POLÍTICA DE SEGURIDAD FISICA Y AMBIENTAL

INSTITUTO DE SALUD PÚBLICA DE CHILE

Fecha de Emisión: 07/12/2016
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 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 gestionar el uso, disposición y protección de todos los Activos de Seguridad de la Información.

2. OBJETIVO.

Colaborar en el cuidado de los Activos de Información previniendo el acceso no autorizado, daños, interferencias, pérdidas o compromiso de los bienes, evitando así los daños que pueden dañar al Instituto de Salud Pública en el desarrollo de sus funciones e imagen.

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 utilización de Activos de Información.

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 27001:2013.

Aplica a los Dominios:
- N° 8 “Administración de Activos”.
- N° 11 “Seguridad Física y Ambiental”

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;
- Política de gestión de riesgo del ISP.
- 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;
- Política de autenticación secreta del Instituto de Salud Pública de Chile;
- Política de trabajo remoto 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 del Instituto de Salud Pública de Chile;
- Política de gestión y uso de redes del Instituto de Salud Pública de Chile;
- Política de desarrollo seguro;
- Política de aseguramiento de continuidad de la seguridad de la información;
- Política de respaldo de información digital, software y sistemas;
- Política de gestión de activos;
- Política de gestión de medios removibles;
- Procedimiento de ejecución de compras y contrataciones, PR-620.00.002;
- Procedimiento de reclutamiento y selección de personal PR-645.00-001;
- Procedimiento de imparcialidad presiones indebidas y confidencialidad,. PR-643.00-002;
- Procedimiento de Mantenciones preventivas y correctivas del equipamiento computacional PR-140.03.001
- Procedimiento de eliminación segura para la reutilización o descarte de equipos, medios de soporte o documentación física. PR-140.03.003
- Procedimiento Respaldo de servidores y Sistemas Institucionales PR-140.02.002

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.

Comité Único de Riesgo, de Calidad y de Seguridad de la Información	**Funciones, según Resolución Exenta N° 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; 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 como la respuesta a los incidentes de seguridad de la información, cuando se solicite.
Usuario(a)	• 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. Todos los activos de información físicos clasificados como críticos deben ser protegidos de accesos no autorizados, en áreas seguras y controladas.

9.2. El ISP debe establecer controles que protejan a la información y a los activos físicos que la procesan, de la divulgación, modificación o robo por personas no autorizadas.

9.3. Los equipos deben ser ubicados en lugares protegidos de modo de reducir el riesgo de accesos no autorizados y de amenazas.

9.4. Se debe proteger los equipos, según sus características, de fallas e interrupciones asegurando la periódica mantención de los equipos de soporte y respaldo, y tomando las medidas necesarias cuándo terceros desarrollen trabajos que puedan interferir con su normal desempeño.

9.5. Los trabajos realizados por terceros deberán entregar toda la documentación relacionada con proyectos y mantenciones del equipamiento del ISP.

9.6. Para las labores de carga y descarga, deben estar claramente definidas las áreas en las cuáles los externos se pueden desplazar e instalar para realizar ésta labor

9.7. El cableado de energía y telecomunicaciones que transporta datos o soporta servicios de información debe ser protegido de intercepciones o daño.

9.8. La instalación y mantención de cables de energía y líneas de telecomunicaciones, debe ser realizada por personal capacitado que sigan los estándares de calidad y seguridad de la industria y que cuenten con la certificación pertinente.

9.9. El equipamiento debe ser correctamente mantenido de modo de asegurar continuidad, disponibilidad e integridad.

9.10. Los equipos institucionales, no deben salir de las instalaciones del Instituto de Salud Pública sin la debida autorización.

9.11. Todos los funcionarios con oficinas personales deben asegurar el cierre de las puertas cuando estas oficinas no estén en uso, de manera que sólo el personal autorizado pueda tener acceso a ellas.

9.12. Nunca se debe realizar visitas de público a los centros de datos e instalaciones de comunicaciones (áreas seguras en general).

9.13. Los funcionarios no deben comer o beber, en áreas seguras, sala de servidores, áreas sensibles, donde se ubiquen equipos computacionales.

9.14. El personal de ISP debe mantener debido resguardo y reserva de la ubicación física de su sala de equipos y áreas sensible, no debe ser divulgada ya que podría ser utilizada para provocar daños en los activos de información de la organización.

9.15. Los funcionarios deben mantener sus escritorios y áreas de trabajo ordenadas, no tener documentación sensible a la vista con el objetivo de que ésta no quede al alcance de personas malintencionadas. Los funcionarios deberán dejar bloqueados y asegurados físicamente bajo llave sus equipos computacionales móviles cuando se ausenten de sus puestos de trabajo.

9.16. Los dispositivos utilizados para imprimir o copiar información sensible deben ubicarse dentro de áreas seguras o bajo la supervisión de algún funcionario designado. También se deberá propender a incorporar mecanismos de seguridad en sus accesos. Será responsabilidad de cada funcionario el retirar sus documentos tan oportunamente como sea necesario para asegurar que no sean accedidos por terceros.

9.17. El equipamiento que realiza labores de procesamiento de información crítica (servidores), debe tener medidas de seguridad adecuada o especial acorde con su criticidad y las respectivas señalizaciones de restricción de acceso.

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.

10. 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.

11. 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

12. 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.

13. CONTROL DE CAMBIOS.

Versión	Fecha	Principales Puntos Modificados	Resumen de Modificaciones
V2		- Introducción - Objetivo	- Se actualiza la Introducción - Se redacta un nuevo Objetivo General

		- Alcance. - Requisito del control normativo iso 27.001:2013. - Referencias normativas. - Documentos relacionados. - Definiciones. - Roles y responsabilidades. - Lineamientos de la presente politica. - Difusión. - Denuncias y notificaciones. - Revisión de la política.	de la Política. - Se mejora el Alcance - Se incorpora requisito de Control Normativo. - Se incorporan y actualizan referencias normativas. - Se incorporan y actualizan documentos relacionados. - Se incorporan y mejoran definiciones. - Se incorporan “roles” y se amplían los contenidos. - Se mejora redacción de lineamientos. - Se actualiza - Se incorporan el punto “denuncias y notificaciones”. - Se cambia “reevaluación” por “revisión de la política y se actualiza.”