Buenas prácticas de seguridad

en Microsoft Windows Server

Autor: Grupo de infraestructuras

Índice

1. Introducción y objetivos de este documento

Este documento es de carácter técnico, y esta destinado a Administradores de sistemas o técnicos con los suficientes conocimientos para administrar sistemas Windows Server, en entornos IaaS (Infraestructura como Servicio).

El presente documento es una guía básica de buenas prácticas para mantener la Seguridad de sistemas IaaS en la Universidad de Sevilla. Este documento no es en ningún caso exhaustivo, y por tanto debe entenderse como **el conjunto mínimo de medidas a adoptar** para mantener razonablemente seguros los sistemas.

La seguridad de sistemas de Información se basa en tres pilares fundamentales:

1. Medidas técnicas.
2. Medidas procedimentales.
3. Concienciación y formación.

Si se descuida alguno de los pilares, la Seguridad se derrumba. Suele decirse que una cadena es tan fuerte como su eslabón más débil, y esto es perfectamente aplicable a la Seguridad de sistemas información.

2. Recomendaciones básicas

Un sistema informático debe ser mantenido y administrado regularmente para evitar problemas de seguridad que supongan correr riesgo de pérdidas de servicio, datos, robos, etc. Para este fin, se deben adoptar una serie de medidas que aseguren la continuidad del servicio manteniendo la seguridad del mismo.

2.1. Actualizaciones del sistema operativo

Las actualizaciones de Windows contienen mejoras y solucionan problemas de productividad, seguridad, fallos de programación, etc. En algunos casos incluyen componentes y características adicionales para el sistema operativo.

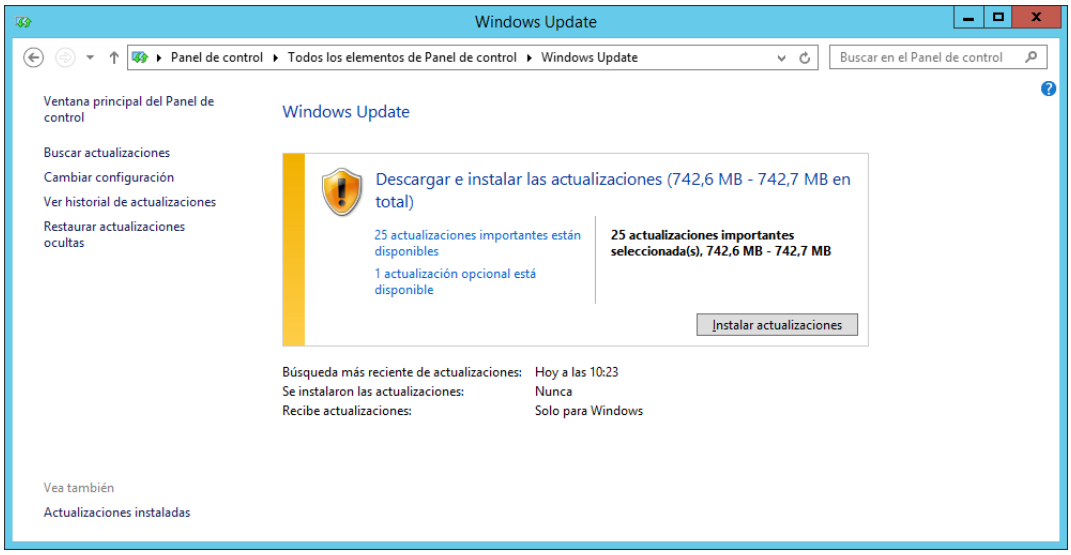
2.1.1 Método de instalación de las actualizaciones

- Desde la web oficial de Microsoft (www.microsoft.com), e instaladas manualmente.
- Desde Windows Update, herramienta que viene incluida con el propio Windows.

Nota: Ninguna actualización ni parche para el sistema operativo deberá ser descargado e instalado si no es a través de esta herramienta, o desde la web oficial de Microsoft. Nunca desde otras páginas web.

Las actualizaciones automáticas se liberan cada **segundo martes de cada mes**. Es importante aplicar dichos parches para evitar ser víctima de ataques.

*Inicio > Panel de control > Windows Update***:**



2.1.2 Planificación de las actualizaciones

Dado que la aplicación de las actualizaciones suele exigir alto grado de consumo de CPU, memoria y disco, y un posterior reinicio de la máquina, se recomienda definir un horario semanal de aplicación de las actualizaciones.

Esta planificación permitirá:

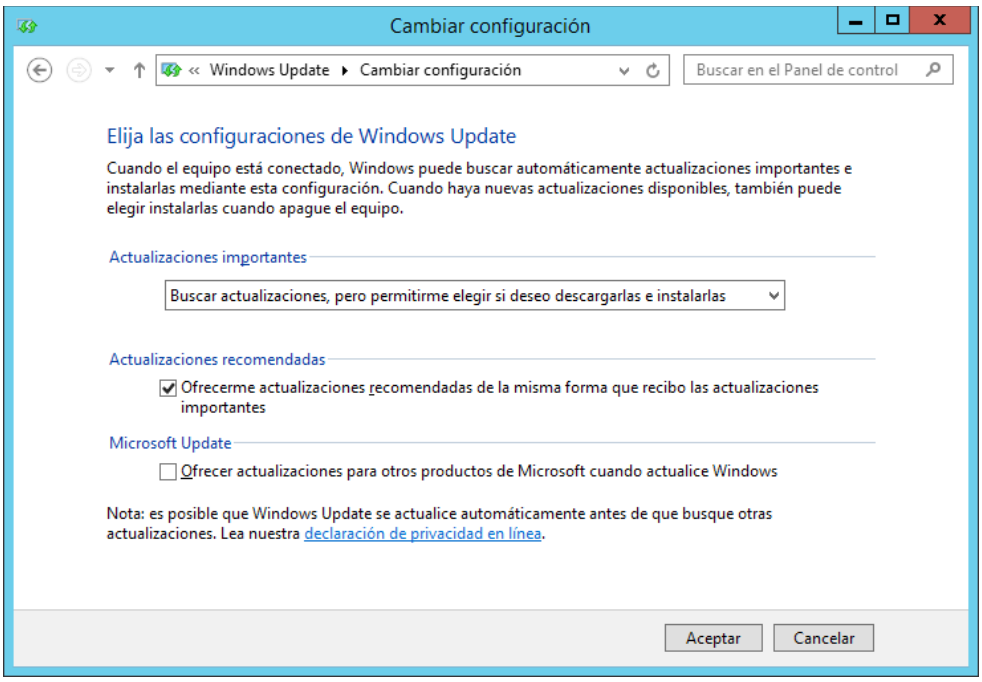
- Llevar a cabo una revisión de las actualizaciones determinando si pueden producir incompatibilidades de algún tipo con el software de terceros que se haya instalado[1].
- Mantener el sistema actualizado, reduciendo las vulnerabilidades de seguridad que el sistema operativo pueda presentar.
- Reducir el impacto en el servicio.
- Simplificar el despliegue de actualizaciones y parches.

2.1.3 Configuración de Windows Update

La configuración por defecto de Windows Update es “Instalar actualizaciones automáticamente (recomendado)”. Para cambiar este comportamiento:

Inicio > Panel de control > Windows Update > Cambiar Configuración:

1 Algunas actualizaciones de Windows pueden ser incompatibles con determinados productos de terceros. Para conocer su compatibilidad con Windows Server, consulte la documentación de dichos productos y en caso de duda contacte con la empresa que suministra el soporte del sistema operativo.



Seleccionar *Buscar actualizaciones, pero permitirme elegir si deseo descargarlas e instalarlas*.

Activar *Ofrecerme actualizaciones recomendadas de la misma forma que recibo las actualizaciones importantes*.

Activar *Ofrecer actualizaciones para otros productos Mircosoft cuando actualice Windows*.

Tal como se ha expuesto anteriormente será necesario planificar una revisión e instalación periódica de actualizaciones de la máquina que deberá ser llevada a cabo por el Administrador de la misma.

2.2. Antivirus

Un antivirus es un programa informático que detecta y elimina virus informáticos, y dependiendo del producto, otras amenazas potenciales.

Un sistema Windows Server no debe funcionar sin un antivirus por el gran número de amenazas que circulan por las redes, especialmente si la máquina está conectada a Internet.

Si no se dispone de un antivirus comercial se puede instalar la versión gratuita de Windows denominado Microsoft Security Essentials o Windows Defender.

Nota: Windows Defender no está incluido por defecto para versiones 2008 y 2012.

Windows defender ya viene incluido en Windows Server 2016; para versiones anteriores será necesario adquirir una licencia válida de un antivirus para versión Windows Server. Se proponen:

- **Kaspersky antivirus para Windows Server**: https://www.kaspersky.com/small-to-medium-business-security/windows-server-security
- **ESET Nod32 antivirus**: https://descargas.eset.es/eset-file-security-for-microsoft-windows-server

3. Software y servicios

Un principio básico de la Seguridad es presentar la *"superficie de ataque"* más pequeña posible. Mientras más paquetes de software instalados en un sistema, mayor es la probabilidad de que aparezcan problemas de seguridad en dichos paquetes. Por tanto, debería eliminarse aquel software que sea innecesario para prestar servicio en nuestro sistema.

El mismo principio se aplica también a los servicios de red. Se deberían ejecutar únicamente los servicios estrictamente necesarios para la funcionalidad deseada del sistema. Por ejemplo, un servidor que ejecute cálculos científicos con *Matlab* o *Mathematica* no debería ejecutar servicios como *apache* o *mysql*.

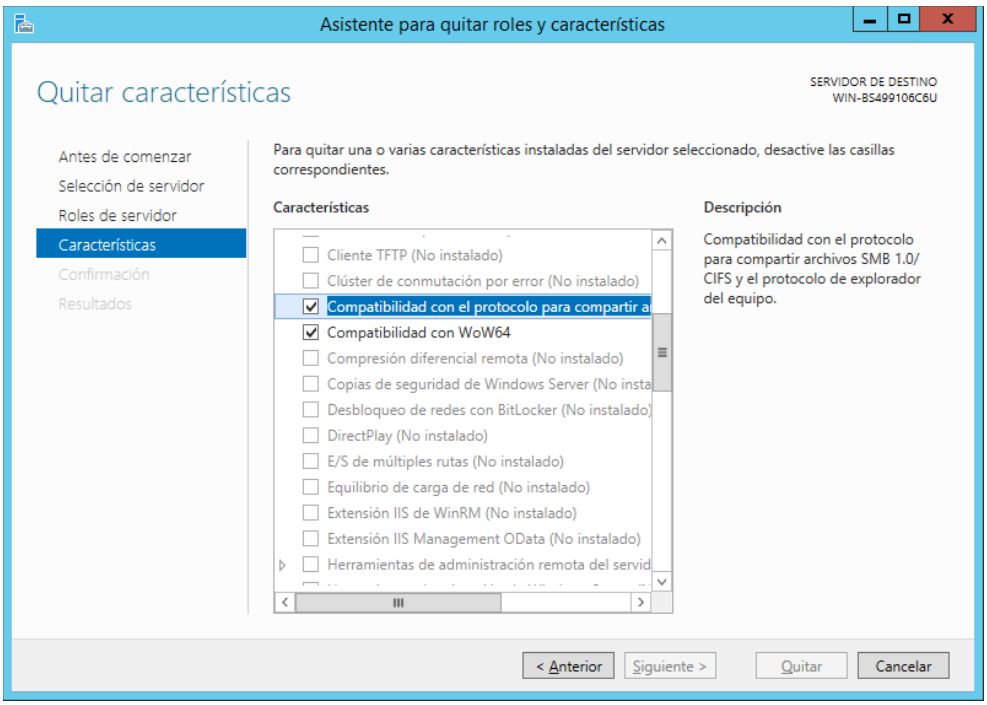
3.1. Roles y servicios del servidor

En Windows un servicio es un proceso o grupo de procesos que se ejecutan en segundo plano de forma transparente para el usuario, y generalmente sin necesidad de que éste interactúe con el mismo.

Todo aquel rol o servicio que no sea necesario debe ser desactivado para evitar problemas de seguridad.

Los roles se administran desde la herramienta Administrador de servidor:

Inicio > Herramientas administrativas > Administrador del servidor > Administrar > Quitar roles y funciones



Los roles de servidor a desplegar dependerán de las funciones que vaya a ejecutar el servidor.

Las siguientes características deben estar desactivadas (desinstaladas):

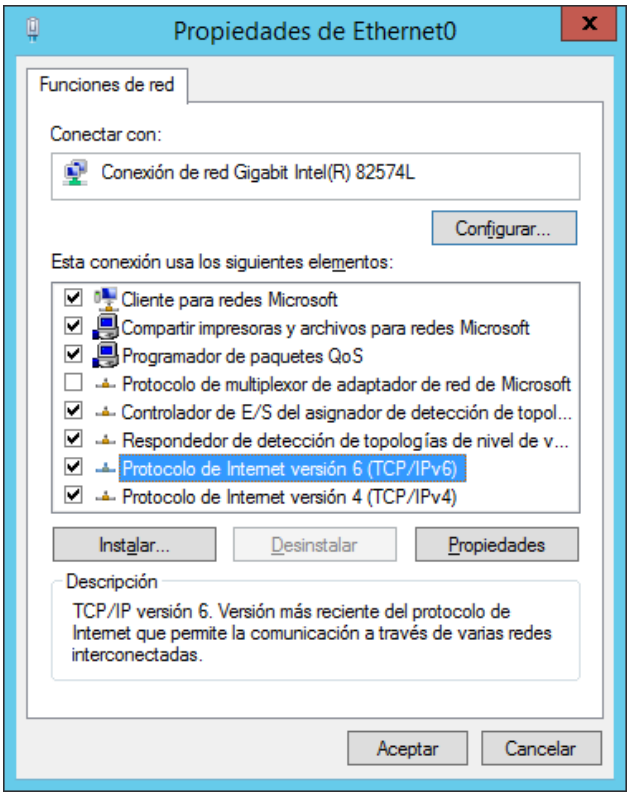
- *Compatibilidad con el protocolo para compartir archivos SMB 1.0/CIFS y el protocolo de explorador de equipo*. Permite compartir archivos usando una versión del protocolo SMB versión 1.0 (inseguro).
- *Asistencia remota*. Esta característica sólo debe usarse en casos muy específicos de soporte por parte de Microsoft.
- *Experiencia de escritorio*. Agrega características multimedia que no son necesarias en un servidor.
- *Reenvío de comentarios Windows*. Envía información de experiencia de usuario a Microsoft.
- *Servicios WLAN*. Proporciona servicios de conectividad inalámbrica, y no será necesario habilitarlo en un sistema IaaS.
- *Servidor de TELNET*. TELNET proporciona un intérprete de comandos inseguro, similar al SSH de UNIX/Linux. Al no incorporar cifrado las credenciales se envía en texto sin codificar.

3.2. Desactivar compatibilidad con protocolo IPv6

IPv6 o IPnG (*IP Next Generation*) es la versión mejorada del protocolo IP. Actualmente no se usa en la Universidad de Sevilla, por lo que hay que desactivarla para reducir el riesgo de posibles ataques.

Para desactivar la compatibilidad con IPv6:

Inicio > Panel de control > Redes e internet > Centro de redes y recursos compartidos > Cambiar configuración del adaptador > Seleccionar adaptador > Botón derecho > Propiedades >

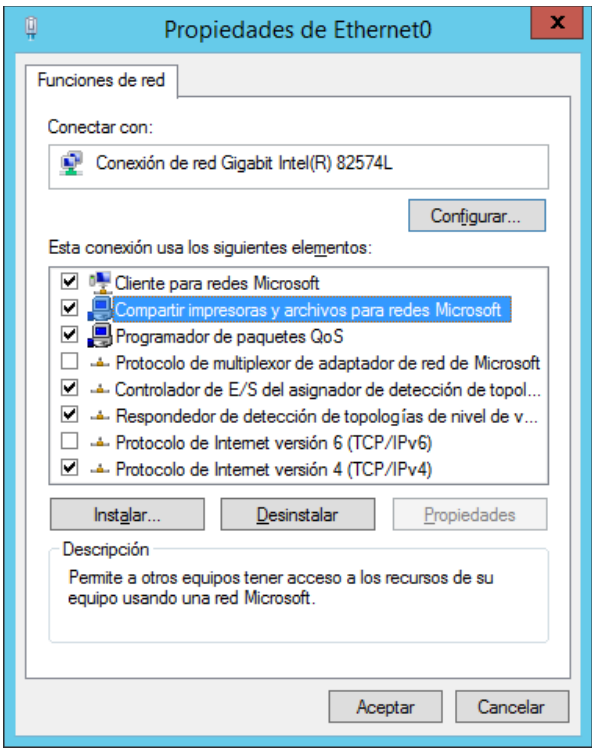


Desmarcar *Protocolo de Internet versión 6 (TCP/IP)* y pulsar Aceptar.

Nota: esta operación deberá repetirse en cada adaptador de red.

3.3. Desactivar el uso de recursos compartidos

Los recursos compartidos de Windows permiten compartir archivos, carpetas e impresoras en redes que usan TCP/IP con cualquier versión de Windows. Si el servidor no va a compartir nada es recomendable desactivar este servicio para evitar problemas de seguridad. Esto debe hacerse para cada adaptador de red.



Desmarcar “Compartir impresoras y archivos para redes Microsoft” y pulsar Aceptar.

Nota: esta operación deberá repetirse en cada adaptador de red.

3.4. Uso de protocolos cifrados

Los protocolos cifrados proporcionan un mecanismo seguro de comunicación entre dos máquinas que “hablan el mismo idioma”. En la medida de lo posible se deben utilizar protocolos cifrados tanto para los servicios del sistema operativo como para los de aplicaciones de terceros (bases de datos, servidores web, etc.). Se debe evitar el uso de protocolos no cifrados en aquellos servicios que transmitan datos confidenciales o autenticaciones (como usuarios y contraseñas).

Por ejemplo, en el caso de montar un servidor web con IIS (*Internet Information Services*) en lugar de acceso por HTTP (Protocolo de Transferencia de Hipertexto) se debería montar mediante un certificado digital y mediante HTTPS (HTTP seguro).

Para conocer los detalles de los protocolos que soportan las aplicaciones de terceros a instalar en Windows Server consulte a su proveedor o en la documentación de la(s) aplicación(es).

Nota: para deshabilitar el uso de protocolos inseguros en IIS consultar https://support.microsoft.com/es-es/kb/187498.

4. Gestión de usuarios

La gestión de usuarios supone la tarea más importante en la administración de un servidor ya que permite la conexión de los usuarios a los recursos del mismo.

El principio de “Menor privilegio” (*less privilege*) establece que para garantizar la seguridad, los usuarios deben tener los privilegios y permisos estrictamente necesarios para su trabajo, tanto para los propios recursos del servidor (carpetas compartidas, impresoras, conexiones por Escritorio Remoto, etc.), como de servicios ejecutándose en el mismo (bases de datos, páginas web, aplicaciones de terceros, etc.).

Recomendaciones generales:

- La cuenta Administrador debe usarse **sólo para tareas administrativas** del servidor tales como inicio y parada de servicios, instalación de software, actualizaciones, reinicios, etc. **Para todo lo demás se deben usar cuentas convencionales**.
- Los usuarios conectados al servidor que necesiten realizar alguna labor administrativa puntual **deberán usar la función “Ejecutar como[1]” del menú contextual para elevar sus privilegios** de forma temporal, efectuar el cambio, y continuar trabajando como usuarios con privilegios limitados.
- **Las políticas de cambio de contraseñas deben ser observadas de forma estricta**, especialmente en cuentas administrativas[2], para mantener la seguridad en todo momento.
- **El Administrador debe mantener un registro de las cuentas de usuario** (por ejemplo en una hoja de cálculo) con un listado de a qué usuario real pertenece cada cuenta, cuál es su rol/función, fecha de alta (en qué momento se le permite acceso), y fecha de baja (cuando finaliza su contratación, etc.). Esto incluye los recursos compartidos del servidor.
- Los usuarios que deban conectarse por Escritorio Remoto[3] deberán ser agregados al grupo de **“Usuarios de Escritorio Remoto”**, y no al grupo “Administradores”.
- **Los recursos compartidos del servidor no deben incluir el grupo especial “Todos” (*Everyone*)**, dado que éste incluye acceso a cualquier usuario, incluso los no autentificados.
- **No se deben crear cuentas de usuario sin contraseña ni cuentas de usuario pertenecientes al grupo Invitados[4]**.

4.1. Política de contraseñas

1 Aquellas operaciones que requieran elevación de privilegios desde línea de comando podrán usar el comando RUNAS desde una consola CMD. Consultar la ayuda mediante runas /? para más información.

2 Las cuentas administrativas en Windows son aquellas que están incluidas en el grupo Administradores. Dichas cuentas tienen todos los privilegios activados.

3 Anteriormente conocido como Terminal Server.

4 El Invitado es un grupo de usuarios que permite acceso “de cortesía” a un sistema y suele tener privilegios limitados. Estas cuentas no deben ser creadas en un servidor.

Una política de contraseñas es un documento que establece una serie de parámetros que deberán ser de obligado cumplimiento para todas las contraseñas de las cuentas de usuario de una empresa. **Cuanto más fuertes sean estas políticas mayor seguridad se agregarán a las cuentas de usuario y por tanto al servidor y a los servicios que presta**.

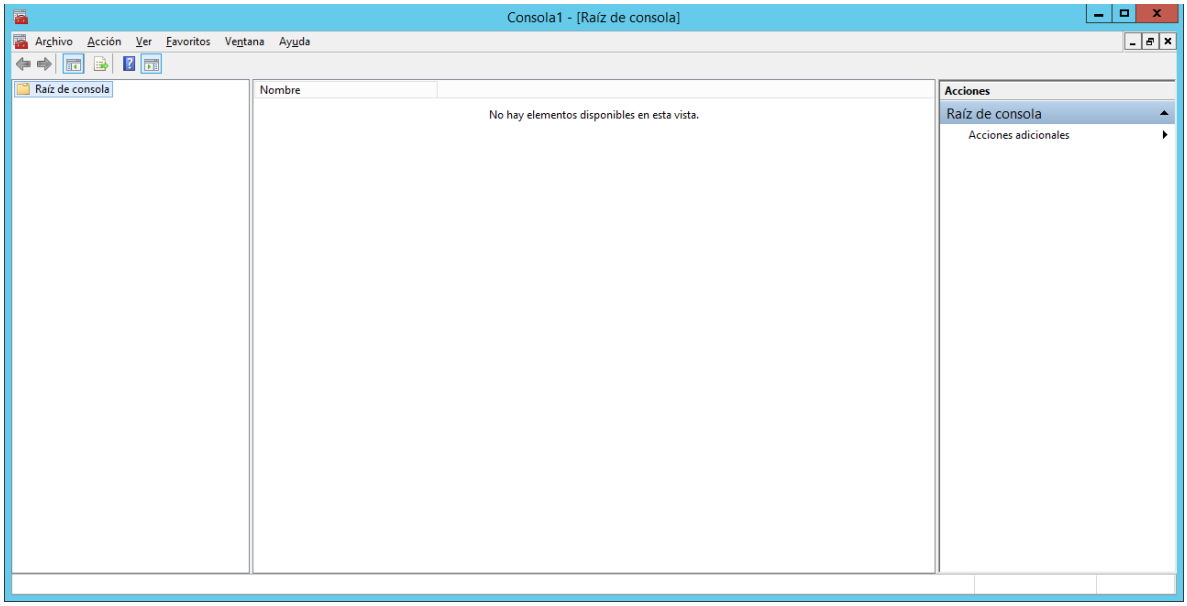
La Universidad de Sevilla dispone de una política de contraseñas con las siguientes características:

- *La **longitud** de la contraseña debe ser como **mínimo de 8 caracteres.***
- *La contraseña debe contener **al menos 4 caracteres alfabéticos.***
- *La contraseña debe contener **al menos 2 caracteres numéricos.***
- *Se recomienda emplear letras mayúsculas y minúsculas.*
- *Se deben evitar secuencias y repeticiones alfabéticas (como abcde o asdfg) y/o numéricas (como 12345 o 0000).*
- *La contraseña **no deberá** contener el **nombre o apellido** del usuario, **ni el documento** de identidad del mismo o su UVUS.*
- *La contraseña **no** debe contener palabras que aparezcan en un diccionario, como **días de la semana o nombres del mes**.*

4.2. Los usuarios y grupos de Windows Server

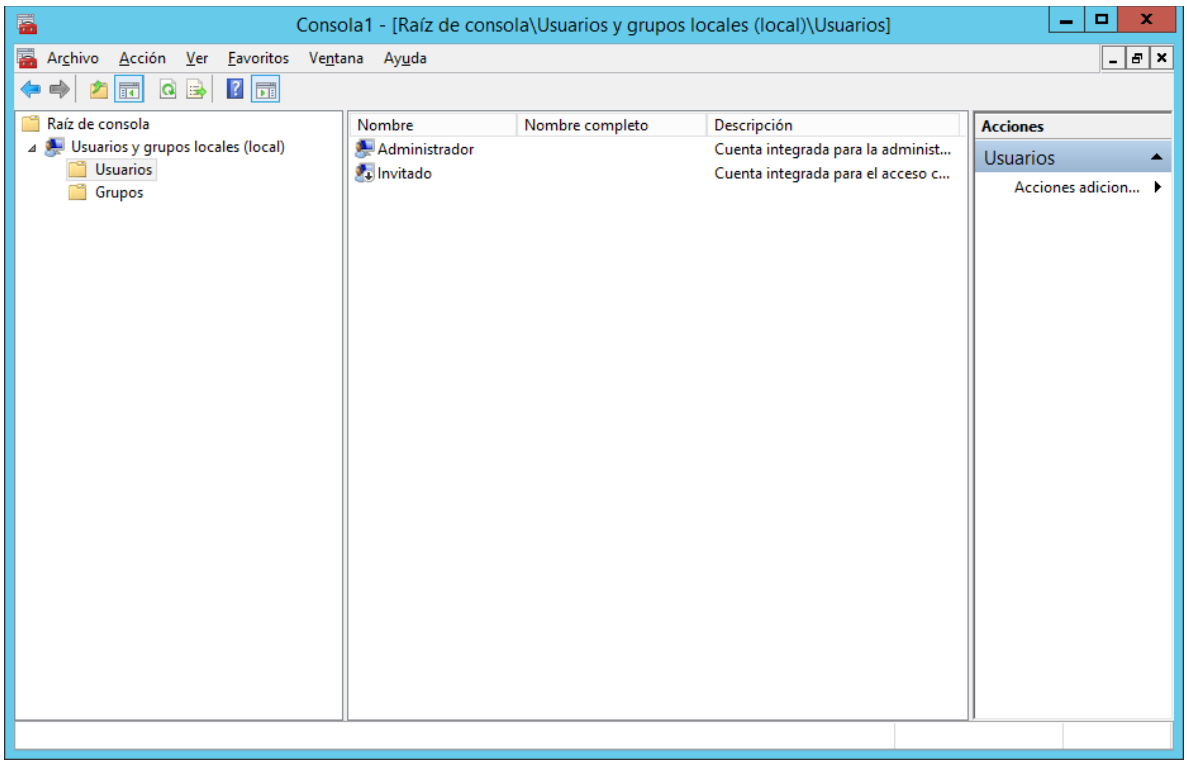
Por defecto, tras instalar Windows Server se crean una serie de usuarios y grupos por defecto[1]; para acceder al panel de administración de Usuarios y grupos locales; para ello:

Inicio > Ejecutar (tecla ⊞ + R) > Escribir el comando: *mmc* > Se mostrará la siguiente ventana:



*Archivo > Agregar o quitar complemento > Seleccionar: **Usuarios y grupos locales** > Agregar > Seleccionar: Este equipo > Aceptar.*

1 Esto puede variar según la versión de Windows y la edición instalada.



Los usuarios por defecto son:

- **Administrador**: este usuario tiene privilegios para administrar todos los aspectos del servidor. Esta cuenta no debe desactivarse[1].
- **Invitado (desactivado por defecto)**: este usuario se utiliza como usuario de cortesía para acceso esporádico al sistema. Tiene privilegios limitados, y está desactivado. **Esta cuenta no debe activarse nunca**.

Los grupos por defecto son (más importantes):

- **Administradores**[2]: administran el sistema operativo y tienen control total sobre el servidor.
- **Administradores de Hyper-V**: administran la infraestructura de máquinas virtuales.
- **Invitados**[3]: representa el grupo de usuarios de cortesía.
- **Operadores de copia de seguridad**: realizan copias de seguridad del sistema o de alguna aplicación; sus privilegios están más limitados que los de un Administrador.
- **Usuarios**: usuarios con limitados privilegios; tienen más privilegios que los Invitados, pero menos que los usuarios avanzados.

1 Salvo que se creen otras cuentas de usuario que pertenezcan al grupo Administradores.

2 A este grupo pertenece el usuario Administrador. Se pueden crear usuarios y al asignarlos a este grupo pasarán a ser Administradores, con control total. Este grupo debe ser estrechamente vigilado.

3 Este grupo no debe contener usuarios.

- **Usuarios avanzados**: usuarios con mayores privilegios que el grupo Usuarios.
- **Usuarios de escritorio remoto**[1]: usuarios con permisos para iniciar sesión remota en el servidor a través del protocolo de Escritorio remoto o RDP.

Para más información sobre usuarios y grupos de usuarios de Windows:

https://docs.microsoft.com/es-es/windows-server-essentials/manage/manage-user-accounts-in-windows-server-essentials

4.3. Auditoría de usuarios y grupos

Las auditorías permiten realizar un seguimiento de las medidas adoptadas por una organización, para asegurar que dichas medidas son efectivas. En este caso, una auditoría de usuarios y grupos permitirá llevar un control de qué usuarios y grupos tienen acceso a los recursos del servidor.

Las auditorías de usuarios y grupos:

- Deberán llevarse a cabo al menos una vez **cada 6 meses**. Si se crean y eliminan usuarios con mucha frecuencia, puede hacerse cada 3 meses o incluso menos.
- Se simplifica si se cumplen las premisas anteriores en las que los usuarios autorizados están identificados y documentados, etc.; de esa manera se ahorra tiempo.
- Cuando el número de usuarios es alto puede automatizarse mediante comandos de consola; ejemplo desde una ventana de comandos:

  Listar todas las cuentas de usuario: ***Net user***

  Listar todos los grupos de usuarios: ***net localgroups***

  Obtener los detalles de una cuenta de usuario, ver los grupos asignados: ***net user < usuario>***

Nota: existen múltiples formas de obtener un listado de las cuentas de usuario desde línea de comando; alternativamente se puede hacer desde la herramienta visual de administración de usuarios y grupos.

5. Servicios de Windows

1 Los usuarios que pertenezcan a este grupo, y al grupo Administradores, podrán iniciar sesión remota en el servidor; por defecto este privilegio está concedido sólo a los Administradores; **no se debe conceder permisos de Administrador a cualquier usuario que necesite conectase por Escritorio remoto al servidor**, ya que eso le daría control total sobre el servidor.

5.1. Acerca del cortafuegos de Windows

El cortafuegos de Windows es un programa que controla las conexiones entrantes y salientes desde y hacia el servidor; el cortafuegos viene activado por defecto para versiones Windows Server 2012 y 2016.

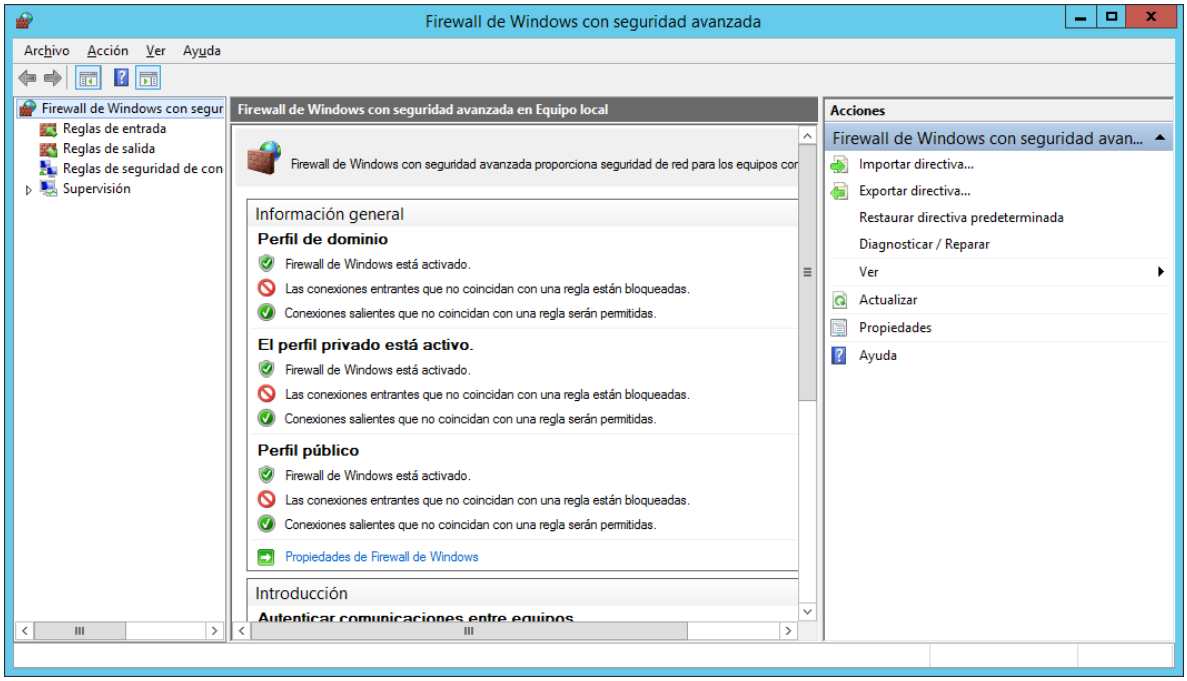
Se compone de una serie de reglas de entrada/salida que se aplican en función de:

- Servicio, puerto, o grupo de funciones
- Perfil/es que ostenta la máquina
- Estado de la regla/s en cuestión

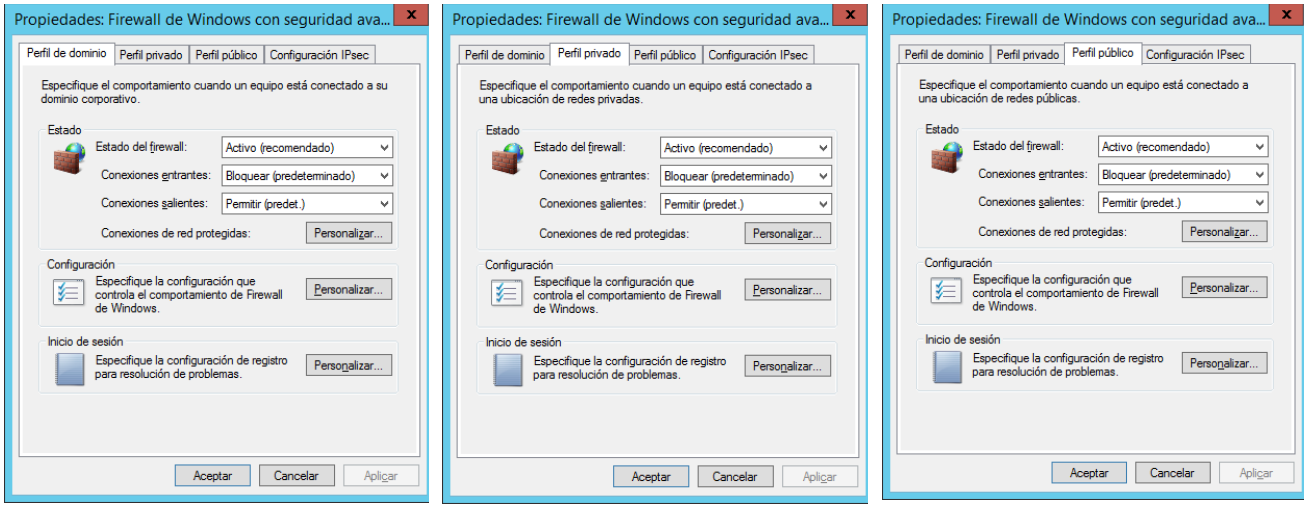
Nota: desactivar el cortafuegos de Windows supone un grave riesgo de seguridad. El cortafuegos sólo debe estar gestionado por el Administrador.

Se puede comprobar que el cortafuegos está operativo o no:

Inicio > Herramientas administrativas > Firewall de Windows con seguridad avanzada



Botón derecho del ratón sobre *Firewall de Windows con seguridad avanzada* > Propiedades



En cada viñeta el campo *Estado del firewall* debe estar seleccionado *Activo (recomendado)*.

Nota: cualquier servicio o aplicación de terceros que se instale en el servidor puede requerir que se abran determinados puertos, se creen reglas, o se levanten servicios adicionales. Esta tarea sólo puede ser acometida por el Administrador, y no puede suponer en ningún momento desactivar el cortafuegos.

5.2. Acerca de los servicios de Escritorio remoto / Terminal Server

Escritorio remoto (anteriormente conocido como Terminal Server) permite la conexión remota a una máquina con Windows, o incluso a Linux, cuando dialogan a través de RDP (*Remote Desktop Protocol*)[1].

Inicialmente mediante RDP sólo se pueden conectar el usuario Administrador, y aquellos usuarios locales, sean o no Administradores, que estén agregados al grupo **Usuarios de Escritorio remoto**.

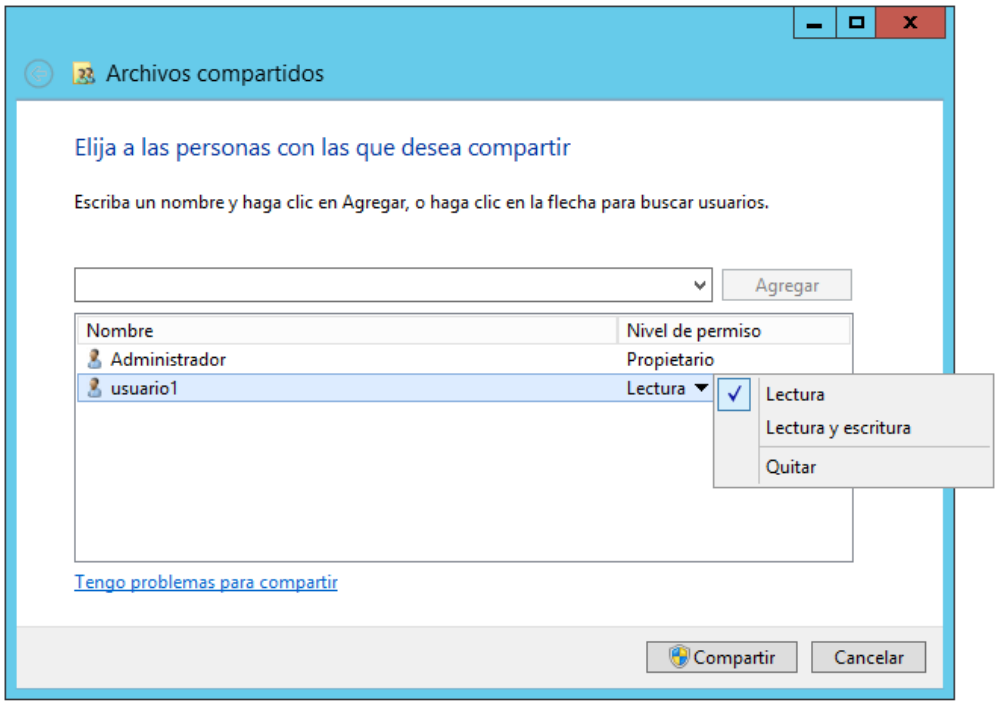
Nota: en ningún momento un usuario que no deba ser Administrador del servidor deberá ser agregado al grupo Administradores para tener acceso mediante Escritorio Remoto al mismo; en su lugar, deberá ser agregado al grupo Usuarios de Escritorio remoto.

Nota: Windows Server permite un máximo de 2 sesiones concurrentes de Escritorio remoto por servidor; para conexiones adicionales será necesario activar y adquirir licencias adicionales para el servidor de Escritorio remoto.

5.3. Acerca del uso de carpetas compartidas

1 A menudo se hace referencia a las sesiones o conexiones de Escritorio remoto o Terminal Server haciendo alusión al nombre de su protocolo: RDP; los tres conceptos son EQUIVALENTES.

Las carpetas compartidas permiten el acceso simultáneo a un mismo recurso por varios usuarios; sin embargo para que un usuario se pueda conectar es necesario que tenga una cuenta en el servidor, y unos permisos que deberán ser ajustados por el Administrador.



Recomendación: no compartir nunca una carpeta o recursos al grupo especial Todos (*Everyone*), y menos aún con permiso de Escritura; este grupo permite acceso a cualquier usuario aunque no se haya autenficado previamente.

Recomendación: Los permisos sobre los recursos compartidos deberán ser auditados cada poco tiempo con el objetivo de asegurarse que sólo el personal autorizado tenga acceso a ellos.

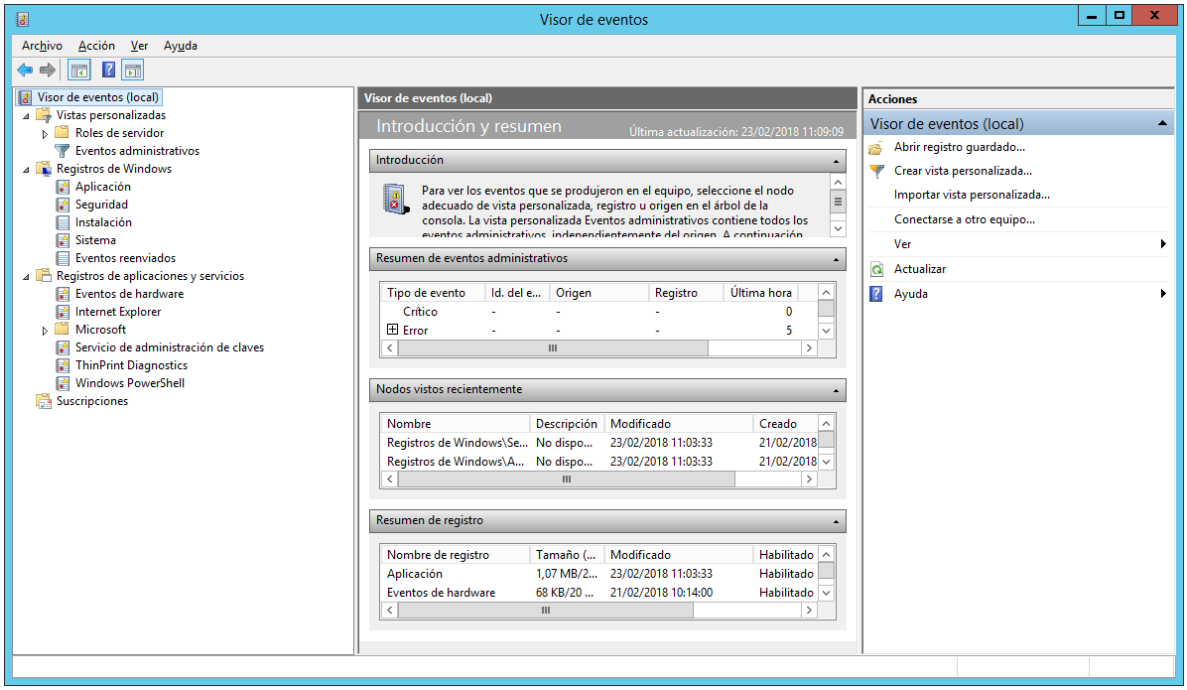
5.4. Acerca del Visor de eventos

El Visor de sucesos de Windows es la herramienta que permite comprobar los eventos que genera Windows, así como otras aplicaciones y servicios instalados sobre este. Se generan eventos en tres grandes categorías:

- **Sistema**: eventos relacionados con el propio sistema operativo (inicio y cierre de sesiones, apagados, reinicios, mensajes de servicios de red, etc.).
- **Aplicaciones**: eventos relacionados con las aplicaciones de terceros y de servicios del propio sistema operativo (bases de datos, servicios de sistema, etc.).
- **Seguridad**: eventos relacionados con la seguridad (acceso a recursos, auditorías, fallos de inicios de sesión, etc.).

Recomendación: es recomendable revisar diariamente los registros a través de la herramienta Visor de sucesos de Windows Server.

Inicio > Herramientas Administrativas > Visor de eventos



Eventos relacionados con las sesiones de Escritorio remoto (Terminal Server):

Para ver los usuarios que han iniciado sesión por RDP, hora de la conexión, etc.:

Visor de eventos > Registros de aplicaciones y servicios > Microsoft > Windows > TerminalServices-LocalsessionManager > Operational