POLÍTICA

DE RELACIÓN CON LOS PROVEEDORES

INSTITUTO DE SALUD PÚBLICA DE CHILE

Fecha de Emisión: 12/12/2016
Versión: 3
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-ISO 27001.Of2013 y el Sistema de Calidad Integrado bajo las normas ISO 9001, NCh-ISO 17025, NCh –ISO 15189, NCh-ISO 17.043, ISO 17034, ISO Guide 35 y BPL/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 gUIDEy accede a ella.

Este documento no se trata de una descripción técnica de mecanismos de seguridad, sino más bien, de una descripción de lo que se desea proteger, el porqué de ello y quién está involucrado.

2. OBJETIVO.

Garantizar el cumplimiento de las normas para la protección de los activos de información de la organización por parte de proveedores, manteniendo el nivel acordado de seguridad y la prestación de servicios conforme a lo contratado.

3. ALCANCES.

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, esta 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 directa o indirectamente a controles de los siguientes dominios de la Norma 27.001 del 2013:

a. Controles del Dominio 6 “Organización de la seguridad de la información”:
b. Controles del Dominio 7 “Seguridad de Recursos Humanos”
c. Controles del Dominio 8 “Administración de Activos”
d. Controles del Dominio 9 “Control de Acceso”:
e. Controles del dominio 11 “Seguridad Física y Ambiental”
f. Controles del Dominio 12 “Seguridad de las Operaciones”:
g. Controles del Dominio 13 “Seguridad en las comunicaciones”.
h. Controles del Domino 14 “Adquisición, desarrollo y mantenimiento de Sistemas”.
i. Controles del Dominio 15 “Relaciones con los proveedores”.
j. Controles del Dominio 16 “Administración de Incidentes de Seguridad de la Información”.
k. Controles del Dominio 17 “Implementación de la continuidad de la Seguridad de la Información”.
l. Controles del Dominio 18 “Cumplimiento”

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 Autenticación Secreta del Instituto de Salud Pública de Chile.
- Política de Instalación y uso de softwares del Instituto de Salud Pública de Chile.
- Política de teletrabajo del Instituto de Salud Pública de Chile.
- Política de instalación y uso de redes del Instituto de Salud Pública.
- Política de Control de Acceso 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 Gestión de Proyectos y Sistemas PR-140.01-001 6
- Procedimiento de Aseguramiento de Calidad (QA) de Software PR-140.01.002
- Procedimiento Respaldo de servidores y Sistemas Institucionales PR-140.02.002

- Procedimiento de Monitoreo y Protección de Registro de Evento PR-140.02.005
- Procedimiento Restauración de Información PR-140.02.006
- Procedimiento de Mantenciones preventivas y correctivas del equipamiento computacional PR-140.03.001
- Procedimiento Control de Acceso a Sistemas Computacionales PR-140.03.002
- Procedimiento de eliminación segura para la reutilización o descarte de equipos, medios de soporte o documentación física. PR-140.03.003
- Instructivo Plan de Pruebas QA IT-140.01.001
- Instructivo Gestión de Incidencias (contingencias) IT-140.02-001
- Instructivo Paso a paso conexión VPN ISP IT-140.02-004
- Parche de Seguridad Microsoft Windows" IT-140.02-008 1
- 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 Reuniones virtuales Online IT-140.03-006
- Instructivo RPD (Escritorio Remoto) IT-140.03-007
- Instructivo Conexión a VPN Equipos MAC IT-140.03-008
- Instructivo de creación de Ticket en Nueva Plataforma Mesa de Ayuda IT-140.03-009
- Instructivo de Reglas – Filtros para Gmail y Outlook IT-140.03-010
- 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.
- **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.

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:** • Velar por el cumplimiento y actualización de la Política General de Seguridad de la Información, presentando propuesta a la alta dirección para su aprobación; • Validar, aprobar y difundir al interior del ISP las Políticas Específicas del Sistema de Seguridad de la Información; • Velar por la implementación de los controles de seguridad en el Instituto; • Gestionar la identificación, evaluación y mitigación de los riesgos que afectan los activos de información y la continuidad de negocio; • Arbitrar conflictos en materia de seguridad de la información y los riesgos asociados y proponer soluciones; • Apoyar el desarrollo de los planes de comunicación, difusión y capacitación en materia de seguridad de la información; • 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; • Generar y proponer proyectos de desarrollo para el cumplimiento de los requisitos técnicos y normativos, dentro del marco presupuestario vigente; • 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; • Coordinar y gestionar la respuesta a incidentes que afecte a los activos de información de la Institución. • 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. • 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. • 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. • Reportar los incidentes de seguridad detectados en el ámbito del uso de autenticación secreta.

9. LINEAMIENTOS DE LA PRESENTE POLITICA.

9.1. Los Inspectores Técnicos de Contrato (ITC), deben tener presente la sensibilización y el cuidado del cumplimiento de ésta política con nuestros proveedores externos, por otra parte el ISP debe sensibilizar periódicamente a su personal sobre los resguardos de Seguridad de la Información con externos.

9.2. Es deber de todo proveedor del ISP, de acuerdo al nivel y tipo de Servicio o producto que entrega, informarse de las políticas de Seguridad de la Información que le apliquen, no pudiendo argumentar bajo ningún punto de vista ignorancia de ellas, asimismo, todo proveedor debe informar a su personal de éstas políticas y de los resguardos que se deben tomar para su cumplimiento.

9.3. El proveedor es directamente responsable de cualquier evento que involucre a alguien de su personal en un evento de Seguridad de la Información.

9.4. Se debe considerar las diferentes etapas de trabajo con proveedores en la Seguridad de la Información: asegurarse que el proveedor se informe antes, que sepa el cumplimiento durante la entrega del producto o servicio, considerando los posibles

cambios necesarios y sepa que después de terminados sus servicios también tiene responsabilidades en la materia.

9.5. Se deben acordar los requisitos de seguridad de la información para mitigar los riesgos asociados al acceso de los proveedores a los activos de la organización con el proveedor y se deberían documentar adecuadamente.

9.6. Los acuerdos con los proveedores deben incluir los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnologías de la información y comunicaciones.

9.7. Se deben controlar, revisar y auditar los servicios recibidos de terceros, en su definición a través de los contratos y durante su entrega mediante acuerdos de confidencialidad, monitoreo y revisión de lo recibido. Cualquier cambio en los servicios deberá pasar por los niveles de aprobación apropiados y ser formalizado a través de un contrato de servicio.

9.8. El Propietario de la Información debe autorizar todos los intercambios de datos y programas con terceros de acuerdo a las definiciones de ISP. Las atribuciones del propietario deben ser reguladas.

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
2		3. Alcance	Se complementa el Alcance incorporando los Procesos Operacionales.
		5. Referencias Normativas	-Se incorporan las siguientes referencias normativas: D.F.L. Núm. 1/19.653 de 2000; Ley Nº 19.880, DFL 1/2005; Decreto Supremo Nº 1.222/1996, del Minsal; Decreto Exento N° 324/2018; Decreto Supremo N°890/1975 del Ministerio de Interior; Resolución Exenta N° 1536/2018
		6. Documentos Relacionados	- Se incorporan nuevas Políticas y Procedimientos relacionados.
		7. Definiciones	- Se revisan las definiciones existentes y se agrega las definiciones de: Seguridad de la Información, integridad, disponibilidad , integridad, y usuario.
		8. Roles y Responsabilidades	- Se reemplaza el “Comité de Seguridad de la Información” por el “Comité único de Riesgo, de Calidad, y de Seguridad de la Información”

		9. Lineamientos 11. Denuncias y Notificaciones 12. Reevaluación de la Política 13. Cumplimiento	- Se actualiza los Lineamientos de la Política - Se indica que se debe notificar al correo seguridad.informacion@ispch,cl. - Se cambia el máximo a cada 4 años de acuerdo al Sistema de Gestión Integrado. - Se amplía el marco del cumplimiento de la Política.