"LINEAMIENTO QUE REGULA EL PROCESO DE LA ADMINISTRACIÓN DE LOS SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN DEL FONDO DE ASEGURAMIENTO EN SALUD DE LA POLICÍA NACIONAL DEL PERÚ – SALUDPOL"

Seguro Saludpol

Firmado digitalmente por BERASTAIN MERINO Hector Hellmuth FAU 20178922581 hard
Motivo: Doy V° B°
Fecha: 04.02.2025 14:10:04 -05:00

OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN

Seguro Saludpol

Firmado digitalmente por ESPEJO FERNANDEZ Oscar Manuel FAU 20178922581 soft
Motivo: Doy V° B°
Fecha: 04.02.2025 13:43:16 -05:00

Código del Documento Normativo	Versión	Resolución de Aprobación	Fecha de Aprobación
LINEAMIENTO N° 001-2025-SALUDPOL/PD	1.0	RPD N° 002-2025-SALUDPOL/PD	04/02/2025

Seguro Saludpol

Firmado digitalmente por CRUZ PALOMINO Johnny Antonio FAU 20178922581 hard
Motivo: Doy V° B°
Fecha: 04.02.2025 12:27:07 -05:00

Seguro Saludpol

Firmado digitalmente por BAUTISTA PIZARRO Wilber FAU 20178922581 hard
Motivo: Doy V° B°
Fecha: 04.02.2025 12:05:41 -05:00

ÍNDICE

CONTENIDO

LINEAMIENTO N° 001-2025-SALUDPOL/PD V 1.0

LINEAMIENTOS QUE REGULAN EL PROCESO DE LA ADMINISTRACIÓN DE LOS SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN DEL FONDO DE ASEGURAMIENTO EN SALUD DE LA POLICÍA NACIONAL DEL PERÚ – SALUDPOL

I. INTRODUCCIÓN

El Decreto Legislativo N° 1174, y sus modificatorias que dispone la adecuación del Fondo de Aseguramiento en Salud de la Policía Nacional del Perú - SALUDPOL, establece que es una institución con personería jurídica de derecho público adscrita al Ministerio del Interior que cuenta con autonomía técnica, administrativa, económica, financiera, presupuestal y contable. Tiene como finalidad recibir, captar y gestionar los fondos destinados al financiamiento de prestaciones de salud u ofrecer coberturas de riesgos de salud a sus beneficiarios.

De acuerdo a lo señalado en el Decreto Legislativo N° 1601, Ley que dicta medida para fortalecer el régimen de salud de la Policía Nacional del Perú al incluir como beneficiarios a cónyuges, convivientes, hijos mayores de policías, y cónyuges sobrevivientes con derecho a pensión. Se modifican aspectos del Fondo de Aseguramiento en Salud de la PNP-SALUDPOL, se integran nuevos miembros al Directorio de SALUDPOL y se establece que los recursos para el aseguramiento de la salud del personal policial equivalen al 6% de sus ingresos, considerando diversas fuentes de financiamiento.

En el contexto de la Política de Aseguramiento Universal en Salud, se promulgaron distintos dispositivos legales dentro del que se contempla a la Ley N° 29344, Ley Marco de Aseguramiento Universal en Salud, que en su artículo 6 establece que el Ministerio de Salud, en ejercicio de su rol rector en el sector salud, tiene la responsabilidad de establecer de manera descentralizada y participativa las normas y las políticas relacionadas con la promoción, la implementación y el fortalecimiento del aseguramiento universal en salud.

Asimismo, las tecnologías de la información constituyen hoy en día elementos claves para el eficiente desempeño de la institución. En ese sentido, se hace necesario disponer de lineamientos, políticas y herramientas que permitan a los funcionarios y servidores del SALUDPOL, cumplir con eficiencia las funciones asignadas, considerando el ámbito y la importancia que han alcanzado las tecnologías de la información.

Finalmente, es preciso señalar que la Resolución Ministerial N° 158-2019-IN, aprueba el Manual de Operaciones del Fondo de Aseguramiento en Salud de la Policía Nacional del Perú – SALUDPOL, el cual describe la organización funcional del SALUDPOL; por lo cual los Documentos Normativos del SALUDPOL se adecuan a la estructura funcional, de acuerdo a los procesos, relaciones de coordinación, articulación interna y externa identificados.

II. OBJETIVO

Establecer un marco normativo que permita la gestión eficiente, segura y sostenible de los sistemas y tecnologías de la información en el Fondo de Aseguramiento en Salud de la Policía Nacional del Perú – SALUDPOL, asegurando su alineación con los objetivos estratégicos institucionales, el cumplimiento de normativas vigentes y la promoción de la innovación tecnológica.

III. ÁMBITO DE APLICACIÓN

El presente Lineamiento es de aplicación obligatoria por todos los órganos del Fondo de Aseguramiento en Salud de la Policía Nacional del Perú – SALUDPOL.

IV. BASE LEGAL

3.1 Constitución Política del Perú.

3.2 Ley N° 26842, Ley General de Salud.

3.3 Ley N° 29733, Ley de protección de datos personales.

3.4 Decreto Legislativo N° 1174, Ley del Fondo de Aseguramiento en Salud de la Policía Nacional del Perú, que adecúa el Fondo de Aseguramiento en Salud de la Policía Nacional del Perú.

3.5 Decreto Legislativo N° 1601 que dicta medidas para fortalecer el régimen de salud del Fondo de Aseguramiento en Salud de la Policía Nacional del Perú – SALUDPOL

3.6 Decreto Legislativo N° 1175, Ley del Régimen de Salud de la Policía Nacional del Perú.

3.7 Decreto Legislativo N° 1267, Ley de la Policía Nacional del Perú.

3.8 Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital

3.9 Decreto Supremo N° 002-2015-IN, que aprueba el Reglamento del Decreto Legislativo N° 1174, Ley del Fondo de Aseguramiento en Salud de la Policía Nacional del Perú.

3.10 Decreto Supremo N° 003-2015-IN, que aprueba el Reglamento del Decreto Legislativo N° 1175, Ley del Régimen de Salud de la Policía Nacional.

3.11 Decreto Supremo N° 004-2019-JUS, que aprueba el Texto Único Ordenado de la Ley N° 27444 Procedimiento Administrativo General.

3.12 Decreto Supremo N° 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N° 1412, Ley de Gobierno Digital.

3.13 Resolución Ministerial N° 158-2019-IN, que aprueba el Manual de Operaciones del Fondo de Aseguramiento en Salud de la Policía Nacional de Perú – SALUDPOL y sus modificatorias.

3.14 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, 2ª Edición", en las entidades integrantes del Sistema Nacional de Informática.

3.15 Resolución Ministerial N° 041-2017-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP/ISO/IEC 12207:2016 Ingeniería de Software y Sistemas. Procesos del ciclo de vida del Software, 3ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

3.16 Resolución de Gerencia General N° 269-2019-IN-SALUDP0L-GG, que aprueba la "Directiva para la Implementación del Lenguaje inclusivo en la Comunicación Oral, Gráfica y Escrita en el Fondo Aseguramiento en Salud de la Policía Nacional del Perú-SALUDPOL".

3.17 Resolución de Gerencia General N° 310-2023-IN-SALUDPOL-GG, que aprueba la "Directiva para la elaboración de documentos normativos del Fondo de Aseguramiento en Salud de la Policía Nacional del Perú - SALUDPOL".

V. DISPOSICIONES GENERALES

5.1 De la Estrategia y Gobernanza de TI

5.1.1 Los objetivos tecnológicos del SALUDPOL deben estar alineados a las metas institucionales y garantizar un marco de operación eficiente.

5.1.2 Los planes en materia de Gobierno y Transformación Digital deben ser desarrollados en el marco de la Ley N° 1412, Ley de Gobierno Digital.

5.1.3 Los riesgos del SALUDPOL deben ser gestionados de manera eficiente, a través de la identificación de amenazas tecnológicas e implementación de planes de mitigación para la corrección de vulnerabilidades.

5.1.4 Los procesos del SALUDPOL deben cumplir con estándares internacionales como la ISO/IEC 27001, a través de la implementación de un Sistema de Gestión de Seguridad de la Información.

5.1.5 Se debe identificar y mantener los datos maestros, sus atributos y relaciones y; desarrollar un modelo de referencia de datos para el SALUDPOL; dicho modelo se basa en estándares internacionales reconocidos, vocabularios y términos descriptivos que le dan contexto y facilitan su intercambio, interpretación y reutilización.

5.2 De la Gestión de Proyectos de TI

5.2.1 La Gestión de Proyectos de TI permite planificar y ejecutar iniciativas tecnológicas dentro de los plazos y presupuestos establecidos.

5.2.2 En la etapa de planificación, es importante definir los objetivos, cronograma y presupuesto, a fin de tener una visión global del proyecto, alinear a todo el equipo y detectar necesidades con antelación.

5.2.3 Definir correctamente los recursos del proyecto, tomando en cuenta la asignación de personal, equipos y tiempo, garantizando todo lo necesario para su ejecución en el menor tiempo posible.

5.2.4 Ejecutar el seguimiento y control frecuente sobre el nivel de progreso del proyecto de TI, haciendo uso de metodologías reconocidas como Scrum, Kanban, Agile Inception, Design Sprint, entre otras.

5.2.5 Administrar los cambios de manera eficiente, minimizando el impacto de las implementaciones en la operación diaria del SALUDPOL.

5.3 Del Ciclo de Gestión de la Información

5.3.1 El recojo de datos consiste en el levantamiento y/o recolección de los datos que se producen de manera institucional a través de los sistemas de información del SALUDPOL. Entre las actividades para este fin están la identificación de necesidades, elaboración de instrumentos para recojo de información, validación del instrumento, y levantamiento, extracción y preparación de base de datos.

5.3.2 El procesamiento de la información es la acumulación, explotación, manipulación y transformación de datos, lo que resulta finalmente en información y permite a las unidades de organización responsables elaborar propuestas de indicadores de gestión y sus fichas técnicas.

5.3.3 Para la generación de informe se ejecuta el análisis de la información, el cual tiene como objetivo ubicar los datos en un contexto, espacio y tiempo para a partir de ello, generar evidencia y fortalecer la toma de decisiones. Asimismo, se ejecuta la elaboración del informe, acorde a los resultados de los indicadores contenidos en el Sistema de Monitoreo y Evaluación.

5.3.4 La distribución de información permitirá fortalecer la gestión del conocimiento institucional a nivel operativo y estratégico, para ello la información debe ser oportuna, relevante y precisa.

5.3.5 La toma de decisiones a nivel estratégico, misional o de soporte debe basarse en la evidencia disponible que permita desarrollar estrategias y tácticas que ayuden a alcanzar los objetivos institucionales orientados a resultados y al beneficiario.

VI. DEFINICIONES OPERACIONALES

6.1 **Agile Inception:** Es una metodología de gestión que se utiliza para establecer las bases de un proyecto de software antes de empezar a desarrollarlo.

6.2 **Amenaza:** Es cualquier situación que pueda perjudicar la seguridad de los datos de un usuario o empresa. Las amenazas pueden provenir de ataques externos o internos, y pueden tener consecuencias negativas para la reputación, la imagen, las funciones o las operaciones de una empresa.

6.3 **Antivirus:** Es un tipo de software que se utiliza para evitar, buscar, detectar y eliminar virus de una computadora. Una vez instalados, la mayoría del software antivirus se ejecutan automáticamente en segundo plano para brindar protección en tiempo real contra ataques de virus.

6.4 **Autenticación multifactor:** Es un proceso de registro que requiere más de una forma de verificación para acceder a una cuenta o aplicación, estas pueden ser: contraseña, código enviado a un teléfono o correo electrónico, respuesta a una pregunta secreta, escaneado de huella dactilar, reconocimiento de voz, reconocimiento facial, entre otros.

6.5 **Big Data:** Es un término que se refiere a la recopilación, almacenamiento, análisis y visualización de grandes volúmenes de datos que son difíciles de procesar con métodos tradicionales. Estos datos pueden ser de tipo no estructurado y de alta velocidad, y pueden incluir imágenes, video, audio y texto.

6.6 **Blockchain:** Es una tecnología que permite registrar transacciones de manera descentralizada y compartida entre una red de computadoras.

6.7 **Centro de Datos:** Es una ubicación física que almacena máquinas de computación y sus equipos de hardware relacionados. Contiene la infraestructura computación que requieren los sistemas de TI, como servidores, unidades de almacenamiento de datos y equipos de red. Es la instalación física que almacena los datos digitales de cualquier empresa.

6.8 **Design Sprint:** Es una metodología de duración breve, pero intensa, que se usa para dar respuesta a problemas importantes de negocios, sobre todo en el inicio de un nuevo producto o servicio, y para recopilar la retroalimentación de los usuarios.

6.9 **Firewalls:** Es un sistema de seguridad que filtra el tráfico de red que entra y sale de un dispositivo o red. Su objetivo es proteger las redes privadas de amenazas externas y accesos no autorizados.

6.10 **IDS:** Un sistema de detección de intrusiones es una tecnología de seguridad de red que identifica y alerta sobre posibles intrusiones.

6.11 **Inteligencia Artificial:** Es un campo de la informática que se encarga de crear sistemas que pueden realizar tareas similares a las que requiere la inteligencia humana. La IA utiliza algoritmos y modelos matemáticos para procesar grandes cantidades de datos y tomar decisiones basadas en patrones y reglas.

6.12 **Inteligencia de Negocio:** Es un conjunto de herramientas y procesos que permiten a las organizaciones recopilar, almacenar, analizar y visualizar datos para tomar decisiones más informadas.

6.13 **IPS:** Un sistema de prevención de intrusiones ayuda a las organizaciones a identificar el tráfico malicioso y bloquea de manera proactiva el ingreso de dicho tráfico a su red.

6.14 **Kanban:** Es una metodología de gestión de proyectos ágil que se basa en la visualización de tareas para organizar el flujo de trabajo. La palabra Kanban es de origen japonés y significa "tablero o panel visual".

6.15 **LAN:** Es un grupo de dispositivos que están conectados entre sí en un área limitada, como una casa u oficina, y que comparten una conexión a internet. Los dispositivos que forman parte de una LAN pueden ser computadoras, teléfonos, tablets, routers, entre otros.

6.16 **Machine Learning:** Es una disciplina de la Inteligencia Artificial (IA) que permite a los sistemas informáticos aprender de los datos y realizar tareas sin instrucciones explícitas.

6.17 **Modelo de referencia de Datos:** Permite describir los datos, su estructura y significado en el contexto de la entidad, para facilitar su descripción, clasificación, calidad, apertura, acceso, reutilización y gestión en general.

6.18 **Phishing:** Es una técnica de ingeniería social que se utiliza para robar información personal, como contraseñas, números de tarjeta de crédito o datos bancarios. Los ciberdelincuentes se hacen pasar por entidades legítimas, como instituciones públicas, bancos o redes sociales, para engañar a las personas.

6.19 **Riesgo:** Es la probabilidad de que una amenaza se convierta en un desastre. El riesgo es la combinación de la probabilidad de que ocurra un evento y sus consecuencias negativas.

6.20 **Scrum:** Es una metodología de gestión de proyectos ágil que ayuda a los equipos a trabajar de manera colaborativa y eficiente para alcanzar objetivos comunes.

6.21 **Usuario:** Es una persona que utiliza un sistema informático o un programa y que se identifica con un nombre de usuario y una contraseña. Para registrarse, el usuario debe proporcionar información personal como su nombre, apellido, correo electrónico o DNI.

6.22 **Vulnerabilidad:** Es la susceptibilidad o fragilidad de un sistema, comunidad o bien a los efectos dañinos de una amenaza.

6.23 **WAN:** Es una red informática que conecta redes más pequeñas en un área geográfica grande. Las WAN pueden ser cableadas o inalámbricas.

6.24 **Wi-Fi:** Es una tecnología de redes inalámbricas que permite a los dispositivos electrónicos conectarse entre sí de manera fluida a una red mediante frecuencias de radio.

6.25 Siglas y acrónimos

6.25.1 **BI:** Business Intelligence.

6.25.2 **IA:** Inteligencia Artificial.

6.25.3 **IDS:** Sistema de detección de intrusos.

6.25.4 **IEC:** Comisión Electrotécnica Internacional.

6.25.5 **IPS:** Sistema de prevención de intrusos.

6.25.6 **ISO:** International Organization for Standardization.

6.25.7 **ITIL:** Biblioteca de Infraestructura de Tecnologías de la Información

6.25.8 **LAN:** Local Area Network.

6.25.9 **ML:** Machine Learning.

6.25.10 **OTI:** Oficina de Tecnología de la Información.

6.25.11 **SALUDPOL:** Fondo de Aseguramiento en Salud de la Policía Nacional del Perú.

6.25.12 **SI:** Sistemas de Información.

6.25.13 **TI:** Tecnologías de la Información.

6.25.14 **WAN:** Wide Area Network.

6.25.15 **Wi-Fi:** Wireless Fidelity.

VII. DISPOSICIONES ESPECÍFICAS

7.1 Del Desarrollo y la Gestión de Software

7.1.1 De la Adquisición de Software

7.1.1.1 La Adquisición de Software es un proceso que permite garantizar que SALUDPOL disponga de las herramientas tecnológicas necesarias para su funcionamiento eficiente y conforme a la normativa vigente sobre propiedad intelectual.

7.1.1.2 La Oficina de Tecnología de la Información (OTI) realiza la identificación y evaluación de las necesidades de software de las diferentes unidades de organización del SALUDPOL para realizar la investigación y detección de las opciones de software disponibles que mejor se adapten a los requerimientos.

7.1.1.3 Es importante realizar la verificación del tipo de licencia que el software a adquirir requiere, a fin de garantizar que su implementación y uso en SALUDPOL cumplan con las leyes de propiedad intelectual y las normativas vigentes.

7.1.1.4 La OTI debe planificar la instalación de los softwares según las necesidades operativas y considerando los horarios de trabajo del personal de las unidades de organización, a fin de minimizar interrupciones a los trabajadores del SALUDPOL y realizar las pruebas de funcionamiento para asegurar que está instalado y configurado correctamente.

7.1.2 Del Desarrollo de Software

7.1.2.1 El Desarrollo de Software de centra en el diseño, implementación, mantenimiento y mejora de aplicaciones.

7.1.2.2 Para el análisis de requisitos, la Oficina de Tecnología de la Información, en coordinación con las unidades de organización del SALUDPOL, deben identificar las necesidades tecnológicas de acuerdo a sus funciones.

7.1.2.3 El desarrollo de software debe involucrar el uso de metodologías ágiles como Scrum, Kanban, Agile Inception, Design Sprint, entre otras que permitan al equipo de desarrollo adaptarse rápidamente a los cambios en las necesidades y requisitos de las unidades de organización del SALUDPOL.

7.1.2.4 El control de lanzamientos y actualizaciones de software, debe llevarse a cabo a través de la gestión de versiones, esto garantiza que la entrega del software y sus actualizaciones se ejecute de manera eficaz.

7.1.2.5 Asegurar que los softwares implementados cumplan con estándares de funcionalidad y seguridad, aplicando pruebas y calidad para la detección de errores y garantizar la calidad de los mismos.

7.2 De la Infraestructura de TI

7.2.1 La Infraestructura de TI incluye todos los componentes físicos y virtuales que soportan la tecnología del SALUDPOL, entre los que se encuentran servidores, dispositivos de almacenamiento y equipos de usuario.

7.2.2 Configurar y mantener de manera eficiente las redes LAN, WAN del SALUDPOL, a fin de asegurar la operatividad de los mismo y garantizar las actividades administrativas de la institución.

7.2.3 Implementar entornos virtuales utilizando herramientas modernas para la consolidación de carga de trabajo, optimización de recursos y mejorar la recuperación ante desastres.

7.2.4 Optimizar el Centro de Datos, diseñando y manteniendo espacios con energía, enfriamiento y seguridad adecuados.

7.3 De las Operaciones y Soporte

7.3.1 El Soporte Técnico a usuarios involucra incidentes de hardware y software, así como la atención de requerimientos referente a servicios de TI.

7.3.2 Los requerimientos e incidencias de las unidades de organización se gestionan a través de una solución de mesa de servicio basada en buenas prácticas de ITIL, para el registro, priorización, atención y solución de los casos.

7.3.3 El monitoreo del funcionamiento de los servidores, redes y sistemas informáticos por parte del especialista de la Oficina de Tecnología de la Información debe ser constante, a fin de garantizar las actividades diarias del SALUDPOL.

7.3.4 Los Planes de Continuidad de Tecnologías de la Información del SALUDPOL deben contemplar el uso de estándares internacionales tales como la ISO/IEC 22301, ISO/IEC 27001, entre otras buenas prácticas.

7.4 De la Innovación y Transformación Digital

7.4.1 La Innovación y Transformación Digital busca incorporar tecnologías disruptivas para mejorar procesos y generar ventajas competitivas.

7.4.2 Explorar tendencias a través del análisis de tecnologías emergente como inteligencia artificial o blockchain, para ser aplicadas en la digitalización de procesos y servicios del SALUDPOL.

7.4.3 Fomentar el uso de herramientas colaborativas, que permitan a los usuarios del SALUDPOL intercambiar información y conocimiento, y producir nuevo conocimiento de forma conjunta.

7.5 De la Seguridad de la Información

7.5.1 La Seguridad de la Información es el conjunto de medidas preventivas y reactivas que protege los activos tecnológicos del SALUDPOL contra amenazas internas y externas.

7.5.2 La gestión de vulnerabilidades es un proceso vital para identificar y corregir fallos en la infraestructura tecnológica, a fin mitigar los riesgos y minimizar las amenazas que puedan impactar de manera negativa al SALUDPOL.

7.5.3 Para mitigar los riesgos asociados a la Seguridad de la Información, es necesario la implementación de sistemas de autenticación multifactor y la gestión de roles, garantizando de esta manera el control de accesos a los servicios informáticos del SALUDPOL.

7.5.4 Garantizar la defensa contra ciberataques a través del uso de herramientas como firewalls, IDS/IPS y soluciones antivirus, manteniendo así la confianza de las unidades de organización y cumplir la normativa vigente.

7.5.5 Los usuarios finales del SALUDPOL, como uno de los activos más importantes dentro de la Seguridad de la Información, deben estar capacitados sobre phishing, contraseñas seguras y uso adecuado de la tecnología, generando conciencia en la materia.

7.6 De la Gestión de Datos

7.6.1 La Gestión de Datos y Análisis se enfoca en la organización, calidad y explotación de datos para la toma de decisiones.

7.6.2 Proponer políticas y lineamientos para garantizar la calidad, privacidad y seguridad de los datos, en el marco de la Gobernanza de Datos en el estado.

7.6.3 Brindar soporte en la administración de datos, para la generación de evidencias a través de la Unidad de Monitoreo y Evidencias para la Gestión.

7.6.4 Utilizar técnicas avanzadas para la administración de grandes volúmenes de datos, aplicando soluciones de Big Data y ML.

VIII. RESPONSABILIDADES

8.1 De la Oficina de Tecnología de la Información

8.1.1 Administrar eficiente y oportunamente los sistemas y tecnologías de la información, determinados en el presente lineamiento.

8.1.2 Garantizar las operaciones y el soporte de TI a las unidades de organización del SALUDPOL, para el correcto uso de los servicios y sistemas de información de la institución.

8.1.3 Gestionar la infraestructura de TI del SALUDPOL, garantizando la operatividad y funcionalidad de los servicios informáticos de la institución.

8.1.4 Implementar sistemas de información cumpliendo estándares internacionales para el desarrollo de software.

8.1.5 Administrar y asegurar la información del SALUDPOL, para evitar su perdida, asegurando la confidencialidad, integridad, disponibilidad, y resguardo contra amenazas.

8.1.6 Liderar la transformación digital en el SALUDPOL, incorporando tecnologías disruptivas para la mejora en los procesos de la institución.

8.2 De la Oficina de Asesoría Jurídica

8.2.1 Emitir opinión legal con respecto a la aprobación de políticas o lineamientos para la gestión de la seguridad de la información y demás normas estándares por implementar.

8.3 De la Unidad de Monitoreo y Evidencias para la Gestión

8.3.1 Analizar la información contenida en los sistemas de información para la generación de evidencias.

8.4 De las Unidades de Organización

8.4.1 Solicitar, en el marco de sus funciones, los requerimientos de nuevos sistemas de información y acceso a los servicios de TI.

IX. DISPOSICIONES COMPLEMENTARIAS FINALES

9.1 La OTI debe velar y asegurar la implementación de normas o estándares en materia de tecnologías de la información en el SALUDPOL.

9.2 Aquellos aspectos operativos no contemplados en el presente lineamiento, deben ser reglamentados e implementados por las unidades de organización del SALUDPOL, en coordinación con la Oficina de Tecnología de la Información.

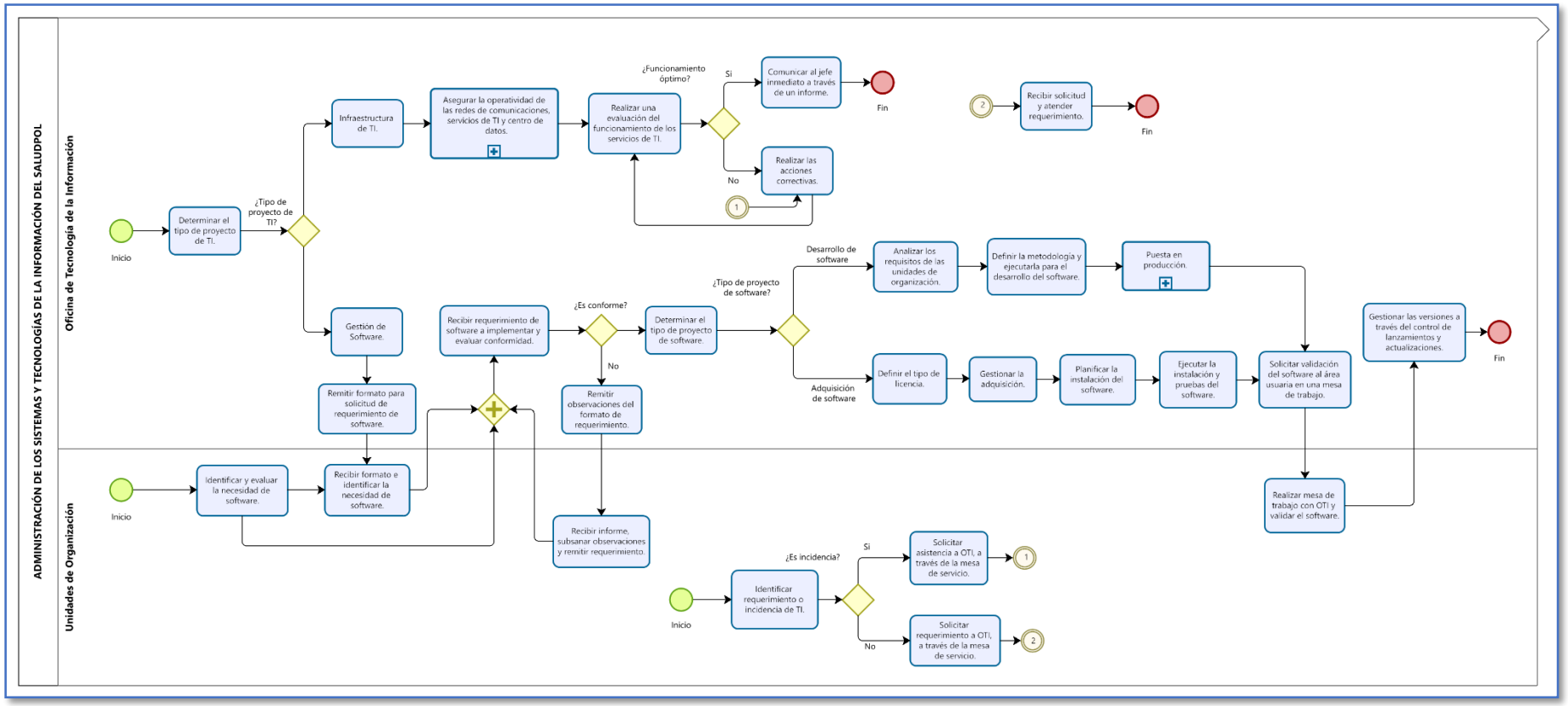
9.3 Las metodologías y/o herramientas específicas que se utilizarán para la administración de los sistemas y tecnologías de la información deben ser procedimentados en los documentos normativos que correspondan, de acuerdo a la complejidad de su composición.

X. VIGENCIA

El presente documento normativo entra en vigencia a partir del día siguiente de su aprobación mediante Resolución de Presidencia de Directorio y debe ser publicada en la página Web de la institución.

XI. ANEXOS

Flujograma



XII. REFERENCIAS BIBLIOGRÁFICAS

12.1 Norma Técnica Peruana NTP/ISO/IEC 12207:2016, Ingeniería de Software y Sistemas. Procesos del ciclo de vida del Software.

12.2 Fundamentos de ITIL 4ta Edición, Fundamentos de la administración de servicios de TI (ITSM).

12.3 ISO/IEC 27001:2022, Seguridad de la Información, Ciberseguridad y Protección de la Privacidad – Sistema de Gestión de Seguridad de la Información – Requisitos.

12.4 Ley N° 1412, Ley de Gobierno Digital.