POLÍTICA DE TRABAJO REMOTO

INSTITUTO DE SALUD PÚBLICA DE CHILE

Fecha de Emisión: 30/11/2011
Versión: 3
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.

Entregar las directrices para mitigar los riesgos cuando se realice actividades de trabajo con conexiones remotas o en dependencias fuera del ISP.

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 27001:2013.

Aplica al Dominio 13 “Seguridad en las comunicaciones” 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 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 control de acceso del Instituto de Salud Pública de Chile;
- Política de autenticación secreta del Instituto de Salud Pública de Chile.
- Política de teletrabajo 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.
- 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.

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. Trabajo Remoto o Teletrabajo.

9.1.1 Solo podrán realizar trabajo remoto en los sistemas del Instituto de Salud Pública aquellas personas con vínculo de cualquier naturaleza con la Institución, previamente autorizadas, de acuerdo al Procedimiento de Control de Acceso de Usuarios a Sistemas.

9.1.2 Las conexiones de trabajo remoto realizadas por los(as) funcionarios(as) del ISP y con sistemas de la Institución, desde cualquier lugar situado fuera de las instalaciones de la Institución, deben estar controladas de modo que se asegure la autenticación de los(as) usuarios(as) que acceden, la autorización para realizar dicho acceso, la confidencialidad de la información transmitida, la limitación de los recursos accedidos por el empleado y la supervisión de las mismas. Estos controles deben ajustarse a lo indicado en la Política de Control de Acceso y el Procedimiento Control de Acceso de Usuarios a Sistemas.

9.1.3 El equipo de trabajo entregado al(a la) funcionario(a) debe cumplir con lo establecido en la Política de Retiro de Activos y estar protegido frente a accesos no autorizados, software dañino y ataques provenientes de Internet. Adicionalmente, el(la) usuario(a) debe garantizar la seguridad física de los equipos bajo su responsabilidad y comprometerse a usarlos exclusivamente para actividades relacionadas con su trabajo institucional, además de la seguridad asociada al uso de redes domésticas, las configuraciones de los servicios de redes inalámbricas, así como la seguridad física y digital relacionada al equipamiento tecnológico (Candados físicos, empotramiento del equipamiento, antivirus actualizados, etc.) que se utilicen para trabajo remoto.

9.1.4 El entorno de trabajo remoto físico debe considerar, al menos, la seguridad física del recinto (uso de candados para equipamiento tecnológico móvil), la seguridad lógica del equipamiento (dispositivos con antivirus licenciados y actualizados) y del entorno local donde se encuentre, una conexión a internet segura y la confidencialidad de la información manejada.

9.1.5 El Subdepartamento TIC, a través de la Sección Administración de Plataforma y Comunicaciones, será responsable de generar la entrega de equipamiento informático y accesos requeridos para el uso de los mismos, bajos los procedimientos establecidos para ello, para equipos de responsabilidad del ISP. Si el equipo es de propiedad privada, se debe cumplir con lo indicado en la Política de Retiro de Activos.

9.2. Acceso Remoto.

9.2.1 Los servicios de acceso remoto permitidos son aquellos que respondan a necesidades de la Institución, tales como desarrollo, mantenimiento y soporte. En estos casos, existen mecanismos técnicos para manejar convenientemente la información transmitida, los sistemas y recursos accedidos, la identidad de los individuos que realizan dichos accesos y las posibles implicancias que el acceso conlleva.

9.2.2 Los servicios de acceso remoto deben ser asignados de manera exclusiva a través de lo descrito en el Procedimiento de Control de Acceso de Usuarios a Sistemas.

9.2.3 El acceso remoto asignado por el Subdepartamento TIC es generado por medio de un protocolo específico para el establecimiento de una VPN de manera directa entre el equipo que se conectará desde el exterior y el cortafuego (firewall) y los sistemas internos de la Institución, proporcionando acceso a los recursos de la red de datos institucional y generando tráfico de datos bajo un formato encriptado, de manera controlada y segura. Con ello, se evita el procesamiento y almacenamiento de información en equipos de propiedad privada.

9.2.4 Las configuraciones de hardware no estándar deben ser aprobadas por la sección de Administración de Plataformas y Comunicaciones, quien requiere aprobar dichas configuraciones de seguridad del hardware para permitir el acceso remoto. De igual modo, los(as) usuarios(as) que deseen implementar soluciones de tecnologías de la información de acceso remoto a la red del ISP deberán obtener, en primer lugar, la autorización por parte de la mencionada sección.

9.2.5 En caso de uso de equipamiento tecnológico con acceso remoto, bajo entornos de redes domésticas o públicas, se deberá asegurar de que esta siempre contenga mecanismos de seguridad. Con ello, será de exclusiva responsabilidad del(de la) usuario(a) su utilización en locales de uso masivo donde la forma de conexión no sea cifrada o de redes abiertas al público en general (Por ejemplo: cafeterías, cibercafés, lugares de esparcimiento o

turísticos, entre otros), y las implicancias relacionadas con materias de seguridad de la información.

9.2.6 Para los casos en que exista problemas en la utilización correcta del acceso remoto, tanto por el método de conexión como en el equipamiento utilizado (En caso de que este pertenezca al ISP), el solicitante debe generar una solicitud con el requerimiento específico a través de los mecanismos descritos en los procedimientos establecidos para ese efecto.

9.3. Consideraciones Generales.

9.3.1. Para minimizar el riesgo de acceso de entrada a las redes del ISP no autorizadas, un(a) usuario(a) remoto nunca deberá almacenar sus contraseñas en archivos en forma de texto o en documentos visibles a personas externas a la Institución. Además, se prohibe el uso, por parte de personas que no pertenezcan a la organización (Familiares, amigos, conocidos, entre otros.), de equipos con una conexión establecida a la red privada virtual.

9.3.2. Está prohibido el uso de todo tipo de dispositivos electrónicos y/o informáticos (Tales como módems externos, BAM modificadas, entre otros), para saltarse el cortafuego (firewall), salvo en casos excepcionales y bajo la autorización y supervisión de la jefatura del Subdepartamento TIC.

9.3.3. Como mecanismo de seguridad y auditoría interna, se realizará monitoreos continuos para verificar los accesos, además de contar con un método para identificar al(a la) usuario(a) remoto y para determinar si está o no autorizado(a). Para ello, será necesario el uso de un identificador de usuario(a) y de un software de control de acceso.

9.3.4. Con el fin de mantener la confidencialidad de la información a la cual se accede mediante el mecanismo de trabajo remoto, todo(a) funcionario(a) o proveedor de servicios debe tener firmado el documento "Compromiso de imparcialidad, presiones indebidas, confidencialidad y seguridad de la información", RG-01-PR-643.00-002, según lo indicado en el Procedimiento de Imparcialidad, Presiones Indebidas y Confidencialidad (Para el caso de funcionarios(as) del ISP), como en el Procedimiento Ejecución Compras y Contrataciones (Para personal externo que preste servicios en el Instituto).

9.3.5. Las medidas de seguridad exigibles deben ser lo más completas posibles, tanto para el caso físico (Espacio físico utilizado, uso de equipamiento tecnológico siempre a la vista del usuarios(as), entre otros), como para los accesos a datos de carácter personal, a través de redes de comunicaciones, los que deben garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local. Se realizará estas conexiones utilizando los mecanismos técnicos que garanticen que la información es íntegra y confiable.

9.3.6. Está prohibido transmitir identificadores de usuario, contraseñas o credenciales, configuraciones de la red interna y/o direcciones a través del acceso remoto. En caso de ser necesario, esta información debe ser enviada de manera cifrada.

9.3.7. En caso de pérdida, robo o hurto del equipamiento tecnológico, si fuese propiedad del ISP, utilizado para trabajo remoto, se debe aplicar el Instructivo de Perdida de Equipos Tecnológico de Administración TIC.

9.3.8. La notificación de toda situación anómala, referida a trabajo remoto, debe formalizarse mediante correo electrónico a seguridad.información@ispch.cl.

9.3.9. Solo el equipamiento tecnológico, tanto de propiedad del ISP como los que forman parte del parque de arrendamiento asociado al contrato vigente de servicio específico, forma parte de los procesos de respaldos descritos en el Procedimiento de Respaldo de Servidores.

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.información@ispch.cl.

11. REVISIÓN DE LA POLÍTICA.

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. 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
V3	-	-	-