
	SERVICIO DE SALUD VIÑA DEL MAR - QUILLOTA	NUMERO: 01
	COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	CODIGO: I
	POLITICAS DE SEGURIDAD DE LA INFORMACION	FECHA: 16 de Abril de 2013
		PAGINA: 1 de 7

POLITICA DE ANTIVIRUS

DIRECCION DEL SERVICIO DE SALUD
VIÑA DEL MAR - QUILLOTA


	SERVICIO DE SALUD VIÑA DEL MAR - QUILLOTA	NUMERO: 01
	COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	CODIGO: I
	POLITICAS DE SEGURIDAD DE LA INFORMACION POLÍTICA DE ANTIVIRUS	FECHA: 16 de Abril de 2013
		PAGINA: 2 de 7

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: 01
	COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	CODIGO: I
	POLITICAS DE SEGURIDAD DE LA INFORMACION POLÍTICA DE ANTIVIRUS	FECHA: 16 de Abril de 2013
		PAGINA: 3 de 7


INDICE

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

	SERVICIO DE SALUD VIÑA DEL MAR - QUILLOTA	NUMERO: 01
	COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	CODIGO: I
	POLITICAS DE SEGURIDAD DE LA INFORMACION POLÍTICA DE ANTIVIRUS	FECHA: 16 de Abril de 2013
		PAGINA: 4 de 7

CONTROL DE VERSIONES

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

	SERVICIO DE SALUD VIÑA DEL MAR - QUILLOTA	NUMERO: 01
	COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	CODIGO: I
	POLITICAS DE SEGURIDAD DE LA INFORMACION POLÍTICA DE ANTIVIRUS	FECHA: 16 de Abril de 2013
		PAGINA: 5 de 7

1.- DECLARACIÓN INSTITUCIONAL

Esta política de antivirus define los criterios y lineamientos esenciales para el Servicio de Salud Viña del Mar – Quillota, en cuanto a la aplicación de medidas de seguridad de software antivirus para todos los usuarios del Servicio de Salud.

Ante la continua amenaza de los virus y los niveles de sofisticación implementados para esparcirse, se hace necesario apoyar la tarea tradicional de los programas antivirus, con el desarrollo de una cultura que permita salvaguardar la información, toda vez que cuando se reciben ataques por virus se merma la productividad, lo que se traduce en pérdida de tiempo y recursos.

2.- OBJETIVOS DE LA POLÍTICA DE ANTIVIRUS

El propósito de esta política es establecer un criterio estándar para la detección oportuna de código malicioso, mediante el empleo del software antivirus y de los criterios para la detección de código malicioso que pudiera estar contenida en documentos o correos provenientes de remitentes fuera del ámbito de confianza.

3.- ÁMBITO DE APLICACIÓN DE LA POLÍTICA DE ANTIVIRUS

El alcance de la política de antivirus abarca a todos los usuarios de sistemas de información y computadores personales del Servicio de Salud Viña del Mar – Quillota.


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 antivirus.
- Aprobar los recursos necesarios para implementación adecuada de las acciones requeridas en la política de seguridad.

Comité de Seguridad

- Elaborar y aprobar la presente política de antivirus.
- 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.

	SERVICIO DE SALUD VIÑA DEL MAR - QUILLOTA	NUMERO: 01
	COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	CODIGO: I
	POLITICAS DE SEGURIDAD DE LA INFORMACION POLÍTICA DE ANTIVIRUS	FECHA: 16 de Abril de 2013
		PAGINA: 6 de 7

- 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.

Sub departamento de Informática


Instalar y mantener actualizado el antivirus institucional, en todos los computadores del Servicio de Salud.

Usuarios del Servicio de Salud

Cumplir a cabalidad las políticas de antivirus del Servicio de Salud.

5.- MARCO GENERAL PARA LAS POLÍTICAS DE ANTIVIRUS

- Se deberá utilizar solamente el antivirus adquirido y licenciado por la Dirección del Servicio de Salud Viña del Mar - Quillota, el antivirus autorizado será instalado en todos los computadores institucionales, por personal de la Unidad de Soporte técnico, del Subdepartamento de TI.
- El antivirus institucional deberá tener la capacidad para ser gestionado centralizadamente y realizar actualizaciones periódicas en forma automática.
- Los usuarios nunca deberán abrir archivos adjuntos a un correo electrónico de procedencia desconocida, sospechosa o fuente no confiable. En ese caso deberá borrar los archivos adjuntos inmediatamente, se recomienda luego vaciar la papelera de reciclaje.
- Se deberá borrar el correo spam, cadenas y cualquier otro correo recibido con estas características. No se debe hacer reenvío de los mismos.
- Nunca se deben descargar archivos de sitios desconocidos o fuentes sospechosas.
- Se debe evitar compartir directamente los discos (carpetas compartidas) del computador con permisos de lectura / escritura, a menos que sea extremadamente necesario por la existencia de un requerimiento del Servicio de Salud.
- Siempre se debe revisar con el antivirus las unidades de discos removibles o memorias flash (pendrive) ante de usarlas.
- En ningún caso, los usuarios del Servicio de Salud pueden copiar, propagar o ejecutar de forma intencionada en equipos que se conecten a la red, programas diseñados para replicarse, dañar, espiar o entorpecer el desempeño de cualquier sistema.
- Cuando se sospeche de una infección o cuando el antivirus detecte una, se debe desconectar el equipo de la red y proceder a su limpieza por parte del usuario, de acuerdo a instructivo entregado para tal efecto. En caso de no poder realizar esta limpieza se debe contactar a la Unidad de Soporte técnico del Subdepartamento de Tecnologías de Información.

	SERVICIO DE SALUD VIÑA DEL MAR - QUILLOTA	NUMERO: 01
	COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	CODIGO: I
	POLITICAS DE SEGURIDAD DE LA INFORMACION POLÍTICA DE ANTIVIRUS	FECHA: 16 de Abril de 2013
		PAGINA: 7 de 7

6.- APLICACIÓN DE LAS POLITICAS DE ANTIVIRUS

La infracción a las obligaciones establecidas en esta política, 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 Subdepartamento de TI no se hará responsable por incidentes producidos por el no cumplimiento de estas políticas de seguridad.

7.- MONITOREO

El Subdepartamento de TI del Servicio de Salud Viña del Mar – Quillota controlará la instalación del antivirus institucional, desinstalando cualquier otro software antivirus no debidamente licenciado por el Servicio de Salud.

8.- GLOSARIO DE TERMINOS

- Spam: Se llama spam, correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor.
- Memorias flash: La memoria flash es una tecnología de almacenamiento que permite la lecto-escritura de múltiples posiciones de memoria en la misma operación.
- Cadenas: Es un tipo de cadena de mensajes que utiliza el correo electrónico como forma de propagación.