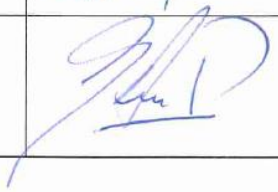
PS-NC-016

POLÍTICA DE SEGURIDAD PARA LA CLASIFICACIÓN Y MANEJO DE INFORMACIÓN

Sistema de Gestión de Seguridad de la Información – Nivel Central

Versión Oficial Actual v03 – octubre 2020

Responsable		Fecha	Firma
Elaborado	Rodrigo Vidal / Unidad Seguridad TIC	Octubre 2020	
Revisado	José Villa / Área Seguridad de la Información (Representante Comité de Seguridad)	Octubre 2020	
Aprobado	Gabriel Reveco / Encargado Ciberseguridad (Presidente Comité de Seguridad de la Información)	Octubre 2020	

Contenido

1 PROPOSITO

Esta Política tiene por objeto establecer los principios, bases, lineamientos, procedimientos y normas necesarios para proteger la información y documentación sensible del Ministerio de Salud (MINSAL), del conocimiento y divulgación a personas o instituciones no autorizadas.

2 ALCANCE O AMBITO DE APLICACIÓN

Todos los recursos computacionales que tengan acceso Internet, de Minsal y sus Áreas dependientes donde sea implementada esta política.

Es aplicable a todo tipo de información, independientemente del soporte en el que se encuentre, por ejemplo; documentos, sistemas de información, redes, sistemas de comunicaciones móviles, sistemas de información, dispositivos móviles, nubes, correo, correo de voz, comunicaciones de voz en general, multimedia, servicio postal, etc., y cualquier otro elemento sensible, como, por ejemplo, cheques en blanco, facturas.

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
A.8 Administración de activos	A.08.01.02	Propiedad de los activos
	A.08.01.03	Uso aceptable de los activos
	A.08.02.01	Clasificación de la información
	A.08.02.02	Etiquetado de la información
	A.08.02.03	Manejo de activos

3 MARCO NORMATIVO Y DOCUMENTOS RELACIONADOS

- **Marco Normativo**

  - ✓ Código Sanitario
  - ✓ Ley 20.584, de derechos y deberes de los pacientes
  - ✓ Ley Nº 20.285 sobre Acceso a la Información Pública.
  - ✓ Ley Nº 19.628 sobre Protección de la Vida Privada.

- ✓ Ley Nº 19.880 que establece las Bases de los Procedimientos Administrativos que rigen los Actos de los Órganos de la Administración del Estado.
- ✓ Ley Nº 19.799, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.
- ✓ Ley 19.223, sobre delitos informáticos.

- **Documentos Relacionados**

- ✓ Documento del Sistema de Gestión de Seguridad de la Información, disponibles en isalud.minsal.cl.

4 ROLES Y RESPONSABILIDADES

- **Comité de Seguridad de la Información**
  - Aprobar las solicitudes de acceso a la información (como producto final) clasificada como pública.

- **Jefe Departamento TIC**
  - Informar de los riesgos a los que se exponen los funcionarios respecto de manejar información confidencial, adoptar las medidas tendientes a evitar dichos riesgos, y entrenar a los funcionarios sobre qué hacer antes esas situaciones. Supervisar los respaldos de software esencial.

- **Encargado de Seguridad de la Información**
  - Llevar al Comité de Seguridad Sectorial la/s solicitud/es de acceso a la información confidencial.

- **Propietario de la información**
  - Clasificar la información según lo definido en esta política y autorizar el acceso a la información considerando los controles adecuados.

- **Encargado de Transparencia Pasiva**
  - Asesorar en materias de clasificación de la información cuando fuera necesario.

- **Funcionarios**
  - Deberá cumplir con las normas establecidas en el presente documento y la Política protección de los datos y privacidad de la información personal.

5 MATERIAS QUE ABORDA.

- Propiedad de los activos
- Uso aceptable de los activos
- Clasificación de la información

- Etiquetado de la información
- Manejo de activos

6 DIRECTRICES DE LA POLÍTICA

6.1 Responsables de los activos de información.

Tipo de activo	Dueño del activo	Responsable administrativo del activo
Software Base de datos Equipos Sistema Formularios	Jefe de la Unidad Administrativa donde se desarrolla el proceso.	Jefe Departamento TIC
Documentos Expediente	Jefe de la Unidad Administrativa donde se desarrolla el proceso.	Jefe de la Unidad Administrativa donde se desarrolla el proceso.
Personas	Jefe de la Unidad Administrativa donde se desarrolla el proceso.	Jefe Departamento de Desarrollo de Personas
Infraestructura	Jefe de la Unidad Administrativa donde se desarrolla el proceso.	Jefe Departamento de Administración

Dueño del activo: corresponde al jefe de la Unidad Administrativa donde se utilicen los diferentes activos de información, en forma permanente para el desarrollo de los procesos propios de dicha unidad.

El dueño del activo es responsable de:

Asegurar que la información y los activos asociados con las instalaciones de procesamiento de la información son clasificados en forma apropiada;

Definir y revisar periódicamente restricciones y clasificación del acceso al activo teniendo en cuenta las políticas aplicables de control de acceso (físico o lógico).

Responsable Administrativo: corresponde al jefe del Departamento al cual pertenecen los diferentes tipos de activos de información.

El responsable administrativo es responsable de:

En conjunto con el dueño del activo, definir y revisar periódicamente restricciones y clasificación del acceso al activo teniendo en cuenta las políticas aplicables de control de acceso.

6.2 Gestión de Inventario y Activos

Todos los activos deberán estar claramente identificados y la importancia de estos para el MINSAL. El dueño del activo deberá elaborar y mantener un inventario de los activos más importantes, que deberá incluir al menos:

- Tipo de activo
- Formato
- Ubicación
- Responsable del activo

Se debe tener en cuenta que la propiedad y la clasificación de la información, debe ser acordada y documentada para cada uno de los activos inventariados. Esto será basándose en:

- Importancia del activo
- Valor para el proceso de negocio
- Clasificación de seguridad
- Niveles de protección de acuerdo con la importancia

Todos los datos e información deben tener un propietario, el cual deberá clasificarlos en los niveles definidos en la sección 6.3 Clasificación de la información.

En el caso de los activos de información no inventariados o de aquellos documentos de carácter transitorio o no oficial (borradores, proyectos, etc.) y que no posean un responsable explícito, será responsabilidad del creador de la información la aplicación de los niveles de seguridad requeridos en el manejo y transmisión de la información generada.

6.3 Clasificación de la información

La información se clasifica de acuerdo con su estado y nivel de confidencialidad, siendo:

6.3.1 **Estado**

En tránsito: la información de uso interno, como son los respaldos a los actos administrativos. Ejemplo: acta, minuta, circular interna, correo electrónico, etc...

Producto final: documentos que soportan información, como son las Leyes, reglamentos, resoluciones, decretos, ordinarios en cualquier medio de soporte.

6.3.2 **Confidencialidad**

Este criterio es solo información de base, pudiendo existir otros criterios de evaluación, como el caso de restricciones legales respecto a la divulgación de la

información, importancia del activo para un proceso en particular u otros. Estos criterios deberán ser descritos en el Inventario de Activos en caso de ser considerados.

Nivel de Clasificación	DESCRIPCIÓN (Criterio de Clasificación)	Restricción de acceso
Secreto	Aquellos documentos que la ley establece como Secretos, no pueden ser divulgados.	La información está disponible solamente para un grupo específico de empleados, que ejercen funciones definidas.
Reservado	Información altamente sensible, de uso exclusivamente interno. Su divulgación podría implicar un impacto no deseado para MINSAL o la violación de normativa vigente. Debe ser declarada como reservada considerando la Ley 20.285.	La información está disponible solamente para un grupo específico de empleados y de terceros autorizados
Uso Interno*	El acceso no autorizado a la información podría ocasionar daños y/o inconvenientes menores a la organización.	La información está disponible para todos los empleados y terceros seleccionados. Esta información puede ser entregada al público sujetos a la normativa vigente, previa consulta al Propietario del Activo.
Pública	Hacer pública la información no puede dañar a la organización de ninguna forma	Pueden ser entregadas utilizando el canal OIRS.

La normativa que ha sido calificada como confidencial o reservada estará enlistada y disponible en las oficinas de información o atención del usuario, según lo dispuesto en la ley Nº 20.285, su reglamento, y las instrucciones generales del Consejo para la Transparencia.

6.4 Manejo de la información

6.4.1 Etiquetado de la información según su clasificación

Para el etiquetado de los activos de información se deberán seguir las siguientes directrices:

a) En general los activos del tipo público no requieren etiquetado, independiente del formato en que se encuentren.

b) Los activos con otros niveles de confidencialidad son etiquetados de la siguiente forma:

- **Documentos en papel:** Si el documento contiene información reservada o de uso interno, se debe indicar el nivel de clasificación al menos en la portada del

documento; si contiene información secreta se debe indicar el nivel de clasificación tanto en la portada como en cada una de las páginas o en el sobre que contiene dicho documento, como también en la carpeta de archivo en la que se guarda el documento.

- **Documentos electrónicos:** Si el documento contiene información reservada o de uso interno, se debe indicar el nivel de clasificación al menos en la portada del documento; si contiene información secreta, se debe indicar dicho nivel de clasificación tanto en la portada como en cada una de las páginas.

- **Correo electrónico:** se indica el nivel de clasificación en la primera línea del cuerpo del correo electrónico.

- **Soporte de almacenamiento electrónico (discos, tarjetas de memoria, etc.):** se debe indicar el nivel de clasificación sobre la superficie de cada soporte.

- **Información transmitida oralmente:** el nivel de clasificación de la información reservada, de uso interno o confidencial que se transmite a través de una comunicación cara a cara, por teléfono o por alguna otra vía de comunicación debe ser comunicado antes que la información propiamente dicha.

6.4.2 **Tratamiento de la información según su clasificación (Estado y confidencialidad)**

La información debe ser tratada de acuerdo con su clasificación, y sus estados; la generación, transmisión, recepción, procesamiento y almacenamiento. En la siguiente tabla se definen las medidas de seguridad para el tratamiento de la información:

			CLASIFICACIÓN DE LA INFORMACIÓN			
PROCESAMIENTO DE LA INFORMACIÓN		**MEDIDAS DE SEGURIDAD**	**SECRETA**	**RESERVADA**	**USO INTERNO**	**PUBLICA**
Almacenamiento		Encriptación necesaria o control de acceso a medios de almacenamiento	O			
		Encriptación opcional		O	O	
		No se requiere encriptar				O
Copiado		Se requiere la aprobación del creador del documento	O			
		Se requiere firma digital para la no repudiación				
		No se restringe el uso			O	O
Transmisión de información	**Redes públicas**	Encriptación necesaria	O			
		Encriptación opcional		O	O	
		No se requiere encriptar				O
	Redes privadas	Encriptación necesaria	O			
		Encriptación opcional		O	O	
		No se requiere encriptar				O
	Correo electrónico	Encriptación necesaria	O			
		Encriptación opcional		O	O	
		No se requiere encriptar				O
		Se requiere firma digital para la no repudiación	O			
		Protección de contraseñas	O			
	Otros medios de transmisión	Encriptación necesaria	O			
		Encriptación opcional	O		O	

	No se requiere encriptar				O
	Se requiere firma digital para la no repudiación	O			
Otros medios digitales	Encriptación necesaria	O			
	Encriptación opcional	O		O	
	No se requiere encriptar				O
	Se requiere firma digital para la no repudiación	O			
Destrucción	Trituración o eliminación en lugares seguros	O	O	O	
	Método y equipamiento de eliminación avanzada				
	Papelero convencional				O
Divulgación a terceros	Se requiere acuerdo de no divulgación	O	O		
	No se puede entregar información a terceros	O	O		
	Se requiere la aprobación del creador del documento		O	O	
	No tiene restricción				O
Etiquetado de bienes físicos	Se requiere etiquetado especial	O			
	Se requiere etiquetado de fecha y clasificación de divulgación		O	O	
	No se requiere etiquetado				O
Etiquetado de documentos	Se requiere etiquetado en cada una de las paginas, portada, títulos	O			
	Se requiere etiquetado clasificación en la portada		O	O	
	No se requiere etiquetado				O
Control de acceso	Acceso gestionado para la administración parcial	O	O	O	
	Sin restricción				O

6.5 Almacenamiento de información

Cuando no está en uso y especialmente en horario inhábil, toda la información SECRETA O RESERVA deberá mantenerse almacenada, de modo de evitar que las personas no autorizadas tengan acceso a ella.

El almacenamiento de información SECRETA O RESERVADA no deberá realizarse en el disco duro u otro componente del computador personal sin autorización del dueño de activo y un sistema de control de acceso adecuado.

Cuando no esté en uso, la documentación escrita que contenga información SECRETA O RESERVADA deberá ser almacenada bajo llave.

El almacenamiento de los medios que contengan información debe ser acorde a las especificaciones del fabricante.

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	Diciembre 2013	Todas	Creación del documento
02	Agosto 2014	Todas	Actualización del documento
03	Octubre 2020	Todas	Actualización del documento