PS-NC-007

POLITICA DE PANTALLAS Y ESCRITORIOS LIMPIOS

Sistema de Gestión de Seguridad de la Información – Nivel Central

Versión Oficial Actual v05 – 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

El propósito de esta política es definir las reglas de uso y control que deben cumplirse para reducir los riesgos de acceso no autorizado, pérdida o daño a la información durante y fuera de las horas normales de trabajo.

2. ALCANCE O AMBITO DE APLICACIÓN

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.

Aplica a la protección de la información contenida en una pantalla de una estación de trabajo, como también cualquier información impresa o escrita que se encuentre expuesta en los escritorios, muebles, o medios de almacenamiento removibles.

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
Seguridad física y ambiental	A.11.02.01	Ubicación y protección del equipamiento
	A.11.02.08	Equipo de usuario desatendido
	A.11.02.09	Política de escritorio y pantalla limpios
Seguridad de las operaciones	A.12.06.02	Restricciones sobre la instalación de software

3. MARCO NORMATIVO Y DOCUMENTOS RELACIONADOS

- Documentos del Sistema de Gestión de Seguridad de la Información (SGSI) de MINSAL, disponibles en isalud.minsal.cl.
- Política Nacional de Ciberseguridad (PNCS)
- 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.

4. ROLES Y RESPONSABILIDADES

Comité de Seguridad de la Información: Definir directrices respecto a cómo tratar la información que se maneja en los escritorios de los funcionarios y pantallas de los funcionarios y externos que prestan servicios en el MINSA.

Jefe Departamento de Tecnologías de Información: Implementar las directrices de seguridad definidas en esta política para el manejo y protección de la información.

Encargado(s) de Seguridad de la Información: Determina los requisitos de Seguridad respecto a cómo tratar la información, junto con velar la correcta aplicación de la presente política.

Usuario: Debe proteger tanto sus artículos personales como los de la Subsecretaria y más aún, toda la información institucional que de él depende y/o utilice

5. MATERIAS QUE ABORDA

- Ubicación y Protección del Equipamiento
- Equipamiento desatendido por el usuario.
- Escritorios y pantallas limpias.
- Protección de seguridad para impresoras.
- Salas y pizarras limpias.
- Restricciones sobre el uso de equipos y la instalación de software

6. DIRECTRICES DE LA POLITICA

6.1 Ubicación y protección del equipamiento

Las áreas de trabajo de los usuarios deben localizarse preferentemente en ubicaciones que no queden expuestas al acceso de personas externas. (Ver Política perímetros de seguridad física y protección del equipamiento).

Los equipos que queden ubicados cerca de zonas de atención o tránsito de público deben situarse de forma que las pantallas no puedan ser visualizadas por personas no autorizadas y deben ser aseguradas, en lo posible, mediante candado de seguridad u otro medio que impida que sean sustraídos.

No se deben ingerir alimentos o bebidas cerca de los equipos o dispositivos de procesamiento de información, así como colocar o manipular líquidos en su cercanía.

6.2 Equipamiento desatendido por el usuario

Toda vez que el usuario se ausente de su lugar de trabajo debe bloquear su estación de trabajo de forma de proteger el acceso a las aplicaciones y servicios de la institución.

Las estaciones de trabajo y equipos portátiles deben tener aplicado el estándar relativo a protector de pantalla definido por el Encargado de Seguridad de la Información, de forma que se active ante un tiempo sin uso.

La pantalla de autenticación a la red de la institución debe requerir solamente la identificación de la cuenta y una clave; y no entregar o solicitar otra información.

La autenticación de usuario debe ser requerida cada vez que el equipamiento se encienda, reinicie, bloquee o después de aparecer el protector de pantalla.

6.3 Escritorios y pantallas limpias

Toda vez que un usuario se ausenta de su lugar de trabajo, junto con bloquear su estación de trabajo, debe guardar en lugar seguro cualquier documento, medio magnético u óptico removible que contenga información confidencial.

Al finalizar la jornada de trabajo, el usuario debe guardar en un lugar seguro los documentos y medios que contengan información confidencial o de uso interno, además desconectarse de los computadores centrales, servidores y estaciones de trabajo de oficina cuando la sesión es finalizada (por ejemplo, no apagar sólo el monitor de la terminal o estación de trabajo).

Se entenderá por lugar seguro aquel que protege el activo de información de accesos de personas no autorizadas, que su contenido no sea alterado y que el activo pueda ser recuperado por las personas autorizadas de manera oportuna (algunos ejemplos son: caja fuerte, archivador, mueble seguro, oficina con llave, etc.).

Si el usuario está ubicado cerca de zonas de atención de público, al ausentarse de su lugar de trabajo debe guardar también los documentos y medios que contengan información de uso interno.

Los equipos de reproducción de información (por ejemplo: impresoras, fotocopiadoras), deben estar ubicados en lugares con acceso controlado y cualquier documentación confidencial o sensible se debe retirar inmediatamente del equipo.

6.4 Protección de seguridad para impresoras.

Las impresoras ubicadas en atención o tránsito de público, deben estar quedar protegidas de acceso no autorizada.

Cualquier información que va a ser impresa en cualquier impresora, debe ser retirada de ella en forma inmediata, evitando de esta forma, el acceso a esta información de personas no autorizadas.

Cuando sea posible y se trate de información sensible, debe implementarse el control de impresión con el uso de clave por usuario.

6.5 Salas y pizarras limpias

Las salas o áreas de reuniones y de capacitación deben quedar limpias de todo el material utilizado.

Después de las reuniones en que se utilicen pizarras, estas deben quedar limpias de la información que se ha expuesta en ellas.

En el caso que se utilice una estación de trabajo para presentaciones, si dicho equipo fuera de uso común, debe eliminarse la información antes presentadas.

6.6 Restricciones sobre el uso de equipos y la instalación de software

Los usuarios no deberán intentar trasgredir o sabotear las medidas de seguridad de los sistemas, ni utilizar herramientas, programas o dispositivos con el objeto de evadir controles, interceptar o decodificar contraseñas o acceder a información para la cual no están autorizados.

Se consideran conductas inapropiadas:

- La utilización del Computador en actividades que no pertenezcan al ámbito de trabajo de la Organización.
- El uso de equipos de la Organización en actividades de lucro personal.
- La desinstalación o inhabilitación consciente de las aplicaciones de seguridad del Computador Institucional, por ejemplo, del antivirus.
- La instalación de software no autorizado por el Departamento TIC.
- La cesión, préstamo o utilización del equipo por terceras personas (amigos, parientes o conocidos)
- La modificación de la configuración del sistema operativo u otras aplicaciones que formen parte del software operativo básico del equipo.
- Abrir el equipo y/o cambiar el hardware o dispositivos que lo componen.
- Utilización no autorizada de acceso a páginas Web.

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	Página o Sección Modificada	Fecha de Aprobación	Motivo del cambio
1	Creación del documento	Octubre 2011	Creación del documento
2	Todas	Agosto 2013	Alineación del documento con la nueva estructura del SGSI declarada en la política general de Seguridad de la Información. En el punto responsabilidades se incluye al Encargado de Seguridad de la Información y Usuario. En el punto Escritorios limpios se incluye una explicación para “lugar seguro. Se incluye el punto “Equipos de reproducción de información. Se incluye la definición de pantalla y escritorio limpio.
3	2. Alcance	Octubre 2014	Se incluyen los controles A.11.3.2 y A.9.2.1 de la norma NCh-ISO 27001.Of2009.
4	Todas	Octubre 2017	▪ Se actualiza la referencia normativa de la versión 2013 de la norma 27001. ▪ Se actualizan las referencias normativas del documento. ▪ Se modifica el formato de la política (código, forma). ▪ Se ajustan los contenidos a los nuevos requisitos de la norma.
5	Todas	Octubre	▪ Se incluye el control A.12.06.02

		2019	▪ Se incluye el punto 6.6 sobre restricciones de instalación de software. ▪ Se cambia el alcance de política Sectorial a Política para el Nivel Central. ▪ Se actualizan los mecanismos de difusión.