Las listas de verificación de refuerzo se basan en las listas de verificación integrales producidas por el Centro para la Seguridad de Internet (CIS). La  [Oficina de Seguridad de la Información](https://security.utexas.edu/) (ISO) ha resumido las listas del CIS hasta los pasos más críticos para sus sistemas, con un enfoque en cuestiones exclusivas del entorno informático de la Universidad de Texas en Austin.

Cómo utilizar la lista de verificación

Imprima la lista de verificación y marque cada elemento que complete para asegurarse de cubrir los pasos críticos para proteger su servidor. La ISO utiliza esta lista de verificación durante las evaluaciones de riesgos como parte del proceso para verificar la seguridad del servidor.

|  |  |
| --- | --- |
| información del servidor | |
| **Dirección MAC** |  |
| **Dirección IP** |  |
| **Nombre de la máquina** |  |
| **Etiqueta de propiedad** |  |
| **Nombre del administrador** |  |
| **Fecha** |  |

| Lista de Verificación  **Paso**  : el número de paso del procedimiento. Si hay una  **Nota UT** para este paso, el número de nota corresponde al número de paso. **Marcar**  (√): esto es para que los administradores marquen cuando completen esta parte. **Tareas pendientes**  : instrucciones básicas sobre qué hacer para proteger el sistema **CIS** respectivo  : número de referencia en el Centro de seguridad de Internet  [Windows Server 2016 Benchmark v1.0.0](https://utexas.box.com/v/CISBenchmarkWindowsServer2016) . El documento CIS describe con mucho más detalle cómo completar cada paso. **Nota de UT**  : la  **nota de UT** en la parte inferior de la página proporciona detalles adicionales sobre el paso para el entorno informático universitario. **Confidencial**  : para sistemas que incluyen  [datos confidenciales](https://security.utexas.edu/policies/data_classification.html) , los pasos requeridos se indican con  **!** símbolo. Se recomiendan todos los pasos. **Otros**  : para sistemas que incluyen  [datos controlados o publicados](https://security.utexas.edu/policies/data_classification.html) , se recomiendan todos los pasos y algunos son obligatorios (indicados por  **!** ). **Min Std**  : esta columna enlaza con el requisito específico para la universidad en el  documento [Estándares mínimos de seguridad para sistemas](https://security.utexas.edu/policies/standards_systems) . | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Paso** | **√** | **Hacer** | **CEI** | **Nota UT** | **Confidencial** | **Otro** | **Estándar mínimo** |
|  |  | **Preparación e instalación** |  |  |  |  |  |
| 1 |  | Si la máquina es una instalación nueva, protéjala del tráfico de red hostil hasta que el sistema operativo esté instalado y reforzado. |  | [§](https://security.utexas.edu/os-hardening-checklist/windows-2016#1) | ! |  | [4.5.1](https://security.utexas.edu/policies/standards_systems#section4.5.1) |
|  |  | **Paquetes de servicio y revisiones** |  |  |  |  |  |
| 2 |  | Instale los últimos service packs y revisiones de Microsoft. |  | [§](https://security.utexas.edu/os-hardening-checklist/windows-2016#2) | ! | ! | [4.5.2](https://security.utexas.edu/policies/standards_systems#section4.5.2) |
| 3 |  | Habilite la notificación automática de la disponibilidad del parche. |  | [§](https://security.utexas.edu/os-hardening-checklist/windows-2016#3) | ! | ! | [4.5. 3](https://security.utexas.edu/policies/standards_systems#section4.5.3) |
|  |  | **Políticas de cuentas de usuario** |  |  |  |  |  |
| 4 |  | Establezca la longitud mínima de la contraseña. | 1.1.4 | [§](https://security.utexas.edu/os-hardening-checklist/windows-2016#4) | ! | ! |  |
| 5 |  | Habilite los requisitos de complejidad de la contraseña. | 1.1.5 | [§](https://security.utexas.edu/os-hardening-checklist/windows-2016#5) | ! |  |  |
| 6 |  | No almacene contraseñas utilizando cifrado reversible. (Por defecto) | 1.1.6 | [§](https://security.utexas.edu/os-hardening-checklist/windows-2016#6) | ! | ! |  |
| 7 |  | Configurar la política de bloqueo de cuenta. | 1.2 | [§](https://security.utexas.edu/os-hardening-checklist/windows-2016#7) | ! | ! |  |
|  |  | **Asignación de derechos de usuario** |  |  |  |  |  |
| 8 |  | Restrinja la capacidad de acceder a esta computadora desde la red a administradores y usuarios autenticados. | 2.2.2 |  |  |  |  |
| 9 |  | No otorgue a ningún usuario el derecho de "actuar como parte del sistema operativo". (Por defecto) | 2.2.3 |  | ! | ! |  |
| 10 |  | Restrinja el acceso de inicio de sesión local a los administradores. | 2.2.6 | [§](https://security.utexas.edu/os-hardening-checklist/windows-2016#10) |  |  |  |
| 11 |  | Negar a las cuentas de invitados la posibilidad de iniciar sesión como un servicio, un trabajo por lotes, localmente o mediante RDP. | 2.2.18-21 |  | ! |  |  |
|  |  | **Configuraciones de seguridad** |  |  |  |  |  |
| 12 |  | Coloque el cartel de advertencia de la Universidad en el texto del mensaje para los usuarios que intenten iniciar sesión. | 2.3.7.4 | [§](https://security.utexas.edu/os-hardening-checklist/windows-2016#12) | ! | ! | [4.5.10](https://security.utexas.edu/policies/standards_systems#section4.5.10) |
| 13 |  | No permitir que los usuarios creen e inicien sesión con cuentas de Microsoft. | 2.3.1.2 | [§](https://security.utexas.edu/os-hardening-checklist/windows-2016#13) | ! | ! |  |
| 14 |  | Deshabilite la cuenta de invitado. (Por defecto) | 2.3.1.3 |  | ! | ! |  |
| 15 |  | Requiere Ctrl+Alt+Supr para inicios de sesión interactivos. (Por defecto) | 2.3.7.2 |  | ! | ! |  |
| dieciséis |  | Configure el límite de inactividad de la máquina para proteger las sesiones interactivas inactivas. | 2.3.7.3 |  | ! | ! |  |
| 17 |  | Configure Microsoft Network Client para firmar siempre digitalmente las comunicaciones. | 2.3.8.1 |  | ! |  |  |
| 18 |  | Configure Microsoft Network Client para firmar digitalmente las comunicaciones si el servidor está de acuerdo. (Por defecto) | 2.3.8.2 |  | ! | ! |  |
| 19 |  | Deshabilite el envío de contraseñas no cifradas a servidores SMB de terceros. | 2.3.8.3 |  | ! |  | [4.5.6](https://security.utexas.edu/policies/standards_systems#section4.5.6) |
| 20 |  | Configure Microsoft Network Server para firmar siempre digitalmente las comunicaciones. | 2.3.9.2 |  | ! |  |  |
| 21 |  | Configure Microsoft Network Server para firmar digitalmente las comunicaciones si el cliente está de acuerdo. | 2.3.9.3 |  | ! |  |  |
|  |  | **Controles de acceso a la red** |  |  |  |  |  |
| 22 |  | Deshabilite la traducción anónima de SID/nombre. (Por defecto) | 2.3.10.1 |  | ! | ! |  |
| 23 |  | No permita la enumeración anónima de cuentas SAM. (Por defecto) | 2.3.10.2 |  | ! | ! | [4.5.5](https://security.utexas.edu/policies/standards_systems#section4.5.5) |
| 24 |  | No permita la enumeración anónima de cuentas y acciones de SAM. | 2.3.10.3 |  | ! |  | [4.5.5](https://security.utexas.edu/policies/standards_systems#section4.5.5) |
| 25 |  | No permita que todos los permisos se apliquen a usuarios anónimos. (Por defecto) | 2.3.10.5 |  | ! | ! | [4.5.12](https://security.utexas.edu/policies/standards_systems#section4.5.12) |
| 26 |  | No permita el acceso anónimo a ninguna canalización con nombre. | 2.3.10.6 |  | ! |  | [4.5.12](https://security.utexas.edu/policies/standards_systems#section4.5.12) |
| 27 |  | Restrinja el acceso anónimo a canalizaciones y recursos compartidos con nombre. (Por defecto) | 2.3.10.9 |  | ! | ! | [4.5.12](https://security.utexas.edu/policies/standards_systems#section4.5.12) |
| 28 |  | No permita que se acceda a ninguna acción de forma anónima. | 2.3.10.11 |  | ! |  |  |
| 29 |  | Requerir el modelo de seguridad y uso compartido "clásico" para cuentas locales. (Por defecto) | 2.3.10.12 |  | ! | ! | [4.5.12](https://security.utexas.edu/policies/standards_systems#section4.5.12) |
|  |  | **Configuración de seguridad de red** |  |  |  |  |  |
| 30 |  | Permitir que el sistema local use la identidad de la computadora para NTLM. | 2.3.11.1 |  |  |  |  |
| 31 |  | Deshabilite el respaldo de sesión NULL del sistema local. | 2.3.11.2 |  |  |  |  |
| 32 |  | Configure los tipos de cifrado permitidos para Kerberos. | 2.3.11.4 |  |  |  |  |
| 33 |  | No almacene valores hash de LAN Manager. | 2.3.11.5 |  | ! | ! | [4.5.13](https://security.utexas.edu/policies/standards_systems#section4.5.13) |
| 34 |  | Configure el nivel de autenticación de LAN Manager para permitir solo NTLMv2 y rechazar LM y NTLM. | 2.3.11.7 |  | ! |  | [4.5.13](https://security.utexas.edu/policies/standards_systems#section4.5.13) |
| 35 |  | Habilite el Firewall de Windows en todos los perfiles (dominio, privado, público). (Por defecto) | 9.|LF||LF|1-3|RF||RF|.1 |  | ! | ! | [4.5.5](https://security.utexas.edu/policies/standards_systems#section4.5.5) |
| 36 |  | Configure el Firewall de Windows en todos los perfiles para bloquear el tráfico entrante de forma predeterminada. (Por defecto) | 9.|LF||LF|1-3|RF||RF|.2 |  | ! | ! |  |
| 37 |  | Configure el Firewall de Windows para restringir los servicios de acceso remoto (VNC, RDP, etc.) a redes autorizadas únicamente para el campus. |  |  |  | ! | [4.6.4](https://security.utexas.edu/policies/irusp#standard4.6.4) |
| 38 |  | Configure el Firewall de Windows para restringir los servicios de acceso remoto (VNC, RDP, etc.) a la VPN del campus. |  |  | ! |  | [4.6.3](https://security.utexas.edu/policies/irusp#standard4.6.3) |
|  |  | **Configuración de seguridad de los miembros del dominio de Active Directory** |  |  |  |  |  |
| 39 |  | Cifre o firme digitalmente datos de canales seguros (siempre). (Por defecto) | 2.3.6.1 |  | ! |  | [4.5.6](https://security.utexas.edu/policies/standards_systems#section4.5.6) |
| 40 |  | Cifre digitalmente los datos del canal seguro (cuando sea posible). (Por defecto) | 2.3.6.2 |  | ! | ! | [4.5.6](https://security.utexas.edu/policies/standards_systems#section4.5.6) |
| 41 |  | Firmar digitalmente datos de canales seguros (cuando sea posible). (Por defecto) | 2.3.6.3 |  | ! | ! | [4.5.6](https://security.utexas.edu/policies/standards_systems#section4.5.6) |
| 42 |  | Requiere claves de sesión seguras (Windows 2000 o posterior). | 2.3.6.6 |  | ! |  |  |
| 43 |  | Configure el número de inicios de sesión anteriores para almacenar en caché. | 2.3.7.6 | [§](https://security.utexas.edu/os-hardening-checklist/windows-2016#43) |  |  |  |
|  |  | **Configuración de la política de auditoría** |  |  |  |  |  |
| 44 |  | Configure la política de auditoría de inicio de sesión de la cuenta. | 17.1 | [§](https://security.utexas.edu/os-hardening-checklist/windows-2016#44) | ! |  |  |
| 45 |  | Configure la política de auditoría de Gestión de cuentas. | 17.2 | [§](https://security.utexas.edu/os-hardening-checklist/windows-2016#45) | ! | ! |  |
| 46 |  | Configure la política de auditoría de inicio y cierre de sesión. | 17,5 | [§](https://security.utexas.edu/os-hardening-checklist/windows-2016#46) | ! | ! |  |
| 47 |  | Configure la política de auditoría de cambio de política. | 17.7 | [§](https://security.utexas.edu/os-hardening-checklist/windows-2016#47) | ! | ! |  |
| 48 |  | Configure la política de auditoría de uso de privilegios. | 17.8 | [§](https://security.utexas.edu/os-hardening-checklist/windows-2016#48) | ! |  |  |
|  |  | **Configuración del registro de eventos** |  |  |  |  |  |
| 49 |  | Configure el método y el tamaño de retención del registro de eventos. | 18.3.12; 18.9.26 | [§](https://security.utexas.edu/os-hardening-checklist/windows-2016#49) | ! | ! | [4.6.1](https://security.utexas.edu/policies/standards_systems#section4.6.1) |
| 50 |  | Configure el envío de registros (por ejemplo, a [Splunk](https://ut.service-now.com/utss/catalogoverview.do?sysparam_citems_id=2bc53c004f8f924031eb7bcd0210c772) ). |  | [§](https://security.utexas.edu/os-hardening-checklist/windows-2016#50) |  |  |  |
|  |  | **Subsistema Linux** |  |  |  |  |  |
| 51 |  | Configure todos los elementos de Linux de acuerdo con la [Guía de refuerzo de Linux](https://security.utexas.edu/os-hardening-checklist/linux-7) , teniendo en cuenta que algunos elementos requerirán herramientas de Windows (como Windows Firewall frente a iptables). |  |  |  |  |  |
|  |  | **Protección de seguridad adicional** |  |  |  |  |  |
| 52 |  | Deshabilite o desinstale los servicios no utilizados. |  |  | ! |  |  |
| 53 |  | Deshabilite o elimine usuarios no utilizados. |  |  | ! |  |  |
| 54 |  | Configure los derechos de usuario para que sean lo más seguros posible: siga el [principio de privilegio mínimo](https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models) |  | [§](https://security.utexas.edu/os-hardening-checklist/windows-2016#53) | ! |  |  |
| 55 |  | Asegúrese de que todos los volúmenes utilicen el sistema de archivos NTFS. |  | [§](https://security.utexas.edu/os-hardening-checklist/windows-2016#55) | ! |  |  |
| 56 |  | Configure los permisos del sistema de archivos. |  | [§](https://security.utexas.edu/os-hardening-checklist/windows-2016#56) | ! |  |  |
| 57 |  | Configurar permisos de registro. |  | [§](https://security.utexas.edu/os-hardening-checklist/windows-2016#57) | ! |  |  |
| 58 |  | No permita el acceso remoto al registro si no es necesario. | 2.3.10.7-8 | [§](https://security.utexas.edu/os-hardening-checklist/windows-2016#58) |  |  |  |
|  |  | **Pasos adicionales** |  |  |  |  |  |
| 59 |  | Establezca la fecha/hora del sistema y configúrelo para sincronizarlo con los servidores de hora del campus. |  | [§](https://security.utexas.edu/os-hardening-checklist/windows-2016#59) | ! |  |  |
| 60 |  | Instale y habilite el software antivirus. |  | [§](https://security.utexas.edu/os-hardening-checklist/windows-2016#60) | ! | ! |  |
| 61 |  | Instale y habilite el software antispyware. |  | [§](https://security.utexas.edu/os-hardening-checklist/windows-2016#61) | ! |  |  |
| 62 |  | Configure el software antivirus para que se actualice diariamente. |  | [§](https://security.utexas.edu/os-hardening-checklist/windows-2016#62) | ! | ! |  |
| 63 |  | Configure el software antispyware para que se actualice diariamente. |  | [§](https://security.utexas.edu/os-hardening-checklist/windows-2016#63) | ! |  |  |
| 64 |  | Proporcionar almacenamiento seguro para datos confidenciales (categoría I) según sea necesario. La seguridad se puede proporcionar mediante medios tales como, entre otros, cifrado, controles de acceso, auditorías del sistema de archivos, protección física de los medios de almacenamiento o cualquier combinación de los mismos que se considere apropiada. |  | [§](https://security.utexas.edu/os-hardening-checklist/windows-2016#64) | ! |  |  |
| sesenta y cinco |  | Instale software para verificar la integridad de los archivos críticos del sistema operativo. |  | [§](https://security.utexas.edu/os-hardening-checklist/windows-2016#65) | ! |  |  |
| 66 |  | Si se utiliza RDP, establezca el nivel de cifrado de la conexión RDP en alto. |  | [§](https://security.utexas.edu/os-hardening-checklist/windows-2016#66) | ! |  |  |
|  |  | **Seguridad física** |  |  |  |  |  |
| 67 |  | A menos que el servidor esté en el UDC o en un clúster de VM administrado, establezca una contraseña de BIOS/firmware para evitar alteraciones en la configuración de inicio del sistema. |  |  |  |  | [4.4.1](https://security.utexas.edu/policies/standards_systems#section4.4.1) |
| 68 |  | No permita que el sistema se apague sin tener que iniciar sesión. (Por defecto) | 2.3.13.1 |  | ! | ! |  |
| 69 |  | Configure el orden de inicio del dispositivo para evitar el inicio no autorizado desde medios alternativos. |  |  | ! |  | [4.4.1](https://security.utexas.edu/policies/standards_systems#section4.4.1) |
| 70 |  | Configure un protector de pantalla para bloquear la pantalla de la consola automáticamente si el host se queda desatendido. |  | [§](https://security.utexas.edu/os-hardening-checklist/windows-2016#70) | ! | ! |  |

|  |  |
| --- | --- |
| Anexo de UT Esta lista proporciona tareas específicas relacionadas con el entorno informático de la Universidad de Texas en Austin. | |
| **1** | Si no hay otras alternativas disponibles, esto se puede lograr instalando un enrutador/firewall SOHO entre la red y el host a proteger. |
| **2** | Hay varios métodos disponibles para ayudarle a aplicar los parches de manera oportuna:  **Servicio de actualización de Microsoft**   * [Microsoft Update](http://www.update.microsoft.com/) verifica su máquina para identificar los parches faltantes y le permite descargarlos e instalarlos. * Esto es diferente a la "Actualización de Windows", que es la opción predeterminada en Windows. Microsoft Update incluye actualizaciones para muchos más productos de Microsoft, como Office y Forefront Client Security. * Este servicio es compatible únicamente con Internet Explorer.   **Windows AutoUpdate a través de WSUS** ITS ofrece un  [servidor de servicios de actualización de Windows Server para uso en el campus](https://ut.service-now.com/utss/catalogoverview.do?sysparam_citems_id=e546bc004f8f924031eb7bcd0210c7b5&sysparam_cat_id=e0d08b13c3330100c8b837659bba8fb4%2CInformation%20Technology&sysparam_sys_id=%3Csubcategory.parent%3E%2CTechnology%20Infrastructure%20&%20Management&sys_click_name=features) utilizando los propios servidores de actualización de Microsoft. Incluye actualizaciones para productos adicionales de Microsoft, al igual que Microsoft Update, y proporciona control administrativo adicional para la implementación de software.  **Microsoft Baseline Security Analyzer** Esta es una aplicación gratuita basada en host que está  [disponible para descargar desde Microsoft](http://technet.microsoft.com/en-us/security/cc184923.aspx) . Además de detallar los parches faltantes, esta herramienta también realiza comprobaciones de la configuración de seguridad básica y proporciona información sobre cómo solucionar cualquier problema encontrado.  **Upguard** Esta es una herramienta de gestión de cumplimiento que garantiza que los parches básicos y el cumplimiento se gestionen de manera consistente (este producto es bastante económico y se puede integrar con [Splunk](https://ut.service-now.com/utss/catalogoverview.do?sysparam_citems_id=2bc53c004f8f924031eb7bcd0210c772) ). |
| **3** | Configurar Actualizaciones Automáticas desde el panel de control de Actualizaciones Automáticas   * En la mayoría de los servidores, debes elegir "Descargar actualizaciones por mí, pero déjame elegir cuándo instalarlas" o "Notificarme pero no descargarlas ni instalarlas automáticamente". * El  [servidor de Windows Server Update Services](https://ut.service-now.com/utss/catalogoverview.do?sysparam_citems_id=e546bc004f8f924031eb7bcd0210c7b5&sysparam_cat_id=e0d08b13c3330100c8b837659bba8fb4%2CInformation%20Technology&sysparam_sys_id=%3Csubcategory.parent%3E%2CTechnology%20Infrastructure%20&%20Management&sys_click_name=features) del campus se puede utilizar como fuente de actualizaciones automáticas. |
| **4** | Configurar la longitud mínima de la contraseña es importante solo si  no existe otro método para garantizar el cumplimiento de [los estándares de contraseñas de la universidad  .](https://security.utexas.edu/policies/irusp#standard16)La Política de seguridad y uso de recursos de información requiere que las contraseñas tengan una longitud mínima de 8 caracteres. Se  recomienda **encarecidamente**  que las contraseñas tengan al menos 14 caracteres (que también es la recomendación del CIS). |
| **5** | Configurar la configuración de complejidad de la contraseña es importante solo si  no existe otro método para garantizar el cumplimiento de [los estándares de contraseñas de la universidad  .](https://security.utexas.edu/policies/irusp#standard16)La Política de seguridad y uso de recursos de información requiere que las contraseñas contengan letras, números y caracteres especiales. Asegúrese de que los administradores de dominio (e incluso las cuentas de administrador departamental/GPO utilizadas por los TSC) tengan un estándar más alto para la complejidad de las contraseñas, deban cambiar sus contraseñas con más frecuencia (por ejemplo, dos veces al año) y se les advierta enfáticamente contra la reutilización de estas credenciales fuera del Contexto de Austin AD. |
| **6** | Si esta opción está habilitada, el sistema almacenará las contraseñas utilizando una forma débil de cifrado que es susceptible de verse comprometida. Esta configuración está deshabilitada de forma predeterminada.  Para obtener más protecciones con contraseña: 1. Actualice el nivel funcional de Active Directory a 2012 R2 o superior. 2. En la clave de Registro HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\SecurityProviders\WDigest, establezca “UseLogonCredential” en 0. 3. Implemente las KB de MS [2928120](https://support.microsoft.com/en-us/help/2928120/ms14-025-description-of-the-security-update-for-group-policy-preferenc) y [2871997](https://docs.microsoft.com/en-us/security-updates/SecurityAdvisories/2016/2871997) . |
| **7** | En lugar de los valores recomendados por CIS, la política de bloqueo de cuenta debe configurarse de la siguiente manera:   * Duración del bloqueo de cuenta: 5 minutos * Umbral de bloqueo de cuenta: 5 intentos fallidos * Restablecer el contador de bloqueo de cuenta: 5 minutos |
| **10** | Cualquier cuenta con esta función puede iniciar sesión en la consola. De forma predeterminada, esto incluye a los usuarios de los grupos Administradores, Usuarios y Operadores de respaldo. Es poco probable que los usuarios no administrativos requieran este nivel de acceso y, en los casos en que el servidor no esté físicamente protegido, otorgar este derecho puede facilitar que el dispositivo se vea comprometido. |
| **12** | El texto del  [cartel de advertencia oficial de la universidad](https://security.utexas.edu/policies/login_banner.html) se puede encontrar en el sitio web de ISO. Puede agregar información localizada al banner siempre que se incluya el banner de la universidad. |
| **13** | El uso de cuentas de Microsoft se puede bloquear configurando el objeto de política de grupo en:  **Configuración del equipo\Configuración de Windows\Configuración de seguridad\Políticas locales\**  **Opciones de seguridad\Cuentas: bloquear cuentas de Microsoft**  Esta configuración se puede verificar auditando la clave de registro:  **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\NoConnectedUser** |
| **43** | La información de inicio de sesión para cuentas de dominio se puede almacenar en caché localmente para permitir que los usuarios que se han autenticado previamente lo hagan nuevamente incluso si no se puede contactar a un controlador de dominio. De forma predeterminada, se almacenarán en caché 10 cuentas localmente, pero existe el riesgo de que, en caso de compromiso, un atacante pueda localizar las credenciales almacenadas en caché y utilizar un ataque de fuerza bruta para descubrir las contraseñas. Por lo tanto, se recomienda reducir este valor para que se pongan en riesgo menos credenciales y las credenciales se almacenen en caché durante períodos de tiempo más cortos en el caso de dispositivos en los que varios usuarios inician sesión con frecuencia.  El siguiente objeto de política de grupo debe configurarse en 4 o menos inicios de sesión:  **Configuración del equipo\Configuración de Windows\Configuración de seguridad\Políticas locales\Opciones de seguridad\Inicio de sesión interactivo: número de inicios de sesión anteriores en caché (en caso de que el controlador de dominio no esté disponible)** |
| **44** | La política de auditoría de inicio de sesión de cuenta registra los resultados de las pruebas de validación de las credenciales enviadas para las solicitudes de inicio de sesión de cuentas de usuario. El servidor autorizado para las credenciales debe tener habilitada esta política de auditoría. Para las máquinas miembros del dominio, esta política solo registrará eventos para cuentas de usuarios locales.  Configure el objeto de política de grupo a continuación para que coincida con la configuración de auditoría enumerada:  **Configuración del equipo\Configuración de Windows\Configuración de seguridad\**  **Configuración avanzada de políticas de auditoría\Políticas de auditoría\Inicio de sesión de cuenta\**   * Validación de credenciales: éxito y fracaso |
| **45** | Configure el objeto de política de grupo a continuación para que coincida con la configuración de auditoría enumerada:  **Configuración del equipo\Configuración de Windows\Configuración de seguridad\**  **Configuración avanzada de políticas de auditoría\Políticas de auditoría\Administración de cuentas\**   * Gestión de cuentas informáticas: éxito y fracaso * Otros eventos de gestión de cuentas: éxitos y fracasos * Gestión de grupos de seguridad: éxito y fracaso * Gestión de cuentas de usuario: éxito y fracaso |
| **46** | Configure el objeto de política de grupo a continuación para que coincida con la configuración de auditoría enumerada:  **Configuración del equipo\Configuración de Windows\Configuración de seguridad\**  **Configuración avanzada de políticas de auditoría\Políticas de auditoría\Inicio de sesión/cierre de sesión\**   * Bloqueo de cuenta: éxito * Cerrar sesión: Éxito * Inicio de sesión: éxito y fracaso * Otros eventos de inicio y cierre de sesión: éxito y fracaso * Inicio de sesión especial: éxito |
| **47** | Configure el objeto de política de grupo a continuación para que coincida con la configuración de auditoría enumerada:  **Configuración del equipo\Configuración de Windows\Configuración de seguridad\**  **Configuración avanzada de políticas de auditoría\Políticas de auditoría\Cambio de políticas\**   * Cambio de política de auditoría: éxito y fracaso * Cambio de política de autenticación: éxito |
| **48** | Configure el objeto de política de grupo a continuación para que coincida con la configuración de auditoría enumerada:  Configuración del equipo\Configuración de Windows\Configuración de seguridad\  Configuración avanzada de políticas de auditoría\Políticas de auditoría\Uso de privilegios\   * Uso sensible de privilegios: éxito y fracaso |
| **49** | La universidad requiere las siguientes configuraciones de registro de eventos en lugar de las recomendadas por CIS Benchmark:   * Aplicación: Tamaño máximo de registro:  **163 840 KB** * Seguridad: tamaño máximo de registro : **983 040 KB** * Configuración: tamaño máximo de registro: **163.840 KB** * Sistema: Tamaño máximo de registro:  **163.840 KB**   El método de retención recomendado para todos los registros es:  **Retener eventos durante al menos 14 días**  Estos son requisitos mínimos. El registro más importante aquí es el registro de seguridad. 1 GB es el mínimo sugerido, pero si tiene un servicio de gran volumen, haga que el archivo sea tan grande como sea necesario para asegurarse de que haya **al menos 14 días** de registros de seguridad disponibles. Cuanto más retrocedan sus registros, más fácil será responder en caso de una infracción. En casos excepcionales, una infracción puede durar meses antes de ser detectada. Puede aumentar la cantidad de días que conserva o puede configurar los archivos de registro para que no sobrescriban los eventos.  Tenga en cuenta que si el registro de eventos alcanza su tamaño máximo y no existen eventos anteriores a la cantidad de días que especificó para eliminar, o si ha deshabilitado la sobrescritura de eventos, no se registrarán nuevos eventos. Esto puede ocurrir deliberadamente como un intento de un atacante de cubrir sus huellas. Para servicios críticos que trabajan con datos confidenciales u otros datos confidenciales, utilice Syslog, [Splunk](https://ut.service-now.com/utss/catalogoverview.do?sysparam_citems_id=2bc53c004f8f924031eb7bcd0210c772) ,  Intrust o un servicio similar para enviar registros a otro dispositivo. Otra opción es configurar Windows para rotar los archivos de registro de eventos automáticamente cuando un registro de eventos alcanza su tamaño máximo como se describe en el artículo  [http://support.microsoft.com/kb/312571](https://ut.service-now.com/utss/catalogoverview.do?sysparam_citems_id=2bc53c004f8f924031eb7bcd0210c772)  usando la entrada de registro AutoBackupLogFiles. |
| **50** | Se recomienda encarecidamente que los registros se envíen desde cualquier dispositivo confidencial a un servicio como [Splunk](https://ut.service-now.com/utss/catalogoverview.do?sysparam_citems_id=2bc53c004f8f924031eb7bcd0210c772) , que proporciona agregación de registros, procesamiento y monitoreo de eventos en tiempo real, entre muchas otras cosas. Esto ayuda a garantizar que los registros se conserven y no se modifiquen en caso de un compromiso, además de permitir el análisis de registros proactivo de múltiples dispositivos.  Las licencias de Splunk están disponibles a través de ITS sin costo alguno. ITS también mantiene un servicio Splunk administrado centralmente que puede aprovecharse. Si utiliza Splunk: asegúrese de que todos los sistemas y servicios clave se registren en Splunk y que la detalle esté configurada adecuadamente. Asegúrese de que las alertas de Splunk estén implementadas para (1) la creación de GPO de nivel raíz, (2) la actividad de la cuenta del administrador de dominio que ocurre fuera de las estaciones de trabajo PAWS, (3) el GPO creado por los administradores de dominio. |
| **54** | Configure los derechos de usuario para que sean lo más seguros posible, siguiendo las recomendaciones de la sección 2.2 del benchmark CIS. Se debe hacer todo lo posible para eliminar Invitado, Todos e INICIAR SESIÓN ANÓNIMA de las listas de derechos de usuario. Siga las mejores prácticas actuales para garantizar que IIS no se ejecute como usuario del sistema. Asegúrese de que las tareas programadas se ejecuten con una cuenta de servicio dedicada y no con una cuenta de administrador de dominio. Para los sistemas que presentan el mayor riesgo, complete [la implementación de PAWS](https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/privileged-access-workstations) y asegúrese de que los registros del sistema se envíen a [Splunk](https://ut.service-now.com/utss/catalogoverview.do?sysparam_citems_id=2bc53c004f8f924031eb7bcd0210c772) . |
| **55** | Los volúmenes formateados como FAT o FAT32 se pueden convertir a NTFS utilizando la utilidad convert.exe proporcionada por Microsoft. Microsoft ha proporcionado  [instrucciones sobre cómo realizar la conversión.](http://support.microsoft.com/kb/314097)Los servidores Windows utilizados con datos de Categoría I deben utilizar el sistema de archivos NTFS para todas las particiones donde se almacenarán datos de Categoría I. |
| **56** | **Tenga mucho cuidado, ya que establecer permisos incorrectos en archivos y carpetas del sistema puede inutilizar el sistema.** |
| **57** | **Tenga mucho cuidado, ya que establecer permisos incorrectos en las entradas del registro puede inutilizar el sistema.** |
| **58** | Algunas herramientas de administración remota, como Microsoft Systems Management Server, requieren acceso remoto al registro de los dispositivos administrados. Deshabilitar el acceso al registro remoto puede provocar que dichos servicios fallen. Si no se requiere acceso al registro remoto, se recomienda detener y deshabilitar el servicio de registro remoto.  Si se requiere acceso remoto al registro, las rutas de acceso remotas al registro aún deben configurarse para que sean lo más restrictivas posible. El siguiente objeto de política de grupo controla qué rutas de registro están disponibles de forma remota:  **Configuración del equipo\Configuración de Windows\Configuración de seguridad\Políticas locales\**  **Opciones de seguridad\Acceso a la red: rutas de registro accesibles de forma remota**  Este objeto debe configurarse para permitir el acceso únicamente a:   * Sistema\CurrentControlSet\Control\ProductOptions * Sistema\CurrentControlSet\Control\Aplicaciones de servidor * Software\Microsoft\Windows NT\Versión actual   Se pueden configurar restricciones adicionales sobre las rutas y subrutas del registro a las que se puede acceder de forma remota con el objeto de política de grupo:  **Configuración del equipo\Configuración de Windows\Configuración de seguridad\Políticas locales\**  **Opciones de seguridad\Acceso a la red: rutas de registro y subrutas accesibles de forma remota** |
| **59** | De forma predeterminada, los miembros del dominio sincronizan su hora con los controladores de dominio mediante  [el servicio de hora de Windows](https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/windows-time-service/windows-time-service) de Microsoft . El controlador de dominio debe configurarse para sincronizar su hora con una fuente de hora externa, como los servidores de hora de la red de la universidad. |
| **60** | ITS proporciona FireAMP, un servicio antivirus administrado basado en la nube, de forma gratuita para todos los dispositivos de propiedad de la universidad. Más información sobre cómo obtener y usar FireAMP se encuentra en  <https://security.utexas.edu/education-outreach/anti-virus> . |
| **61** | Sólo es necesario instalar software antispyware si el servidor se utiliza para explorar sitios web no relacionados específicamente con la administración del servidor,  *lo cual no se recomienda* . ITS proporciona software antispyware sin cargo adicional. Como mínimo, se debe instalar SpyBot Search and Destroy. También recomendamos la instalación de una aplicación antispyware secundaria, como SpyWare Blaster, EMS Free Surfer o AdAware.  Una medida adicional que se puede tomar es instalar  [Firefox](http://www.mozilla.com/en-US/firefox/personal.html)  con los   complementos [NoScript](https://addons.mozilla.org/en-US/firefox/addon/722/)  y  [uBlock .](https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/) |
| **62** | FireAMP es la solución AV recomendada. |
| **63** | **Spyware Blaster**  : habilitar la función de actualización automática requiere la compra de una suscripción adicional.  **SpyBot Search and Destroy**  : las tareas de actualización automática se pueden crear dentro del propio programa y se programan mediante el Programador de tareas de Windows.   1. En la aplicación Spybot, haga clic en Modo --> Vista avanzada. 2. Haga clic en Configuración en el lado izquierdo de la ventana. 3. Ahora debería ver una opción denominada "Programador". Seleccione esa opción. 4. Agregar la tarea para actualizar automáticamente es relativamente sencillo.    * Haga clic en  **Agregar**  para crear una tarea.    * Haga clic en  **Editar**  para editar el programa de tareas.    * En la ventana Tarea programada que aparece, ingrese lo siguiente en el   campo **Ejecutar :**      + **C:\Archivos de programa\Spybot - Buscar y destruir\SpybotSD.exe" /AUTOUPDATE /TASKBARHIDE /AUTOCLOSE**    * Haga clic en la  pestaña **Programar**  y elija una hora para que se actualice. La duración de la actualización es muy breve, pero requiere un uso intensivo del procesador, así que considere programarla para que se realice durante períodos de bajo uso. La tarea debe programarse diariamente. |
| **64** | Windows proporciona el sistema de cifrado de archivos como mecanismo integrado para permitir el cifrado de archivos y carpetas de usuarios individuales. Sin embargo, tenga en cuenta las advertencias que implica el uso de EFS antes de implementarlo para uso general. También existen otras opciones como  [PGP](http://www.pgp.com/)  y  [GNUPG](http://www.gnupg.org/)  .  Otra opción de cifrado a considerar es el cifrado de todo el disco, que cifra todo el contenido de la unidad en lugar de solo archivos y carpetas específicos. Windows viene con BitLocker para esto.  Si se utiliza el cifrado junto con datos confidenciales,   se debe implementar una de las soluciones enumeradas en los [Métodos de cifrado aprobados (se requiere EID).](https://security.utexas.edu/iso-policies/approved-encryption-methods) |
| **sesenta y cinco** | Windows tiene una función llamada Protección de recursos de Windows que verifica automáticamente ciertos archivos clave y los reemplaza si se dañan. Está habilitado de forma predeterminada.  Puede realizar una auditoría mucho más profunda utilizando Tripwire; considere esto para sus sistemas de mayor riesgo. Las versiones modernas de Tripwire requieren la compra de licencias para poder utilizarlas. La consola de gestión de Tripwire puede resultar de gran ayuda para gestionar instalaciones más complejas. |
| **66** | Esta configuración se configura por objeto de política de grupo en:  **\Configuración del equipo\Plantillas administrativas\Componentes de Windows\Servicios de Escritorio remoto\Host de sesión de Escritorio remoto\Seguridad**  Este objeto de política debe configurarse de la siguiente manera:   * Establecer el nivel de cifrado de la conexión del cliente: Alto * Requerir el uso de una capa de seguridad específica para conexiones remotas (RDP): SSL (TLS 1.0) * Requerir autenticación de usuario para conexiones remotas mediante la autenticación a nivel de red: habilitada |
| **70** | 1. Abra el panel de control Propiedades de pantalla. 2. Seleccione la pestaña Protector de pantalla. 3. Seleccione un protector de pantalla de la lista. Aunque hay varios disponibles, considere usar uno simple como "En blanco". 4. El valor de  **Esperar**  no debe ser superior a 15 minutos. 5. Seleccione la  opción **Al reanudar, proteger con contraseña**  . |