# POLÍTICA

# DE GESTIÓN Y USO DE REDES

# INSTITUTO DE SALUD PÚBLICA DE CHILE

**Fecha de Emisión: 09/08/2019**
**Versión: 1**
**Fecha de actualización: 14/01/2022**

**INDICE**

## 1. 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 2013 y el Sistema de Gestión Integrado bajo 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 debe trabajar tanto en la instalación como en la utilización de softwares en equipos y servidores de uso institucional.

## 2. OBJETIVO.

Proporcionar los lineamientos para garantizar la protección de la información en las redes, y establecer las restricciones en cuanto a la navegación web para los sistemas de información del Instituto de Salud Pública.

## 3. ALCANCE.

El alcance de esta Política incluye a todos(as) los(as) funcionarios(as) de planta, contrata, honorarios y toda aquella persona natural o jurídica que preste servicios al ISP y que, a raíz de ello, tenga la necesidad de realizar diversos accesos a los sistemas físicos y lógicos que la organización posea, incluyendo los archivos de documentación, las aplicaciones comerciales, bases de datos, aplicaciones desarrolladas internamente, equipos, instalaciones, sistemas y redes.

Esta Política abarca todos los Procesos operacionales, de apoyo y estratégicos que requieran en cualquiera de sus etapas la aplicación de controles de acceso tanto lógico cómo físicos.

Asimismo, abarca a todos los activos de información que el ISP posee, de manera que la no inclusión explícita en el presente documento no constituye argumento para no proteger activos de información que se encuentren en otras formas. Esta política cubre toda la información impresa o escrita en papel, almacenada electrónicamente, trasmitida por correo o usando medios electrónicos, mostrada en películas o hablada en una conversación.

## 4. REQUISITO DEL CONTROL NORMATIVO ISO 27.001:2013.

Aplica al Dominio 13 “Seguridad en las comunicaciones” en cualquier ámbito definido en los alcances.

## 5. 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 Nº 19.880, que establece 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°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°20.521 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"
- NCh-ISO 27001:2013, Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos.

## 6. DOCUMENTOS RELACIONADOS.

- Resolución 2761 del 30 de Octubre de 2018 que crea el "Comité único de riesgo, de calidad, y de seguridad de la información".
- Política Nacional de Ciber Seguridad 2019-2022;
- Política General de Seguridad de la Información del Instituto de Salud Pública de Chile.
- Política de Control de acceso del Instituto de Salud Pública de Chile.
- Política de autenticación secreta del Instituto de Salud Pública de Chile.
- Política de teletrabajo del Instituto de Salud Pública de Chile.
- Política de relación con proveedores del Instituto de Salud Pública de Chile.
- Política de instalación y uso de softwares.
- Procedimiento de ejecución de compras y contrataciones PR-620.00.002.
- Procedimiento de imparcialidad presiones indebidas y confidencialidad. PR-643.00-002.
- Instructivo Gestión de Incidencias (contingencias) (IT-610.00-001).
- Procedimiento de Mantenciones preventivas y correctivas del equipamiento computacional (PR-611.00-001).
- Procedimiento Respaldo de servidores (PR-611.00-003).
- Procedimiento Control de acceso de usuarios a sistemas (PR-611.00-004).
- Procedimiento de Gestión de Proyectos y Sistemas (PR-611.00-011).
- Procedimiento de Monitoreo, Registro y Protección de Registro de Eventos (PR-611.00-013).
- Instructivo Asignación de Equipamiento Tecnológico de Administración TIC (IT-611.00-002).

- Instructivo Pérdida de Equipamiento Tecnológico de Administración TIC (IT-611.00-003).
- Documento Estrategia de Trabajo Red SSI 2019.

## 7. 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.
- **Red:** Conexión entre equipos computacionales que permite compartir datos y recursos.
- **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.
- **Negocio:** bien o servicio prestado por una organización.
- **Software:** producto intangible que permite a un equipo computacional desempeñar diversas tareas por medio de instrucciones lógicas, a través de diferentes tipos de programas.
- **Malware:** software malicioso diseñado para causar daños o provocar mal funcionamiento a equipos computacionales independientes o conectados a la red.

## 8. ROLES Y RESPONSABILIDADES.

| | |
|---|---|
| **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>• Validar, aprobar y difundir 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 y gestionar la respuesta a incidentes que afecte a los activos de 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. |
| **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. |

## 9. LINEAMIENTOS DE LA PRESENTE POLITICA.

### 9.1 Gestión de Redes

9.1.1 La administración de los equipos de comunicación como router y switch, es responsabilidad del Subdepartamento TIC.

9.1.2 La administración de control de acceso de equipos computacionales a la red externa y/o interna, es responsabilidad del Subdepartamento TIC.

9.1.3 Los servicios de red deben ser monitoreados constantemente para prevenir la indisponibilidad de la red.

9.1.4 No está permitido el acceder a recursos de la red interna desde fuera de las instalaciones del ISP, por medio de software, aplicaciones o herramientas que no sean las que el Subdepartamento TIC facilita para tales efectos.

9.1.5 Está restringido el acceso a sitios web de entretenimiento, videos, radios y redes sociales. Para solicitar liberación de estos servicios, debe ser gestionado por la Jefatura directa por medio del procedimiento de Control de Acceso a Usuarios, con la respectiva justificación.

**9.2 Uso de Red de Datos**

9.2.1 No está permitido utilizar equipos computacionales para acceder a servicios locales o remotos a los que el usuario no tenga autorización explícita o, en su uso, intentar violar la seguridad de acceso de cualquier equipo computacional o red.

9.2.2 No está permitido hacer uso de los servicios de la red de la Institución para transmitir publicidad ilegal y/o para lucrar con estos servicios.

9.2.3 No intente acceder a áreas restringidas de una red, sistemas informáticos, software de seguridad o cuentas de usuario, sin la aprobación del propietario o de la Institución.

9.2.4 Utilice la red de la Institución para temas relacionados con el trabajo. Tenga en cuenta que la red ISP forma parte de la Red MINSAL, con acuerdos acerca del uso y fines de las comunicaciones que usted como usuario debe respetar.

9.2.5 Por razones de seguridad de la información, cualquier solicitud de conexión a la red de datos de la Institución mediante equipamiento externo, deberá ser solicitado por la jefatura directa del solicitante a través de documentación formal, indicando la justificación del requerimiento y quedando el uso de este equipamiento bajo responsabilidad de la jefatura solicitante.

9.2.6 No está autorizado el montaje de servidores, que por sus funcionalidades puedan comprometer el buen funcionamiento y la seguridad de la red. Para su instalación se deberá entregar la documentación respectiva, justificando su instalación para evaluación de factibilidad.

9.2.7 La red Institucional cuenta con servidores de directorio activo, en donde a través de esta, se generan y distribuyen políticas de configuración y/o servicios.

9.2.8 Todas las direcciones de red (IP), son suministradas por la Sección Administración de Plataformas y Comunicaciones del Subdepartamento TIC. No intente realizar configuraciones por su cuenta.

9.2.9 Los usuarios deberán ser autorizados formalmente por la jefatura directa para tener acceso a la red de datos y con indicación a los servicios a los cuales podrán acceder, por medio de los procedimientos correspondientes para tal efecto.

## 10. DIFUSIÓN.

Esta Política 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.

## 11. 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.información@ispch.cl .

## 12. REVISIÓN DE LA POLÍTICA.

Esta política, deberá ser revisada como máximo cada 4 años, y en la medida que requiera actualizaciones.

## 13. 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 www.ispch.cl /Seguridad de la información/Políticas de Seguridad de la Información, 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.

## 14. CONTROL DE CAMBIOS.

| Versión | Fecha | Principales Puntos Modificados | Resumen de Modificaciones |
|---|---|---|---|
| V0 | | | |