CONSEJO DIRECTIVO
CUARTA SESION EXTRAORDINARIA
Lima, 30 de junio de 2022

ACUERDO Nº 5-4E-ESSALUD-2022

VISTOS:

Los Memorandos N°s 539 y 608-GCTIC-ESSALUD-2022, de la Gerencia Central de Tecnologías de Información y Comunicaciones, con los que se propone la aprobación de la *"Política Institucional de Seguridad de la Información"* y de la *"Política Institucional de Gobernanza y Gestión de Datos"*; los Informes Técnicos N°s 005 y 006-GPC-GCPP-ESSALUD-2022, los Informes N°s 062 y 063-GOP-GCPP-ESSALUD-2022 y el Memorando N° 3683-GCPP-ESSALUD-2022 de la Gerencia Central de Planeamiento y Presupuesto; la Nota N° 760-GCAJ-ESSALUD-2022 e Informe N° 229-GNAA-GCAJ-ESSALUD-2022 de la Gerencia Central de Asesoría Jurídica; y el Memorando N° 1224-GG-ESSALUD-2022 de la Gerencia General, y;

En virtud de las facultades conferidas, por mayoría, el Consejo Directivo;

ACORDÓ:

1. **APROBAR** la *"Política Institucional de Seguridad de la Información"*.

2. **APROBAR** la *"Política Institucional de Gobernanza y Gestión de Datos"*.

3. **DISPONER** que la Gerencia Central de Tecnologías de Información y Comunicaciones emita las disposiciones y/o realice las acciones necesarias, para la implementación de las políticas aprobadas en los numerales 1 y 2 del presente Acuerdo.

4. **EXONERAR** el presente Acuerdo del trámite de lectura y aprobación del acta para su inmediata ejecución.

FELIPE NOBLECILLA PASCUAL
SECRETARIO GENERAL (e)
ESSALUD

POLÍTICA INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN

Versión	Fecha	Elaborado:	Revisado:	Aprobado:
V1.0		Gerencia Central de Tecnologías de Información y Comunicaciones	Gerencia Central de Planeamiento y Presupuesto	Consejo Directivo
			Gerencia Central de Asesoría Jurídica	

CONTENIDO

V°B°
Ing. R. SANCHEZ
Gerente Central
ESSALUD

1. Introducción

El Seguro Social de Salud - ESSALUD, reconoce como activo vital toda información generada en sus procesos; por ello, está comprometido a salvaguardar la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de recomendaciones y mecanismos, basados en las Normas Técnicas Peruanas vigentes, estándares internacionales y mejores prácticas en el manejo de la seguridad de la información, con el objetivo de minimizar los riesgos de seguridad de la información, asegurando la continuidad de sus operaciones y manteniendo un nivel óptimo de calidad en los servicios que brinda.

Se debe tener en cuenta que la seguridad de la información se define como la salvaguarda del activo de información debidamente clasificado para su confidencialidad, asegurando que solo quienes estén autorizados puedan acceder a la información; su integridad, asegurando que la información y sus métodos de procesos sean exactos y completos; y, su disponibilidad, asegurando que los usuarios autorizados tengan acceso a la información cuando la requieran.

El Seguro Social de Salud - ESSALUD, con la presente política reconoce que los activos de información son fundamentales para la gestión de los servicios de salud y el otorgamiento de las prestaciones económicas y sociales que brinda a sus asegurados y grupos de interés; por lo tanto, se debe adoptar una posición consciente y vigilante respecto al uso y limitaciones de los recursos y servicios informáticos críticos que la institución posee.

La Política Institucional de Seguridad de la Información de ESSALUD, es un documento que declara las intenciones y orientaciones generales institucionales con relación a la seguridad de la información, constituyéndose como un eje fundamental para la gestión de la seguridad de los activos de información y el compromiso institucional, en el marco de Gobierno y Transformación Digital con la aplicación de políticas, reglamentos, procedimientos, directivas, lineamientos, estructura organizacional y soluciones de plataformas tecnológicas sobre la base de normas técnicas, estándares probados y reconocidos y la aplicación de buenas prácticas a nivel institucional.

2. Objetivo

Establecer el marco general que regule la seguridad de la información y el resguardo de los activos de información del Seguro Social de Salud – ESSALUD, minimizando los riesgos en sus procesos y manteniendo la continuidad de sus operaciones.

3. Marco Normativo

3.1. Ley N° 27056, Ley de Creación del Seguro Social de Salud - EsSalud y su Reglamento, aprobado por Decreto Supremo N° 002-99-TR, y sus modificatorias.

3.2. Ley N° 30096, Ley de delitos informáticos, y sus modificatorias.

3.3. Ley N° 29733, Ley de Protección de Datos Personales y su Reglamento, aprobado por Decreto Supremo N° 003-2013-JUS, y sus modificatorias.

3.4. 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.

3.5. Decreto de Urgencia N° 006-2020, que crea el Sistema Nacional de Transformación Digital.

3.6. Decreto de Urgencia N° 007-2020, que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.

3.7. Decreto Supremo N° 070-2013-PCM, que modifica el Reglamento de la Ley de Transparencia y Acceso a la Información Pública, aprobado por Decreto Supremo N° 072-2013-PCM.

3.8. Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital y su Reglamento aprobado por Decreto Supremo N° 029-2021-PCM.

3.9. Decreto Legislativo N° 1353, decreto legislativo 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.

3.10. 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.

3.11. Resolución Ministerial N° 166-2017-PCM, que modifica el artículo 5 de la Resolución Ministerial N° 004-2016-PCM, referente al Comité de Gestión de Seguridad de la Información.

3.12. Resolución Ministerial N° 087-2019-PCM, que aprueba disposiciones sobre la conformación y funciones del Comité de Gobierno Digital.

3.13. Resolución Ministerial N° 688-2020/MINSA, que aprobó la Directiva Administrativa N° 294-MINSA/2020/OGTI Directiva Administrativa que establece el tratamiento de datos personales relacionados con la salud o datos personales en salud.

3.14. Resolución de Presidencia Ejecutiva N° 767-PE-ESSALUD-2015, que aprueba el Texto Actualizado y Concordado del Reglamento de Organización y Funciones del Seguro Social de Salud - ESSALUD, y sus modificatorias.

4. Ámbito de Aplicación

La Política de Seguridad de la Información involucra a todas las unidades de organización del Seguro Social de Salud. Es dirigida al personal indistintamente de su régimen laboral, modalidad de contratación y nivel jerárquico; así como a las personas naturales o jurídicas que prestan servicios a la institución, con quienes se hayan suscrito contratos o convenios y tengan acceso a los activos de información y a la red de datos de la entidad a nivel nacional.

5. Principios de la Seguridad de la Información[1]

La seguridad de la información implica la aplicación y gestión de controles de seguridad adecuados para la salvaguarda del activo de información, minimizando los riesgos y manteniendo la continuidad de sus operaciones, para ello busca garantizar sus tres principios:

5.1. Disponibilidad

La información y los activos asociados deben estar accesibles a los usuarios autorizados toda vez que lo requieran, garantizando el acceso oportuno a la información.

5.2. Confidencialidad

Asegurar que la información solamente sea accesible por las personas autorizadas, previniendo el acceso no autorizado sea éste deliberado o accidental.

[1] Adaptado de la NTP ISO/IEC 27001:2014

5.3. Integridad
Salvaguardar que la información sea exacta, confiable y esté completa y correcta, protegiéndola de cambios indebidos o no autorizados.

6. Documentos normativos u orientadores que se desprenden de la Política Institucional de Seguridad de la Información

La presente Política Institucional es de carácter general, para asegurar su cumplimiento se deben establecer documentos normativos a través de distintos tipos, tales como: Manuales, metodologías, directivas, procedimientos u otros documentos normativos que permitirán lograr los objetivos de la seguridad de la información en el Seguro Social de Salud – ESSALUD.

7. Definiciones

7.1. 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.[2]

7.2. Control: Cualquier acción o proceso que se utiliza para mitigar el riesgo de seguridad de la información.[3]

7.3. Custodio de la información: Es una unidad de organización de la entidad, un cargo, un líder de proceso o grupo de trabajo encargado de administrar, vigilar los activos de información y hacer efectivos los controles de seguridad que el propietario de la información defina y requiera, así como los medios en los cuales residen o se soportan.

7.4. Propietario de la información: Los propietarios de la información son los titulares de los órganos centrales y/o desconcentrados del Seguro Social de Salud, y que tienen la responsabilidad de definir el tratamiento y los niveles de seguridad que se implementarán para el uso de la información que corresponde al ámbito de su competencia. El Propietario de la Información, también es el Propietario de los Riesgos de dicha información.

7.5. Riesgo: Combinación de la probabilidad de ocurrencia de un evento y sus consecuencias.[4]

7.6. Seguridad de la Información: Es el conjunto de acciones establecidas con la finalidad de preservar la confidencialidad, integridad y disponibilidad de la información, independientemente del soporte que los contenga.[5]

7.7. 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 la búsqueda de la protección de sus activos de información.[6]

7.8. Usuarios de los activos de información: 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.

---

[2] Adaptado del numeral 8.2.2 Identificación de activos. NTP ISO/IEC 27005:2018
[3] Adaptado del numeral 2.16. 2 Términos y definiciones de la ISO/IEC 27000:2014
[4] Adaptado del numeral 2.68. 2 Términos y definiciones de la ISO/IEC 27000:2014
[5] Adaptado del numeral 2.33. 2 Términos y definiciones de la ISO/IEC 27000:2014
[6] Adaptado del numeral 3.2.1, 3.2. 3 Sistemas de Gestión de la Seguridad de la Información de la ISO/IEC 27000 2014

7.9. **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.[7]

8. **Declaración de la Política Institucional de Seguridad de la Información**

El Seguro Social de Salud - ESSALUD es la entidad que se encarga de brindar prestaciones de salud, económicas y sociales a sus asegurados y grupos de interés y reconoce como activo principal a toda información en sus procesos, salvaguardando la integridad, confidencialidad y disponibilidad de la información, con el compromiso de satisfacer los requisitos de las normas técnicas peruanas y estándares internacionales de seguridad de la información, de la mejora continua del sistema de gestión de seguridad de la información, la continuidad operativa de la entidad y el cumplimiento de la normatividad legal vigente.

La Alta Dirección de ESSALUD, demuestra liderazgo y se compromete a brindar los recursos necesarios en función a la disponibilidad de los recursos presupuestales y disponer la implementación de estrategias y directrices que permitan la adecuada gestión de la seguridad de la información, alineadas a la normativa vigente y en función de la evaluación y tratamiento de los riesgos de seguridad de la información.

Todo tratamiento de activos de información que incluyan datos personales se efectúa conforme a lo establecido en la Ley de Protección de Datos Personales o a la normativa institucional vigente.

9. **Objetivos Institucionales de Seguridad de la Información**

9.1. Proteger, salvaguardar y mantener la confidencialidad, integridad y disponibilidad de la información y los activos de información, respectivamente, garantizando su exactitud, el acceso cuando esta se requiera y mitigando vulnerabilidades que la afecten.

9.2. Incentivar y fortalecer una cultura en seguridad de la información al personal de ESSALUD.

9.3. Asegurar que la información producida, procesada y almacenada sea de propiedad de ESSALUD, estableciendo controles y mecanismos de seguridad de la información.

9.4. Proteger los activos de infraestructura tecnológica, sus plataformas tecnológicas y software institucional que posee ESSALUD para la prestación de sus servicios.

9.5. Asegurar plataformas tecnológicas y sistemas de información auditables; y de acuerdo con su criticidad, se registren y documenten los incidentes relacionados a la seguridad de la información.

9.6. Garantizar la continuidad y cumplimiento de las acciones que permitan planificar, operar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información.

9.7. Establecer mecanismos de control y sanción cuando el dato o información institucional es alterada por cualquier circunstancia.

V°B° Ing. R. SAMEAS Gerente General ESSALUD

[7] Adaptado del numeral 2.89. 2 Términos y definiciones de la ISO/IEC 27000:2014