GABINETE DIRECCIÓN
PLANIFICACIÓN ESTRATÉGICA Y CONTROL DE GESTIÓN
ASESORÍA JURÍDICA
ESM / EHH / WMS / MTC

**ACTUALIZA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y DEJA SIN EFECTO RESOLUCIÓN EXENTA N° 1395/2019.**

**RESOLUCIÓN EXENTA N°** 00047 / 06. 01. 2023

**VISTOS:** Providencia Interna N°2969, de fecha 19 de diciembre de 2022, de la Jefa (S) de asesoría Jurídica; Correo electrónico de fecha 15 de diciembre de 2022, de profesional de la Unidad de Planificación Estratégica y Control de gestión.

**CONSIDERANDO:**

**PRIMERO:** Que, el Instituto de Salud Pública de Chile, en adelante "El Instituto" o "ISP" reconoce la importancia de la información, así como los activos de información de la misma, por ser relevantes para la Dirección y el funcionamiento del mismo, ya que su deficiencia o ausencia podrían representar un peligro para la continuidad del Servicio o al menos suponer daños importantes por pérdidas irreversibles de datos, equipos e infraestructura.

Del mismo modo, los accesos y usos de la información, deben ser considerados en las normas, reglas, estándares y procedimientos que se deriven de ella y demás políticas anexas.

**SEGUNDO:** Que, con el objeto de dar una mejor respuesta a los requisitos de seguridad de la información, es necesario actualizar la "Política General de Seguridad de la Información" contenida en la Resolución Exenta N° 1395, de fecha 31 de mayo de 2019.

**TERCERO:** Que, con fecha 28 de noviembre de 2022, se levanta el Acta N° 3/2022 del Comité Único de Riesgo, de Calidad y de Seguridad de la Información en que consta el acuerdo de enviar a la Dirección del Instituto de Salud Pública de Chile para revisión y aprobación la "Política General de Seguridad de la Información versión 5", la que ya fue visada por el Comité; y,

**TENIENDO PRESENTE** lo dispuesto en D.F.L. N° 1/19.653 de 2000 que "Fija Texto Refundido, Coordinado y Sistematizado de La Ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado"; en la Ley Nº 19.880, que "Establece Bases de los Procedimientos Administrativos que Rigen los Actos de los Órganos de la Administración del Estado"; la Ley N° 20.285 "Sobre acceso a la información pública"; en los artículos 60 y 61 letra b) del Decreto con Fuerza de Ley Nº 1, de 2005, que "Fija el Texto Refundido, Coordinado y Sistematizado del Decreto Ley N° 2.763, de 1979 y de las Leyes N° 18.933 y N° 18.469"; y 4º letra b), 10º letra b) y 52º del Decreto Supremo Nº 1.222, de 1996, de la misma Secretaría de Estado, que "Aprueba el Reglamento del Instituto de Salud Pública de Chile; así como lo establecido en la Resolución Nº 7, de 2019 de la Contraloría General de la República; Decreto Supremo N° 83/2005, "Norma Técnica sobre seguridad y confidencialidad del documento electrónico"; Ley N°19.223/1993 "Tipifica figuras penales relativas a la informática"; y la Norma ISO IEC 27001 del 2020 "Tecnología de la información-Técnicas de Seguridad- Sistemas de Gestión de la

Seguridad de la Información-Requisitos"; Decreto Supremo N°890/1975 "Sobre Seguridad del Estado"; y las facultades que me entrega el Decreto Exento N° 51/2020, del Ministerio de Salud, es que dicto la siguiente:

**R E S O L U C I Ó N**

**1.- APRUÉBASE** la siguiente: **POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN.**

## I. INTRODUCCIÓN.

Para dar cumplimiento al proceso de modernización del Estado, el Instituto de Salud Pública de Chile (ISP), aprobó el presente documento, teniendo en consideración la NCh-ISO27001 Of 2020 y el Sistema de Gestión Integrado que contiene las normas ISO 9001, ISO/IEC 17025, ISO 15189, ISO/IEC 17043, ISO 17034 y Norma Técnica 139/2012 de Buenas Prácticas de Laboratorio de la OMS.

Para los efectos de esta Política, los documentos electrónicos constituyen un activo para la entidad que los genera y obtiene. La información que contiene es el resultado de una acción determinada y sustenta la toma de decisiones, por parte de quien la administra y accede a ella.

Este documento no se trata de una descripción técnica de mecanismos de seguridad, sino más bien, del marco en que se organiza el Sistema de Seguridad de la Información en el Instituto de Salud Pública.

## II.- OBJETIVOS DE LA POLÍTICA.

### 1. Objetivo General

Establecer el lineamiento institucional, en cuanto a las responsabilidades en el resguardo de los activos de información y la gestión de sus riesgos; entregando el marco general para el acceso, manipulación, procesamiento, transmisión, protección, almacenamiento o cualquier otro tratamiento que se realice sobre los activos de información del ISP, para lograr niveles adecuados de confidencialidad, integridad y disponibilidad, asegurando la continuidad operacional del ISP.

### 2. Objetivos específicos:

a) Establecer el marco del Sistema de Seguridad de la Información del ISP.
b) Indicar los mecanismos de aprobación, difusión, revisión y cumplimiento de esta política y las que de ella deriven.
c) Establecer para todo el personal interno y externo de la institución el deber de gestionar la seguridad de la información, informándose y promoviendo la comprensión de sus responsabilidades individuales y de equipo.

## III.- ALCANCES.

El alcance de la presente política responde en particular al objetivo A.5 "Proporcionar orientación y apoyo de la dirección para la seguridad de la información, de acuerdo con los requisitos del negocio y con las regulaciones y leyes pertinentes", no obstante, afecta a todos los procesos operacionales, estratégicos y de soporte de la institución, que impactan directamente en el cumplimiento de los objetivos y productos estratégicos y que además, forman parte de los procesos que la institución gestiona (Formulario A1).

Adicionalmente, es la base en materia de seguridad de la información para el resto de dominios de la NCh-ISO 27001 del 2020.
Asimismo, ésta comprende la totalidad de los activos de la información que el ISP posee o administra, sin exclusión alguna.

**IV.- REQUISITO DEL CONTROL NORMATIVO** NCh-ISO IEC 27001:-2020.

- Aplica a los 114 Controles de la Norma NCh-ISO 27001/2020

**V.- REFERENCIAS NORMATIVAS.**

- D.F.L. Núm. 1/19.653 de 2000 Fija Texto Refundido, Coordinado y Sistematizado de La Ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado;
- Ley N°19.880 del 29 de mayo de 2003 del Ministerio Secretaría General de la Presidencia, "Establece las bases de los procedimientos administrativos que rigen los actos de los Órganos de la Administración del Estado";
- Ley N°20.285 del 20 de agosto de 2008 "Sobre acceso a la información pública" del Ministerio Secretaría General de la Presidencia
- Decreto con Fuerza de Ley Nº 1, de 2005, que "Fija el Texto Refundido, Coordinado y Sistematizado del Decreto Ley N° 2.763, de 1979 y de las Leyes N° 18.933 y N° 18.469";
- Decreto Supremo Nº 1.222, de 1996, del Ministerio de Salud que aprueba el Reglamento del Instituto de Salud Pública de Chile;
- Decreto Exento N° 324/2018 "Aprueba Programa Marco de los Programas de Mejoramiento de la Gestión de los Servicios en el año 2019;
- Ley N°19.223 de 1993 del Ministerio de Justicia "Tipifica figuras penales relativas a la informática";
- Decreto Supremo N°890 del 3 de julio de 1975 del Ministerio de Interior "Fija texto actualizado y refundido de la Ley 12.927, sobre seguridad del Estado";
- Resolución Exenta N° 1536, de fecha 18 de junio de 2018 que "Aprueba Código de Ética del Instituto de Salud Pública de Chile".
- Ley N°19.799, del 10 de octubre de 2014 del Ministerio de Economía Fomento y Reconstrucción "Sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma";
- Ley N°20.521 del 23 de julio de 2011 del Ministerio de Economía, Fomento y Turismo "Modifica la Ley Nº 19.628, sobre protección de datos de carácter personal para garantizar que la información entregada, a través de predictores de riesgo, sea exacta, actualizada y veraz";
- Decreto Supremo N°83 del 12 de enero de 2005, del Ministerio Secretaría General de la Presidencia "Aprueba norma técnica para los Órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos"
- Ley 21.459 sobre delitos informáticos
- NCh-ISO 27001:2020, Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos.

**VI.- DOCUMENTOS RELACIONADOS.**

- Política Nacional de Ciber Seguridad 2017-2022;
- Resolución 2761 del 30 de octubre de 2018 que crea el "Comité único de riesgo, de calidad, y de seguridad de la información".
- Política de Desarrollo Seguro.
- Política de Gestión de Activos.
- Política de Gestión de medios removibles
- Política de Seguridad Física y Ambiental.
- Política de Autenticación Secreta.

- Política de aseguramiento de la continuidad operacional
- Política de control de acceso.
- Política de gestión y uso de redes
- Política de relaciones con los proveedores
- Política de respaldo de información digital, software y sistemas.
- Política de instalación y uso de software y prevención contra código malicioso.
- Política de trabajo remoto.
- Código de ética del Instituto de Salud Pública de Chile.
- Procedimiento de ejecución de compras y contrataciones (PR-620.00.002).
- Procedimiento de imparcialidad presiones indebidas y confidencialidad. (PR-643.00-002).
- Procedimiento reclutamiento y selección de personal (PR-645.00-001).
- Instructivo creación y actualización de perfiles de cargo (IT-645.00.001).
- Instructivo Comité de selección (IT-645.00-002).
- Instructivo reclutamiento y selección del personal (IT-645.00-003).
- Instructivo Inducción (IT-645.00-004).
- Instructivo de egreso (IT-645.00-005).
- Procedimiento de gestión de equipos de laboratorio (PR-602.00-001).
- Instructivo Gestión de Incidencias (contingencias) (IT-610.00-001).
- Procedimiento de Mantenciones preventivas y correctivas del equipamiento computacional (PR-140.03-001).
- Procedimiento Respaldo de servidores y sistemas institucionales (PR-140.0-.002).
- Procedimiento Control de acceso a sistemas computacionales (PR-140.03-002).
- Procedimiento de Gestión de Proyectos y Sistemas (PR-140.01-001).
- Procedimiento de Monitoreo y Protección de Registro de Eventos (PR-140.02-005).
- Procedimiento de restauración de información (PR-140.02-006)
- Procedimiento de eliminación segura de unidades de almacenamiento de datos (PR-140.03-003).
- Instructivo Asignación de Equipamiento Tecnológico de Administración TIC (IT-140.03-004).
- Instructivo Pérdida de Equipamiento Tecnológico de Administración TIC (IT-140.03-005).
- Instructivo paso a paso conexión VPN ISP (IT-140.02-004).
- Instructivo parche de Seguridad Microsoft Windows (IT-140.02-008)
- Instructivo de pérdida de equipamiento tecnológico de administración TIC. (IT-140.03.005)
- Instructivo de reuniones virtuales on line. (IT-140.03-006).
- Instructivo RPD (Escritorio remoto) (IT-140.03-007).
- Instructivo conexión a VPN Equipos MAC (IT-140.03-008)
- Guía de Sincronización de relojes de los sistemas del ISP.
- Instructivo protocolo de contingencia ante corte de suministro eléctrico (IT-650.00-003).
- Guía para el control de acceso y áreas de carga y descarga dentro del Instituto de Salud Pública (GT-644.00-002).

**VII.- DEFINICIONES.**

- **Activos de Información:** son todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para el Instituto de Salud Pública de Chile, en adelante "El Instituto" o "ISP". Se constituyen por:
  - La Información propiamente tal, en sus múltiples formatos (papel; digital; texto; imagen; audio; video; transmisión verbal, etc.).
  - Los Equipos, Sistemas e infraestructura que soportan esta información.
  - Las Personas que utilizan la información y que tienen el conocimiento de los procesos institucionales.
- **Seguridad de la Información:** Preservación de la confidencialidad, integridad y disponibilidad de la información. (Ref. ISO 27000:2018).

- **Confidencialidad:** Propiedad de que la información no se pone a disposición o no es revelada a individuos, entidades o procesos no autorizados. (Ref. ISO 27000:2018).
- **Integridad:** Propiedad de precisión y exhaustividad. (Ref. ISO 27000:2018).
- **Disponibilidad:** Propiedad de estar disponible y utilizable según requisito de una entidad autorizada. (Ref. ISO 27000:2018)
- **Política de Seguridad de la Información**: conjunto de normas con el objetivo de proteger la información contra una amplia gama de amenazas para asegurar la continuidad del servicio y minimizar los daños, procurando la preservación de la confidencialidad, disponibilidad e integridad de la información.
- **Propietario de la información**: es el responsable de la información y de los procesos que la manipulan, sean estos manuales, mecánicos o electrónicos. Debe participar activamente en la definición del valor de la información para el negocio, de manera que se pueda definir los controles apropiados para protegerla.
- **Riesgo:** efecto de la incertidumbre en los objetivos. **(**Ref. ISO 27000:2018).
- **Riesgo de Seguridad de la Información**: corresponde a una amenaza potencial que podría afectar activos de información, vinculados a los procesos de soporte institucional y/o a los procesos de provisión de productos estratégicos (bienes y servicios), establecidos en las definiciones estratégicas institucionales y, por tanto, causar daño a la organización.
- **Usuario:** Es toda persona interna o externa que accede y utiliza Activos de Información institucionales.

## VIII.- ROLES Y RESPONSABILIDADES.

| Rol | Responsabilidad |
|---|---|
| **Comité Único de Riesgo, de Calidad, y de Seguridad de la Información** | **Funciones según Res. 2761/2018, En el ámbito de la Gestión de la Seguridad de la Información:**<br>• Velar por el cumplimiento y actualización de la Política General de Seguridad de la Información, presentando propuesta a la alta dirección para su aprobación;<br>• Aprobar al interior del ISP las Políticas Específicas del Sistema de Seguridad de la Información;<br>• Velar por la implementación de los controles de seguridad en el Instituto;<br>• Gestionar la identificación, evaluación y mitigación de los riesgos que afectan los activos de información y la continuidad de negocio;<br>• Arbitrar conflictos en materia de seguridad de la información y los riesgos asociados y proponer soluciones;<br>• Apoyar el desarrollo de los planes de comunicación, difusión y capacitación en materia de seguridad de la información;<br>• Conocer los incidentes que pudieran afectar a la seguridad de la información al interior de la organización, con el fin de establecer acciones preventivas y correctivas;<br>• Generar y proponer proyectos de desarrollo para el cumplimiento de los requisitos técnicos y normativos, dentro del marco presupuestario vigente;<br>• Informar a la alta dirección, en los intervalos que se convenga, sobre el Sistema de Seguridad de la Información. |
| **Encargado de Seguridad de la Información (ESI)** | • Velar por la implementación de las políticas de seguridad de la información al interior del ISP, de su control y de su correcta aplicación;<br>• Coordinar la incorporación y modificación de las Políticas de Seguridad de la Información en el Sistema de Gestión Integrado.<br>• Coordinar y gestionar la respuesta a incidentes que afecte a los activos de |

| Rol | Responsabilidad |
|---|---|
| | información de la Institución.<br>• Establecer puntos de enlace con los encargados de seguridad de otros organismos públicos y especialistas externos, que permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes.<br>• Coordinar las acciones del Comité único de Riesgo, de Calidad y de Seguridad de la Información correspondientes al Sistema de Seguridad de la Información.<br>• Apoyar en la implementación de la Ley de Transformación Digital del Estado. |
| **Encargado de Ciberseguridad (ECI)** | • Apoyar en la implementación de la Ley de Transformación Digital del Estado.<br>• Apoyar en el establecimiento de estrategias y planes para asegurar la información, los sistemas y las plataformas en las que se almacena la misma, ante ataques e incidentes (ciberataques).<br>• Realizar recomendaciones a las distintas áreas, para prevenir la ocurrencia de ciberataques, los posibles fallos en las plataformas y otro tipo de incidentes que pongan en riesgo la información propia o de terceros.<br>• Apoyar en la prevención y respuesta ante incidentes de seguridad informática.<br>• Controlar permanentemente revisiones a los sistemas y plataformas, para detectar riesgos que permitan acceso a información sensible, sistemas y plataformas. |
| **Alta Dirección/Director(a) del Instituto** | • Aprobar la Política General de Seguridad de la Información y de las estrategias y mecanismos de control para el tratamiento de los riesgos que afecten los activos de información de la institución que se generen como resultado de los reportes o propuestas del Comité. |
| **Jefaturas de Departamento** | • Asegurar la aplicación y cumplimiento de las políticas, procedimientos e instructivos de Seguridad de la Información al interior de cada Departamento, Subdepartamento, Sección o Unidad según corresponda. |
| **Jefaturas de Subdepartamento y Secciones / Unidades** | • Velar por la toma de decisiones respecto del activo de información, política o procedimiento relacionado con algún ámbito de Seguridad de la Información.<br>• Promover al interior de su equipo de trabajo tanto la denuncia cómo la respuesta, cuándo se solicite, a los incidentes de seguridad de la información. |
| **Usuario** | • Dar cumplimiento a las directrices establecidas en la presente Política, referidas a las acciones permitidas y prohibidas de autenticación secreta.<br>• Reportar los incidentes de seguridad detectados en el ámbito del uso de autenticación secreta. |

## IX:- LINEAMIENTOS DE LA PRESENTE POLÍTICA.

### 1 Lineamiento Institucional

El ISP mantiene una Política General de Seguridad de la Información, alineada a los objetivos estratégicos institucionales estableciendo de este modo su compromiso con la administración, custodia y uso de la información en la institución, manifestando así su disposición a cumplir los requisitos establecidos en las normativas y en la legislación vigente para seguridad de la información, por cuanto se reconoce que la información es un bien valioso, estratégico y sensible que requiere protección permanente y especializada, por lo que esta política es conocida, comprendida e implementada por todos los funcionarios y sus respectivas jefaturas, en el marco de sus competencias.

**2 Objetivos del Sistema de Seguridad de la Información:**

a) Asegurar el cumplimiento de la legislación y reglamentación vigente aplicable.
b) Mantener las políticas actualizadas, para asegurar su vigencia y nivel de eficacia.
c) Asegurar la implementación de esta política, identificando los recursos necesarios para ello.
d) Proteger los recursos de información del Instituto y la tecnología utilizada para su procesamiento de cualquier amenaza, ya sea interna o externa, deliberada o accidental; para asegurar el cumplimiento de la integridad, confidencialidad y disponibilidad de la información.
e) Promover la incorporación de esta Política en la cultura institucional.

**3 Aprobación de la Política:**

La Política General de Seguridad de la Información y sus actualizaciones serán aprobadas por la alta Dirección del Instituto de Salud Pública, siendo el "Comité Único de Riesgo, de Calidad y de Seguridad de la Información" el que propondrá las modificaciones y actualizaciones pertinentes.

**4 Difusión y Capacitación de la Seguridad de la Información:**

Para la difusión de los contenidos de la Seguridad de la Información, se elaborará un Plan Anual de Difusión y Capacitación, el cual debe ser aprobado por el Comité único de riesgo, de calidad y de Seguridad de la Información, no obstante se utilizarán medios de difusión disponible, así como, también instancias de capacitación llevadas a cabo para este efecto. Posibles medios a utilizar son los siguientes:

- Intranet institucional.
- Inducción y capacitación al personal interno y externo.
- Web institucional.
- Correos masivos.

**5 Obligación de informar eventos de Seguridad de la Información:**

Toda persona adscrita a ésta Política tiene la obligación de comunicar en el menor plazo posible cualquier evento que represente un riesgo para la confidencialidad, integridad o disponibilidad de la información o sus activos al correo seguridad.informacion@ispch.cl.

**6 Sanción en caso de incumplimiento.**

El incumplimiento de las obligaciones emanadas de esta Política, así como de las Específicas del Sistema, u otros documentos que rigen a los organismos públicos, los cuales se tienen presente para la promulgación de esta Política o que deriven de estos, serán sancionados de acuerdo a la normativa y/o acuerdos vigentes.

Cuando el incumplimiento de la Política se refiera a personas respecto de las cuales no es posible hacer efectiva responsabilidad administrativa, así como de aquellas empresas que se encuentren prestando servicios para el Instituto y les afecta la presente Política, será considerado como un incumplimiento grave de las obligaciones que establece el contrato, procediéndose al término anticipado del mismo, sin perjuicio de las acciones civiles y penales que se deriven de tales infracciones.

## X.- DIFUSIÓN DE LA POLÍTICA.

La Política de Seguridad de la Información será difundida, de acuerdo al control de la información documentada bajo Sistema de Gestión Integrado, así también el Encargado de Seguridad de la Información gestionará su actualización en la web pública, las publicaciones correspondientes.

Esta Política, sus normas, procedimientos y estándares, así como sus correspondientes actualizaciones y/o modificaciones, como también las resoluciones, oficios y/o circulares que emanen del Instituto de Salud Pública de Chile, del Encargado de Seguridad de la Información, o de la RED de expertos, cuando corresponda; se publicarán tanto en el sitio del Sistema de Seguridad de la Información, como en la página web del ISP.

## XI.- DENUNCIAS Y NOTIFICACIONES.

El personal del ISP, sus proveedores o terceros deben notificar toda debilidad, incidente o evento asociado a actividades no permitidas o malas prácticas de acceso que pudiera derivar en un posible incumplimiento, uso indebido u otra situación asociada, inmediatamente, al correo seguridad.informacion@ispch.cl.

## XII.- REVISIÓN DE LA POLÍTICA.

Esta política, deberá ser revisada como máximo cada 4 años, de acuerdo a lo indicado en Sistema de Gestión de Calidad Integrado, no obstante, se recomienda una revisión anual.

## XIII.- CUMPLIMIENTO

Todo el personal del Instituto de Salud Pública de Chile, entiéndase funcionarios de planta, sujetos a contrata, de reemplazos y o suplencias, estudiantes en práctica, asesores, consultores, personal a honorarios y cualquiera que desempeñe funciones en o para el Instituto de Salud Pública de Chile, deberá dar cumplimiento en lo que le corresponda de esta Política General de Seguridad de la Información y de las específicas que les apliquen.

Para el caso de terceros, y por el sólo hecho de participar en un proceso de compras del servicio, el oferente deberá dar cumplimiento a las Políticas, Procedimientos e Instructivos que se encuentren publicados en la página web del Instituto de Salud Pública, enlace https://www.ispch.cl/politicas-de-seguridad-de-la-informacion/, habilitado en la página Web del Instituto de Salud Pública de Chile y sus actualizaciones, que se presumen conocidas por el contratista o adjudicatario para todos los efectos legales.

**2.- DÉJASE SIN EFECTO,** la Resolución Exenta N° 1395 de fecha 31 de mayo de 2019

Anótese, comuníquese y archívese

**Q.F. HERIBERTO GARCÍA ESCORZA**
**DIRECTOR (S)**
**INSTITUTO DE SALUD PÚBLICA DE CHILE**

Distribución:
- Dirección.
- Unidad de Planificación Estratégica y Control de Gestión
- Unidad de Gestión de Calidad
- Unidad de Auditoría Interna
- Unidad de Asesoría Jurídica
- Unidad de Tecnologías de la Información y la Comunicación TIC.
- Unidad de Comunicaciones e Imagen Institucional
- Dpto. ANAMED
- Dpto. Salud Ocupacional
- Dpto. Administración y Finanzas
- Dpto. Salud Ambiental
- Dpto. Laboratorio Biomédico Nacional y de Referencia
- Dpto. Asuntos Científicos
- Depto. Dispositivos médicos.
- Encargado de Seguridad de la Información
- Coordinador de Riesgo Institucional
- Subdepto. Servicios Generales
- Subdepto. Gestión de las personas.
- OIRS
- SALPRI
- Oficina de Partes

Resol. A1/N°17
ID 890961
5/01/2023

Suscrito Fielmente
Ministro de Fé
Mauricio Orellana Valdés