POLÍTICA DE INSTALACIÓN Y USO DE SOFTWARE Y PREVENCIÓN CONTRA CÓDIGO MALICIOSO INSTITUTO DE SALUD PÚBLICA DE CHILE

Fecha de Emisión: 09/08/2019
Versión: 1
Fecha de actualización: 21/11/2019

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 Of 2013 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.

Establecer las medidas para la instalación y la utilización de software en equipos computacionales y servidores, pertenecientes al Instituto de Salud Pública, con el fin de asegurar la continuidad operativa, y prevenir fallas de los sistemas y ataques debido a malware.

3. ALCANCE.

El alcance de esta Política incluye 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, 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 software.

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, almacenada electrónicamente, trasmitida por correo o usando medios electrónicos, mostrada en películas o hablada en una conversación.

4. REQUISITO DEL CONTROL NORMATIVO ISO 27001:2013.

- Aplica a los Controles del Dominio 12 “Seguridad de las operaciones” en cualquier ámbito definido en el alcance.

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 Decreto con Fuerza de Ley 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;
- 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 Decreto con Fuerza de Ley 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 Norma Ch-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, 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 Control de Acceso del Instituto de Salud Pública de Chile;
- La Política de Autenticación secreta del Instituto de Salud Pública de Chile;
- La Política de Teletrabajo del Instituto de Salud Pública de Chile;
- La Política de Relación con Proveedores 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;
- 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).
- **Red:** Conexión entre equipos computacionales que permite compartir datos y recursos.
- **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.
- **Código Malicioso:** El código malicioso es un tipo de código informático o script web dañino diseñado para crear vulnerabilidades en el sistema que permiten la generación de puertas traseras, brechas de seguridad, robo de información y datos, así como otros perjuicios potenciales en archivos y sistemas informáticos.

8. ROLES Y RESPONSABILIDADES.

Comité Único de Riesgo, de Calidad, y de Seguridad de la Información	**Funciones según Resolución Exenta N° 2761, de 2018,del Instituto de Salud Pública de Chile, 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 ISP; • 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 afecten 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 Direcciónde l 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 genere como resultado de los reportes o propuestas del Comité . Único de Riesgo, de Calidad y de Seguridad de la Información.

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; y • Promover al interior de su equipo de trabajo tanto la denuncia como la respuesta, cuando 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 instalación y uso de software y prevención contra código malicioso; y • Reportar los incidentes de seguridad detectados en el ámbito del instalación y uso de software y prevención contra código malicioso

9. LINEAMIENTOS DE LA POLÍTICA.

9.1 Está prohibida la instalación y/o uso de software no autorizado por el área Tecnología de la Información y Comunicaciones.

9.2 El área Tecnología de la Información y Comunicaciones TIC es responsable de administrar la lista de aplicaciones permitidas.

9.3 El área Tecnología de la Información y Comunicaciones es responsable de administrar los accesos y restricciones de navegación sobre sitios web, para lo cual deberá considerar herramientas informáticas de gestión de listas blancas y negras.

9.4 Todo software existente y que no sea de administración TIC debe ser informado formalmente al área Tecnología de la Información y Comunicaciones.

9.5 Cuando se desee instalar cualquier software, sea o no de administración TIC, la jefatura respectiva debe hacer la solicitud a la Unidad Tecnología de la Información y Comunicaciones quien estará encargado de hacer la instalación. El uso de software no licenciado está estrictamente prohibido. Todo software que se pretenda instalar debe guardar relación con las áreas de competencia institucionales.

9.6 El(la) usuario(a) es responsable de dar aviso la Unidad Tecnología de la Información y Comunicaciones, por medio de la mesa de ayuda institucional, de cualquier anomalía detectada en relación al funcionamiento de un software.

9.7 La Unidad Tecnología de la Información y Comunicaciones es responsable de la eliminación de software de equipos computacionales que sean posibles amenazas para la seguridad de los datos, previo análisis con la persona responsable de autorizar el uso del software.

9.8 Está prohibido abrir software, archivos ejecutables o macros desde algún correo de fuente desconocida, sospechosa o que no sea de confianza. Si el(la) usuario(a) recibe un correo con contenido sospechoso debe dar aviso la Unidad Tecnología de la Información y Comunicaciones para que tome las medidas pertinentes.

9.9 Con el fin de mitigar las vulnerabilidades, el equipamiento computacional de la institución debe contar con conexiones que provean de forma segura actualizaciones automáticas de seguridad para los sistemas operativos y aplicaciones que corresponda.

9.10 El equipamiento computacional de la institución conectado al dominio organizacional debe contar con la instalación de un software de detección, análisis y reparación de malware.

9.11 En el caso de que un equipo computacional no sea propiedad de la institución, este deberá contar con antivirus actualizado y actualizaciones de seguridad al día. Esta validación la realizará la Unidad Tecnología de la Información y Comunicaciones antes de la conexión del equipo a la red.

9.12 La actualización de software, así como las actualizaciones y parches de seguridad, en el ambiente operacional, debe ser realizado por la Unidad Tecnología de la Información y Comunicaciones.

9.13 La Unidad Tecnología de la Información y Comunicaciones debe estar en condiciones de hacer un restablecimiento a un estado anterior en el ambiente operacional en caso de fallas por instalaciones nuevas (proceso de Rollback).

9.14 La Unidad Tecnología de la Información y Comunicaciones debe implementar un control de versión del software.

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 toda debilidad, incidente o evento asociado a actividades no permitidas o malas prácticas de acceso que pudieran derivar en un posible incumplimiento, uso indebido u otra situación asociada, inmediatamente, al correo seguridad.informacion@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 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 ISP, deberá dar cumplimiento, en lo que le corresponda, a esta Política.

Para el caso de terceros, y por el solo hecho de participar en un proceso de compras del ISP, 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 las Modificaciones
1	21/11/2019	Título	- Se amplía el título a “prevención contra código maliciosa”
		2. Objetivo	- Se incorpora en el objetivo la prevención contra malware.
		3. Alcance	- Se corrigen el párrafo 2 del Alcance
		7. Definiciones	- Se incorpora la definición de “Código malicioso”
		9. Lineamientos de la Política	Se corrigen los lineamientos existentes y se incorporan lineamientos que incluyen la prevención contra código malicioso.
		12. Revisión de la Política	- Se mejora la redacción.