

 Gobierno de Chile	SERVICIO DE SALUD VIÑA DEL MAR - QUILLOTA	NUMERO: 16
	COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	CODIGO: I
	POLITICAS DE SEGURIDAD DE LA INFORMACION	FECHA: 16 de Abril de 2013
		PAGINA: 1 de 9

POLÍTICA DE SEGURIDAD EN LA CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN

DIRECCION DEL SERVICIO DE SALUD
VIÑA DEL MAR - QUILLOTA

	SERVICIO DE SALUD VIÑA DEL MAR - QUILLOTA	NUMERO: 16
	COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	CODIGO: I
	POLITICAS DE SEGURIDAD DE LA INFORMACION CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN	FECHA: 16 de Abril de 2013
		PAGINA: 2 de 9

NOTA DE CONFIDENCIALIDAD

LA INFORMACIÓN CONTENIDA EN EL PRESENTE DOCUMENTO, ES DE PROPIEDAD Y USO EXCLUSIVO DEL SERVICIO DE SALUD VIÑA DEL MAR – QUILLOTA, PARA LOS FINES QUE DETERMINE, Y SOLO LOS FUNCIONARIOS DE ESTA INSTITUCIÓN EXPRESAMENTE AUTORIZADOS PODRÁN CONOCER Y UTILIZAR SU CONTENIDO DE ACUERDO A SU FINALIDAD.

Firmas de los responsables.

ELABORADO POR	REVISADO POR	APROBADO POR
----- Representante del Comité de Seguridad	----- Encargado de Seguridad	----- Director(a) del Servicio

	SERVICIO DE SALUD VIÑA DEL MAR - QUILLOTA	NUMERO: 16
	COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	CODIGO: I
	POLITICAS DE SEGURIDAD DE LA INFORMACION CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN	FECHA: 16 de Abril de 2013
		PAGINA: 3 de 9

INDICE

- 0.- Control de versiones
- 1.- Declaración institucional
- 2.- Objetivos de la política de seguridad en la clasificación y manejo de la información
- 3.- Ámbito de aplicación de la política de seguridad en la clasificación y manejo de la información
- 4.- Roles y responsabilidades
- 5.- Marco general para las políticas de seguridad en la clasificación y manejo de la información
- 6.- Aplicación
- 7.- Monitoreo
- 8.- Glosario de términos

	SERVICIO DE SALUD VIÑA DEL MAR - QUILLOTA	NUMERO: 16
	COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	CODIGO: I
	POLITICAS DE SEGURIDAD DE LA INFORMACION CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN	FECHA: 16 de Abril de 2013
		PAGINA: 4 de 9

CONTROL DE VERSIONES

REVISIONES DEL DOCUMENTO DE POLITICA				
Nº Revisión	Fecha Aprobación	Motivo de la revisión	Páginas Modificadas	Autor
0(Cero)		Elaboración inicial	Todas	RCA
1				
2				
3				

 Gobierno de Chile	SERVICIO DE SALUD VIÑA DEL MAR - QUILLOTA	NUMERO: 16
	COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	CODIGO: I
	POLITICAS DE SEGURIDAD DE LA INFORMACION CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN	FECHA: 16 de Abril de 2013
		PAGINA: 5 de 9

1.- DECLARACIÓN INSTITUCIONAL

De acuerdo a lo establecido por la Ley N° 20.285 Sobre acceso a la información pública “es pública la información elaborada con presupuesto público y toda otra información que obre en poder de los órganos de la Administración”, en consecuencia la información tratada en el Servicio de Salud Viña del Mar – Quillota está completamente dentro del alcance definido por este cuerpo legal y su propiedad corresponde al Estado de Chile, así como también los sistemas asociados a ella, los cuales deben ser protegidos de acuerdo a su valor y criticidad.

Desde la perspectiva del Sistema de Gestión de Seguridad de la Información; la información que se maneja en el Servicio de Salud Viña del Mar – Quillota posee diferentes niveles de criticidad en cuanto al riesgo que representa su eventual divulgación, adulteración o indisponibilidad. Por lo anterior, se hace necesario diferenciar la información según el nivel de riesgo que genera su compromiso.

El Servicio de Salud Viña del Mar – Quillota ha decidido segregar la información teniendo como base el riesgo asociado al compromiso de su confidencialidad.

2.- OBJETIVOS DE LA POLÍTICA DE SEGURIDAD EN LA CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN

La presente política tiene por objetivo describir a modo general las acciones a realizar para la clasificación y manejo de la información al interior del Servicio de Salud Viña del Mar – Quillota.

3.- ÁMBITO DE APLICACIÓN LA POLÍTICA DE SEGURIDAD EN LA CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN

Esta política define las Categorías de Clasificación de la Información, y las reglas de manejo, copiado, almacenamiento, autorización de acceso y derecho a saber de la información.

4.- ROLES Y RESPONSABILIDADES

Director/a del Servicio de Salud Viña del Mar- Quillota

- Sancionar las propuestas realizadas por el comité de seguridad, respecto a las políticas de seguridad en la clasificación y manejo de la información
- Aprobar los recursos necesarios para implementación adecuada de las acciones requeridas en la política.

Comité de Seguridad

- Elaborar y aprobar la presente política de seguridad de clasificación y manejo de la información.

	SERVICIO DE SALUD VIÑA DEL MAR - QUILLOTA	NUMERO: 16
	COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	CODIGO: I
	POLITICAS DE SEGURIDAD DE LA INFORMACION CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN	FECHA: 16 de Abril de 2013
		PAGINA: 6 de 9

- Supervisar la implementación de la presente política.
- Proponer estrategias y soluciones específicas para la implementación de los controles necesarios para implantar la presente política.
- Monitorear los incidentes de seguridad y proponer estrategias para dar solución a las situaciones de riesgo detectadas en esta política.
- Monitorear el avance general en la implementación de la presente política.
- Divulgar la política de seguridad al interior de la institución.
- Implementar las medidas de seguridad definidas en la presente política.
- Mantener esta política de seguridad y sus procedimientos actualizados, con el fin de asegurar su vigencia y nivel de eficacia.
- Designar a los propietarios de la Información

Propietario de la Información

- Manejo, copiado, almacenamiento, autorización de acceso y derecho a saber de la información.
- Clasificar la información que le ha sido asignada, de acuerdo al esquema de clasificación definido para la institución.
- Autorizar la divulgación de información, considerando los controles adecuados.

5.- MARCO GENERAL PARA LAS POLÍTICAS DE SEGURIDAD EN LA CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN

5.1.- CATEGORÍAS DE CLASIFICACIÓN DE LA INFORMACIÓN

- La información del Servicio de Salud Viña del Mar – Quillota o de terceros confiados al Servicio de Salud Viña del Mar – Quillota, deben ser clasificados en una de las tres siguientes categorías; Confidencial, Uso Interno o Pública.
- La definición de cada una es:
 - **A.- Confidencial:** El acceso a la información debe ser restringido severamente basado en el concepto de necesidad de conocer. Por su sensibilidad, esta información deberá ser resguardada con especial recelo, limitando su acceso sólo a aquellas personas que, previamente autorizadas por el Propietario de la información, requieran su conocimiento. En atención al impacto que puede ocasionar su divulgación o adulteración se dispone que esta información deberá ser protegida, tanto en su almacenamiento como envío o trasmisión, de manera tal que se asegure que sólo tenga acceso a ella el personal debidamente autorizado.
 - **B.- Uso Interno:** Es aquella información susceptible de ser comunicada internamente sin restricciones, y sólo podrá ser divulgada a un tercero cuando

	SERVICIO DE SALUD VIÑA DEL MAR - QUILLOTA	NUMERO: 16
	COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	CODIGO: I
	POLITICAS DE SEGURIDAD DE LA INFORMACION CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN	FECHA: 16 de Abril de 2013
		PAGINA: 7 de 9

previamente exista autorización del Propietario de la Información para su entrega, la que en todo caso deberá acreditarse.

- **C.- Pública:** Es aquella información cuya difusión ha sido definida como pública, Dicha información deberá ser otorgada por el Propietario de la Información.

5.3.- ROTULACIÓN DE LA INFORMACIÓN

- Toda información Confidencial, Uso Interno o Pública, debe ser rotulada de acuerdo al estándar definido por el Comité de Seguridad de la información.
- La información debe rotularse independiente de estar almacenada en distintos medio: documentos electrónicos, documentos impresos, documentos manuscritos, cintas, CD, DVD, etc.
- El propietario de la información es el responsable de asignarle la rotulación pertinente, en conformidad a lo prescrito por la Ley 20.285, y la presente política.
- La asignación de propiedad de la información, debe incluir la información que se recibe desde el exterior. En caso, también el propietario es el responsable de asignar la clasificación y rotulación correspondiente.
- Desde que la información es creada hasta que es eliminada o desclasificada, deberá mantener la rotulación definida en su clasificación original.
- Cuando se consolida información clasificada en distintas categorías, la información resultante debe ser rotulada con la categoría mas restrictiva.

5.2.- DESCLASIFICACION DE INFORMACIÓN

- La desclasificación de la información, esto es, cambiar la categoría de Confidencial a uso Interno o Público; o de Uso Interno a Público, se efectuará de acuerdo a lo establecido en el procedimiento correspondiente.
- Al efectuar dicha desclasificación, se deberá notificar a las personas relacionadas con la información que se desclasifica.

5.4.- ALMACENAMIENTO DE LA INFORMACIÓN CONFIDENCIAL

- Cuando no está en uso y especialmente en horario inhábil, toda la información Confidencial deberá mantenerse almacenada, de modo de evitar que personas no autorizadas tengan acceso a ella.
- El almacenamiento de información Confidencial no deberá realizarse en el disco duro u otro componente del computador asignado sin un sistema de control de acceso adecuado. La información Confidencial y de Uso Interno deberá ser grabada en disco duro de red para garantizar su seguridad y respaldo.
- Cuando no está en uso, la documentación escrita que contenga información Confidencial deberá ser almacenada bajo llave.

	SERVICIO DE SALUD VIÑA DEL MAR - QUILLOTA	NUMERO: 16
	COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	CODIGO: I
	POLITICAS DE SEGURIDAD DE LA INFORMACION CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN	FECHA: 16 de Abril de 2013
		PAGINA: 8 de 9

5.5.- AUTORIZACIÓN DE ACCESO A INFORMACIÓN SENSIBLE (CONFIDENCIAL O DE USO INTERNO)

- El acceso a la información sensible deberá ser autorizada previa y explícitamente por el Propietario de la Información, de acuerdo al procedimiento y considerando las restricciones legales a la entrega de información.
- Los acuerdos de No-Divulgación de información que se suscriban con terceros deberán incluir cláusulas referentes al uso de la información y su eventual divulgación posterior.
- Aunque la información no sea considerada sensible, se recomienda a los funcionarios no comentar con sujetos o entes externos este tipo de información.
- Toda la información que vaya a ser entregada al público por la OIRS, deberá ser revisada en conformidad a los procedimientos establecidos
- Las actividades que requieren acceso a la información sensible sólo podrán ser realizadas por funcionarios autorizados según lo establecido en el procedimiento respectivo.

5.6.- MANEJO DE INFORMACIÓN CONFIDENCIAL EN REUNIONES

- A las reuniones donde se tratará información Confidencial, sólo podrán asistir las personas que hayan sido previamente invitadas, las que en todo caso deberán ser validadas por propietario de la Información.
- Si divulga oralmente información Confidencial en una reunión, seminario, discurso o presentación, el expositor deberá exponer la clasificación de la información y exigir discreción. Si se utilizan transparencias o presentaciones, éstas deberán indicar la clasificación de la información, y no podrán ser distribuidas a los asistentes o a terceros. Si se utiliza pizarra, ésta deberá ser borrada al término de la reunión.

5.7.- DERECHO A SABER

- Los funcionarios tienen derecho a saber, de antemano, los riesgos que corren en el lugar de trabajo a consecuencia de la exposición a información restringida. El Jefe de la unidad respectiva deberá informar de tales riesgos, adoptar las medidas tendientes a evitarlos, y entrenar a los funcionarios sobre qué hacer ante esas situaciones.
- Las políticas y procedimientos de seguridad deberán ser conocidos por todos los funcionarios del Servicio de Salud Viña del Mar – Quillota. Además, se podrá autorizar para casos puntuales y clasificados su conocimiento a consultores o auditores que lo requieran, y bajo prohibición de divulgarlos.

5.8.- CONSIDERACIONES DE ACCESO A COMPUTADORES Y RED

- Los funcionarios sólo deberán conectarse a los computadores o redes del Servicio de Salud Viña del Mar – Quillota que le hayan sido asignados. Cualquier excepción

	SERVICIO DE SALUD VIÑA DEL MAR - QUILLOTA	NUMERO: 16
	COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	CODIGO: I
	POLITICAS DE SEGURIDAD DE LA INFORMACION CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN	FECHA: 16 de Abril de 2013
		PAGINA: 9 de 9

deberá atender a un propósito justificable y haber sido aprobado por el Subdepartamento de TI.

- El Subdepartamento de TI no podrá tener acceso libre y sin control a los datos sensibles de las estaciones de trabajo. De ser requerido, deberá contar con la presencia del dueño del equipo o alguien designado por este.
- El Subdepartamento de TI, previa autorización del encargado de Seguridad podrá examinar archivos privados cuando se presente una emergencia como infección de virus o caídas de sistemas. Si esto ocurre, deberán ser notificados el usuario propietario de los archivos, y el Comité de Seguridad de la Información.
- Si un funcionario está trabajando con información Confidencial deberá tomar las medidas necesarias e inmediatas para no exponer esa información a una lectura no autorizada por parte de un tercero.
- Nunca se debe prestar a otros el computador asignado, portátil, PDA, (Personal Digital Assistant), u otro equipamiento computacional, que contenga información Confidencial.

6.- APLICACIÓN DE LAS POLITICAS DE CLASIFICACION Y MANEJO DE LA INFORMACION

La infracción a las obligaciones establecidas en esta norma, podrá constituir una violación al principio de probidad administrativa, y será sancionada en conformidad a lo dispuesto en la Ley N° 18.834, sobre Estatuto Administrativo. Lo anterior es sin perjuicio de la responsabilidad civil o penal que corresponda.

El Servicio de Salud Viña del Mar – Quillota deberá determinar las sanciones por el mal uso de las políticas de seguridad en la clasificación y manejo de la información.

7.- MONITOREO

El Subdepartamento de TI del Servicio de Salud Viña del Mar – Quillota verificará la aplicación de estas políticas de seguridad en la clasificación y manejo de la información.

8.- GLOSARIO DE TERMINOS

- RRFF: Recursos Físicos
- RRHH: Recursos Humanos
- TI: Tecnologías de Información