UNIVERSIDAD CENTRAL DE VENEZUELA
RECTORADO
DIRECCIÓN DE TECNOLOGÍA DE
INFORMACIÓN Y COMUNICACIONES

Dirección de Tecnología de Información y Comunicaciones

Normativas de Seguridad en la administración y uso de la solución de Antivirus corporativo.

El servicio de Antivirus corporativo tiene como finalidad proteger las estaciones de trabajo y servidores conectados a la Red de Servicios Integrados de la UCV de ataques de codigo malicioso como virus, spyware, troyanos, etc.

Entre las políticas a cumplir se tiene:

1. Se debe utilizar la solución de antivirus adquirida por la DTIC para toda la UCV, la cual es corporativa y licenciada.
2. Aplicar a nivel de sistema operativo todas las actualizaciones críticas y de seguridad emitidas por el fabricante del sistema operativo.
3. Utilizar una contraseña robusta para el acceso a la cónsola de monitoreo. Una contraseña robusta debe cumplir con las siguientes reglas para su creación:
    a. Las contraseñas deben modificarse periódicamente, al menos cada 3 meses.
    b. Las claves de acceso y/o contraseñas deben tener al menos 8 caracteres.
    c. Deben estar integrados por una combinación de caracteres numéricos y alfabéticos, con una combinación de caracteres en mayúscula y minúscula. Los caracteres numéricos preferiblemente no deben estar al principio o fin de la clave. Si el sistema de computación lo permite, es conveniente incluir al menos un carácter especial (¡@#$%^&_+=?/).
    d. No debe responder a nada que pueda ser fácilmente relacionado al usuario tal como nombre del usuario, numero de cedula de identidad, apodo, nombres de familiares o mascotas, fecha de nacimiento, placa del carro, numero telefónico, dirección, el reverso de cualquiera de los anteriores, entre otros.
    e. No debe responder a palabras existentes en el diccionario o acrónimos.

4. Configurar las siguientes opciones en la solución antivirus:
    a. Habilitar la limpieza de archivos infectados como primera opción, como segunda opción enviar los archivos contaminados a cuarentena y como tercera opción eliminarlos.
    b. Activar la notificación de evento al administrador y las alertas visuales a los usuarios informando sobre riesgos y/o desactualizaciones.

c. Verificar que se cumplan diariamente las actualizaciones de la base de datos de virus.
d. Los medios extraibles como unidades de diskettes, USB, memorias flash, etc, deben ser revisados con el antivirus antes de acceder la información de ellos.
e. Las estaciones de trabajo deben ser escaneadas de forma obligatoria por lo menos una vez a la semana.
f. Los usuarios no pueden desactivar el antivirus.

5. Si existiera alguna amenaza que comprometa a uno o varios servicios (aplicación), deshabilitar o bloquear el acceso a los mismos hasta que se apliquen las medidas correctivas correspondientes, y notificar a los usuarios los motivos y tiempo estimado de la suspensión.

6. Ofrecer el servicio anti-spam para filtrar los correos no deseados o utilizar el servicio anti-spam ofrecido por la DTIC. Es necesario, llevar un registro de la cantidad de correos de este tipo que son filtrados diariamente, a fin de mejorar este servicio y evitar posibles colapsos del servicio de correo o de la red.

7. Activar la revisión de los correos entrantes y salientes de las estaciones de trabajo de cada usuario.

8. Habilitar y configurar en cada aplicación de mensajería instantánea el chequeo por parte del antivirus de los archivos que se transmitan por esa vía.

9. Desconectar rápidamente de la red los computadores que resulten infectados para evitar que pongan en peligro otros computadores de su Facultad y/o Dependencia Central.

10. No ejecutar programas de origen dudoso.

11. Los registros de logs del sistema deben ser configurados de tal forma que la información se encuentre disponible por períodos que sirvan de insumo en el caso de ocurrir un incidente de seguridad.
12. Informar lo antes posible a la DTIC, de cualquier evento irregular que no pueda ser detectado o corregido por la solución de Antivirus ESET. De esta manera el personal de la DTIC puede atender el caso o elevarlo lo mas pronto posible a la empresa ESET.