Responsabilidades de los administradores del servicio de Antivirus Corporativo en las Facultades y Dependencias Centrales de la UCV.

Entre las responsabilidades que debe cumplir el personal encargado de la administración del servicio de Antivirus Corporativo, se indican las siguientes:

1. Instalar y/o actualizar la solución de antivirus corporativo debidamente licenciada, en un servidor que permita la administración y distribución remota de las actualizaciones a todos los equipos.

2. Monitorear diariamente desde la cónsola de servicio, los equipos incorporados a la solución de Antivirus Corporativo con el fin de detectar posibles virus, huellas desactualizadas, entre otros aspectos.

3. En el caso de la presencia de virus o riesgos de seguridad, implementar mecanismos de alerta y notificar a la DTIC, para tomar las acciones necesarias que permitan controlar y erradicar el problema lo antes posible y evitar la propagación del virus a un mayor número de equipos en la UCV.

4. Revisar en forma habitual los medios de comunicación, las páginas que alertan sobre la aparición de nuevos virus y sus procedimentos de erradicación, así como los correos informativos emitidos por la DTIC ante la identificación y las medidas a seguir ante la aparición de nuevas amenazas.

5. Realizar un monitoreo constante del tráfico y el comportamiento de aplicaciones, con la finalidad de obtener las características normales de la red que sirvan de punto base para la detección de situaciones anómalas en la red de la Universidad.

6. Desarrollar procedimientos para analizar, distribuir y realizar actualizaciones del sistema operativo y aplicaciones en los clientes de cada plataforma, ya que las actualizaciones de software son la principal forma que tienen los clientes de protegerse contra las vulnerabilidades de seguridad.

7. Desactivar o eliminar todos los servicios que no sean necesarios en los computadores. A través de estos servicios penetra buena parte de los ataques. Por lo tanto, si se eliminan las amenazas, se

dispondrán de menos entradas para realizar ataques y se tendrán que mantener menos servicios actualizados con parches, aunque estén protegidos por un firewall.

8. Mantener siempre actualizado el software de los servidores, es decir los equipos que ofrezcan servicios públicos (HTTP, FTP, correo, DNS, etc.), aunque estén protegidos por un firewall.

9. Instalar en los computadores software legal, debido a que las copias piratas tienen grandes riesgos ante problemas de seguridad por su dudosa procedencia.

10. Implementar una política de contraseñas robustas. Con contraseñas complejas, resulta más difícil descifrar archivos de contraseñas en equipos infectados o atacados. De este modo, ayuda a evitar que se produzcan daños cuando un equipo es atacado o, al menos, limita esta posibilidad. Por ejemplo, algunos virus realizan ataques de tipo diccionario o de fuerza bruta para obtener acceso a los equipos.

11. Mantener a los usuarios informados mediante boletines informativos periódicos donde se alerta sobre nuevos virus y se emitan recomendaciones para ser aplicadas en los computadores.

12. Identificar en su entorno de red los posibles puntos de entrada de infección o ataques, así como almacenamiento y transmisión de virus.

13. La Unidad de Tecnología debe ser vigilante para asegurar que el usuario no instale de manera arbitraria aplicaciones en el computador, para ello, la cuenta del usuario no deberá pertenecer a la lista de administradores del equipo ni el usuario conocer la cuenta del administrador. Podrán existir excepciones si estuvieren debidamente justificadas y soportadas.