
 Gobierno de Chile	SERVICIO DE SALUD VIÑA DEL MAR QUILLOTA	NUMERO: 01
	COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	FECHA: junio de 2014
	PROCEDIMIENTO POLITICA DE ANTIVIRUS	PAGINA: 1 de 3

**PROCEDIMIENTO
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	FECHA: junio de 2014
	PROCEDIMIENTO POLITICA DE ANTIVIRUS	PAGINA: 2 de 3

Es responsabilidad de cada usuario de sistemas de información y computadores personales cumplir a cabalidad las políticas de antivirus del Servicio de Salud.

PROCEDIMIENTO GENERAL POLÍTICA DE ANTIVIRUS

El antivirus adquirido, y licenciado por la Dirección del Servicio de Salud Viña del Mar – Quillota, será instalado en todos los computadores institucionales solamente por personal de la Unidad de Soporte técnico, del Subdepartamento de Tecnologías de Información (TI). El usuario no debe desinstalar la solución antivirus de su computador.

SÍNTOMAS MÁS COMUNES DE VIRUS

La mejor forma de detectar un virus es, obviamente un antivirus, pero en ocasiones los antivirus pueden fallar en la detección. En estos casos debemos notar algunos síntomas posibles:

- Los programas comienzan a ocupar más espacio de lo habitual. Se reduce el espacio libre en la memoria RAM.
- Aparecen o desaparecen archivos y/o mensajes de error no comunes. Programas que normalmente funcionaban bien, comienzan a fallar y generar errores durante la sesión.
- Cambia el tamaño de un programa o un objeto.
- Aparecen mensajes u objetos extraños en la pantalla.
- Las operaciones se realizan con más lentitud de lo habitual.
- Los objetos que se encuentran en la pantalla aparecen ligeramente distorsionados.
- Se modifican sin razón aparente el nombre de los archivos.
- No se puede acceder al disco duro.


QUÉ HACER SI ENCUENTRA SÍNTOMAS DE INFECCIÓN

Cuando se sospeche de una infección, o cuando el antivirus detecte una, los pasos a seguir con los siguientes:

1. Desconecte su computador de la red.
2. Antes de emprender cualquier acción, haga una copia de seguridad de todos los datos críticos a una unidad externa (CD, DVD, Pendrive, etc.).
3. Si fuera necesario, descargue las últimas actualizaciones de la base de datos del antivirus. No utilice el computador infectado para descargar las actualizaciones, sino utilice el de un compañero de oficina. También podría obtener actualizaciones para su software antivirus en CD-ROM solicitándolo a la Unidad de Soporte técnico, del Subdepartamento de TI.
4. Realice un análisis completo del sistema.

SI SE ENCUENTRAN VIRUS DURANTE EL ANÁLISIS

El antivirus le notificará si se encuentra virus durante la verificación y le ofrecerá varias opciones para tratar con los objetos infectados.

	SERVICIO DE SALUD VIÑA DEL MAR QUILLOTA	NUMERO: 01
	COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	FECHA: junio de 2014
	PROCEDIMIENTO POLITICA DE ANTIVIRUS	PAGINA: 3 de 3

En la gran mayoría de los casos, los computadores personales están infectados por gusanos, programas troyanos o virus, y los datos perdidos pueden ser recuperados con éxito.

Las principales alternativas de acción son:

1. El antivirus le provee la opción de desinfectar los objetos infectados, ponerlos en cuarentena, borrar los gusanos y troyanos. Un informe proveerá los nombres del software malicioso descubierto en su computador.
2. En algunos casos, se puede necesitar una utilidad especial para recuperar datos que han sido corrompidos. Utilizando el computador de un compañero de oficina, visite el sitio de su proveedor de software antivirus y busque información acerca del virus, troyano o gusano que infectó su computador, descargue cualquiera de las utilidades especiales que estén disponibles.
3. Algunos virus no pueden ser removidos de los objetos infectados, incluso podrían corromper información en su computador, y puede ser imposible restaurar esta información. Si un virus no puede ser removido de un archivo, el archivo debe borrarse.

En caso de no poder realizar la limpieza se debe contactar a la Unidad de Soporte técnico del Subdepartamento de TI.

Firmas de los responsables.

 <p>ELABORADO POR Jefe Unidad Tecnología de Información Representante del Comité de Seguridad</p>	 <p>REVISADO POR Encargado de Seguridad de la Información Encargado de Seguridad</p>	 <p>APROBADO POR DIRECCIÓN Director(a) del Servicio</p>
--	---	--