/ 10,000.00 | Gerencia de Tecnologías de Información y Comunicaciones |
| 5 | Establecer un plan para cumplimiento de objetivos de Seguridad  de la Información. | Informe de plan de cumplimiento. | 1 |  |  | 1 | Revisión y conformidad de informe. | S/ 10,000.00 |  |  | S/ 10,000.00 | Gerencia de Tecnologías de Información y Comunicaciones |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Cod. | Actividades | Unidad de Medida | Programación de Metas Físicas 2025 | | | | Medio de verificación | Programación de Metas Financiadas 2025 | | | | Responsable |
| IIT | IIIT | IVT | Total | IIT | IIIT | IVT | Total |  |
| 6 | Definir metodología para Evaluación de riesgos de seguridad de la información, en base a la NTP-ISO/IEC 27005:2022 o  normativas Institucional. | Metodología. | 1 |  |  | 1 | Revisión y conformidad de metodología. | S/ 10,000.00 |  |  | S/ 10,000.00 | Gerencia de Tecnologías de Información y Comunicaciones |
| 7 | Realizar identificación, análisis, evaluación y valoración de riesgo de seguridad de la  información | Informe de identificación de análisis. |  | 1 |  | 1 | Revisión y conformidad de informe. |  | S/ 10,000.00 |  | S/ 10,000.00 | Gerencia de Tecnologías de Información y Comunicaciones |
| 8 | Analizar y determinar estratégicamente el Plan de tratamiento de  Riesgos. | Informe de Plan de Tratamiento de Riegos. |  | 1 |  | 1 | Revisión y conformidad de informe. |  | S/ 10,000.00 |  | S/ 10,000.00 | Gerencia de Tecnologías de Información y Comunicaciones |
| 9 | Elaborar Documento de aplicabilidad de controles de la NTP-ISO-  IEC 27002:2022. | Documento de Aplicabilidad |  | 1 |  | 1 | Revisión y conformidad de informe. |  | S/ 10,000.00 |  | S/ 10,000.00 | Gerencia de Tecnologías de Información y Comunicaciones |
| 10 | Elaborar el Plan de Capacitación y Concienciación en SI. | Informe de Plan de Capacitación |  | 1 |  | 1 | Revisión y conformidad de informe. |  | S/ 10,000.00 |  | S/ 10,000.00 | Gerencia de Tecnologías de Información y Comunicaciones |
| 11 | Elaborar el Plan de Comunicación. | Informe de Plan de Comunicación |  | 1 |  | 1 | Revisión y conformidad de informe. |  | S/ 7,000.00 |  | S/ 7,000.00 | Gerencia de Tecnologías de Información y Comunicaciones |
| 12 | Elaborar el plan para monitorear, medir y evaluar de la efectividad  del SGSI | Informe de Plan de monitoreo. |  | 1 |  | 1 | Revisión y conformidad de informe. |  | S/ 10,000.00 |  | S/ 10,000.00 | Gerencia de Tecnologías de Información y Comunicaciones |
| Etapa 2 - Implementación (hacer) | | | | | | | | | | | | |
| 1 | Ejecutar el Plan para cumplir los objetivos de SI. | Informe de ejecución de plan de cumplimiento. |  |  | 1 | 1 | Revisión y conformidad de informe. |  |  | S/ 15,000.00 | S/ 15,000.00 | Gerencia de Tecnologías de Información y Comunicaciones |
| 2 | Ejecutar actividades y procedimiento referidos | Informe de  implementación de plan de |  |  | 1 | 1 | Revisión y conformidad de |  |  | S/ 15,000.00 | S/ 15,000.00 | Gerencia de Tecnologías de Información y |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Cod. | Actividades | Unidad de Medida | Programación de Metas Físicas 2025 | | | | Medio de verificación | Programación de Metas Financiadas 2025 | | | | Responsable |
| IIT | IIIT | IVT | Total | IIT | IIIT | IVT | Total |  |
|  | a la implementación de Plan de tratamiento de  Riesgos | tratamiento de riesgos. |  |  |  |  | informe. |  |  |  |  | Comunicaciones |
| 3 | Ejecutar el Plan de Capacitación y Concienciación en SI. | Informe de capacitación y concientización. |  |  | 1 | 1 | Revisión y conformidad de informe. |  |  | S/ 15,000.00 | S/ 15,000.00 | Gerencia de Tecnologías de Información y Comunicaciones |
| 4 | Ejecutar el Plan de Comunicación | Informe de ejecución de plan de comunicación |  |  | 1 | 1 | Revisión y conformidad de informe. |  |  | S/ 10,000.00 | S/ 10,000.00 | Gerencia de Tecnologías de Información y Comunicaciones |
| 5 | Implementar los controles del Anexo A de la Norma de acuerdo al Documento de aplicabilidad y al Plan de  Tratamiento de riesgos. | Informe de  implementación de controles. |  |  | 1 | 1 | Revisión y conformidad de informe. |  |  | S/ 15,000.00 | S/ 15,000.00 | Gerencia de Tecnologías de Información y Comunicaciones |
| 6 | Actualizar el Documento de aplicabilidad con los controles implementados | Informe de Documento de Aplicabilidad actualizado. |  |  | 1 | 1 | Revisión y conformidad de informe. |  |  | S/ 15,000.00 | S/ 15,000.00 | Gerencia de Tecnologías de Información y Comunicaciones |
| 7 | Realizar evaluaciones de riesgos de SI cuando ocurran cambios significativos y actualizar el Hacer Plan de  Tratamiento de riesgos. | Informe de evaluación de riesgos |  |  | 1 | 1 | Revisión y conformidad de informe. |  |  | S/ 15,000.00 | S/ 15,000.00 | Gerencia de Tecnologías de Información y Comunicaciones |
| ETAPA 3 - MONITOREO Y REVISIÓN | | | | | | | | | | | | |
| 1 | Seguimiento al Plan de tratamiento de riesgos | Informe de seguimiento de Plan de tratamiento de riesgos. |  |  | 1 | 1 | Revisión y conformidad de informe. |  |  | S/ 15,000.00 | S/ 15,000.00 | Gerencia de Tecnologías de Información y Comunicaciones |
| 2 | Ejecutar el Plan para monitorear, medir, analizar y evaluar la  efectividad del SGSI. | Informe de ejecución del Plan de monitoreo. |  |  | 1 | 1 | Revisión y conformidad de informe. |  |  | S/ 15,000.00 | S/ 15,000.00 | Gerencia de Tecnologías de Información y Comunicaciones |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Cod. | Actividades | Unidad de Medida | Programación de Metas Físicas 2025 | | | | Medio de verificación | Programación de Metas Financiadas 2025 | | | | Responsable |
| IIT | IIIT | IVT | Total | IIT | IIIT | IVT | Total |  |
| 3 | Realizar la auditoría interna del SGSI. | Informe de auditoría interna. |  |  | 1 | 1 | Revisión y conformidad de informe. |  |  | S/ 15,000.00 | S/ 15,000.00 | Gerencia de Tecnologías de Información y Comunicaciones |
| 4 | Realizar la revisión del SGSI por la Alta Dirección. | informe de revisión por la Alta Dirección, |  |  | 1 | 1 | Revisión y conformidad de informe. |  |  | S/ 15,000.00 | S/ 15,000.00 | Gerencia de Tecnologías de Información y Comunicaciones /CGTD |
| ETAPA 4 - MANTENER Y MEJORAR | | | | | | | | | | | | |
| 1 | Revisar y atender las No Conformidades e implementar las acciones correctivas detectadas en las auditorias, resultados de la revisión por la Dirección y/o tratamiento de los  incidentes. | Informe de No conformidades. |  |  | 1 | 1 | Revisión y conformidad de informe. |  |  | S/ 15,000.00 | S/ 15,000.00 | Gerencia de Tecnologías de Información y Comunicaciones |
| 2 | Implementar y documentar la mejora continua | Informe de mejora continua. |  |  | 1 | 1 | Revisión y conformidad de informe. |  |  | S/ 15,000.00 | S/ 15,000.00 | Gerencia de Tecnologías de Información y Comunicaciones |
| 3 | Auditoría de certificación del sistema de gestión de seguridad de la información (SGSI) (SUJETO A DECISIÓN DEL CTGD Y DISPONIBILIDAD PRESUPUESTAL) | Certificación SGSI. |  |  | 1 | 1 | Certificación 27001 |  |  |  |  | Gerencia de Tecnologías de Información y Comunicaciones/Empresa Externa. |
| Total | | | | | | | | | | | S/ 317,000.00 | |