**Administracion Sistemas y Redes**

|  |
| --- |
| **Enlaces** |
| * [**https://learn.microsoft.com/es-es/training/paths/windows-server-deploymentconfiguration-administration/**](https://learn.microsoft.com/es-es/training/paths/windows-server-deployment-configuration-administration/) * [**https://access.redhat.com/documentation/eses/red\_hat\_enterprise\_linux/8/pdf/ configuring\_basic\_system\_settings/red\_hat\_enterprise\_linux-8configuring\_basic\_system\_settings-es-es.pdf**](https://access.redhat.com/documentation/eses/red_hat_enterprise_linux/8/pdf/configuring_basic_system_settings/red_hat_enterprise_linux-8-configuring_basic_system_settings-es-es.pdf) * [**https://www.redbooks.ibm.com/redbooks/pdfs/gg243376.pdf**](https://www.redbooks.ibm.com/redbooks/pdfs/gg243376.pdf) (Cap. 1, 3, 4, 5, 12, 17, 22 y 24) |
| **Videos** |
| Video 1  Video 2  Video 3 |
| **Apuntes** |
| Definición de la administración con privilegios mínimos.  Implementación de los privilegios delegados.  Conclusiones |

# Definición de la administración con privilegios mínimos.

200 XP

* 5 minutos.

Una empresa de especialistas en seguridad de TI ha estado trabajando en Contoso. Acaban de generar un informe para el panel principal. El informe indica que la mayoría de las infracciones de seguridad o los incidentes de pérdida de datos de Contoso en el pasado fueron el resultado de un error humano, actividades malintencionadas o ambas cosas.

El informe proporcionó varios ejemplos, incluido el inicio de sesión con privilegios administrativos y la realización de tareas de usuario estándar. En un ejemplo que ya se ha mencionado, un usuario que inició sesión con derechos de los administradores de empresa y abrió un archivo adjunto de correo electrónico que ejecutó un código malintencionado. Dicho código tiene derechos administrativos completos en la empresa Contoso porque el usuario que lo ejecutó tenía derechos administrativos completos.

## Información general.

El privilegio mínimo es el concepto de restringir los derechos de acceso únicamente a los derechos necesarios para realizar una tarea o un rol de trabajo específico. Puede aplicar este principio a:

* Las cuentas de usuario.
* Las cuentas de servicio.
* Los procesos informáticos.

Aunque este principio es fácil de entender, puede ser complejo de implementar. Como resultado, en muchos casos, no se adhiere a los privilegios mínimos.

El principio indica que todos los usuarios deben iniciar sesión con una cuenta de usuario que tenga los permisos mínimos necesarios para completar la tarea actual y nada más. Este principio proporciona protección contra código malintencionado, entre otros ataques. Se aplica a los equipos y a los usuarios de esos equipos.

Por supuesto, el problema es que los administradores no quieren iniciar sesión con una cuenta de usuario estándar para sus tareas cotidianas y, a continuación, cerrar la sesión y volver a iniciarla como administrador cuando necesiten restablecer la contraseña de un usuario. Es una tarea que consume mucho tiempo y es un problema. Para solucionar este problema, debe encontrar una forma de identificar los riesgos de seguridad típicos. A continuación, debe planear un principio menos intrusivo de los privilegios mínimos.

## Identificación de las entidades de seguridad.

En un entorno local, debe determinar qué entidades de seguridad (usuarios y grupos) pertenecen a los grupos administrativos. En Active Directory Domain Services (AD DS), hay una serie de grupos administrativos confidenciales. Estos se describen en la siguiente tabla.

Expandir tabla

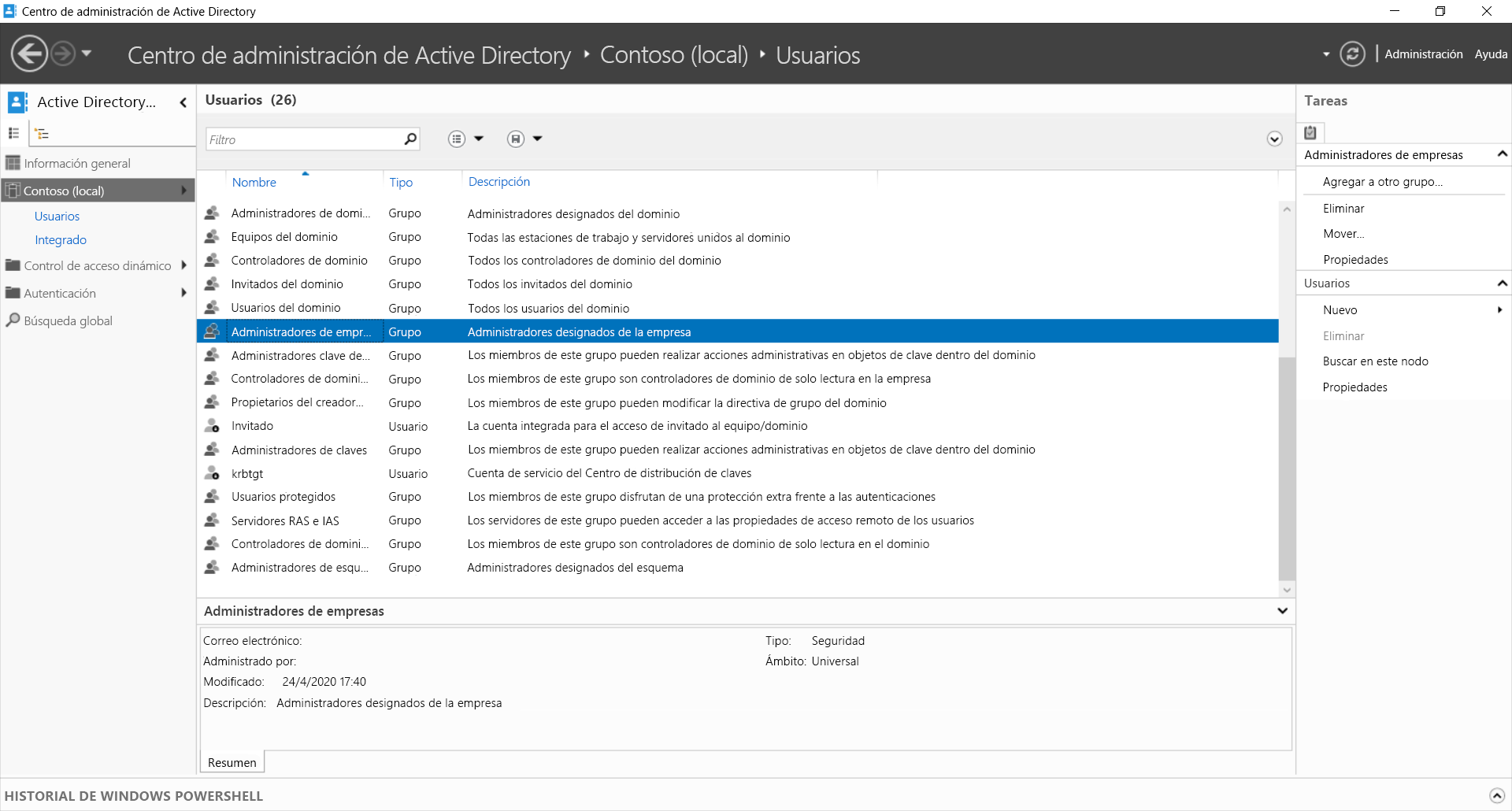
| **Grupo** | **Descripción** |
| --- | --- |
| Administradores de empresas | Este grupo de seguridad Universal reside en la carpeta Usuarios del dominio raíz del bosque de AD DS. Los miembros pueden realizar cualquier tarea administrativa en cualquier parte del bosque. Hay algunas tareas de administración que requieren la pertenencia a administradores de empresa. De forma predeterminada, solo la cuenta del usuario administrador del dominio raíz del bosque pertenece a los administradores de empresa. |
| Administradores de dominio | Este grupo de seguridad global reside en la carpeta Usuarios de cada dominio del bosque de AD DS. Los miembros pueden realizar cualquier tarea administrativa en cualquier parte del bosque. De forma predeterminada, solo la cuenta de usuario administrador del dominio local pertenece a los administradores del dominio. |
| Administradores de esquema | Este grupo de seguridad universal reside en la carpeta Usuarios del dominio raíz del bosque. Los miembros pueden modificar las propiedades del esquema de AD DS. Los cambios de esquema son poco frecuentes, pero muy significativos en su efecto. De forma predeterminada, solo la cuenta del usuario administrador del dominio raíz del bosque pertenece a los administradores del esquema. |
| Administradores | Este grupo de seguridad local de dominio reside en la carpeta Integración de AD DS. El grupo local de administradores también existe en todos los equipos del bosque de AD DS. Los administradores tienen acceso completo y sin restricciones al equipo o dominio. Normalmente, los grupos de administradores de empresas y del dominio se agregan a los grupos de administradores de todos los equipos del bosque. |

**Nota.**

El esquema de AD DS es una colección de objetos y sus propiedades, que a veces también se denomina clases y atributos.

Otros grupos integrados que tienen privilegios de seguridad incluyen:

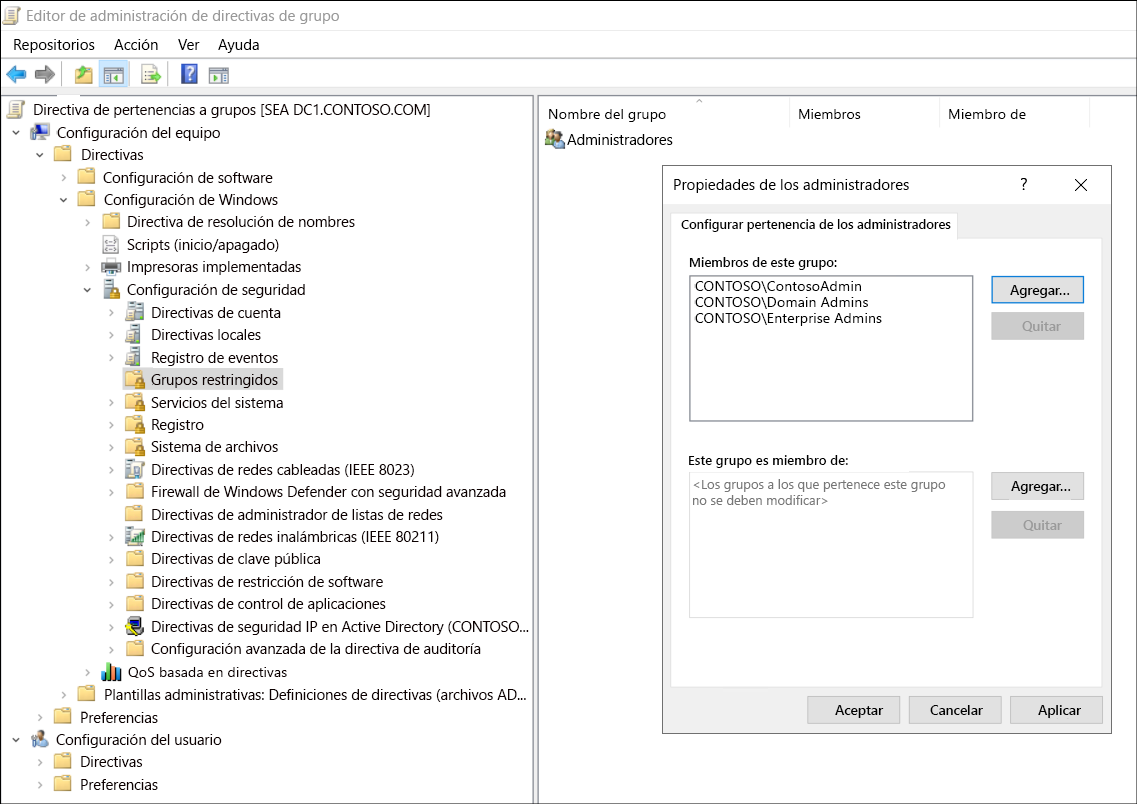
* Operadores de cuentas.
* Operadores de servidores.
* Administradores de claves.
* Administradores claves de empresa.



## Modificación de pertenencias a grupos.

Una vez determinados los usuarios y grupos que pertenecen a los grupos administrativos, puede realizar los cambios necesarios. Puede usar los Objetos de directiva de grupo (GPO) en un entorno de AD DS para acelerar este proceso. Use la característica **Grupos restringidos** para controlar la pertenencia a grupos en todos los equipos que afecten los Objetos de directiva de grupo. Utilice el siguiente procedimiento:

1. Abra **Administración de la directiva de grupo** y, a continuación, cree y vincule un GPO al objeto de dominio.
2. Abra el GPO para su edición.
3. Busque la **Configuración del equipo**, las **Directivas**, la **Configuración de Windows**, la **Configuración de seguridad** y los **Grupos restringidos**.
4. Haga clic con el botón derecho o active el menú contextual de los **Grupos restringidos** y seleccione **Agregar grupo**.
5. En el cuadro de diálogo **Agregar grupo**, agregue el grupo requerido.
6. Agregue los miembros al grupo o agregue el grupo a otro grupo como miembro.
7. Seleccione **Aceptar** para completar el proceso.



## Determinación de los derechos asignados actualmente.

Después de modificar las entidades de seguridad de su entorno, debe determinar qué derechos tienen esas entidades de seguridad. Obviamente, si un usuario pertenece a un grupo administrativo confidencial, como los Administradores, ese usuario puede realizar cualquier tarea y ejercer cualquier derecho en el equipo o dominio en el que existe el grupo.

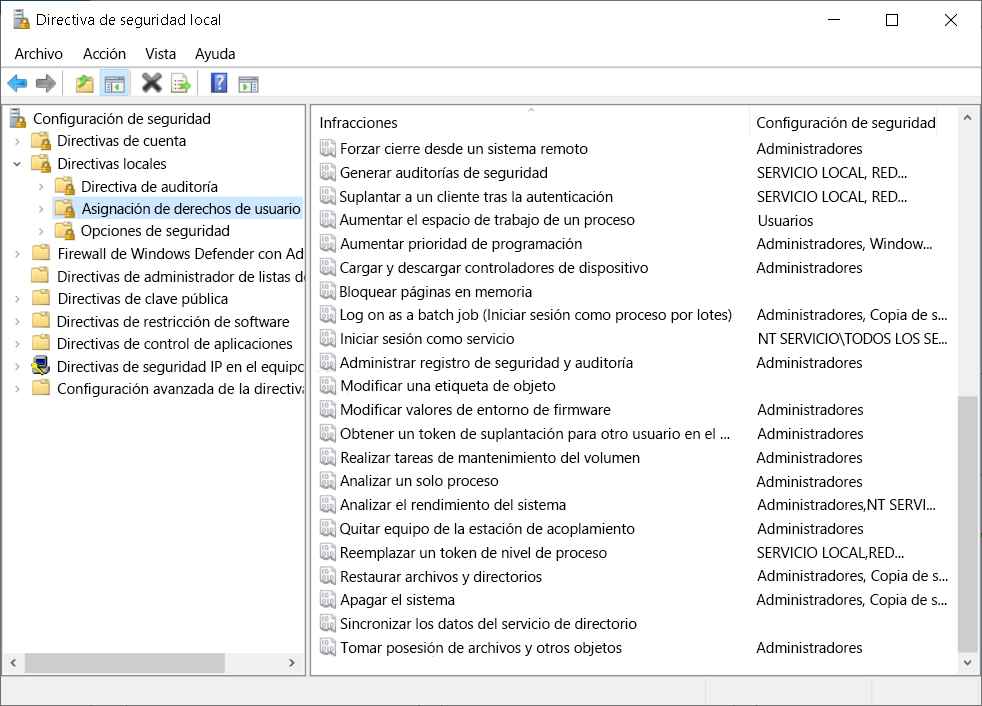
**Nota.**

Un derecho es la capacidad de realizar una tarea administrativa. Un permiso es la capacidad de obtener acceso a un objeto en el sistema de archivos, en AD DS o en cualquier otro lugar.

Sin embargo, un usuario puede pertenecer a otros grupos a los que se les han asignado derechos o privilegios. También podría ser el caso de que a un usuario se le asigne directamente un derecho.

Puede usar la consola de la **Directiva de seguridad local** para determinar qué derechos se asignan. Utilice el siguiente procedimiento:

1. Seleccione **Inicio** y, a continuación, seleccione **Herramientas administrativas de Windows**.
2. Seleccione **Directiva de seguridad local**.
3. En **Directiva de seguridad local**, expanda **Directivas locales** y, a continuación, expanda **Asignación de derechos de usuario**.
4. Revise y, si es necesario, edite el valor de la **Configuración de seguridad** para cada **Directiva** enumerada.



**Sugerencia.**

Asigne siempre una directiva a un grupo, y no directamente a un usuario. Esto ayudará al proceso de administración que se esté realizando. Cuando el rol de trabajo de alguien cambia, solo necesita cambiar la pertenencia a grupos en lugar de volver a visitar todas las asignaciones de derechos de usuario que asignó a su cuenta de usuario.

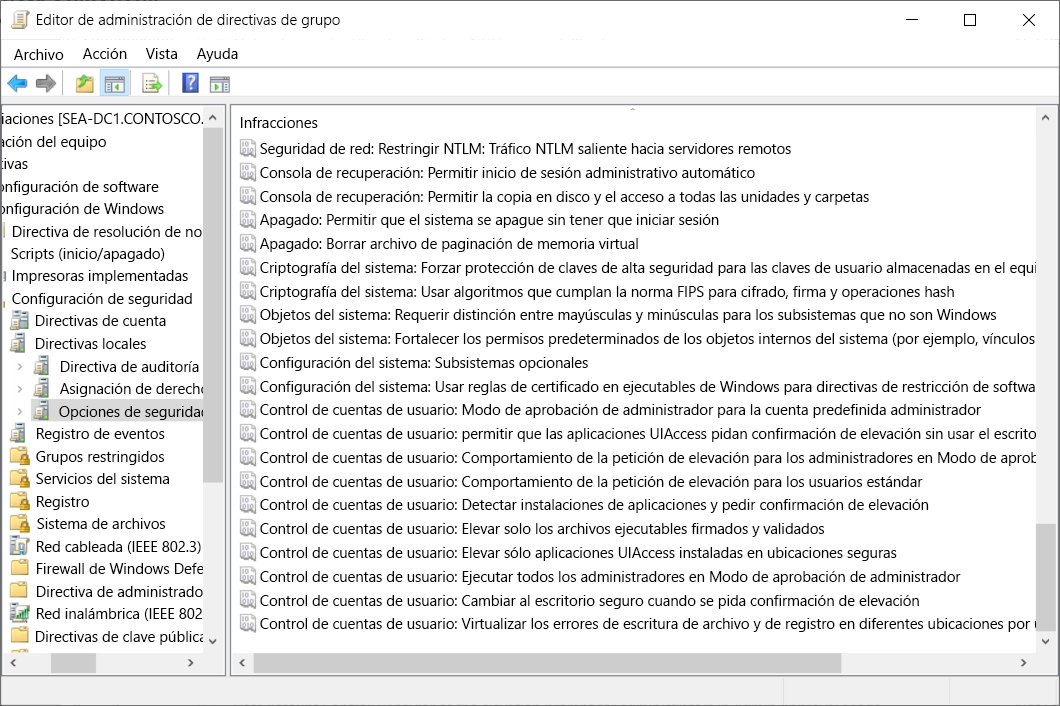
## Implementación del Control de cuentas de usuario.

El Control de cuentas de usuario (UAC) es una característica de seguridad que permite a los usuarios limitar el estado de su cuenta administrativa a la de una cuenta de usuario estándar. Sin embargo, cuando el usuario quiere realizar una tarea que requiera una funcionalidad administrativa denominada Elevación, se solicita a este que confirme la elevación. De forma predeterminada, UAC solicita al usuario que intente la elevación, tal como se indica a continuación:

* Si el usuario es un administrador, se le pedirá que confirme la elevación.
* Si el usuario es un usuario estándar, se le pedirán las credenciales administrativas.

Puede controlar los mensajes y el comportamiento de UAC mediante el uso de GPO.

1. Abra un GPO vinculado correctamente para editarlo y vaya a **Configuración del equipo**, **Directivas**, **Configuración de Windows**, **Configuración de seguridad**, **Directivas locales** y **Opciones de seguridad**.
2. Para las cuentas administrativas, abra la configuración **User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode** (Control de cuentas de usuario: comportamiento de la petición de elevación para los administradores en modo de aprobación de administrador), seleccione **Define this policy setting** (Definir esta configuración de directiva) y, a continuación, seleccione la opción requerida.
3. Para usuarios estándar, abra la configuración **User Account Control: Behavior of the elevation prompt for standard users** (Control de cuentas de usuario: comportamiento de la petición de elevación para los usuarios estándar), seleccione **Define this policy setting** (Definir esta configuración de directiva) y, a continuación, seleccione la opción requerido.



## Implementación de Just Enough Administration (JEA).

Just Enough Administration (JEA) es una tecnología administrativa que permite aplicar principios de Control de acceso basado en roles (RBAC) a través de sesiones remotas de Windows PowerShell. En lugar de permitir a los usuarios roles generales que les permitan realizar tareas que no están directamente relacionadas con sus requisitos de trabajo, JEA le permite configurar puntos de conexión especiales de Windows PowerShell que proporcionan la funcionalidad necesaria para realizar una tarea específica.

JEA permite bloquear sesiones administrativas para que solo se pueda realizar un conjunto específico de tareas a través de una sesión remota de Windows PowerShell. Asimismo, JEA aumenta la seguridad al limitar las tareas que se pueden realizar. Configure JEA creando y modificando los archivos de funcionalidad de rol y los archivos de configuración de sesión.

**Importante.**

Tenga en cuenta que JEA solo admite la comunicación remota de Windows PowerShell.

# Implementación de los privilegios delegados.

200 XP

* 10 minutos

Estudie el informe que una empresa de especialistas en seguridad de TI creó para Contoso. Se dará cuenta de que las cuentas de usuario que son miembros de grupos con privilegios elevados, como los Administradores de empresa y los Administradores de dominio, tienen acceso total a todos los sistemas y datos. Ya sabe que esas cuentas deben estar estrechamente protegidas.

Sin embargo, hay usuarios que requieren determinados derechos de administrador para realizar sus tareas. Por ejemplo, el personal del departamento de soporte técnico debe ser capaz de restablecer contraseñas y desbloquear cuentas para los usuarios normales, mientras que el personal de TI será responsable de la instalación de aplicaciones en clientes o servidores, o de realizar copias de seguridad.

Aunque Active Directory y los servidores miembro cuentan con grupos integrados que tienen asignados privilegios predeterminados (como Operadores de copia de seguridad y Operadores de cuenta), es posible que estos no se ajusten a sus necesidades. Por lo tanto, debe determinar la mejor manera de proporcionar este acceso administrativo limitado.

## Uso del Asistente para la delegación de controles.

El privilegio delegado proporciona una manera de conceder autoridad limitada a los usuarios o grupos especificados. Puede delegar privilegios más granulares a usuarios o grupos mediante el **Asistente para la delegación de controles**. Este asistente le permite asignar permisos en el nivel de la unidad de sitio, del dominio o de la organización. El asistente tiene las siguientes tareas predefinidas que puede asignar:

* Crear, eliminar y administrar cuentas de usuario.
* Restablecer contraseñas de usuario y forzar el cambio de contraseña en el siguiente inicio de sesión.
* Leer toda la información del usuario.
* Crear, eliminar y administrar grupos.
* Modificar la pertenencia de un grupo.
* Unir un equipo al dominio (solo disponible en el nivel de dominio).
* Administrar vínculos de directiva de grupo.
* Generar un conjunto de resultados de la directiva (planeación).
* Generar un conjunto de resultados de la directiva (registro).
* Crear, eliminar y administrar cuentas de inetOrgPerson.
* Restablecer las contraseñas de inetOrgPerson y forzar el cambio de contraseña en el siguiente inicio de sesión.
* Leer toda la información de inetOrgPerson.

También puede combinar permisos para crear y asignar tareas personalizadas.

Para iniciar el **Asistente para la delegación de controles**, abra Usuarios y equipos de Active Directory y busque la unidad organizativa (OU) de la que quiera delegar el control.

**Nota.**

También puede delegar el control en el objeto de dominio.

**Sugerencia.**

Para delegar el control en un sitio, use la herramienta Sitios y servicios de Active Directory para delegar el control.

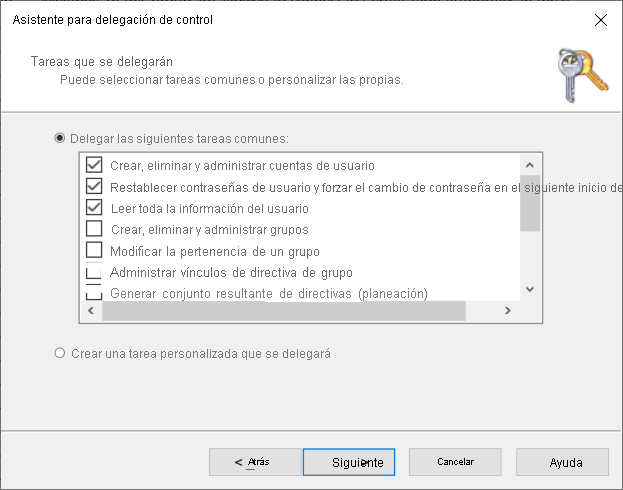
Después, siga el procedimiento siguiente:

1. Haga clic con el botón derecho en el menú contextual y seleccione **Delegar control**; a continuación, haga clic en **Siguiente**.
2. En el **Asistente para la delegación de controles**, seleccione el usuario o grupo al que quiere delegar el control y, a continuación, seleccione **Siguiente**.

**Sugerencia.**

Recuerde que debe evitar asignar derechos a usuarios específicos. En su lugar, debe usar grupos, aunque el grupo contenga solo un usuario. Esto facilita la administración continua.

1. En la página **Tareas que se delegarán**, seleccione los elementos que necesite de una lista de tareas comunes, o bien seleccione una tarea personalizada para delegar. Por ejemplo, para delegar la capacidad de administrar cuentas de usuario, seleccione lo siguiente:
   * Crear, eliminar y administrar cuentas de usuario.
   * Restablecer contraseñas de usuario y forzar el cambio de contraseña en el siguiente inicio de sesión.
   * Leer toda la información del usuario.
2. Seleccione **Finalizar**.

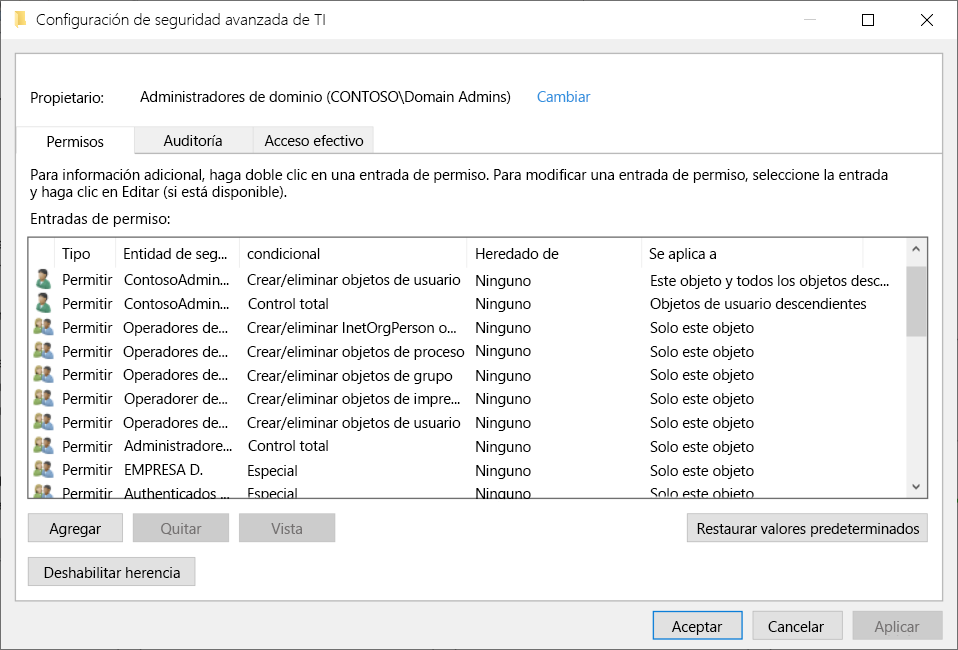


**Importante.**

Después de haber asignado el acceso delegado, tenga en cuenta que no puede usar el **Asistente para la delegación de controles** para revisar la configuración.

Para revisar las tareas delegadas que se han configurado previamente:

1. En el menú de **Usuarios y equipos de Active Directory**, seleccione **Ver** y, a continuación, seleccione **Características avanzadas**.
2. Busque la unidad organizativa que ha delegado. Haga clic con el botón derecho o active el menú contextual y seleccione **Propiedades**.
3. En el cuadro de diálogo **Nombre de la unidad organizativa Propiedades**, seleccione la pestaña **Seguridad** y, a continuación, seleccione **Avanzada**.
4. Busque la entidad de seguridad a la que delegó el control y revise los permisos. También puede cambiar los permisos delegados aquí.



**Nota.**

El **Asistente para la delegación de controles** proporciona una interfaz sencilla basada en el Asistente para la configuración de permisos de AD DS en objetos de AD DS.

## Demostración.

En el siguiente video se muestra cómo usar el **Asistente para la delegación de controles** para implementar privilegios delegados. Los pasos principales del proceso son:

1. Abra **Usuarios y equipos de Active Directory**.
2. Cree un nuevo grupo llamado **Jefes de ventas**en la unidad organizativa **Jefes**.
3. Agregue un usuario al grupo **Jefes de ventas**.
4. Ejecute el **Asistente para la delegación de controles**, y asegúrese de que esté apuntando a la unidad organizativa **Ventas**.
5. Asigne al grupo **Administradores de ventas** el permiso **Reset user passwords and force password change at next logon** (Restablecer contraseñas de usuario y forzar el cambio de contraseña en el siguiente inicio de sesión) en la unidad organizativa **Ventas**.
6. Inicie sesión como miembro del grupo **Jefes de ventas** y compruebe que el usuario puede restablecer una contraseña para los usuarios en la unidad organizativa **Ventas**, pero no en la unidad organizativa **Búsqueda**.

## Revisión rápida.

Principio del formulario

**1.**

**Uno de los administradores de IT de Contoso quiere delegar la administración de equipos a un equipo pequeño de soporte técnico de TI. Todos los equipos están en el departamento de Ventas y sus cuentas residen en la unidad organizativa de ventas. Teniendo en cuenta los procedimientos recomendados, ¿cómo debería actuar el administrador?**



Debe crear un grupo para el equipo de administración del equipo de ventas y, a continuación, crear una delegación de tareas personalizada para ese equipo en la unidad organizativa Ventas. La tarea personalizada será para los objetos del equipo.



Debe crear un grupo para el equipo de administración del equipo de ventas y, a continuación, crear una delegación de tareas común para ese equipo en la unidad organizativa Ventas.



Debe crear una delegación de tareas personalizada para los usuarios del equipo de administración de equipos de ventas en la unidad organizativa Ventas. La tarea personalizada será para los objetos del equipo.

Comprobar las respuestas

# Uso de estaciones de trabajo con privilegios de acceso.

200 XP

* 5 minutos

Al revisar el informe de seguridad que han creado los asesores de Contoso, ya sabe que los hackers malintencionados se centrarán en las estaciones de trabajo que usan habitualmente los administradores con acceso de alto nivel a la infraestructura. Por lo tanto, es importante asegurarse de que dichas estaciones de trabajo sean seguras.

## ¿Qué es una estación de trabajo de acceso con privilegios?.

Una estación de trabajo de acceso con privilegios (PAW) es un equipo que puede usar para realizar tareas de administración, como la administración de sistemas de identidades, servicios en la nube y otras funciones confidenciales. Este equipo se protegerá de Internet y se bloqueará para que solo se puedan ejecutar las aplicaciones de administración necesarias.

**Precaución.**

Asegúrese de que las cuentas de usuario administrativo no se pueden usar como cuentas de usuario estándar.

Recuerde que nunca debe usar esta estación de trabajo para estar en Internet, mirar el correo electrónico y usar otras aplicaciones de usuario final comunes; asimismo, debe tener un control estricto de la aplicación. No debe permitir la conexión a redes inalámbricas o a dispositivos USB externos. Una PAW debe implementar características de seguridad como Multi-Factor Authentication (MFA).

**Sugerencia.**

Debe configurar los servidores con privilegios para que no acepten conexiones de una estación de trabajo sin privilegios.

Microsoft recomienda usar Windows 10 Enterprise para las PAW. Esto se debe a que Windows 10 Enterprise admite características de seguridad que no están disponibles en otras ediciones. Estas características de Windows Defender se describen en la tabla siguiente.

Expandir tabla.

| **Característica.** | **Descripción.** |
| --- | --- |
| Control de aplicaciones de Windows Defender | Se aleja del modelo de confianza de aplicaciones tradicional, en el que se supone que todas las aplicaciones son de confianza de forma predeterminada, y establece una opción en la que las aplicaciones deben ganar confianza para ejecutarse. |
| Credential Guard de Windows Defender | Protege los hash de contraseña NTLM, los vales de concesión de vales de Kerberos y las credenciales que almacenan las aplicaciones como credenciales de dominio. Dado que ya no se almacenan en la autoridad de seguridad local (LSA), el robo de credenciales se puede bloquear incluso en un sistema en peligro. |
| Device Guard de Windows Defender | Combina las características del control de aplicaciones de Windows con la capacidad de usar el hipervisor de Hyper-V de Windows para proteger los procesos del modo kernel de Windows de la inyección y ejecución de código malintencionado o no comprobado. |
| Windows Defender Exploit Guard | Permite a los administradores definir y administrar directivas para reducir los ataques y las vulnerabilidades de seguridad, la protección de la red y para proteger las aplicaciones sospechosas del acceso a carpetas de destino común. |

## Perfiles de hardware de PAW.

Es importante recordar que los administradores también son usuarios. Esto significa que usarán el correo electrónico, explorarán Intenet y ejecutarán aplicaciones de productividad como Microsoft Office. Si el equipo del administrador es una PAW, afectará gravemente a la productividad del usuario en tareas no administrativas.

**Precaución.**

Merece la pena recordar que los usuarios tienden a abandonar soluciones seguras que limitan la productividad en favor de soluciones no seguras que mejoran la productividad.

Para mantener la seguridad, los usuarios administradores deben disponer de dos estaciones de trabajo. Una estación de trabajo es una PAW, mientras que la otra se usa para las tareas cotidianas que no requieren elevación. Puede lograr esta separación mediante perfiles de hardware de PAW. Microsoft recomienda usar uno de los siguientes perfiles de hardware:

* Hardware dedicado. Separa los dispositivos dedicados en tareas de usuario y tareas administrativas. La estación de trabajo de administración debe admitir mecanismos de seguridad de hardware, como un módulo de plataforma segura (TPM), e implementar las características de seguridad de Windows 10 Enterprise ya mencionadas.
* Uso simultáneo. Un único dispositivo que puede ejecutar tareas de usuario y tareas administrativas simultáneamente mediante la ejecución de dos sistemas operativos, donde uno es un sistema de usuario y el otro es un sistema de administrador. Para ello, puede ejecutar un sistema operativo independiente en una VM de uso diario.

**Precaución.**

Si usa un único dispositivo, asegúrese de que la PAW se ejecuta en el equipo físico, mientras que la estación de trabajo normal se ejecuta como una VM. Esto le proporcionará el nivel correcto de seguridad.

En la tabla siguiente se describen las ventajas e inconvenientes de estos elementos.

Expandir tabla.

| **Escenario.** | **Ventajas.** | **Inconvenientes.** |
| --- | --- | --- |
| Hardware dedicado | Separación de seguridad sólida | Requiere dos dispositivos. Esto requiere más espacio y costos de implementación. |
| Uso simultáneo | Menores costos de hardware | Compartir el mismo teclado y mouse puede dar lugar a errores y suponer riesgos de seguridad. |

## Revisión rápida.

Principio del formulario

**1.**

**¿Qué función de Windows 10 Enterprise le permite proteger las credenciales de usuario durante el proceso de inicio de sesión y qué se necesita para habilitar esta función?**



Credential Guard de Windows Defender proporciona esta protección. Para implementar Credential Guard de Windows Defender, necesita la característica Hyper-V e, idealmente, un bloqueo de TPM y de Unified Extensible Firmware Interface (UEFI).



Device Guard de Windows Defender proporciona esta protección. Para implementar Device Guard de Windows Defender, necesita la característica Hyper-V, el arranque seguro e, idealmente, un bloqueo TPM y UEFI.



Credential Guard de Windows Defender proporciona esta protección. Para implementar Credential Guard de Windows Defender, necesita la característica Hyper-V, el arranque seguro e, idealmente, un bloqueo TPM y UEFI.

Comprobar las respuestas

# Uso delos servidores de salto.

Completado100 XP

* 5 minutos

El informe de seguridad que se ha creado para Contoso recomienda la implementación de Servidores de saltos además del uso de las PAW. Tras determinar cómo usar las PAW, decide investigar los servidores de saltos para averiguar cómo podrían beneficiar al departamento de IT de Contoso.

## ¿Qué son los servidores de salto?.

Un servidor de salto es un servidor protegido que se usa para obtener acceso a los dispositivos y administrarlos en una zona de seguridad diferente, como una red interna y una red perimetral. El servidor de saltos puede funcionar como el único punto de contacto y administración.

En el caso de las organizaciones de tamaño medio, los servidores de saltos pueden proporcionar un medio para mejorar la seguridad en ubicaciones donde la seguridad física es más desafiante. Por ejemplo, en sucursales donde no hay ningún centro de datos. En el caso de las organizaciones de gran tamaño, los administradores pueden implementar servidores de saltos hospedados en centros de datos, ya que estos servidores de saltos pueden proporcionar un acceso muy controlado a los servidores y controladores de dominio.

Los servidores de saltos no suelen tener datos confidenciales, pero las credenciales de usuario se almacenan en la memoria y los hackers malintencionados pueden interesarse por esas credenciales. Por ese motivo, se deben proteger los servidores de salto.

**Sugerencia.**

Normalmente, se usa una PAW para obtener acceso a un servidor de saltos y así garantizar el acceso seguro.

Este servidor se ejecutará en hardware dedicado que admite características de seguridad basadas en hardware y software, como:

* Credential Guard de Windows Defender, para cifrar las credenciales de dominio en la memoria.
* Credential Guard remoto de Windows Defender, para evitar que las credenciales remotas se envíen al servidor de saltos, en lugar de usar vales de inicio de sesión único de Kerberos (versión 5).
* Device Guard de Windows Defender:
  + Uso de la integridad de código forzada de hipervisor (HVCI) para usar la seguridad basada en la virtualización y así aplicar los componentes en modo kernel para seguir con la directiva de integridad de código.
  + Uso de la integridad del código de configuración para permitir a los administradores crear una directiva de integridad de código personalizada y especificar software de confianza.

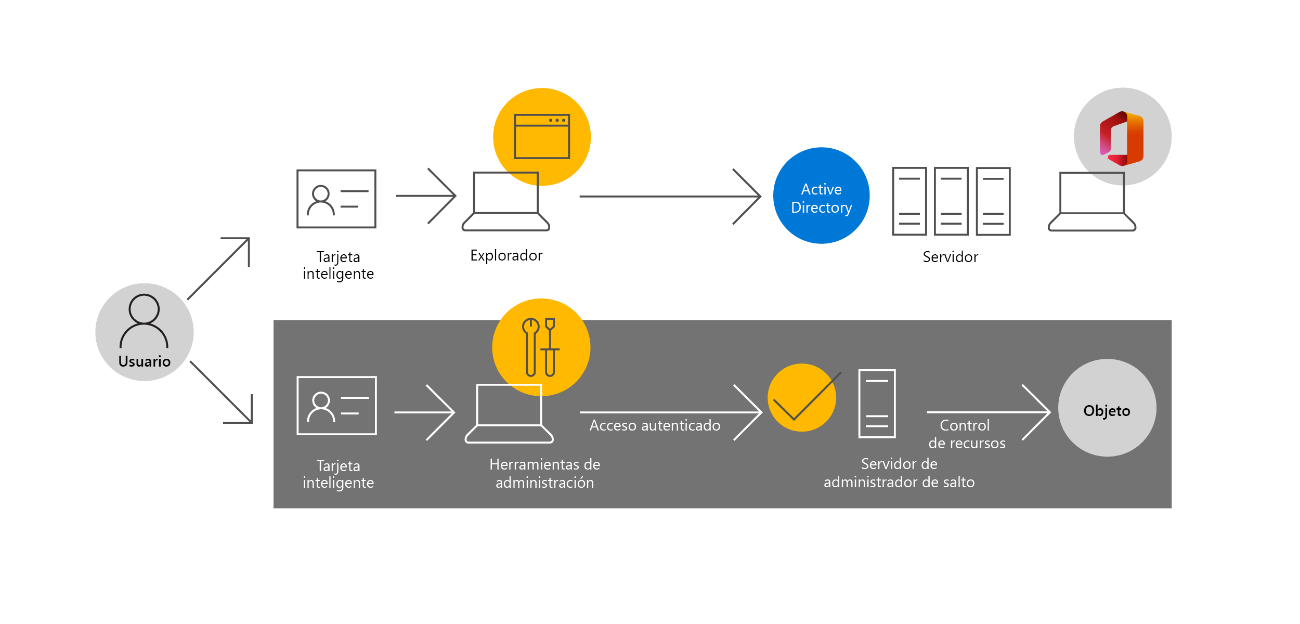
Mediante el uso de servidores de saltos, ya sea con o sin PAW, puede crear zonas de seguridad lógicas. Dentro de una zona, los equipos tienen configuraciones de seguridad y conectividad similares. Puede usar los GPO para configurar estas opciones en un entorno de dominio.

**Sugerencia.**

Los usuarios administrativos pueden conectarse a los servidores de salto mediante el Protocolo de escritorio remoto (RDP) y las tarjetas inteligentes para realizar tareas administrativas.

## Implementación de servidores de salto.

En el gráfico siguiente se muestra una implementación típica de servidor de salto y PAW. Un usuario administrativo usa una tarjeta inteligente para autenticarse en una estación de trabajo estándar mediante una cuenta estándar. El usuario puede acceder a las aplicaciones estándar para realizar tareas cotidianas de productividad de la oficina. Además, el administrador también tiene una cuenta administrativa y usa una tarjeta inteligente para autenticarse en su PAW administrativa. Esto, a su vez, se conecta al servidor de salto administrativo configurado, que tiene acceso administrativo al objeto adecuado.



Cuando se implementan servidores de saltos, hay una serie de cosas que debe tener en cuenta. Se incluyen los siguientes:

* La Puerta de enlace de escritorio remoto. Si un administrador debe conectarse directamente a un servidor de destino (mediante RDP), implemente la Puerta de enlace de Escritorio remoto. Esto le permite implementar restricciones en las conexiones con el servidor de saltos y en los servidores de destino que se usarán para realizar la administración.
* Hyper-V. Considere la posibilidad de implementar VM para cada administrador en los servidores de salto. Cada VM se puede configurar para permitir un determinado número de tareas administrativas o un subconjunto de ellas. Por lo tanto, debe instalar Hyper-V en los servidores de salto.

**Sugerencia.**

Puede exigir el cierre de estas VM después de completar las tareas administrativas. Al apagar las VM cuando no están en uso, se reduce la superficie expuesta a ataques.

* Características de servidor. Para implementar servidores de salto, los equipos del servidor deben admitir las siguientes características:
  + El arranque seguro UEFI.
  + La compatibilidad con la virtualización.
  + Los controladores de modo kernel firmados.
* Las herramientas de administración remota. Siempre debe usar herramientas de administración remota para administrar servidores. Instale Windows Admin Center y las Herramientas de administración de servidor remoto (RSAT) en las VM del administrador (o del servidor de salto físico si no implementa Hyper-V).

**Precaución.**

También debe evitar el uso de herramientas de administración remota en equipos de uso general.

* Conectividad RDP. Asegúrese de que los administradores se conectan mediante RDP a sus VM cuando realizan tareas administrativas.

# Prueba de conocimientos.

200 XP

* 5 minutos

## Comprobación de conocimientos.

Principio del formulario

**1.**

**Un administrador quiere aumentar la seguridad ajustando el comportamiento predeterminado de la solicitud de elevación de UAC para usuarios estándar. ¿Cuál de los siguientes valores de la directiva de grupo sería apropiado ajustar para lograr este objetivo?**



El administrador debe cambiar la configuración **User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode** (Control de cuentas de usuario: comportamiento de la solicitud de elevación para administradores en el modo de aprobación de administrador). Debe elegir la opción: **Solicitar credenciales**.



El administrador debe cambiar la configuración **User Account Control: Behavior of the elevation prompt for standard users** (Control de cuentas de usuario: comportamiento de la solicitud de elevación para usuarios estándar). Debe elegir la opción: **Automatically deny elevation requests** (Denegar automáticamente las solicitudes de elevación).



El administrador debe cambiar la configuración **User Account Control: Behavior of the elevation prompt for standard users** (Control de cuentas de usuario: comportamiento de la solicitud de elevación para usuarios estándar). Debe elegir la opción: **Solicitar credenciales**.

**2.**

**Un administrador crea una delegación personalizada mediante el Asistente para la delegación de controles. El administrador delega los derechos administrativos del grupo de ventas en objetos de equipo en la unidad organizativa Ventas. En concreto, el grupo tiene concedido el permiso Crear objetos seleccionados en la carpeta y Eliminar los objetos seleccionados de la carpeta, además de Control total sobre los objetos de equipo. Más adelante, el administrador quiere modificar estos permisos delegados. ¿Qué debe hacer?**



El administrador debe volver a ejecutar el **Asistente para la delegación de controles** y, esta vez, asignar permisos de denegación. El valor "Deny" invalida los permisos.



El administrador debe volver a ejecutar el **Asistente para la delegación de controles** y, esta vez, escoger los permisos de delegación nuevos.



El administrador debe revisar la configuración de seguridad en la unidad organizativa Ventas; para ello, debe habilitar las **Características avanzadas** de **Usuarios y equipos de Active Directory**. A continuación, debe revisar la configuración de seguridad avanzada para la unidad organizativa.

**3.**

**Un administrador de Contoso está implementando una configuración de un servidor de salto para mejorar la seguridad. Decide virtualizar el servidor de salto e instalar las herramientas administrativas requeridas en esa VM. ¿Qué más debe hacer este administrador?**



Además, el administrador debe configurar una PAW. A continuación, debe trasladar la VM del servidor de salto a esta PAW.



Además, el administrador debe configurar una PAW. Después, debe configurar MFA para conectarse a su VM del servidor de salto desde la PAW.



No es necesario que el administrador realice ninguna tarea adicional.

Comprobar las respuestas

# Resumen.

Completado100 XP.

* 3 minutos.

Como administrador de Windows Server en Contoso, es responsable de administrar y mantener la infraestructura del servidor local. La primera tarea fue determinar cuál es la mejor manera de administrar Windows Server con el principio de privilegios mínimos.

En este módulo, aprendió a resolver qué cuentas de usuario se van a usar al realizar tareas administrativas y cómo realizar la administración de Windows Server de forma segura. Ahora puede aplicar el principio de privilegios mínimos e identificar cuentas con privilegios integradas. También comprende cuándo debe usar estaciones de trabajo de acceso con privilegios.

## Saber más

Para obtener más información, consulte los documentos siguientes:

* [Just Enough Administration (JEA)](https://learn.microsoft.com/es-es/powershell/scripting/learn/remoting/jea/overview).
* [Implementación de modelos administrativos de menor privilegio](https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models).
* [Grupos de seguridad de Active Directory](https://learn.microsoft.com/es-es/windows/security/identity-protection/access-control/active-directory-security-groups).
* [Implementación de hosts administrativos seguros](https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/plan/security-best-practices/implementing-secure-administrative-hosts).