Instalación de sistemas operativos y seguridad de sistemas informáticos

1. ¿Qué es el proceso de hardening en seguridad informática?

El término Hardening en seguridad informática es el proceso de de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo, esto se logra eliminando software, servicios, usuarios, etc; innecesarios en el sistema; así así como cerrando puertos que tampoco estén en uso además de además de otros métodos.

2. ¿Cuáles son algunas de las actividades clave en un proceso de hardening?

las actividades propias de un proceso de hardening se pueden contar las siguientes:

- Configuraciones necesarias para protegerse de posibles ataques físicos o de hardware de la máquina.
- Instalación segura del sistema operativo.
- Activación y/o configuración adecuada de servicios de actualizaciones automáticas.
- Configuración de servicios de sistema.
- Configuración de los protocolos de Red.
- Configuración adecuada de permisos de seguridad en archivos y carpetas del sistema.
- Configuración de opciones de seguridad de los distintos programas.
- Configuración de acceso remoto.
- Configuración adecuada de cuentas de usuario.
- Cifrado de archivos o unidades según las necesidades del sistema.

3. ¿Qué precauciones se deben tomar en la configuración de la BIOS para mejorar la seguridad?

Existen varias características de seguridad comunes en el BIOS:

- Contraseñas del BIOS.

- Encriptación de unidades.
- Módulo de plataforma segura (TPM).
- Geolocalización, borrado de datos de forma remota, etc.

- Encriptación de unidades: es posible encriptar un disco duro para evitar el robo de datos: sin la contraseña correcta, la PC no arranca y no puede descifrar los datos.

- Módulo de plataforma segura: si se producen demasiados intentos de autorización incorrectos, el TPM(El chip del TPM es un procesador de criptografía seguro diseñado para realizar operaciones criptográficas.) activa su lógica de ataques de diccionario y evita más intentos de autorización.

4. ¿Qué es el Secure Boot y cómo ayuda a proteger el arranque del sistema operativo?

Secure Boot o arranque seguro, es un modo para UEFI que trae Windows desde Windows 8, y que impide la ejecución de cualquier software no firmado o certificado en el arranque del sistema. Con ello se intenta evitar la carga de malware o aplicaciones que no sean de fiar cuando inicias el ordenador.

- Los sistemas GNU/Linux ofrecen la posibilidad de modificar los parámetros de arranque desde el gestor de arranque GRUB.

- Si obtenemos acceso al menú de arranque grub, tenemos la posibilidad de acceder con permisos de root, por lo que debemos de proteger el GRUB con contraseña.

5. ¿Cómo se puede proteger el gestor de arranque GRUB en sistemas Linux?

Con contraseña.

6. ¿Qué es BitLocker y cómo funciona para cifrar volúmenes en sistemas Windows?

BitLocker es una aplicación de cifrado que nos permite proteger nuestro disco duro de un posible robo de información. Encontramos esta herramienta disponible en sistemas Windows desde Windows Vista. Cifra volúmenes enteros. Esto quiere decir que puede cifrar todo el disco duro o simplemente una parte de él. Utiliza un algoritmo de cifrado AES en modo CBC con una clave de 128 bits.

7. ¿Dónde se puede almacenar la clave de cifrado de BitLocker?

La clave se puede alojar en 5 lugares distintos.

- En una cuenta de Microsoft. Para encontrar la clave de cifrado sólo hay que iniciar sesión en otro dispositivo.

- En una copia impresa. Este método es poco recomendable porque la clave estaría de manera relativamente sencilla al alcance del atacante.

- En una unidad flash USB. Es posible alojar nuestra clave en un pendrive que deberemos conectar al ordenador para abrir el cifrado.

- En una cuenta de Azure Active Directory. En el caso de que tu PC sea parte de una organización, lo más probable es que tu clave de BitLocker se encuentre en la cuenta de Azure AD asociada con el PC.

- La clave la guardó el administrador del sistema. Esto aplica en los casos en los que tu PC está conectado a un dominio, sea dentro de un equipo de trabajo o un centro educativo. El administrador del sistema deberá proporcionar la clave de BitLocker en este caso.

8. ¿Qué tipos de volcados de memoria existen en Windows y cómo se pueden configurar?

Existen algunos tipos de volcado de memoria como lo son:

- Volcado de memoria completa: Registra todo el contenido de la memoria de Windows hasta el momento en que el equipo se detiene repentinamente.

- Volcado de memoria del núcleo: Solamente registra la memoria del núcleo, esto permite acelerar el proceso de grabación en el registro en el momento de la falla del equipo.

- Volcado de memoria pequeña: Registra solo alguna información que es útil a la hora de identificar la razón del fallo en el equipo.

9. ¿Dónde se puede encontrar información sobre errores en sistemas Linux?

En los sistemas Linux los archivos de debug no están agrupados como en Windows. Se puede hacer una clasificación de los problemas que surgen durante la ejecución del sistema operativo.

- Incidencias en el kernel.
- Incidencias en las aplicaciones.

- Incidencias en el hardware.

Podemos encontrar información de errores en archivos de logs dentro del directorio /var/logs/ tales como kern.log, dmesg o syslog entre otros. Disponemos de utilidades para hacer un seguimiento de las incidencias del sistema tales como lsoft, strace, top, etc.

10. ¿Qué es la aleatorización de la memoria virtual y cómo ayuda a proteger contra malware?

La aleatoriedad en la disposición del espacio de direcciones (ASLR) es una técnica de seguridad informática relacionada con la explotación de vulnerabilidades basadas en la corrupción de memoria. Con el fin de impedir que un atacante salte de forma fiable a una función explotable en concreto de la memoria, ASLR dispone de forma aleatoria las posiciones del espacio de direcciones de las áreas de datos clave de un proceso, incluyendo la base del ejecutable y las posiciones de la pila, el heap y las librerías.

11. ¿Cuáles son los diferentes tipos de antivirus según su objetivo específico?

Vamos a clasificarlos según diferentes criterios como son:

- Según su finalidad.
- Según su objetivo específico.
- Según su ejecución: online/offline, pasivo/activo.

Tipos de antivirus según su finalidad

- Antivirus preventivos: Se caracterizan porque analizan la entrada y salida de todos los datos en tu ordenador con la finalidad de interceptar posibles amenazas, anticipándose a la infección del equipo por parte de programas maliciosos.

- Antivirus identificadores: Son antivirus que exploran el sistema operativo de tu ordenador con la finalidad de identificar posibles virus existentes en el mismo. Rastrean secuencias de bytes de códigos específicos.

- Antivirus descontaminadores: Cuando el virus ya se encuentra identificado en nuestro ordenador, el antivirus de tipo descontaminador se encarga de eliminar esta infección. Tiene algunas funciones similares a los antivirus identificadores.

Tipos de antivirus según su objetivo específico

- Firewall o cortafuegos: controla la entrada y la salida de datos de tu ordenador y bloquea “como un muro” toda aquella actividad que le resulte dudosa. Actúa de forma preventiva.

• Antipop-up: se encarga únicamente de evitar que algunas webs abran de forma automática ventajas emergentes que puedan resultar molestas al navegar por Internet.

• Antispyware o antiespías: tiene el objetivo de detectar y eliminar programas espías que se hayan instalado en nuestro equipo sin nuestro consentimiento. La finalidad de estos programas espías maliciosos y silenciosos es recabar información sobre el usuario (contraseñas, hábitos de navegación, etc.) para pasarla de forma ilegal a terceros.

• Antispam:Su objetivo específico es el de identificar emails de dudosa procedencia y mandarlos directamente a la bandeja de spam.

• Antimalware: Los antimalware están diseñados para analizar, detectar, prevenir y eliminar software malicioso en nuestros equipos, es decir, malware.

12. ¿Qué características de seguridad ofrece Windows Defender en Windows 10?

a. Ofrece la protección antivirus más reciente.

b. busca continuamente malware, virus y amenazas de seguridad. Además de esta protección en tiempo real, las actualizaciones se descargan automáticamente para ayudar a mantener el dispositivo seguro y protegerlo de amenazas.

13. ¿Cómo se puede configurar una política de contraseñas robusta en el sistema operativo?

A través del Editor de directivas de seguridad local o mediante directivas de grupo si estás en un entorno empresarial. En sistemas Linux, las políticas de contraseñas suelen estar definidas en archivos de configuración como /etc/login.defs o en archivos específicos de cada servicio de autenticación que estés utilizando, como PAM (Pluggable Authentication Modules).

14. ¿Qué medidas se pueden tomar para limitar los privilegios de los usuarios?

- Limitar los privilegios de los usuarios es una práctica fundamental para garantizar la seguridad de un sistema:

- Principio de menor privilegio: Aplica el principio de menor privilegio, lo que significa otorgar a los usuarios solo los permisos necesarios para realizar sus tareas específicas y nada más.

- Grupos de usuarios: Organiza a los usuarios en grupos según sus roles y responsabilidades.

- Cuentas de usuario privilegiadas: Limita el número de cuentas de usuario con privilegios elevados, como cuentas de administrador.

- Control de acceso basado en roles (RBAC): Implementa un modelo de control de acceso basado en roles que asigna privilegios a los usuarios según su función dentro de la organización.

- Políticas de contraseña para cuentas privilegiadas: Aplica políticas estrictas de contraseñas para las cuentas de usuario privilegiadas, como la longitud mínima de la contraseña, la complejidad y la caducidad de la misma.

- Auditoría de privilegios: Realiza auditorías periódicas para revisar los privilegios de los usuarios y asegurarse de que estén alineados con las necesidades del negocio.

Monitoreo de actividades privilegiadas: Implementa herramientas de monitoreo y registro de actividades para supervisar el uso de privilegios elevados.

Capacitación y concienciación: Proporciona capacitación regular a los usuarios sobre la importancia de la seguridad de la información y la gestión adecuada de los privilegios.

15. ¿Cómo se puede configurar la auditoría de sistema para detectar intentos de ataque?

- Identificar eventos de interés: Antes de configurar la auditoría, identifica los eventos que podrían indicar un intento de ataque.

- Habilitar la auditoría: En sistemas Windows, puedes habilitar la auditoría a través de la Directiva de Seguridad Local. En sistemas Linux, puedes configurar la auditoría mediante herramientas como Auditd.

- Definir reglas de auditoría: Configura reglas de auditoría específicas para los eventos que deseas monitorear.

- Establecer políticas de retención de registros: Define políticas claras de retención de registros para asegurarte de que los registros de auditoría se conserven durante el tiempo suficiente para su análisis posterior.

- Centralizar los registros de auditoría: Centraliza los registros de auditoría en un sistema de registro central o un servidor de administración de registros.

- Configurar alertas: Configura alertas para eventos de auditoría específicos que puedan indicar un intento de ataque.

- Monitoreo continuo: Realiza un monitoreo continuo de los registros de auditoría para detectar cualquier actividad sospechosa o anomalía.

- Análisis forense: En caso de un posible ataque, realiza un análisis forense de los registros de auditoría para investigar el incidente, determinar el alcance del ataque y tomar medidas correctivas adecuadas.

16. ¿Qué servicios y protocolos de red se deben deshabilitar si no son necesarios?

- Servicios de compartición de archivos e impresoras: Si no necesitas compartir archivos o impresoras en red, deshabilita servicios como SMB (Server Message Block) en sistemas Windows o NFS (Network File System) en sistemas Unix/Linux.

Servicios de acceso remoto: Deshabilita servicios como Telnet, FTP y servicios de escritorio remoto (como RDP en Windows) si no necesitas acceso remoto a tu sistema.

Servicios de servidor web: Si no necesitas ejecutar un servidor web en tu sistema, deshabilita servicios como Apache, Nginx u otros servidores web para evitar posibles vulnerabilidades asociadas con ellos.

- Servicios de base de datos: Desactiva servicios de base de datos como MySQL, PostgreSQL o SQL Server si no estás utilizando activamente una base de datos en tu sistema.

- Servicios de proxy y túneles VPN: Si no necesitas ejecutar un servidor proxy o un túnel VPN en tu sistema, deshabilita estos servicios para evitar posibles riesgos de seguridad.

- Servicios de gestión remota: Deshabilita servicios de gestión remota como SNMP (Simple Network Management Protocol) si no los estás utilizando activamente para monitoreo y gestión de red.

- Protocolos de enrutamiento dinámico: Si no estás utilizando enrutamiento dinámico en tu red, deshabilita protocolos como OSPF (Open Shortest Path First) o RIP (Routing Information Protocol) para evitar posibles ataques de envenenamiento de tablas de enrutamiento.

- Servicios de correo electrónico: Si no necesitas ejecutar un servidor de correo electrónico en tu sistema, deshabilita servicios como SMTP (Simple Mail Transfer Protocol) o POP3 (Post Office Protocol) para evitar posibles riesgos de seguridad asociados con ellos.

17. ¿Cómo se puede configurar adecuadamente el acceso remoto a un sistema?

- Evaluar necesidades: Antes de configurar cualquier método de acceso remoto, determina quiénes necesitarán acceder al sistema de forma remota y con qué frecuencia.

- Elegir un método de acceso remoto seguro: Hay varios métodos de acceso remoto disponibles, como SSH (Secure Shell), RDP (Remote Desktop

Protocol), VPN (Virtual Private Network), entre otros.

Configura el cortafuegos: Configura el cortafuegos del sistema para permitir el tráfico entrante y saliente necesario para el método de acceso remoto que estés utilizando.

Implementa medidas de autenticación sólidas: Utiliza autenticación multifactor (MFA) siempre que sea posible para añadir una capa adicional de seguridad.

- Encripta la comunicación: Siempre que sea posible, utiliza protocolos de comunicación seguros que cifren los datos transmitidos entre el cliente y el servidor, como SSH para acceso remoto en sistemas Unix/Linux y VPN para acceso remoto a redes privadas.

- Gestiona adecuadamente los usuarios y los privilegios: Limita el número de usuarios que tienen acceso remoto al sistema y asegúrate de que solo tengan los privilegios necesarios para realizar sus tareas. Esto reduce el riesgo de acceso no autorizado o uso indebido.

- Monitoriza y registra las sesiones de acceso remoto: Configura la auditoría del sistema para registrar las sesiones de acceso remoto y supervisa activamente los registros en busca de actividades sospechosas.

- Actualiza regularmente el software: Mantén actualizado el software del sistema y cualquier software relacionado con el acceso remoto para asegurarte de que estás protegido contra las últimas vulnerabilidades de seguridad.

18. ¿Qué medidas se pueden tomar para proteger los archivos y carpetas del sistema?

Medidas que puedes tomar para protegerlos:

Asignar permisos adecuados: Utiliza el sistema de permisos del sistema operativo para asignar permisos adecuados a los archivos y carpetas.

Implementar el principio de menor privilegio: Sigue el principio de menor privilegio y otorga los permisos mínimos necesarios para que los usuarios realicen sus tareas. Cifrado de archivos sensibles: Utiliza el cifrado de archivos para proteger archivos sensibles.

Realizar copias de seguridad regulares: Implementa un plan de copia de seguridad regular para asegurarte de que los archivos importantes están protegidos contra pérdidas de datos debido a errores humanos,

Auditoría de archivos: Configura la auditoría de archivos para supervisar y registrar los accesos a archivos y carpetas sensibles. Utilizar sistemas de detección de

intrusiones: Implementa sistemas de detección de intrusiones (IDS) o sistemas de prevención de intrusiones (IPS) para monitorear y detectar actividades maliciosas o intentos de acceso no autorizado a archivos y carpetas del sistema.

Actualizar y parchear regularmente: Mantén tu sistema operativo y cualquier software relacionado con la gestión de archivos actualizado con los últimos parches de seguridad para proteger contra vulnerabilidades conocidas que podrían ser explotadas por los atacantes.

Concientización y capacitación del usuario: Educa a los usuarios sobre la importancia de proteger los archivos y carpetas del sistema. que podrían llevar a la descarga de malware.

19. ¿Cómo se puede configurar el cifrado de archivos y mensajería?

Cifrado de archivos:

Utilizar software de cifrado de archivos:

- Emplea herramientas de cifrado de archivos como VeraCrypt, BitLocker (para Windows), o dm-crypt/LUKS (para Linux) para cifrar discos completos, particiones o carpetas específicas.

- Sigue las instrucciones proporcionadas por el software para crear un volumen cifrado o cifrar archivos individuales. Cifrar archivos con GPG (GNU Privacy Guard):

- GPG es una herramienta de cifrado de código abierto que se utiliza comúnmente para cifrar y firmar correos electrónicos y archivos.

- Puedes cifrar archivos usando GPG mediante la línea de comandos o integrando GPG con herramientas de gestión de archivos como GNU Tar. Utilizar servicios de almacenamiento en la nube con cifrado integrado:

- Utiliza servicios de almacenamiento en la nube que ofrecen cifrado de extremo a extremo, como Tresorit, Sync.com o pCloud.

- Asegúrate de habilitar la opción de cifrado en tu cuenta y sigue las instrucciones proporcionadas por el proveedor del servicio.

Cifrado de mensajería:

Utilizar aplicaciones de mensajería seguras:

- Utiliza aplicaciones de mensajería que ofrecen cifrado de extremo a extremo, como Signal, WhatsApp (cuando se habilita el cifrado de extremo a extremo), Telegram (en los chats secretos) o Wire.

- Asegúrate de que las opciones de cifrado estén habilitadas en la configuración de la aplicación. Cifrar correos electrónicos:

- Emplea protocolos de cifrado como PGP (Pretty Good Privacy) o S/MIME para cifrar correos electrónicos.

- Configura tu cliente de correo electrónico para utilizar PGP o S/MIME y sigue las instrucciones proporcionadas para generar claves y configurar el cifrado. Utilizar VPN para comunicaciones seguras:

- Utiliza una red privada virtual (VPN) para cifrar el tráfico de Internet entre tu dispositivo y el servidor VPN.

- Elige proveedores de VPN confiables que utilicen protocolos de cifrado sólidos como OpenVPN, IKEv2/IPsec o WireGuard. Evitar el uso de mensajería no cifrada:

- Evita el uso de aplicaciones de mensajería y correo electrónico que no ofrecen cifrado de extremo a extremo, ya que el contenido podría ser interceptado y leído por terceros.

20. ¿Qué recomendaciones hay para un sistema de respaldos frecuentes?

- Planificación regular: Realiza respaldos de manera regular, preferiblemente de forma automática, para asegurarte de que los datos importantes estén protegidos en todo momento.

- Implementa un sistema de versionado: Utiliza un sistema que mantenga múltiples versiones de los archivos respaldados.

- Almacena en ubicaciones diferentes: Mantén copias de seguridad en ubicaciones físicas diferentes para protegerse contra pérdidas debido a desastres naturales o eventos catastróficos.

- Utiliza cifrado: Encripta tus copias de seguridad para proteger la confidencialidad de los datos almacenados, especialmente si están almacenados en la nube o en dispositivos portátiles.

- Prueba regularmente las restauraciones: Realiza pruebas periódicas de restauración para asegurarte de que tus copias de seguridad sean efectivas y puedan restaurarse correctamente cuando sea necesario.

- Monitorea los registros de respaldo: Verifica los registros de respaldo para identificar cualquier problema o error en el proceso de respaldo y toma medidas correctivas según sea necesario.

21. ¿Qué es el módulo de plataforma segura (TPM) y cómo ayuda a la seguridad?

El Módulo de Plataforma Segura (TPM) es un chip de hardware que se utiliza para almacenar claves de cifrado, certificados digitales y otros datos relacionados con la seguridad de forma segura. Ayuda a proteger la integridad del sistema y los datos al proporcionar funciones de seguridad como la generación segura de claves, la autenticación de hardware y la medida de la integridad del sistema operativo. El TPM también puede utilizarse para habilitar funciones de seguridad como el inicio seguro (Secure Boot) y la protección de datos mediante el cifrado de disco completo.

22. ¿Cómo se puede proteger el sistema de ficheros en Linux?

Proteger el sistema de archivos en Linux:

- Permisos de archivo y directorio: Utiliza los permisos adecuados para archivos y directorios. Utiliza el comando chmod para establecer permisos específicos que limiten el acceso a archivos y directorios solo a usuarios autorizados.

- Control de acceso obligatorio (MAC): Implementa mecanismos de control de acceso obligatorio como SELinux (Security-Enhanced Linux) o AppArmor para aplicar políticas de seguridad adicionales y restringir el acceso a recursos del sistema.

- Cifrado de datos: Utiliza sistemas de archivos con características de seguridad, como ext4 con atributos extendidos, o sistemas de archivos cifrados como dm-crypt/LUKS, para proteger los datos almacenados en el disco.

- Auditoría del sistema de archivos: Habilita la auditoría del sistema de archivos para registrar eventos como la creación, modificación y eliminación de archivos. Utiliza herramientas como auditd para configurar y supervisar la auditoría del sistema de archivos.

- Verificación de integridad: Utiliza herramientas como Tripwire o AIDE para realizar verificaciones de integridad del sistema de archivos. Estas herramientas generan una base de datos de hash de los archivos críticos del sistema y luego verifican si estos hash han cambiado, lo que podría indicar una modificación no autorizada.

23. ¿Qué utilidades existen en Linux para hacer seguimiento de incidencias?

Utilidades en Linux para hacer seguimiento de incidencias:

- Syslog: El sistema de registro estándar en la mayoría de las distribuciones de Linux. Utiliza syslog para recopilar y registrar mensajes del sistema y de las aplicaciones en archivos de registro.

- Journalctl: Utilidad para consultar y analizar registros de eventos del sistema almacenados en el registro del diario de systemd. Permite filtrar, buscar y examinar registros con facilidad.

- Auditd: El servicio de auditoría del kernel en Linux que registra eventos de auditoría del sistema. Puedes configurar auditod para registrar eventos específicos relacionados con la seguridad del sistema y supervisar las actividades del usuario y del sistema.

- Fail2ban: Una aplicación de seguridad que protege tu sistema contra ataques de fuerza bruta al monitorizar los registros de servicios como SSH y firewall, y bloquear direcciones IP que realicen intentos de inicio de sesión fallidos repetidos.

24. ¿Cómo funcionan los antivirus identificadores y descontaminadores?

- Antivirus Identificadores: Funcionan mediante la comparación de archivos sospechosos con una base de datos de firmas conocidas de malware.

- Antivirus Descontaminadores: Trabajan para eliminar o desinfectar el malware detectado en un sistema.

25. ¿Qué es un firewall y cómo ayuda a la seguridad?

Un firewall es un sistema de seguridad que controla y filtra el tráfico de red basado en un conjunto de reglas definidas. Actúa como una barrera entre una red interna privada y redes externas no confiables, como Internet. Ayuda a la seguridad al bloquear o permitir el tráfico de red según las políticas de seguridad establecidas, protegiendo así la red y los sistemas contra amenazas externas e internas no autorizadas. Los firewalls pueden ser tanto hardware como software y pueden implementarse en diferentes niveles de la red, como en el nivel de host, de red o de aplicación.

26. ¿Qué es un antispyware y cuál es su objetivo?

Un antispyware es un tipo de software diseñado para detectar, prevenir y eliminar programas espía (spyware) de un sistema informático. El spyware es un tipo de software malicioso que recopila información sobre las actividades de un usuario sin su conocimiento o consentimiento. El objetivo del antispyware es proteger la privacidad del usuario y la seguridad del sistema detectando y eliminando el spyware del sistema.

27. ¿Qué es un antimalware y cómo se diferencia de un antivirus?

Un antimalware es un término más amplio que abarca cualquier tipo de software diseñado para detectar, prevenir y eliminar una variedad de amenazas informáticas maliciosas, incluyendo virus, gusanos, troyanos, spyware, adware, rootkits y otros tipos de software no deseado o malintencionado. Por otro lado, un antivirus es un tipo específico de antimalware que se centra principalmente en detectar, prevenir y eliminar virus informáticos. En resumen, mientras que el término "antivirus" se refiere específicamente a la protección contra virus, el término "anti malware" incluye una gama más amplia de amenazas informáticas.

28. ¿Cómo se puede configurar la política local del sistema operativo?

- Abrir el Editor de directivas de grupo

Navegar por las directivas.

- Configurar las políticas: Dentro de cada categoría, puedes encontrar políticas específicas que puedes configurar según tus necesidades.

Guardar los cambios.

29. ¿Qué es un antimalware y cómo se diferencia de un antivirus?

Un antimalware es un término más amplio que abarca cualquier tipo de software diseñado para detectar, prevenir y eliminar una variedad de amenazas informáticas maliciosas, incluyendo virus, gusanos, troyanos, spyware, adware, rootkits y otros tipos de software no deseado o malintencionado. Por otro lado, un antivirus es un tipo específico de antimalware que se centra principalmente en detectar, prevenir y eliminar virus informáticos. En resumen, mientras que el término "antivirus" se refiere específicamente a la protección contra virus, el término "anti malware" incluye una gama más amplia de amenazas informáticas.

30. ¿Cómo se puede configurar la política local del sistema operativo?

La configuración de la política local del sistema operativo puede variar dependiendo del sistema operativo específico que estés utilizando.

- Abrir el Editor de directivas de grupo local.
- Navegar por las directivas.
- Configurar las políticas.

Guardar los cambios.

31. ¿Qué recomendaciones hay para la configuración de servicios de sistema?

Algunas recomendaciones para la configuración de servicios del sistema son:

- Desactivar servicios innecesarios.
- Configurar correctamente los permisos.
- Aplicar actualizaciones de seguridad.
- Monitorizar los servicios.
- Limitar los puntos de acceso

.

32. ¿Cómo se puede restringir el software permitido en el sistema?

Para restringir el software permitido en un sistema, puedes seguir estas recomendaciones:

- Utilizar cuentas de usuario restringidas.
- Implementar políticas de ejecución de aplicaciones.
- Utilizar listas de control de acceso (ACL).
- Aplicar reglas de firewall.
- Monitorizar y auditar el software.