



Gobierno  
de Chile

MINISTERIO DE SALUD

DIVISIÓN JURÍDICA

SECRETARÍA DE REDES ASISTENCIALES

JEFE DE GABINETE

VISTADO

SECRETARÍA DE REDES ASISTENCIALES

APRUEBA POLÍTICA DE CONTROL DE ACCESO.

EXENTA N° 1157 /

SANTIAGO, 29 DIC. 2014

**VISTOS:** Lo dispuesto en la ley N° 19.880 que establece Bases de los Procedimientos Administrativos; en el D.F.L N°1, de 2005, del Ministerio de Salud, que fija el texto refundido, coordinador y sistematizado del decreto ley N° 2763, de 1979 y las leyes N° 18.933 y N°18.469; en el decreto supremo N° 136, de 2004, del Ministerio de Salud, que aprueba Reglamento Organico del Ministerio de Salud; en la ley N° 19.799 sobre documentos electronicos, forma electronica y servicios de certificación de dicha firma; en el D.S N° 83, de 2004, del Ministerio Secretaria General de la Presidencia, que aprueba Norma Técnica para Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos; en la ley N° 19.233 sobre delitos informaticos; en la Norma Chilena NCh-ISO 27001.OI2009 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos; en el Memorándum A22 N° 178, de 29 de octubre de 2014, del Jefe de Departamento Gestión Sectorial de TIC; en la resolución N° 1.600, de 2008, de la Contraloría General de la República; y

#### CONSIDERANDO:

1° Que, las nuevas tecnologías de la información y de las comunicaciones (TIC) al ser incorporadas progresivamente a los procesos institucionales y al quehacer personal de los funcionarios al ejercer sus labores en el Ministerio de Salud, presentan una serie de beneficios, ventajas y oportunidades de diversa índole, pero conlleva también ciertos riesgos, que pueden afectar a los activos de información institucional.

2° Que, se oficializó la norma técnica sobre seguridad y confidencialidad del documento electrónico para los órganos de la Administración del Estado a través del Decreto Supremo N°83, del Ministerio Secretaria General de la Presidencia, de 2005.

3° Que, por consiguiente, gestionar la seguridad de la información es un imperativo que se debe cumplir en el marco de la normativa gubernamental existente, tales como: Ley N° 19.799, 2002 sobre documentos electrónicos, firma electrónica y servicios de certificación de firma del Ministerio de economía Fomento y Reconstrucción, Ley N° 19.628, de 1999 sobre protección a la vida privada y datos personales del Ministerio Secretaria General de la Presidencia, Ley N° 19.223, de 1993 sobre delitos informáticos del Ministerio de Justicia, y que consiste básicamente en la realización de todas aquellas actividades y tareas que sean necesarias para establecer los niveles de seguridad que la propia institución determine, basándose para ello en metodologías y técnicas estándares en estas materias, con el firme propósito de lograr introducir un ciclo de mejoramiento continuo y sostenible en el tiempo, que permita lograr niveles de integridad, confidencialidad y disponibilidad, con todos sus

activos de información relevantes para la institución, como un principio clave en la gestión de procesos.

4° Que, debido a la implementación del sistema de seguridad de la información en conjunto por la Subsecretaría de Redes Asistenciales y la Subsecretaría de Salud Pública, se ha creado la Política General de Seguridad de Información, la cual se aprobó para este año 2014, mediante Resolución Exenta N° 781 del 14.10.2014, de ambas Subsecretarías, según los requisitos de la Norma NCh-ISO 27001 y lo dispuesto por la red de expertos, quienes tienen por función asesorar al Ministerio del ramo en el proceso de formulación, ejecución, preevaluación, evaluación y seguimiento de los Programas de Mejoramiento de Gestión. (Decreto N° 334, dc 2012 del Ministerio de Hacienda, que aprueba el reglamento a que se refiere el artículo 6° de la Ley N° 19.553 para la aplicación del incremento por desempeño institucional que indica).

5° Que, mediante memorandum A22 N° 178, de 2014 de Jefe del departamento de Gestión Sectorial de TIC, se solicitó aprobar las Políticas del PMG Sistema de Seguridad de la Información, en el marco de las metas de gestión año 2014, aprobadas mediante Decreto Exento N° 1290, de 2013 del Ministerio de Salud y Ministerio de Hacienda.

6° Que, conforme a lo anterior, resulta necesario contar con una política de autorización de nuevos recursos de procesamiento de información, y por consiguiente, dicto la siguiente:

#### **RESOLUCIÓN:**

**1° APRUÉBASE** la Política de control de acceso para la Subsecretaría de Salud Pública y la Subsecretaría de Redes Asistenciales, cuyo texto es el siguiente:

#### **POLÍTICA CONTROL DE ACCESO**

##### **1. PROPOSITO**

Establecer las definiciones que regulan el acceso a los medios compartidos de información del Ministerio de Salud (MINSAL).

##### **2. ALCANCE**

Esta política se aplica a toda información que se encuentra en las carpetas compartidas, bases de datos, sistemas computacionales, servidores, etc. del MINSAL.

Esta política es aplicable a todos los funcionarios (planta, contrata, reemplazos y suplencia), personal a honorarios y terceros (proveedores, compra de servicios, etc.), que presten servicios para las Subsecretarías de Salud Pública y Redes Asistenciales.

##### **3. DOCUMENTOS RELACIONADOS<sup>1</sup>**

- Procedimiento gestión de derechos de acceso y devolución de activos.
- NCh-ISO27001.Of2009 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información – Requisitos, punto 11.1.1.
- Normativa del Sistema de Gestión de Seguridad de la Información.

<sup>1</sup> Las políticas o procedimientos referenciados pueden ser consultados en [http://web.minsal.gub.ve/seguridad\\_de\\_la\\_informacion](http://web.minsal.gub.ve/seguridad_de_la_informacion)

#### 4. ROLES Y RESPONSABILIDADES

**Administrador de Sistemas:** Deben definir los accesos a los datos por parte de los usuarios de la institución y terceros, cuidando de mantener una adecuada segregación de funciones; gestionar los accesos definidos.

**Jefe Departamento de Gestión Sectorial de Tecnologías y Comunicaciones:** Debe disponer los controles y reglas de control de acceso.

**Unidad de Infraestructura, Telecomunicaciones y Seguridad (Soporte TIC) / Unidad de Administración y Operaciones:** gestionar los derechos de acceso a los medios de procesamiento de información que tenga a su cargo según lo descrito en esta política.

#### 5. POLITICA

##### 5.1 Cumplimiento de la legislación

Las medidas de control de acceso a la información definidas deben cumplir y ser consistentes con lo dispuesto por las normas y requerimientos legales definidos en el documento "Normativa del Sistema de Gestión de Seguridad de la Información".

##### 5.2 Control de acceso a la Información

Todos los funcionarios del MINSAL, incluso terceros, deberán tener acceso sólo a la información que necesitan para el desarrollo legítimo de sus funciones y actividades dentro de la organización. La asignación de privilegios y acceso a los activos de información deben estar basados en las necesidades de las áreas y aprobados por el propietario de los activos.

Estas necesidades de acceso deben ser determinadas por las respectivas jefaturas, en función de las tareas asignadas al cargo del funcionario.

Para todo medio de procesamiento de información al que se necesite conceder accesos (por ejemplo: servidores, aplicaciones, carpetas compartidas, etc.), el dueño de la Información en conjunto con el Departamento de Gestión Sectorial TIC debe designar un responsable del medio, quién será encargado de autorizar los permisos de acceso y solicitar los espacios necesarios.

Sólo se deben conceder accesos a terceros previa solicitud del dueño del medio de procesamiento de información y el dueño de la información, y nunca antes de haberse firmado un acuerdo de confidencialidad. Las cuentas de acceso a terceros deben tener especificado un tiempo de expiración el que debe ser controlado por el Administrador del sistema, la Unidad de Infraestructura Telecomunicaciones y Seguridad, y la Unidad de Administración y Operaciones, según corresponda.

El Comité de Seguridad de la Información Sectorial tiene las facultades de suspender o eliminar los accesos a cualquier persona que represente riesgo en la confidencialidad, integridad o disponibilidad de la información.

Cualquier intento de acceso no autorizado a los equipos, carpetas compartidas, sistemas e información será considerado un incidente grave, por lo que debe reportarse de inmediato según lo descrito en el procedimiento de Gestión de Incidentes de Seguridad de la Información.

Ante cualquier daño a un activo de información se procederá de acuerdo a lo descrito en la Política General de Seguridad de la Información (Sanciones) y el Procedimiento Acuerdos de Confidencialidad en contratos con terceros.

### 5.3 Administración del acceso

La administración de perfiles de usuario en las aplicaciones radica en los usuarios administradores de cada aplicación y las jefaturas de división correspondiente. La responsabilidad de asignar un determinado perfil a un usuario corresponderá a la Jefatura de División solicitante o a quien se delegue.

No se podrá otorgar el acceso a los sistemas a ningún usuario hasta que se haya completado el proceso de autorización y registro de acuerdo al Procedimiento de gestión de derechos de accesos y devolución de activos.

Para facilitar la administración de los accesos, se deben definir perfiles de acceso asignables a grupos de usuarios que, por sus responsabilidades en la organización, presenten necesidades de acceso equivalentes.

Las Unidades de Administración y Operaciones e Infraestructura, Telecomunicaciones y Seguridad implementan las reglas de control de acceso solicitadas por los Administradores de Aplicación y las Jefaturas de División correspondiente.

### 5.4 Administración de accesos especiales

El otorgamiento de accesos con mayores privilegios (por ejemplo acceso a: bases de datos, código fuente, etc.) a funcionarios que no pertenezcan a las Unidades de Administración y Operaciones e Infraestructura Telecomunicaciones y Seguridad, debe ser solicitado por la Jefatura de la División responsable o quien delegue, al Encargado de Seguridad de la Información justificando la solicitud.

### 5.5 Segregación de funciones

Los derechos de acceso deben ser asignados a perfiles individuales, de forma tal que las acciones realizadas con los accesos otorgados, sean de responsabilidad directa del funcionario.

El otorgamiento de accesos respecto a recursos de información del MINSAL debe considerar una adecuada segregación de funciones, de modo que un mismo funcionario no pueda disponer, por su voluntad, del control de un proceso de negocios completo.

Las excepciones a la regla anterior deben ser aprobadas por la Jefatura de División correspondiente y autorizadas por el Jefe de Departamento de Gestión Sectorial TIC.

### 5.6 Revisión de los derechos de acceso

Las Unidades de Administración y Operaciones e Infraestructura Telecomunicaciones y Seguridad, son responsables de los accesos de los administradores de aplicaciones, de tal forma que se establezca un control efectivo desde el registro inicial de la cuenta hasta el momento en que requiera ser modificada, revocada o eliminada (ver Procedimiento de gestión de derechos de acceso y devolución de activos).

Los derechos de accesos deben ser revisados:

- A intervalos regulares no mayores a 6 meses.
- Después de cualquier cambio mayor en la organización.
- Los accesos de cuentas con mayores privilegios, deben ser revisados al menos 2 veces al año.

### 5.7 Revocación de los acceso lógicos

Ante situación de un cambio de cargo de funcionario, se deben revisar sus permisos de acceso lógico asignados y verificar que éstos sigan siendo válidos de acuerdo a su nueva función.

Cuando un funcionario termina su relación laboral con el MINSAL, todos sus permisos de acceso a la información deben ser revocados.

Es responsabilidad de las Jefaturas Directas informar formalmente las desvinculaciones de acuerdo a lo descrito en el procedimiento de gestión de derechos de acceso y devolución de activos.

### 5.8 Revocación de los accesos

Los Usuarios Líderes de aplicación deben revisar en forma periódica los perfiles de usuario del personal vigente y solicitar a la Unidad de Infraestructura, Telecomunicaciones y Seguridad (Soporte TIC) la actualización de éstos cada vez que ocurra un cambio en la definición de funciones. Cualquier cambio en las funciones de una persona que acceda a información del negocio deberá verse reflejado en sus privilegios de acceso.

**2º ESTABLÉZCASE** la obligación del Departamento de Gestión de Personas de la Subsecretaría de Salud Pública, de difundir la política fijada en este instrumento y al Departamento de Gestión Sectorial TIC, de velar por su estricto cumplimiento.

**3º INSTRÚYASE** al Jefe del Departamento de Gestión Sectorial TIC y a los Encargados de Seguridad de la Información, que realicen las acciones tendientes a la implementación de la presente Política en materias de su competencia.

### ANÓTESE Y COMUNÍQUESE



*Jaime Burrows Oyarzún*  
**DR. JAIME BURROWS OYARZÚN**  
 Subsecretario de Salud Pública



*Dr. Angelica Verdugo Sobral*  
**DRA. ANGELICA VERDUGO SOBRAL**  
 Subsecretaria de Redes Asistenciales

#### Distribución:

- Gabinete Sra. Ministra de Salud.
- Subsecretaría de Salud Pública.
- Subsecretaría de Redes Asistenciales.
- Departamento de Gestión Sectorial de Tecnologías y Comunicaciones.
- Departamento de Gestión de Personas de la Subsecretaría de Salud Pública.
- División Jurídica.
- Oficina de Partes.

