PS-NC-008

POLITICA DE SEGURIDAD PARA EL CONTROL DE ACCESO LÓGICO

Sistema de Gestión de Seguridad de la Información – Nivel Central

Versión Oficial Actual v02 – Octubre del 2019

	Responsable	Fecha	Firma
Elaborado	Rodrigo Vidal / Encargado PMG SSI	Octubre 2019	
Revisado	José Villa / Área Seguridad de la Información (Representante Comité de Seguridad)	Octubre 2019	
Aprobado	Gabriel Reveco / Encargado Ciberseguridad (Presidente Comité de Seguridad de la Información)	Octubre 2019	

MINISTERIO DE SALUD
COMITÉ SEGURIDAD DE LA INFORMACIÓN

MINISTERIO DE SALUD
ENCARGADO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Contenido

1 PROPOSITO

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

2 ALCANCE O AMBITO DE APLICACIÓN

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

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 la Subsecretaría de Salud Pública y la Subsecretaría de Redes Asistenciales.

En cuanto a las temáticas de protección abordadas, el ámbito de aplicación de esta política corresponde al (a los) Dominio(s) de Seguridad de la Información y Controles de Seguridad respectivos, detallados a continuación:

Alcance de Dominios y Controles de Seguridad de la Información (Nch-ISO 27001:2013)		
Nombre del Dominio	ID Control ISO 27001	Nombre del Control
Control de acceso	A.09.01.01	Política de control de acceso
	A.09.01.02	Accesos a las redes y a los servicios de la red

3 MARCO NORMATIVO Y DOCUMENTOS RELACIONADOS

- Marco Normativo
  - NCh-ISO27001:2013: Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información – Requisitos.
  - El Marco Jurídico referido a los Sistemas de Seguridad de la Información (SSI), publicado en el portal del CSIRT del Ministerio del Interior.
    - Decretos Supremos y Normas Internacionales de Seguridad de la Información y Ciberseguridad:
    - Leyes relacionadas

- **Documentos Relacionados**
  - Procedimiento gestión de derechos de acceso y devolución de activos.
  - Política Seguridad en la Red.

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 TIC**
  - Debe disponer los controles y reglas de control de acceso.

- **TIC Administración y Operaciones / Soporte TIC**
  - Gestionar los derechos de acceso a los medios de procesamiento de información que tenga a su cargo según lo descrito en esta política.

5 MATERIAS QUE ABORDA.

- Política de control de acceso.
- Accesos a las redes y a los servicios de la red.

6 DIRECTRICES DE LA POLÍTICA

6.1 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”.

6.2 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 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.

El Comité de Seguridad de la Información del Nivel Central 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.

6.3 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 con el 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.

El área de Operaciones TIC implementa las reglas de control de acceso solicitadas por los Administradores de Aplicación y las Jefaturas de División correspondiente.

6.4 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 al área de Operaciones TIC, debe ser solicitado por la Jefatura de la División responsable o quien delegue, al Encargado de Seguridad de la Información y Encargado de Ciberseguridad, justificando la solicitud.

6.5 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 TIC.

6.6 Revisión de los derechos de acceso

El área de Operaciones TIC, es responsable 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.

6.7 Revocación de los accesos 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 con 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 con lo descrito en el procedimiento de gestión de derechos de acceso y devolución de activos.

6.8 Revocación de los accesos

Los Usuarios Líderes de aplicación deben revisar en forma periódica los perfiles de usuario del personal vigente y solicitar al área Operaciones 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.

7 MECANISMO DE DIFUSIÓN.

La comunicación de la presente política se efectuará de manera que el contenido de la documentación sea accesible y comprensible para todos los usuarios, a lo menos se deberá hacer difusión mediante los siguientes canales:

- Publicación en la intranet de Minsal http://isalud.minsal.cl/
- Correo informativo.

8 PERÍODO DE REVISIÓN.

La revisión del contenido de esta Política se efectuará a lo menos cada dos años por el Comité de Seguridad de la Información, o atendiendo necesidades de cambios para garantizar su idoneidad, adecuación y efectividad.

9 EXCEPCIONES AL CUMPLIMIENTO DE LA POLÍTICA

Frente a casos de especiales, el Comité de Seguridad de la Información evaluará y podrá establecer condiciones puntuales de excepción en el cumplimiento de las presentes directrices, siempre que no infrinja la legislación vigente. Toda excepción debe ser documentada y generar un proceso de revisión de la política, que determine si se deben agregar directrices en lo particular.

10 HISTORIAL Y CONTROL DE VERSIONES

Versión	Fecha	Pág. o Sección modificada	Motivo del cambio
01	Octubre 2014	Todas	Creación del Documento
02	Octubre 2019	Todas	Cambio de formato de documento. Se actualizan las referencias normativas. Se actualizan dominios de la norma ISO 27001.