



Resolución Ministerial

Lima, 31 de Agosto del 2026

Visto, el Expediente N° SEG20250000050, que contiene el Informe N° D000029-2025-SEG-MINSA, el Informe N° D000051-2025-SEG-MINSA, el Informe N° D000013-2026-SEG-MINSA, el Informe N° D000021-2026-SEG-MINSA, y el Memorándum N° D002733-2026-OGTI-MINSA de la Oficina General de Tecnologías de la Información; el Informe N° D000009-2025-DGOS-DIMON-YN-C-MINSA de la Dirección General de Operaciones en Salud; el Informe N° D001390-2025-DIGDOT-DIBAN-MINSA de la Dirección General de Donaciones, Trasplante y Banco de Sangre; el Memorándum N° D001631-2025-DIGEP-MINSA de la Dirección General de Personal de la Salud; el Memorándum N° D000772-2025-DGAIN-MINSA de la Dirección General de Aseguramiento e Intercambio Prestacional, el Memorándum N° D003593-2025-DIGEMID-MINSA de la Dirección General de Medicamentos Insumos y Drogas; el Memorándum N° D004664-2025-DIGTEL-MINSA de la Dirección General de Telesalud, Referencia y Urgencias; el Informe N° 0002-2026-GFMRA de la Dirección General de Gestión de Riesgo de Desastres y Defensa Nacional en Salud; el Informe N° D000116-2025-DIGESA-EA-US-MINSA de la Dirección General de Salud Ambiental e Inocuidad Alimentaria; el Informe N° D000554-2025-OGC-OIP-MINSA y el Informe N° D000445-2025-OGC-OIP-MINSA de la Oficina General de Comunicaciones, el Memorándum N° D003138-2025-OGA-MINSA de la Oficina General de Administración; el Informe N° D000091-2025-OGDESC-APC-MINSA de la Oficina General de Gestión Descentralizada; el Informe N° D000005-2026-CDC-UTI-JCT-MINSA del Centro Nacional de Epidemiología, Prevención y Control de Enfermedades; el Memorándum N° D003525-2025-OGGRH-MINSA de la Oficina General de Gestión de Recursos Humanos; el Informe N° D000219-2025-OGPPM-OOM-MINSA e Informe N° D000221-2025-OGPPM-OPEE-MINSA de la Oficina General de Planeamiento, Presupuesto y Modernización; así como, el Informe N° D000809-2026-OGAJ-MINSA de la Oficina General de Asesoría Jurídica;

CONSIDERANDO:

Que, los numerales I, II y VI del Título Preliminar de la Ley N° 26842, Ley General de Salud, disponen que la salud es condición indispensable del desarrollo humano y medio fundamental para alcanzar el bienestar individual y colectivo, y que la protección de la salud es de interés público, siendo responsabilidad del Estado regularla, vigilarla y promoverla. Asimismo, dispone que es de interés público la provisión de servicios de salud, cualquiera sea



la persona o institución que los provea, siendo responsabilidad del Estado promover las condiciones que garanticen una adecuada cobertura de prestaciones de salud a la población, en términos socialmente aceptables de seguridad, oportunidad y calidad;

Que, el numeral XIV del Título Preliminar de la Ley N° 26842, Ley General de Salud, establece que la información en salud es de interés público y que toda persona está obligada a proporcionar a la Autoridad de Salud la información que le sea exigible de acuerdo a ley. La información que el Estado tiene en su poder es de dominio público, con las excepciones que establece la ley;

Que, asimismo, el artículo 123 de la Ley N° 26842, modificado por la Única Disposición Complementaria Modificatoria del Decreto Legislativo N° 1161, Ley de Organización y Funciones del Ministerio de Salud, precisa que el Ministerio de Salud es la Autoridad de Salud de nivel nacional. Como Organismo del Poder Ejecutivo, tiene a su cargo la formulación, dirección y gestión de la política de salud y actúa como la máxima autoridad normativa en materia de salud;

Que, el numeral 9) del artículo 3 del Decreto Legislativo N° 1161, Ley de Organización y Funciones del Ministerio de Salud, señala que el Ministerio de Salud tiene como ámbito de competencias a la Investigación y tecnologías en salud;

Que, el artículo 4 del Decreto Legislativo N° 1161, Ley de Organización y Funciones del Ministerio de Salud y sus modificatorias, establece que el Sector Salud está conformado por el Ministerio de Salud, como organismo rector, las entidades adscritas a él y aquellas instituciones públicas y privadas de nivel nacional, regional y local, y las personas naturales que realizan actividades vinculadas a las competencias establecidas en dicha Ley, y que tienen impacto directo o indirecto en la salud, individual o colectiva;

Que, los sub numerales 4-A1 y 4-A2 del artículo 4 del antes citado Decreto Legislativo, modificado por el Decreto Legislativo N° 1504, Decreto Legislativo que fortalece al Instituto Nacional de Salud para la prevención y control de las enfermedades, refiere que, la potestad rectora del Ministerio de Salud comprende la facultad que tiene para normar, supervisar, fiscalizar y, cuando corresponda, sancionar, en los ámbitos que comprenden la materia de salud. La rectoría en materia de salud dentro del sector la ejerce el Ministerio de Salud por cuenta propia o, por delegación expresa, a través de sus organismos públicos adscritos y, dentro del marco y los límites establecidos en la dicha Ley, la Ley Orgánica del Poder Ejecutivo, las normas sustantivas que regulan la actividad sectorial y, las normas que rigen el proceso de descentralización; Asimismo, el Ministerio de Salud, ente rector del Sistema Nacional de Salud, y dentro del ámbito de sus competencias, determina la política, regula y supervisa la prestación de los servicios de salud, a nivel nacional, en las siguientes instituciones: Essalud, Sanidad de la Policía Nacional del Perú, Sanidad de las Fuerzas Armadas, instituciones de salud del gobierno nacional y de los gobiernos regionales y locales, y demás instituciones públicas, privadas y público-privadas.

Que, el literal h) del artículo 5 del precitado Decreto Legislativo, establece como una de las funciones rectoras del Ministerio de Salud, dictar normas y lineamientos técnicos para la adecuada ejecución y supervisión de la política nacional y políticas sectoriales de salud, la gestión de los recursos del sector, así como para el otorgamiento y reconocimiento de derechos, fiscalización, sanción y ejecución coactiva en las materias de su competencia;

Que, los artículos 1, 3 y 9 de la Ley N° 29733, Ley de Protección de Datos Personales, establecen que la Ley tiene el objeto de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su tratamiento adecuado, en un marco de respeto de los demás derechos





Resolución Ministerial

Lima, 31 de Agosto del 2026

fundamentales que en ella se reconocen; que la Ley es de aplicación a los datos personales contenidos o destinados a ser contenidos en bancos de datos personales de administración pública y de administración privada, cuyo tratamiento se realiza en el territorio nacional. Siendo objeto de especial protección los datos sensibles, datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos; opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual; precisando además que, el titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser preparadas y acordadas con el tratamiento que se vaya a efectuar y con la categoría de datos personales que se trate;

Que, mediante Decreto de Urgencia N° 006-2020, se aprueba el Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital, cuyo numeral 4) del artículo 5 establece que el referido sistema tiene como finalidad fortalecer el acceso y la inclusión a las tecnologías digitales en el país y la confianza digital fomentando la seguridad, transparencia, protección de datos personales y gestión ética de las tecnologías en el entorno digital para la sostenibilidad, prosperidad, bienestar social y económico del país;

Que, mediante Decreto de Urgencia N° 007-2020, se emite el Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, el cual, en el artículo 1, señala que tiene por objeto establecer las medidas que resultan necesarias para garantizar la confianza de las personas en su interacción con los servicios digitales prestados por entidades públicas y organizaciones del sector privado en el territorio nacional. De esta manera, el literal e) del artículo 3 del precitado Decreto de Urgencia define al incidente de seguridad digital como aquel evento o serie de eventos que pueden comprometer la confianza, la prosperidad económica, la protección de las personas y sus datos personales, la información, entre otros activos de la organización, a través de tecnologías digitales;

Que, el artículo 1 del Decreto Legislativo N° 1412, "Decreto Legislativo que aprueba la Ley de Gobierno Digital", establece el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso



M. CUBA



C. ESPINOZA



B. OSTOS



L. HILDEBRANT P.



A. CASPECH



M. MARAVI



M. DIAZ



D. GESA



J. F. OCHOA



J. GUTIERREZ



C. ALVARADO



F. ORTIZ



C. ROJAS J.



J. MUÑOCH



J. CUADROS M.



R. ROJAS



S. ESTRELLA



L. ZENAZ



transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública, en los tres niveles de gobierno;

Que, asimismo el artículo 30 del precitado Decreto Legislativo define la Seguridad Digital como el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas;

Que, el numeral 94.2 del artículo 94 del Decreto Supremo N° 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N° 1412, establece que el Marco de Seguridad Digital del Estado Peruano integra aquellas normas que conforman los ámbitos de defensa, inteligencia, justicia e institucional, establecidos en el artículo 32 de la Ley y se articula y sustenta en la normas, procesos, roles, responsabilidades y mecanismos regulados e implementados a nivel nacional en materia de Seguridad de la Información. La seguridad digital es un ámbito del Marco de Confianza Digital establecido en el Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento;

Que, la Resolución Directoral N° 022-2022-INACAL/DN, aprueba entre otras, la Norma Técnica Peruana NTP-ISO/IEC ISO 27001:2022 de Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3ª Edición, que Reemplaza a la NTP-ISO/IEC 27001:2014, la cual tiene como objeto especificar los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización;

Que, la Norma Técnica Peruana NTP-ISO/IEC ISO 27001:2022, en su numeral 5.2, establece que la alta dirección debe establecer una política de seguridad de la información que sea apropiada al propósito de la organización, que incluya objetivos de seguridad de la información o proporcione el marco de referencia para fijar los objetivos de seguridad de la información, así como que incluya el compromiso de satisfacer los requisitos aplicables relacionados a la seguridad de la información; y, el compromiso de mejora continua del sistema de gestión de seguridad de la información. Del mismo modo, establece que la política de seguridad de la información debe estar disponible como información documentada, ser comunicada dentro de la organización; y, estar disponible a las partes interesadas, según corresponda;

Que, el numeral 4.1 del artículo 4 de la Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD, que establece la implementación y mantenimiento del sistema de gestión de seguridad de la información en las entidades públicas, dispone que, el Titular de la entidad pública es responsable de la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), para lo cual, como mínimo, debe aprobar las políticas y objetivos para implementar, operar, mantener y mejorar el referido sistema;

Que, el artículo 52 del Reglamento de Organización y Funciones del Ministerio de Salud, aprobado por Decreto Supremo N° 008-2017-SA y modificatorias, establece que la Oficina General de Tecnologías de la Información es el órgano de apoyo del Ministerio de Salud, responsable de implementar el gobierno electrónico; planificar, implementar y gestionar los sistemas de información del Ministerio; administrar la información estadística y científica en salud del Sector Salud; realizar la innovación y el desarrollo tecnológico, así como del soporte de los equipos informáticos del Ministerio de Salud. Asimismo, es responsable de establecer soluciones tecnológicas, sus especificaciones, estándares; diseñar, desarrollar y mejorar las





Resolución Ministerial

Lima, 31 de Agosto del 2026

plataformas informáticas de información en el Sector Salud. Asimismo, establece requerimientos técnicos para la adquisición, aplicación, mantenimiento y uso de soluciones tecnológicas, en el ámbito de competencia del Ministerio de Salud;

Que, asimismo, los literales a) y c) del artículo 53 del Decreto Supremo N° 008-2017-SA y modificatorias, establecen que son funciones de la Oficina General de Tecnologías de la información, proponer y supervisar la implementación de políticas, normas, lineamientos, planes, estrategias, programas y proyectos en materia de desarrollo de tecnologías de la información, estadística y gestión de la información; gobierno electrónico y su operatividad; así como políticas de seguridad de tecnologías de la información y comunicación del Ministerio de Salud, para asegurar la integridad, confidencialidad y disponibilidad de la misma en el marco de la normativa vigente. De igual forma, promover el desarrollo tecnológico de la información y comunicación para servicios y trámites de calidad de los ciudadanos;

Que, la Resolución Ministerial N° 431-2015-MINSA, que aprueba el Documento Técnico "Política de Seguridad de la Información del Ministerio de Salud – MINSA", fue formulada en cumplimiento de los parámetros de la Norma Técnica Peruana ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2da edición. Por lo que, en atención a los cambios normativos emitidos, a la fecha, referidos a la gestión de seguridad de la información, se hace necesaria la derogación del referido documento técnico;

Que, en dicho contexto, la Oficina General de Tecnologías de la Información en el marco de sus funciones de conformidad con lo dispuesto en el Reglamento de Organización y Funciones del Ministerio de Salud, ha elaborado el Documento Técnico: Lineamientos de Política de Seguridad de la Información y Ciberseguridad del Ministerio de Salud, con la finalidad de contribuir con la protección de los activos de información del Ministerio de Salud, garantizando su confidencialidad, integridad y disponibilidad, para acelerar la transformación digital del sector salud; en concordancia con los principios en materia de gobierno digital, protección de datos personales y transformación digital del sector salud; tomando como base, la normativa vigente, en materia de seguridad y confianza digital;

Con el visado de la Oficina General de Tecnologías de la Información; de la Dirección General de Operaciones en Salud; de la Dirección General de Donaciones, Trasplante y Banco





de Sangre; de la Dirección General de Personal de la Salud; de la Dirección General de Aseguramiento e Intercambio Prestacional, de la Dirección General de Medicamentos Insumos y Drogas; de la Dirección General de Telesalud, Referencia y Urgencias; de la Dirección General de Gestión de Riesgo de Desastres y Defensa Nacional en Salud; de la Dirección General de Salud Ambiental e Inocuidad Alimentaria; de la Oficina General de Administración; de la Oficina General de Comunicaciones; de la Oficina General de Gestión Descentralizada;; del Centro Nacional de Epidemiología, Prevención y Control de Enfermedades; de la Oficina General de Gestión de Recursos Humanos; de la Oficina General de Planeamiento, Presupuesto y Modernización; de la Oficina General de Asesoría Jurídica; de la Secretaría General; del Despacho Viceministerial de Salud Pública; y del Despacho Viceministerial de Prestaciones y Aseguramiento en Salud;

De conformidad con lo dispuesto en la Ley N° 29733, Ley de Protección de Datos Personales; el Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital, Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento; el Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital; el Decreto Legislativo N° 1161, Ley de Organización y Funciones del Ministerio de Salud y sus modificatorias; el Reglamento de Organización y Funciones del Ministerio de Salud, aprobado mediante Decreto Supremo N° 008-2017-SA, y modificatorias; así como, la Resolución Directoral N° 022-2022-INACAL/DN, que aprueba entre otras, la Norma Técnica Peruana NTP-ISO/IEC ISO 27001:2022 de Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. 3ra Edición;

SE RESUELVE:

Artículo 1.- Aprobar el Documento Técnico: Lineamientos de Política de Seguridad de la Información y Ciberseguridad del Ministerio de Salud, que como anexo adjunto forma parte integrante de la presente Resolución Ministerial.

Artículo 2.- Encargar a la Oficina General de Tecnologías de la Información que efectúe la difusión, implementación, supervisión y asistencia técnica del Documento Técnico que se aprueba mediante la presente Resolución Ministerial.

Artículo 3.- Dejar sin efecto la Resolución Ministerial N° 431-2015/MINSA que aprueba el Documento Técnico "Política de Seguridad de la Información del Ministerio de Salud - MINSA".

Artículo 4.- Disponer la publicación de la presente Resolución Ministerial en el Diario Oficial El Peruano y encargar a la Oficina de Transparencia y Anticorrupción de la Secretaría General la publicación de la presente Resolución Ministerial y su anexo en la sede digital del Ministerio de Salud (www.gob.pe/minsa), en el mismo día de su publicación en el Diario Oficial El Peruano.

Regístrese, comuníquese y publíquese.

LUIS WILLIAMS DYER FERNÁNDEZ
Ministro de Salud



DOCUMENTO TÉCNICO:

**LINEAMIENTOS DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD DEL MINISTERIO DE SALUD**



DOCUMENTO TÉCNICO:
LINEAMIENTOS DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD DEL
MINISTERIO DE SALUD

ÍNDICE

ÍNDICE	2
I. INTRODUCCIÓN	3
II. FINALIDAD	4
III. OBJETIVO	4
IV. ÁMBITO DE APLICACIÓN.....	4
V. BASE LEGAL.....	4
VI. CONTENIDO.....	5
VII. RESPONSABILIDADES	19
VIII. BIBLIOGRAFÍA	19



I. INTRODUCCIÓN

Con el avance de las tecnologías de la información y la digitalización de los procesos institucionales; los activos de información (que incluyen información o elemento relacionado con el tratamiento de la misma que tenga valor para la entidad), están cada vez más expuestos a diversos riesgos. Estos riesgos pueden originarse por errores humanos, fallos técnicos, accesos no autorizados, ataques cibernéticos, y otros incidentes deliberados de seguridad.

La seguridad de la información y la ciberseguridad se convierten en pilares estratégicos para proteger los activos de información, considerando su confidencialidad, integridad, disponibilidad, trazabilidad y resiliencia. La seguridad de la información y la ciberseguridad no solo se implementan por necesidades operativas, sino en cumplimiento de la legislación vigente, como la Ley N° 29733, Ley de Protección de Datos Personales, el Decreto Legislativo 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital; el Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital; el Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el marco de confianza digital; y dispone medidas para su fortalecimiento. Además, se deben implementar los requisitos de seguridad establecidos en la Norma Técnica Peruana NTP ISO/IEC 27001:2014 aprobada mediante Resolución Ministerial N° 004-2016-PCM y su actualización.

El literal a) del artículo 105, del 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, establece que las entidades públicas deben implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI). El numeral 1.1 del artículo 1 de la Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD reafirma la obligatoriedad de esta implementación en las entidades públicas

Complementariamente, la norma NTP ISO/IEC 27001:2022 vigente regula el análisis, diseño, implementación, operación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (en adelante, SGSI). En su numeral 5.2 establece como requisito la implementación y difusión de una Política de Seguridad de la Información que debe:

- a) Ser apropiada al propósito de la organización;
- b) Proporcionar el marco de referencia para fijar los objetivos de seguridad de la información;
- c) Incluir el compromiso de satisfacer los requisitos aplicables relacionados a la seguridad de la información;
- d) Incorporar el compromiso de mejora continua del sistema de gestión de seguridad de la información.
- e) Estar disponible como información documentada;
- f) Ser comunicada dentro de la organización;
- g) Estar disponible a las partes interesadas, según corresponda.



DOCUMENTO TÉCNICO:
LINEAMIENTOS DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD DEL
MINISTERIO DE SALUD

II. FINALIDAD

Contribuir con la protección de los activos de información del Ministerio de Salud - MINSA, garantizando su confidencialidad, integridad y disponibilidad, para acelerar la transformación digital del sector salud.

III. OBJETIVO

Establecer los lineamientos de política de seguridad de la información y ciberseguridad del MINSA.

IV. ÁMBITO DE APLICACIÓN

El presente documento técnico es de aplicación obligatoria para todos los órganos y unidades orgánicas de la Unidad Ejecutora N° 001 Administración Central - MINSA; y para las Instituciones Prestadoras de Servicios de Salud que hacen uso de los Sistemas de Información puestos a disposición por el MINSA; así como para las personas naturales y jurídicas que le prestan servicios al MINSA, en lo que les corresponda.

V. BASE LEGAL

- 5.1 Ley N° 25323, Ley de creación del Sistema Nacional de Archivos.
- 5.2 Ley N° 27269, Ley de Firmas y Certificados Digitales.
- 5.3 Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública.
- 5.4 Ley N° 28716, Ley de Control Interno de las Entidades del Estado.
- 5.5 Ley N° 29733, Ley de Protección de Datos Personales y su modificatoria.
- 5.6 Ley N° 31572, Ley del Teletrabajo.
- 5.7 Decreto Legislativo N° 1161, Decreto Legislativo que aprueba la Ley de Organización y Funciones del Ministerio de Salud, y sus modificatorias.
- 5.8 Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
- 5.9 Decreto de Urgencia N° 006-2020-PCM, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.
- 5.10 Decreto de Urgencia N° 007-2020-PCM, Decreto de Urgencia que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento.
- 5.11 Decreto Supremo N° 008-92-JUS, Decreto Supremo que aprueba el Reglamento de la Ley N° 25323, que crea el Sistema Nacional de Archivos.
- 5.12 Decreto Supremo N° 052-2008-PCM, Decreto Supremo que aprueba el Reglamento de la Ley de Firmas y Certificados Digitales.
- 5.13 Decreto Supremo N° 008-2017-SA, Decreto Supremo que aprueba el Reglamento de Organización y Funciones del Ministerio de Salud y modificatorias.
- 5.14 Decreto Supremo N° 050-2018-PCM, Decreto Supremo que establece la definición de Seguridad Digital de ámbito nacional.
- 5.15 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.
- 5.16 Decreto Supremo N° 029-2021-PCM, Decreto Supremo que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones,



DOCUMENTO TÉCNICO:
LINEAMIENTOS DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD DEL
MINISTERIO DE SALUD

requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo

- 5.17 Decreto Supremo N° 002-2023-TR, Decreto Supremo que aprueba el Reglamento de la Ley N° 31572, Ley del Teletrabajo.
- 5.18 Decreto Supremo N° 007-2024-JUS, Decreto Supremo que aprueba el Reglamento de la Ley de Transparencia y Acceso a la Información Pública.
- 5.19 Decreto Supremo N° 085-2023-PCM, Decreto Supremo que aprueba la Política Nacional de Transformación Digital al 2030.
- 5.20 Decreto Supremo N° 016-2024-JUS, Decreto Supremo que aprueba el Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales.
- 5.21 Resolución Ministerial N° 074-2017/MINSA, que aprueba la Directiva Administrativa N° 227-MINSA/2017/OGTI, Directiva Administrativa de Organización del Sistema de Gestión de Seguridad de la Información del Ministerio de Salud.
- 5.22 Resolución Ministerial N° 166-2017- PCM, que modifica el artículo 5 de la Resolución Ministerial N° 004-2016-PCM
- 5.23 Resolución Ministerial N° 119-2018-PCM, que dispone la creación de un Comité de Gobierno Digital en cada entidad de la Administración Pública.
- 5.24 Resolución Ministerial N° 087-2019-PCM, que aprueba disposiciones sobre la conformación y funciones del Comité de Gobierno Digital.
- 5.25 Resolución Ministerial N° 688-2020-MINSA, que aprueba la Directiva Administrativa N° 294-MINSA/2020/OGTI, Directiva Administrativa que establece el tratamiento de los datos personales relacionados con la salud o datos personales en salud.
- 5.26 Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/SGTD, que aprueba la Directiva N° 001-2023-PCM/SGTD, Directiva que establece el perfil y responsabilidades del Oficial de Seguridad y Confianza Digital.
- 5.27 Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD, que establece la implementación y mantenimiento del Sistema De Gestión de Seguridad de la Información en las entidades públicas.
- 5.28 Resolución Secretarial N° D000147-2025-SG-MINSA, que crea la Unidad Funcional de Seguridad Digital dependiente de la Oficina General de Tecnologías de la Información.
- 5.29 Resolución Directoral N° 022-2022-INACAL/DN, que aprueba Normas Técnicas Peruanas sobre turismo, acuicultura y otros.

VI. CONTENIDO

6.1. DEFINICIONES OPERATIVAS

- 6.1.1 **Acceso a la información pública:** Es el derecho que tiene toda persona de buscar, recibir y difundir información que obra en poder del Estado.
- 6.1.2 **Activo de información crítico:** Es la información que considerando su confidencialidad, integridad y disponibilidad; se determina como indispensable y que debe ser custodiada permanentemente, para la continuidad operativa del proceso en que se utiliza.
- 6.1.3 **Activo de información:** Es cualquier Información o elemento relacionado con su tratamiento (software, equipo de cómputo y telecomunicaciones, servicio de correo electrónico, servicio de internet, archivadores, entre otros) que tiene valor para la entidad, en este caso el MINSA



DOCUMENTO TÉCNICO:
LINEAMIENTOS DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD DEL
MINISTERIO DE SALUD

- 6.1.4 Amenaza:** Es la causa potencial de un incidente de seguridad no deseado, que puede resultar en daño a un sistema u entidad, en este caso el MINSA.
- 6.1.5 Bloqueo:** Es la medida que consiste en la identificación y reserva de los datos personales adoptando medidas técnicas y organizativas para impedir su tratamiento, incluyendo su visualización, durante el periodo en que se esté procesando alguna solicitud de actualización, inclusión, rectificación o supresión.
- 6.1.6 Ciberseguridad:** Es la 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.
- 6.1.7 Código fuente:** Es un archivo o conjunto de archivos que contienen el código escrito en un lenguaje de programación de un sistema de información o aplicativo informático.
- 6.1.8 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 y la transformación digitales. 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.
- 6.1.9 Confidencialidad:** Es la característica de la información por la cual se requiere o exige que el acceso y tratamiento de la misma, sea realizado por personas, entidades y/o procesos debidamente autorizados.
- 6.1.10 Controles de seguridad de la información:** Son medidas organizacionales, físicas y tecnológicas que permiten mitigar el riesgo de que se vulnere la confidencialidad, integridad y disponibilidad de los activos de información
- 6.1.11 Datos personales:** Es la información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados. Comprende aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, de localización, identificadores en línea o de cualquier otro tipo concerniente a aspectos físicos, económicos, culturales o sociales de las personas naturales que las identifica o las hace identificables. Se considera identificable cuando se puede verificar la identidad de la persona de manera directa o indirectamente a partir de la combinación de datos a través de medios que puedan ser razonablemente utilizados.
- 6.1.12 Datos sensibles:** Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos; opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; información relativa a los datos genéticos, datos neuronales, datos morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponden a la esfera más íntima; e información relacionada a la salud física o mental, a la vida sexual u otras análogas que afecten su intimidad.



DOCUMENTO TÉCNICO:
LINEAMIENTOS DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD DEL
MINISTERIO DE SALUD

- 6.1.13 Disponibilidad:** Es la característica de la información de estar accesible cuando y donde lo requiera una persona, entidad o proceso.
- 6.1.14 Documento archivístico:** Documento producido (recibido o emitido) en el ejercicio de una función, procedimiento, actividad, tarea o acción por persona natural, pública o privada, contiene información de cualquier fecha, forma, soporte físico y cualquier otro que se genere como resultado del avance tecnológico. Entiéndase también como documento de archivo.
- 6.1.15 Incidente de Seguridad de la Información:** Es un evento singular o serie de eventos de seguridad de la información, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones del negocio, la confianza, la prosperidad económica, la protección de las personas y sus datos personales, otros activos de información y de amenazar la seguridad de la información.
- 6.1.16 Integridad:** Es la característica de la información de ser exacta y completa.
- 6.1.17 Interoperabilidad:** La Interoperabilidad es la capacidad de interactuar que tienen las organizaciones diversas y dispares para alcanzar objetivos que hayan acordado conjuntamente, recurriendo a la puesta en común de información y conocimientos, a través de los procesos y el intercambio de datos entre sus respectivos sistemas de información.
- 6.1.18 Marco de Confianza Digital:** Se constituye en el conjunto de principios, modelos, políticas, normas, procesos, roles, personas, empresas, entidades públicas, tecnologías y estándares mínimos que permiten asegurar y mantener la confianza en el entorno digital.
- 6.1.19 Proceso:** Es el conjunto de actividades mutuamente relacionadas que interactúan y que agregan valor, las cuales transforman elementos de entrada en productos.
- 6.1.20 Propietario de Activo de información:** Es la unidad de organización o usuario responsable de definir el tratamiento y protección de un activo de información. Evalúa qué tan crítico es el activo de información, gestiona sus riesgos de seguridad asociados a fin de implementar los controles de seguridad para proteger su confidencialidad, integridad y disponibilidad.
- 6.1.21 Riesgo de seguridad digital:** Efecto de la incertidumbre relacionada con el uso, desarrollo y gestión de las tecnologías digitales y datos, en el curso de cualquier actividad. Resulta de la combinación de amenazas y vulnerabilidades en el entorno digital y es de naturaleza dinámica. Puede socavar el logro de los objetivos económicos y sociales al alterar la confidencialidad, integridad y disponibilidad de las actividades o el entorno, así como poner en riesgo la protección de la vida privada de las personas. Incluye aspectos relacionados con los entornos físicos y digitales, las actividades críticas, las personas y organizaciones involucradas en la actividad y los procesos organizacionales que la respaldan.
- 6.1.22 Router:** Es un dispositivo de red que interconecta diferentes redes informáticas, como la red de tu casa y la conexión a Internet de tu proveedor, y se encarga de dirigir y enviar el tráfico de datos entre ellas para que tus dispositivos



DOCUMENTO TÉCNICO:
LINEAMIENTOS DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD DEL
MINISTERIO DE SALUD

tecnológicos (ordenadores, móviles, etc.) puedan comunicarse y acceder a Internet, ya sea por cable (Ethernet) o de forma inalámbrica (Wi-Fi).

- 6.1.23 Seguridad de la información:** Concepto asociado al conjunto de medidas que las organizaciones adoptan para la preservación de la confidencialidad, Integridad y disponibilidad de la información, considerando tanto la información contenida en medios manuales o automatizados.
- 6.1.24 Servicio digital:** Es aquel servicio provisto de forma total o parcial a través de Internet u otras redes equivalentes, que se caracteriza por ser parcial o totalmente automatizado y utilizar de manera intensiva las tecnologías digitales y datos, permitiendo, al menos una de las siguientes prestaciones: i) Adquirir un bien, servicio, información o contenido, ii) Buscar, compartir, usar y acceder a datos, contenido o información sobre productos, servicios o personas, iii) Pagar un servicio o bien (tangible o intangible) y, iv) El relacionamiento entre personas.
- 6.1.25 Sistema de Información:** Es el concepto asociado al conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes que interactúan para el tratamiento y administración de datos e información generada que debe cubrir una necesidad o un objetivo, así como estar organizada y disponible para su uso posterior.
- 6.1.26 Sistema de Gestión de Seguridad de la Información (SGSI):** Comprende el conjunto de políticas, lineamientos, procedimientos, recursos y actividades asociadas, que gestiona una entidad con el propósito de proteger sus activos de información, de manera independiente del soporte en que estos se encuentren. Asimismo, contempla la gestión de riesgos e incidentes de seguridad de la información y seguridad digital, la implementación efectiva de medidas de ciberseguridad, y acciones de colaboración y cooperación.
- 6.1.27 Software:** Son componentes lógicos necesarios para hacer posible la realización de funciones y tareas específicas por parte de los equipos informáticos o de telecomunicaciones.
- 6.1.28 Teletrabajo:** Es la modalidad especial de prestación de labores. Se caracteriza por el desempeño subordinado de aquellas labores que no requieren presencia física del trabajador o servidor civil en el centro de trabajo, con la que mantiene vínculo laboral. Se realiza a través de la utilización de las plataformas y tecnologías digitales. Se consideran todas las formas de trabajo fuera de la oficina, incluyendo los ambientes de trabajo no tradicionales, tales como los ambientes denominados "trabajo a distancia", "trabajo flexible", "trabajo remoto" y "trabajo virtual".
- 6.1.29 Unidad de organización:** Es la forma genérica que se usa para mencionar a los órganos, unidades orgánicas, entre otros afines.
- 6.1.30 Usuario:** Es toda persona, sea funcionario o servidor público, consultor, practicante, u otro, sin importar el régimen laboral o de contratación al que esté sujeto, que ha sido debidamente autorizado para el uso de uno o varios servicios informáticos del MINSA.



6.2. ACRÓNIMOS

- API : Interfaz de Programación de Aplicaciones (por sus siglas en inglés)
- HL7 FHIR: Health Level Seven - Fast Health Interoperability Resources
- MINSA : Ministerio de Salud.
- NTP : Norma Técnica Peruana.
- OGTI : Oficina General de Tecnologías de la Información del MINSA.
- PIDE : Plataforma de Interoperabilidad del Estado (PIDE).
- SGSI : Sistema de Gestión de Seguridad de la Información.
- SSID : Identificador del conjunto de servicios (por sus siglas en inglés)
- VPN : Red privada virtual (por sus siglas en inglés)

6.3. PRINCIPIOS

La Política de Seguridad de la Información y ciberseguridad del MINSA se sustenta en los siguientes principios:

- **Principio de Confidencialidad:** Garantiza que la información sea accesible únicamente para aquellas personas autorizadas a tener acceso a la misma.
- **Principio de Integridad:** Salvaguarda la exactitud y la totalidad de la información y los métodos de procesamiento.
- **Principio de Disponibilidad:** Garantiza que los usuarios autorizados tengan accesos a la información y los recursos correspondientes, conforme a los privilegios asignados y bajo las políticas establecidas, garantizando disponibilidad íntegra y oportuna en función de la demanda.
- **Principio de no repudio:** Evita que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o no la recibió.
- **Principio de auditabilidad:** Asegura que los eventos generados por un sistema sean registrados para su monitoreo y control posterior.
- **Principio de Legalidad:** Garantiza el cumplimiento de las leyes, reglamentaciones y demás disposiciones normativas a las que está sujeta la entidad.
- **Principio de Calidad:** Salvaguarda la veracidad, exactitud y actualización de la información que administra.
- **Principio de Seguridad:** Adopta las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos y de la información.
- **Principio de concientización y formación:** Asegura la ejecución de acciones de formación, sensibilización y concientización en seguridad de la información a los usuarios para fortalecer la cultura de seguridad de la información.
- **Principio de responsabilidad:** Todas y todos los usuarios son responsables de su conducta en cuanto a la seguridad de la información, ciñéndose estrictamente a las normas legales vigentes y a los controles establecidos.
- **Principio de mejora continua:** Revisa la eficacia de los controles de seguridad establecidos e implementados, a fin de que estos sigan respondiendo a los cambios y a la constante evolución del riesgo y del entorno tecnológico.



6.4. FUNCIONES CLAVES EN CIBERSEGURIDAD

El MINSA debe implementar un marco de ciberseguridad compuesto por las siguientes funciones claves:

- **Identificar:** Amenazas, vulnerabilidades y activos de información clave con potencial impacto en la entrega y operación de los servicios digitales del MINSA.
- **Proteger:** Sistemas de información que resguardan la atención médica, la información clínica y los servicios de salud.
- **Detectar:** Eventos de ciberseguridad (posible violación de la ciberseguridad) de manera oportuna.
- **Responder:** Atender oportunamente los incidentes de seguridad, con el propósito de minimizar el impacto sobre los sistemas de información que soportan las operaciones del MINSA.
- **Recuperar:** Los sistemas de información afectados con procedimientos seguros y planificados.
- **Coordinar:** Con otros actores institucionales una respuesta articulada.
- **Trazabilidad:** En cada acción digital para garantizar transparencia, rendición de cuentas y aprendizaje institucional.

6.5. LINEAMIENTOS DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD DEL MINSA

El MINSA, como Autoridad Nacional de Salud y ente rector del Sistema Nacional de Salud, declara su compromiso con la protección integral de la información institucional y de los datos personales que gestiona, se compromete además con incorporar las mejores prácticas de seguridad de la información y ciberseguridad, orientadas a la protección de la confidencialidad, la integridad, la disponibilidad y la resiliencia frente a amenazas internas y externas, así como a los riesgos de seguridad digital que pudieran materializarse en el MINSA - Administración Central, y en las IPRESS que utilizan los sistemas de información que administra.

Respecto a la seguridad de la información, el MINSA a través de la OGTI, establece, implementa, mantiene y mejora continuamente el Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma técnica peruana NTP ISO/IEC 27001 vigente, con el objetivo de fortalecer la confianza en sus servicios digitales, salvaguardar los derechos de los ciudadanos, asegurar la continuidad operativa de los sistemas de información prioritarios del MINSA y promover una cultura de seguridad y ciberseguridad en todo el ámbito de aplicación del presente documento técnico.

El MINSA a través de OGTI, reconoce en la ciberseguridad una condición fundamental para garantizar el derecho a la salud, proteger la vida y promover el bienestar de las personas, por lo que promueve el uso de sistemas digitales seguros y de la generación de marcos de confianza pública, desde un enfoque de colaboración multisectorial.

El MINSA establece los siguientes lineamientos en materia de seguridad de la información y ciberseguridad:



DOCUMENTO TÉCNICO:
LINEAMIENTOS DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD DEL
MINISTERIO DE SALUD

- Establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información, conforme a la norma técnica peruana NTP ISO/IEC 27001 en la versión vigente y a las otras normas aplicables.
- Gestionar los riesgos de seguridad de la información y de la ciberseguridad, mediante la identificación, análisis, evaluación y tratamiento de los riesgos que puedan afectar los servicios digitales y los derechos de los ciudadanos.
- Promover una cultura de seguridad de la información y de la ciberseguridad, haciendo énfasis en que los usuarios conozcan sus responsabilidades y reciban capacitación periódica.
- Proteger los datos personales que trate, conforme a la Ley N° 29733 Ley de Protección de Datos Personales y su modificatoria, su norma reglamentaria, aprobada con Decreto Supremo N° 016-2024-JUS y a las demás normas complementarias.
- Asegurar la continuidad de los servicios prioritarios para la operación, mediante controles técnicos, organizativos, así como planes de contingencia y recuperación ante incidentes de seguridad digital y ciberseguridad.
- Velar por el cumplimiento normativo y contractual relacionado con la seguridad de la información y de la ciberseguridad, incluyendo a los proveedores.
- Mejorar de forma continua en lo concerniente a la ciberseguridad institucional, garantizando que los avances tecnológicos están acompañados de controles efectivos y de capacidades humanas adecuadas para prevenir y mitigar riesgos de seguridad digital.
- Cumplir con los requisitos que resulten aplicables sobre confianza digital, interoperabilidad segura, protección de datos y cumplimiento normativo.
- Adoptar medidas técnicas y organizativas para asegurar la resiliencia de los sistemas y de los servicios digitales que sustentan la atención y la gestión en salud.
- Establecer mecanismos de reporte y comunicación efectiva de incidentes de seguridad digital al Centro Nacional de Seguridad Digital.
- Fomentar la capacitación y la sensibilización de los usuarios como línea de defensa activa contra los riesgos de seguridad de la información y de la ciberseguridad.
- Exigir a terceros y proveedores tecnológicos el cumplimiento de estándares de ciberseguridad reconocidos internacionalmente, así como el cumplimiento de las obligaciones de confidencialidad y de seguridad, establecidas en la Ley N° 29733 Ley de Protección de Datos Personales y su modificatoria y en su reglamento o la norma que la subrogue o modifique.
- Garantizar la trazabilidad de las acciones digitales para fines de auditoría, investigación y mejora continua.
- Establecer mecanismos formales para la comunicación controlada de la Política de Seguridad de la Información y Ciberseguridad, así como de los resultados generales del SGSI.

6.6. PRINCIPALES CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

El MINSA establece los principales controles de seguridad para el Sistema de Gestión de Seguridad de la Información y de la Ciberseguridad que deben ser usados por todos sus órganos, unidades orgánicas, así como por las Instituciones Prestadoras de Servicios de Salud que hacen uso de los Sistemas de Información puestos a disposición por el MINSA; así como para las personas



J. GUTIERREZ

DOCUMENTO TÉCNICO:
LINEAMIENTOS DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD DEL
MINISTERIO DE SALUD

naturales y jurídicas que le prestan servicios. Estos controles de seguridad de la información se encuentran agrupados en ocho (08) secciones, tal como sigue:

A. Control de Accesos

- Todo acceso debe otorgarse bajo el principio de mínimo privilegio ("todo está prohibido a menos que esté expresamente permitido"), aplicando los criterios de necesidad de saber y de necesidad de uso.
- El acceso debe basarse en los roles y las funciones asignadas a los usuarios con vínculo laboral o contractual vigente.
- Todo acceso es individual, autenticado y trazable.
- Toda solicitud de acceso debe ser atendida conforme al plazo definido por la unidad de organización competente.

A.1. Otorgamiento, modificación y revocación de accesos

- El acceso se otorga, modifica o revoca mediante un proceso formal, documentado y autorizado, que inicia con una solicitud del área usuario líder y se concreta con la aprobación de la Oficina General de Tecnologías de la Información.
- La autorización de acceso debe ser emitida por la unidad de organización (propietario de activo de la información) o de quien ésta designe, en función del nivel de clasificación de la información y de las funciones asignadas al usuario.
- El registro de las solicitudes y de las autorizaciones de accesos debe conservarse conforme a lo establecido en la Directiva N° 001-2023-AGN/DDPA denominada "Norma de administración de archivos en las entidades públicas", aprobada con Resolución Jefatural N° 000107-2023-AGN/JEF y su modificatoria o las que haga sus veces o sustituya.

A.2. Credenciales y responsabilidad del usuario

- Las credenciales son personales e intransferibles; el usuario es responsable de su custodia y uso adecuado.
- Está prohibido compartir contraseñas, instalar software con o sin licencia, instalar dispositivos o conectar equipos sin la autorización expresa de la OGTI.
- La OGTI o la que haga sus veces es la única autorizada para instalar el software, el hardware o las herramientas que impliquen intervención en equipos y usuarios, previa presentación de la solicitud formal correspondiente.
- Permitir a los usuarios cambiar su contraseña cuando lo requieran.

A.3. Control y configuración de accesos

- Establecer normas y configuraciones técnicas para el control de accesos a activos de información, plataformas y servicios informáticos.
- Todo acceso remoto a la red institucional se realiza únicamente a través del VPN seguro suministrado por el MINSA, debidamente aprobado, registrado y auditado.
- Queda restringido el acceso remoto, mediante el VPN, para los usuarios que desarrollan funciones bajo la modalidad de teletrabajo desde el extranjero, con el fin de garantizar la protección de la información institucional y reducir los riesgos de seguridad de la información y ciberseguridad asociados a accesos remotos internacionales.



DOCUMENTO TÉCNICO:
LINEAMIENTOS DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD DEL
MINISTERIO DE SALUD

- El acceso a los códigos fuente, librerías y elementos críticos debe estar restringido, controlado y auditado, según las reglas establecidas por la unidad de organización competente de la OGTI.
- Establecer la obligatoriedad de implementar mecanismos alternativos de verificación y apertura de accesos, para verificar la identidad de los usuarios.

A.4. Gestión del ciclo de vida de los accesos

- La OGTI del MINSA o la que haga sus veces, con privilegio administrador, mantiene un registro actualizado de usuarios y privilegios de acceso a todos los sistemas de información que se utilizan en el MINSA.
- La cancelación de accesos debe ser inmediata al término del vínculo laboral o contractual, la que debe ser comunicada por la unidad de organización correspondiente.
- La OGTI y los propietarios de activos de la información revisarán periódicamente la vigencia y la pertinencia de los accesos a fin de garantizar su adecuada implementación.

B. Clasificación, manejo, almacenamiento y transmisión de la Información

Los propietarios de activo de la información son los responsables de:

B.1. Clasificación de la información

- La clasificación de la información debe alinearse con lo establecido en el Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública, aprobado mediante Decreto Supremo N° 021-2019-JUS.
- Documentar la clasificación y/o valoración de la información que corresponda en cada uno de los sistemas de información puestos a disposición por el MINSA.

B.2. Asignación de controles de acceso a la información, según su clasificación

- Información pública: Acceso abierto, conforme al principio de publicidad.
- Información Confidencial: Control de acceso físico y digital. Transmisión por canales seguros y correos institucionales autorizados.

B.3. Manejo y almacenamiento de la información

- Documentos físicos: custodia en archivos cerrados o ambientes controlados. Incluyen documentos archivísticos.
- Documentos digitales: repositorios institucionales con cifrado y control de acceso. Incluyen documentos archivísticos.
- Dispositivos extraíbles: uso autorizado y cifrado.
- Seleccionar algoritmos y métodos criptográficos reconocidos y adecuados para la confidencialidad, integridad y autenticidad.
- Asignar responsabilidades claras para la administración y actualización de los controles criptográficos.
- Proteger las claves para evitar su divulgación, modificación no autorizada o pérdida.



B.4. Transmisión

- La transmisión de la información debe darse por los canales cifrados y seguros, siempre que se cuente con el marco habilitante, sea de tipo normativo, convenio interinstitucional, acuerdo específico, entre otros, donde se habilite de manera expresa la posibilidad de la transmisión de información; en particular en aquellos casos donde se transfieran datos personales e información relacionada con la salud.
- Prohibición de transmisión de la información a cuentas personales o medios no autorizados.

C. Seguridad en el Uso de Activos de información

- El MINSA es responsable de la gestión de los activos de información, garantizando que se utilicen para fines lícitos u oficiales. Además, cada unidad de organización del MINSA es responsable de la gestión de los activos de información, en lo que les compete.

C.1. Asignación

- Documentar la entrega de activos de información mediante un acta de asignación.

C.2. Protección de Información de documentos físicos y digitales.

- Aplicar los controles de protección ante copias, para impedir la copia no autorizada de información confidencial.
- Implementar mecanismos de respaldo para la información cuyo propietario de activo de la información la haya considerado activo de información crítico.

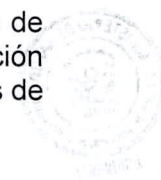
C.3. Uso Aceptable

- Establecer las condiciones de uso aceptable que el usuario debe firmar.
- Restringir la navegación en sitios no relacionados con las funciones institucionales asignadas de los usuarios.
- Prohibir las prácticas de envío masivo de correos electrónicos, juegos en línea, streaming, entre otros.
- Prohibir la instalación de complementos o extensiones en los navegadores, que permitan evadir los controles institucionales como el uso del VPN, señalando expresamente que su incumplimiento genera responsabilidad funcional, en el marco de la Ley de Servicio Civil, Ley N° 30057 y las leyes conexas.

D. Seguridad Física y Ambiental

El MINSA debe tener en cuenta lo siguiente:

- Solo pueden ingresar a ambientes donde se alojan activos de información críticos los usuarios que cuentan con la autorización previa correspondiente.
- El ingreso a instalaciones y ambientes donde se alojan activos de información críticos es regulado por la unidad de organización responsable de su seguridad física, bajo procedimientos formales de autorización y registro.



DOCUMENTO TÉCNICO:
LINEAMIENTOS DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD DEL
MINISTERIO DE SALUD

- Se debe controlar el registro y la vigilancia de las entradas y salidas de los usuarios, de las visitas y de los proveedores.
- Mantener registros auditables de ingresos, salidas y movimientos de equipos informáticos.

D.1. Protección de la Infraestructura

- Instalar cámaras, alarmas y sistemas de control perimetral.
- Implementar cerraduras electrónicas para áreas sensibles.
- La unidad de organización responsable del sistema de videovigilancia debe custodiar esta información, debiendo establecer el procedimiento para la eliminación segura de dicha información cuando corresponda, sin incurrir en exceso de almacenamiento; asimismo debe determinar el plazo máximo de almacenamiento de las grabaciones, de acuerdo a la disponibilidad técnica.

D.2. Seguridad Ambiental

- Monitorear la temperatura, humedad, humo y riesgos eléctricos, entre otros, de las instalaciones físicas.
- Realizar las pruebas periódicas de detectores de humo, extintores y sistemas de supresión, a ser definidos por la unidad de organización competente.

D.3. Control de Medios y Equipos

- La unidad de organización responsable del control del ingreso y salida de los bienes muebles que son parte de los activos de información del MINSA, debe de mantener el registro actualizado de los activos de información que salgan temporalmente de las instalaciones.
- Cifrar los discos y proteger los dispositivos informáticos contra robos o pérdidas.

D.4. Escritorio y Pantalla Limpios

- Configurar el bloqueo automático de sesión.
- Guardar los medios removibles en gabinetes cerrados fuera del horario laboral.
- Los documentos impresos y los archivos de soporte deben ser custodiados de forma segura, de acuerdo con la forma de clasificación de la información que corresponda.

D.5. Eliminación Segura de Activos de información

- Aplicar métodos certificados de eliminación segura y aplicar, cuando corresponda, las disposiciones para eliminación de documentos del Archivo General de la Nación.
- Retirar etiquetas institucionales de los activos de información eliminados antes de la disposición final.

E. Seguridad en Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.

- La OGTI aplica los principios de desarrollo seguro como parte de la atención de requerimientos de desarrollo realizados por parte de las unidades de organización del MINSA.



DOCUMENTO TÉCNICO:
LINEAMIENTOS DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD DEL
MINISTERIO DE SALUD

- Los servicios web o APIs públicas o internas deben implementarse con mecanismos seguros de autenticación, autorización y cifrado.
- La OGTI conduce los análisis de vulnerabilidades y las pruebas de seguridad en todas las fases del ciclo de vida de sistemas de información, incluyendo las pruebas de penetración antes del pase a producción.
- Los proveedores que realizan desarrollo o mantenimiento de sistemas de información a ser utilizados en el MINSA deben cumplir los criterios técnicos en materia de seguridad establecidos en la Directiva Administrativa N° 230-MINSA/2017/OGTI, "Directiva Administrativa que establece los estándares y criterios técnicos para el desarrollo de los sistemas de información en salud", aprobada con Resolución Ministerial N° 120-2017-MINSA; o norma que haga sus veces.

E.1. Entornos Segregados

- Mantener los ambientes electrónicos independientes para el desarrollo, calidad y producción de sistemas de información.
- Prohibir el uso de datos sensibles reales en entornos de desarrollo y calidad. En el caso de que sea necesario, aplicar enmascaramiento o anonimización.

E.2. Desarrollo Seguro

- Adoptar buenas prácticas de codificación segura y estándares utilizados en desarrollo seguro de software.
- Validar entradas y eliminar o neutralizar elementos maliciosos en los datos para evitar inyección del código u otras vulnerabilidades.
- Mantener repositorios seguros para el código fuente, con control de versiones y auditoría.

E.3. Interoperabilidad segura

- Establecer y adoptar estándares de interoperabilidad como HL7 FHIR, asegurando que sean compatibles con los requisitos establecidos en la PIDE.
- Establecer políticas de cifrado para la Protección de Datos en Tránsito y en Reposo.

E.4. Seguridad de la red del MINSA y protección de la información

- Administrar los equipos de comunicación (switch y router) únicamente mediante conexión por cable de consola, evitando configuraciones a través de la red local y/o inalámbrica.
- Deshabilitar el acceso remoto a los equipos de comunicación (switch y router), reduciendo el riesgo de conexiones no autorizadas desde fuera de la red local.
- Cambiar la contraseña predeterminada de los equipos de comunicación (switch y router), por una contraseña robusta, única y de uso exclusivo en cada router.
- Realizar la actualización del firmware de los equipos de comunicación (switch y router), a versiones vigentes (última actualización validada y estable por el fabricante de la marca del equipo).
- Para el caso de las redes inalámbricas, se debe configurar el SSID como no visible, de manera que el nombre de la red no se muestre públicamente.



DOCUMENTO TÉCNICO:
LINEAMIENTOS DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD DEL
MINISTERIO DE SALUD

- El acceso a las redes inalámbricas debe ser autenticado y debe mantener un registro actualizado a cargo de la OGTI.

F. Gestión de Incidente de Seguridad de la información y ciberseguridad

- Todo incidente de seguridad de la información y ciberseguridad puede ser reportado por un usuario a la OGTI, a través de todos los canales autorizados que se dispongan, de acuerdo con los procedimientos establecidos por la OGTI.
- Se deben dar tratamiento a los eventos y/o vulnerabilidades de seguridad de la información y ciberseguridad reportadas, asimismo, se debe evaluar, clasificar y priorizar el evento, así como, determinar si es un incidente.
- Asimismo, para el caso de los eventos relacionados a la seguridad física de las instalaciones del MINSA, se debe reportar a la unidad de organización a cargo de dicha instalación.

F.1. Registro de Incidentes de Seguridad de la Información

- Utilizar un sistema centralizado para documentar todos los incidentes de seguridad de la información.
- Generar informes periódicos para el control interno y la auditoría por incidentes de seguridad de información y ciberseguridad.

F.2. Escalamiento y Comunicación

- Activar protocolos de comunicación interna y externa.
- Garantizar la trazabilidad de todas las notificaciones de incidentes de seguridad de la información y ciberseguridad.

F.3. Aprendizaje y Mejora Continua

- Incorporar incidentes de seguridad y ciberseguridad en el análisis de riesgos de seguridad digital.
- Actualizar procedimientos y controles relacionados a los incidentes de seguridad de la información y seguridad, en base a lecciones aprendidas.

G. Copias de respaldo y recuperación de Información

- Las copias de respaldo de los activos de información críticos del MINSA deben asegurar la continuidad operativa y la recuperación ante incidentes de seguridad, fallas o desastres.
- Las copias de respaldo de los activos de información críticos del MINSA deben realizarse de forma programada, automática y según procedimientos documentados.
- Todas las copias de respaldo de los activos de información críticos del MINSA deben protegerse con controles físicos y lógicos para evitar alteraciones y accesos no autorizados.
- Las copias de respaldo de los activos de información críticos del MINSA deben ser verificadas mediante pruebas periódicas de restauración, para garantizar su validez.



DOCUMENTO TÉCNICO:
LINEAMIENTOS DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD DEL
MINISTERIO DE SALUD

- Las copias de respaldo de los activos de información críticos del MINSA deben almacenarse en lugares seguros, en una ubicación alterna o mediante servicios externos confiables.

G.1. Gestión del ciclo de vida de las copias de respaldo (backup)

- Definir los activos de información críticos del MINSA a respaldar.
- Definir el periodo de retención de las copias de respaldo, de acuerdo con la normatividad vigente.
- Aplicar procesos seguros de eliminación o destrucción de copias de respaldo cuando ya no sean necesarias, mediante borrado seguro o destrucción física.
- Mantener un inventario actualizado de todas las copias de respaldo almacenadas y su ubicación.

G.2. Control técnico

- Se debe revisar periódicamente la vigencia tecnológica de los equipos y software empleados para el respaldo y la recuperación, documentando cualquier riesgo de seguridad digital identificado por la unidad de organización competente.
- Se deben realizar las verificaciones periódicas de restauración para validar la operatividad y la consistencia de las copias de respaldo.

H. Protección contra software malicioso y código no autorizado

La OGTI para evitar el ingreso de softwares maliciosos o códigos no autorizados a los activos de información del MINSA, establece los siguientes controles de seguridad de la información:

- Las descargas, la instalación o la ejecución de softwares deben ser autorizadas por la OGTI.
- El uso de medios removibles (como USB y discos externos) debe ser controlado y autorizado, aplicando un análisis previo.
- Todo correo electrónico y archivo adjunto debe pasar por filtros antimalware y otros controles de seguridad de la información antes de llegar al usuario.
- Los sistemas de información deben estar actualizados con parches de seguridad que mitiguen vulnerabilidades explotables por malware.
- Los usuarios no deben desactivar las herramientas de protección ni instalar softwares sin aprobación formal de la OGTI.
- Capacitar a los usuarios sobre riesgos de seguridad digital tipo malware, phishing; y sobre buenas prácticas de seguridad de la información y ciberseguridad.

6.7. EVALUACIÓN

Los lineamientos de política de seguridad de la información y ciberseguridad del MINSA establecidos en el presente documento técnico son evaluados de manera documentada al menos una vez al año, o cuando presenten cambios significativos en el contexto legal, organizacional o de riesgo de la información del MINSA.



DOCUMENTO TÉCNICO:
LINEAMIENTOS DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD DEL
MINISTERIO DE SALUD

La evaluación es responsabilidad del Oficial de Seguridad y Confianza Digital del MINSA, en coordinación con la Unidad Funcional de Seguridad Digital del MINSA, cuyo resultado es comunicado a la Secretaría General, en su calidad de máxima autoridad administrativa del MINSA.

VII. RESPONSABILIDADES

- 7.1. El MINSA, a través de la Oficina General de Tecnologías de la Información, es responsable de la difusión, asistencia técnica, supervisión y evaluación del cumplimiento del presente Documento Técnico hasta sus órganos y unidades orgánicas.
- 7.2. Los órganos, unidades orgánicas del MINSA son responsables del cumplimiento de los lineamientos establecidos en el presente documento técnico.
- 7.3. Las Instituciones Prestadoras de Servicios de Salud que usan los Sistemas de Información puestos a disposición por el MINSA, son responsables de implementar y cumplir el presente Documento Técnico.
- 7.4. Las personas naturales y jurídicas que le prestan servicios al MINSA deben implementar y cumplir el presente Documento Técnico en lo que les corresponda.

VIII. BIBLIOGRAFÍA

- Norma ISO/IEC 27000:2018 – Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información – Descripción general y vocabulario.
- Norma ISO/IEC 27002:2022 – Seguridad de la información, ciberseguridad y protección de la privacidad: controles de seguridad de la información.
- Norma ISO/IEC 27003:2017 – Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información – Orientación.
- Norma ISO/IEC 27014:2020 - Seguridad de la información, ciberseguridad y protección de la privacidad: gobernanza de la seguridad de la información.
- Norma ISO/IEC 27035:2023 - Tecnología de la información — Técnicas de seguridad — Gestión de incidentes de seguridad de la información
- Especificación Técnica ISO/IEC TS 27100:2020 – Tecnología de la información – Ciberseguridad – Visión general y conceptos.
- Norma ISO/IEC 27110:2021 Tecnología de la información, ciberseguridad y protección de la privacidad. Directrices para el desarrollo del marco de referencia de ciberseguridad.

