POLÍTICA

DE DESARROLLO SEGURO

INSTITUTO DE SALUD PÚBLICA DE CHILE

Fecha de Emisión: 21/11/2019
Versión: 2
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 generales que debe seguir todo equipo de desarrollo de software al interior del Instituto de Salud Pública y los grupos de desarrollo de los proveedores, exigiendo la construcción de sistemas de alta calidad en las instituciones en las etapas de diseño, desarrollo, pruebas, marcha blanca y en ambiente de producción.

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 controles de continuidad operacional.

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

5. REFERENCIAS NORMATIVAS.

- El Decreto con Fuerza de Ley. N° 1/19.653, de 2000, del Ministerio de Salud, que fija texto refundido, coordinado y sistematizado de La Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado;
- La Ley N° 19.880, de 2018, 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°20.285, de 2008, del Ministerio Secretaría General de la Presidencia sobre acceso a la información pública.;
- El Decreto con Fuerza de Ley N° 1, de 2005, 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 y N° 18.469”;
- El Decreto Supremo N° 1.222, de 1996, del Ministerio de Salud, que aprueba el Reglamento del Instituto de Salud Pública de Chile;
- La Ley N°19.223, de 1993, del Ministerio de Justicia, que tipifica figuras penales relativas a la informática;
- El Decreto Supremo N°890, de 1975, del Ministerio de Interior, que fija texto actualizado y refundido de la Ley 12.927, sobre seguridad del Estado;
- La Resolución Exenta N°1536, de 2018, del Instituto de Salud Pública, que aprueba el Código de Ética del Instituto de Salud Pública de Chile;
- La Ley N°19.799, de 2014, del Ministerio de Economía Fomento y Turismo, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma;
- La Ley N°20.521, de 2011, del Ministerio de Economía, Fomento y Turismo, que 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;

- 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; y
- La Norma Ch-ISO 27001:2013, Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos.
-

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 Ciber Seguridad 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;
- La Política de Instalación y Uso de Softwares;
- El Procedimiento de Ejecución de Compras y Contrataciones, PR-620.00.002;
- El 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 Restauración de Información PR-140.02.006
- Procedimiento Control de Acceso a Sistemas Computacionales PR-140.03.002
- Instructivo Plan de Pruebas QA IT-140.01.001
- 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
- El documento Estrategia de Trabajo Red SSI 2019.

7. DEFINICIONES.

- **Activos de Información:** 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 constituye por:
    - La Información propiamente tal, en sus múltiples formatos (papel; digital; texto; imagen; audio; video; transmisión verbal, etcétera).
    - Los equipos, sistemas e infraestructura que soportan esta información.
    - las personas que utilizan la información y que tienen el conocimiento de los procesos institucionales.
- **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.
- **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).
- **Disponibilidad:** Propiedad de estar disponible y utilizable, según requisito de una entidad autorizada, (Ref ISO 27000:2018)
- **Integridad:** Propiedad de precisión y exhaustividad, (Ref ISO 27000:2018).
- **Malware:** Software malicioso diseñado para causar daños o provocar mal funcionamiento a equipos computacionales independientes o conectados a la red.
- **Negocio:** Bien o servicio prestado por una organización.
- **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**: Persona 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 de que se pueda definir los controles apropiados para protegerla.
- **Red:** Conexión entre equipos computacionales que permite compartir datos y recursos.

- **Riesgo de Seguridad de la Información**: 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.
- **Seguridad de la Información:** Preservación de la confidencialidad, integridad y disponibilidad de la información, (Ref ISO 27000:2018).
- **Software:** Producto intangible que permite a un equipo computacional desempeñar diversas tareas por medio de instrucciones lógicas, a través de diferentes tipos de programas.
- **Usuario:** 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 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 Dirección 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 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 desarrollo seguro; y • Reportar los incidentes de seguridad detectados en el ámbito del desarrollo seguro.

9. LINEAMIENTOS DE LA PRESENTE POLÍTICA.

9.1. Para mantener la seguridad de los desarrollos, se deberá implementar una separación de ambientes para desarrollo, aseguramiento de la calidad (QA) y producción.

9.2. La Unidad o de TIC debe proporcionar los requisitos técnicos necesarios para cada proceso selección del RR.HH. de manera de asegurar el conocimiento técnico y confiabilidad del personal del área.

9.3. Cada uno de los ambientes deberá contar con los niveles de restricción y acceso que permitan asegurar su independencia y adecuado código de versión (bitbucket) de los proyectos y mantenciones.

9.4. Todo lineamiento de seguridad debe ser incluido en los requisitos para los sistemas de información nuevos o mantenciones de los sistemas de información existentes.

9.5. Se debe definir y estandarizar los criterios de seguridad y de calidad en cada fase del ciclo de desarrollo de los sistemas.

9.6. Los criterios de seguridad deben abarcar el uso de librerías y framework de seguridad de autores confiables y actualizados.

9.7. Las consultas a las bases de datos deben considerar la seguridad necesaria para mitigar y prevenir ataques, implementando medidas de protección acorde a la tecnología y plataforma vigentes utilizada.

9.8. La validación de los datos debe utilizar técnicas que aseguren que solo los datos con el formato correcto podrán ser utilizados en los sistemas que se desarrollará.

9.9. La información de los proyectos debe mantenerse independiente de cada uno de ellos, para asegurar su consistencia e integridad, considerando además cada uno de los ambientes de desarrollo, aseguramiento de calidad (QA) y producción.

9.10. Los desarrolladores deben monitorear de manera continua el proceso de diseño y construcción, a fin de evitar, encontrar y solucionar vulnerabilidades en los sistemas.

9.11. Se debe considerar las normas de codificación, y dónde sea necesario, obligar su uso.

9.12. En las pruebas de aseguramiento de calidad (QA), se debe verificar la seguridad en los hitos del proyecto.

9.13. En el marco del desarrollo seguro las pruebas de seguridad de la información se verificarán de acuerdo a lo siguiente:

9.13.1. Confidencialidad consiste en la capacidad de garantizar que la información, almacenada en el sistema informático o transmitida por la red, solamente va a estar disponible para aquellas personas autorizadas a acceder a dicha información, es decir, que, si los contenidos cayesen en manos ajenas, estas no podrían acceder a la información o a su interpretación. Es necesario acceder a la información mediante autorización y control.

9.13.2. Integridad supone que la información se mantiene inalterada ante accidentes o intentos maliciosos. Sólo se podrá modificar la información mediante autorización.

9.13.3. La disponibilidad supone que el sistema informático se mantenga trabajando sin sufrir ninguna degradación en cuanto a accesos. Es necesario que se ofrezcan los recursos que requieran los usuarios autorizados cuando se necesiten. La información deberá permanecer accesible a elementos autorizados.

9.14. Para conseguir los objetivos de la confidencialidad, integridad y disponibilidad se utilizan los siguientes mecanismos:

- Autenticación, que permite identificar al emisor de un mensaje, al creador de un documento o al equipo que se conecta a una red o a un servicio.
- Autorización, que controla el acceso de los usuarios a zonas restringidas, a distintos equipos y servicios después de haber superado el proceso de autenticación.
- Encriptación, que ayuda a ocultar la información transmitida por la red o almacenada en los equipos, para que cualquier persona ajena no autorizada, sin el algoritmo y clave de descifrado, pueda acceder a los datos que se quieren proteger.
- Realización de copias de seguridad e imágenes de respaldo, para que en caso de fallos nos permita la recuperación de la información perdida o dañada.
- Antivirus, como su nombre indica, consiste en un programa que permite estar protegido contra las amenazas de los virus.
- Cortafuegos o firewall, programa que audita y evita los intentos de conexión no deseados en ambos sentidos, desde los equipos hacia la red y viceversa.
- Utilización firma electrónica o certificado digital, son mecanismos que garantizan la identidad de una persona o entidad evitando el no repudio en las comunicaciones o en la firma de documentos.

9.15. La Unidad de TIC, debe elaborar y mantener una lista de todos los sistemas de información indicando la criticidad de cada uno.

9.16. El desarrollo de trabajo externo debe seguir los mismos lineamientos definidos en esta Política.

10. DIFUSIÓN.

Esta Política será difundida de acuerdo al control de la información documentada bajo el 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 que pudiera 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 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 ISP, deberá dar cumplimiento en lo que le corresponda de esta Política General de Seguridad de la Información y de las específicas que les aplique.

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 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, 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 las Modificaciones
1		6. Documentos relacionados 9. Lineamientos de la siguiente política	- Se actualizan documentos relacionados de acuerdo a sus nuevos códigos. - Se incorporan los lineamientos 9.13 y 9.14.