

Métodos de evaluación

Restricciones de uso del software

Revisar documentación: determinar que la licencia de software y su uso están activos y se realizan correctamente en el sistema. Discutirlo con el propietario del sistema, el personal de adquisición, el personal de CM y el responsable de seguridad.

Restricciones de uso del software  
-Software de código abierto-

Revisar documentación: determinar que la licencia de software y su uso están activos y se realizan correctamente en el sistema. Discutirlo con el propietario del sistema, el personal de adquisición, el personal de CM y el responsable de seguridad.

Software instalado por el usuario

Revisar documentación: determinar si el software de código abierto está activo en el sistema y las restricciones adecuadas para su uso. Hablar con el propietario del sistema y el responsable de seguridad

Software instalado por el usuario  
-Alertas de instalaciones no autorizadas-

Revisar documentación: determinar si el sistema alerta al personal adecuado cuando un usuario intenta cargar software no autorizado. Realizar una prueba de carga de software y observar resultados. Hablar con el propietario del sistema y el responsable de seguridad.

Software instalado por el usuario  
-Prohibir la instalación sin estatus privilegiado-

Revisar documentación: determinar si sólo los titulares de cuentas con privilegios pueden cargar software en el sistema. Probar cargando el software y observar los resultados. Hablar con el propietario del sistema y el responsable de seguridad.

Examinar

Política de gestión de la configuración, procedimientos con restricciones de uso de software, plan de seguridad, acuerdos contractuales del software, leyes de derechos de autor, documentación de la licencia del sitio, lista de restricciones de uso del software; informes de seguimiento de la licencia del software.

Política de gestión de la configuración, procedimientos con restricciones de uso del software de código abierto, plan de gestión de la configuración, plan de seguridad.

Revisar documentación: determinar qué nivel de instalación de software está permitido para los usuarios normales del sistema. Para mantener el control sobre los tipos de software instalados, determinar si la organización ha identificado las acciones permitidas y prohibidas en relación con la instalación de software. Hablar con el propietario del sistema y el responsable de seguridad.

Revisar documentación: determinar si el sistema alerta al personal adecuado cuando un usuario intenta cargar software no autorizado. Realizar una prueba de carga de software y observar resultados. Hablar con el propietario del sistema y el responsable de seguridad.

Revisar documentación: determinar si sólo los titulares de cuentas con privilegios pueden cargar software en el sistema. Probar cargando el software y observar los resultados. Hablar con el propietario del sistema y el responsable de seguridad.

Guía SP  
800-53A

Entrevistar

Personal con responsabilidades de seguridad de la información, administradores de sistemas/redes, personal que opera, utiliza y/o mantiene el sistema de información, personal con responsabilidades de gestión de licencias de software.

Personal con responsabilidades para establecer y hacer cumplir restricciones sobre el uso de software de código abierto, personal con responsabilidades de seguridad de la información, administradores de sistemas/redes.

Personal con responsabilidades en la gestión del software instalado por el usuario, personal que opera, utiliza y/o mantiene el sistema de información, personal que supervisa el cumplimiento con la política de software instalado por el usuario, personal con responsabilidades de seguridad de la información; administradores de sistemas/redes.

Personal con responsabilidades en la gestión del software instalado por el usuario, personal que opera, utiliza y/o mantiene el sistema de información, personal con responsabilidades en materia de seguridad de la información, administradores de sistemas/redes, desarrolladores de sistemas.

Personal con responsabilidades en la gestión del software instalado por el usuario, personal que opera, utiliza y/o mantiene el sistema de información.

Prueba

Proceso para el seguimiento del uso de software protegido por licencias de cantidad, proceso organizativo para controlar/documentar el uso de la tecnología de intercambio de archivos entre pares, mecanismos automatizados que implementen el seguimiento de las licencias de software, mecanismos automatizados que implementen y controlen el uso de la tecnología de intercambio de archivos entre pares.

Proceso para restringir el uso de software de código abierto, mecanismos automatizados para aplicar las restricciones al uso de software de código abierto.

Procesos que rigen el software instalado por el usuario, mecanismos automatizados que aplican las normas/métodos para regular la instalación de software por parte de los usuarios, mecanismos automatizados que controlan el cumplimiento de la política.

Procesos de la organización que rigen el software instalado por el usuario, mecanismos automatizados para alertar al personal/las funciones cuando se detecta la instalación no autorizada de software.

Procesos que rigen el software instalado por el usuario, mecanismos automatizados para prohibir la instalación de software sin estatus privilegiado.