ES-17 CONFIGURACIÓN DE SEGURIDAD ANTIMALWARE

1. Normatividad Relacionada

NO-05 Respaldo de la Información
NO-07 Responsabilidad de Usuarios
NO-09 Prevención, Detección y Eliminación de Malware
NO-13 Comandos Especiales y Administración de Componentes Tecnológicos
NO-14 Administración y Configuración de Parámetros de Seguridad
NO-24 Retiro de Componentes Tecnológicos
NO-25 Uso del Correo Electrónico
NO-26 Acceso a Internet
NO-36 Seguridad y Uso Adecuado de Computadores Portátiles
NO-37 Seguridad y Uso Adecuado de Computadores de Escritorio
NO-39 Seguridad y Uso de Equipos de Terceros
NO-40 Software y Hardware Utilizado

2. Objetivos

Establecer la configuración de parámetros básicos de seguridad para disminuir el riesgo de presencia de Malware en los diferentes Componentes Tecnológicos de la UAEAC.

3. Componentes Tecnológicos Afectados

Todos los Componentes Tecnológicos de la UAEAC que tengan instalado el antimalware corporativo.

4. Descripción

Se deben configurar los siguientes parámetros:

- Prevención de Amenazas: **Activado**
- Control Web: **Activado**
- Desinfección automática de archivos: **Activado**
- En el caso que la desinfección falle, se debe enviar el archivo a un directorio en cuarentena y posteriormente eliminarlo.
- Revisión de archivos entrantes
- Revisión de medios extraíbles al momento de accederlo
- Revisión de archivos comprimidos
- Mostrar ícono del agente en la barra de tareas

- No excluir ningún tipo de archivo en la revisión
- Análisis Completo: **Una vez por semana en todos los directorios y archivos del Componente Tecnológico.**
- Guardar registro de los resultados de la última revisión de la herramienta antimalware: **SI**
- Actualizar diariamente los archivos DAT.
- Actualizaciones periódicas de producto (motor de antimalware)
- Realizar las actualizaciones a través de la consola.
- Todos los agentes deben estar registrados en la consola de administración.
- Modificación de políticas en los agentes: **Restringido para usuarios finales**.