POLÍTICA DE RELACIÓN CON LOS PROVEEDORES
INSTITUTO DE SALUD PÚBLICA DE CHILE

Fecha de Emisión: 12/12/2016
Versión: 2
Fecha de actualización: 09/08/2019

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 y el Sistema de Gestión Integrado, bajo las normas ISO 9001, ISO IEC 17025, ISO 15189, ISO IEC 17043, ISO 17034, ISO Guide 35 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 software en equipos y servidores de uso institucional.

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. ALCANCE.

El alcance de esta Política abarca a todos(as) los(as) funcionarios(as) de planta, contrata, honorarios y a toda 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, las bases de datos, las aplicaciones desarrolladas internamente, los equipos, las instalaciones, los sistemas y las redes.

Esta Política considera a todos los procesos operacionales, de apoyo y estratégicos que requieran en cualquiera de sus etapas la aplicación de controles de acceso tanto lógico como físicos.

Asimismo, esta incluye 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. Así esta política cubre toda la información impresa o en soporte papel, la almacenada electrónicamente, la trasmitida por correo u otro medio electrónico, la mostrada en películas o la utilizada 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 27001:2013:

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.

- El Decreto Supremo N°890, de 1975, del Ministerio de Interior que fija el texto actualizado y refundido de la Ley N°12.927, sobre seguridad del Estado;
- La Ley N°19.223, de 1993, del Ministerio de Justicia, que tipifica las figuras penales relativas a la informática;
- El Decreto Supremo N°1.222, de 1996, del Ministerio de Salud que aprueba el reglamento del Instituto de Salud Pública de Chile;
- El D.F.L. N°1-19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que fija texto refundido, coordinado y sistematizado de La Ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado;
- La Ley N°19.880, de 2003, del Ministerio Secretaría General de la Presidencia, que establece las bases de los procedimientos administrativos que rigen los actos de los órganos de la administración del Estado;
- La Ley N°19.880, de 2003, del Ministerio Secretaría General de la Presidencia, que establece las bases de los procedimientos administrativos que rigen los actos de los órganos de la administración del Estado;
- El Decreto Supremo N°83, de 2005, del Ministerio Secretaría General de la Presidencia, que aprueba la norma técnica para los órganos de la administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos;
- El D.F.L. N°1, de 2006, del Ministerio de Salud, que fija el texto refundido, coordinado y sistematizado del Decreto Ley N°2.763, de 1979, y de las Leyes N°18.933, de 1990, y N°18.469, de 1985;
- La Ley N°20.285, de 2008, del Ministerio Secretaría General de la Presidencia, sobre acceso a la información pública;

- La Ley N°20.521, de 2011, del Ministerio de Economía, Fomento y Turismo, que modifica la Ley N°19.628, de 1999, sobre protección de datos de carácter personal para garantizar que la información entregada, a través de predictores de riesgo, sea exacta, actualizada y veraz;
- La NCh-ISO 27001:2013, Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información – Requisitos;
- La Ley N°19.799, de 2014, del Ministerio de Economía Fomento y Reconstrucción, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma; y
- La Resolución Exenta N°1.536, de 2018, del Instituto de Salud Pública, que aprueba el código de ética del Instituto de Salud Pública de Chile.

6. DOCUMENTOS RELACIONADOS.

- La Resolución Exenta N°2761, del 30 de octubre de 2018, del Instituto de Salud Pública, que crea el Comité Único de Riesgo, de Calidad y de Seguridad de la Información;
- La Política nacional de ciberseguridad 2019-2022;
- La Política general de seguridad de la información del Instituto de Salud Pública de Chile;
- La Política de autenticación secreta del Instituto de Salud Pública de Chile.
- La Política de instalación y uso de softwares del Instituto de Salud Pública de Chile.
- La Política de teletrabajo del Instituto de Salud Pública de Chile.
- La Política de instalación y uso de redes del Instituto de Salud Pública.
- La Política de control de acceso del Instituto de Salud Pública de Chile.
- El Procedimiento de ejecución de compras y contrataciones, PR-620.00.002;
- El Procedimiento de imparcialidad presiones indebidas y confidencialidad,. PR-643.00-002;
- El Instructivo gestión de incidencias (Contingencias), IT-610.00-001;
- El Procedimiento de mantenciones preventivas y correctivas del equipamiento computacional, PR-611.00-001;
- El Procedimiento respaldo de servidores, PR-611.00-003;
- El Procedimiento control de acceso de usuarios a sistemas, PR-611.00-004;
- El Procedimiento de gestión de proyectos y sistemas, PR-611.00-011.
- El Procedimiento de monitoreo, registro y protección de registro de eventos, PR-611.00-013;
- El Instructivo asignación de equipamiento tecnológico de administración TIC, IT-611.00-002;
- El Instructivo pérdida de equipamiento tecnológico de administración TIC, IT-611.00-003; y
- El 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, entre otra);
  - Los equipos, sistemas e infraestructura que soportan esta información; y
  - 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**: 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:** 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.

	Funciones, según Resolución Exenta N° 2761/2018, en el ámbito de la Gestión de la Seguridad de la Información:
Comité Único de Riesgo, de Calidad y de 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; y • 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; y • 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 esta 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 las ellas. Asimismo, todo proveedor debe informar a su personal de estas 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 de que el proveedor se informe en la licitación o etapa previa, 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. Los ITC deben asegurase de incorporar 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 debería 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. Los ITC deben 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 explícitamente en los contratos.

10. DIFUSIÓN.

Esta Política será difundida de acuerdo al control de la información documentada del Sistema de Gestión Integrado. Así también, el Encargado de Seguridad de la Información gestionará su actualización en la web institucional.

11. DENUNCIAS Y NOTIFICACIONES.

El personal del ISP, sus proveedores o terceros deben notificar inmediatamente 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, al correo electrónico: seguridad.información@ispch.cl.

12. REVISIÓN DE LA POLÍTICA.

Esta Política deberá ser revisada de acuerdo al PR-100.00-001, Procedimiento Control de la Información Documentada (que a la fecha considera un máximo de 4 años), o en la medida que el análisis de riesgo lo amerite.

13. CUMPLIMIENTO.

Todo el personal del Instituto de Salud Pública de Chile, entiéndase como tal a funcionarios(as) de planta, a contrata, reemplazo, suplencia, estudiante en práctica, asesor, consultor, honorarios y cualquier persona que desempeñe funciones en o para el Instituto de Salud Pública de Chile,

deberá dar cumplimiento, en lo que le corresponda, a esta Política General de Seguridad de la Información y a las específicas que le apliquen.

Para el caso de terceros, y por el solo hecho de participar en un proceso de compras del servicio, el oferente deberá dar cumplimiento a las políticas, procedimientos e instructivos vigentes que se encuentren publicados en la página web del Instituto de Salud Pública, http://www.ispch.cl/seguridad_informacion/politicas, lo que se presume conocido 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 incorpora las siguientes referencias normativas: D.F.L. Núm. 1/19.653 de 2000; Ley N°19.880, DFL 1/2005; Decreto Supremo N°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 incorpora nuevas políticas y procedimientos relacionados.
		7. Definiciones	→ Se revisa 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	→ Se actualiza los Lineamientos de la Política.
		11. Denuncias y Notificaciones	→ Se indica que se debe notificar al correo seguridad.informacion@ispch,cl.
		12. Reevaluación de la Política	→ Se cambia el máximo a cada 4 años de acuerdo al Sistema de Gestión Integrado.
		13. Cumplimiento	- Se amplía el marco del cumplimiento de la Política.