

Software seguro

Microsoft Dynamics NAV 5.00

Security Hardening Guide

Notas del producto

2007

Tabla de contenido

Introducción	4
Recomendaciones de seguridad para Microsoft Dynamics™ NAV	5
C/SIDE Database Server para Dynamics NAV y TCPS	5
Hacer que el servicio de servidor sea seguro	6
SQL Server	6
C/SIDE Database Server para Microsoft Dynamics NAV	8
Servidor de aplicaciones para Microsoft Dynamics NAV	9
Automated Data Capture System para Microsoft Dynamics NAV	9
Dynamics NAV Employee Portal	9
Contraseñas y acceso a la base de datos	9
Copias de seguridad	10
Sistema operativo y actualizaciones	10
Archivos de licencia	10
Plan de recuperación	10
Seguridad física	11
Empleados	11
Administrador	12
Protección del sistema operativo de servidor	13
Autenticación	14
Contraseñas seguras	14
Definición de la directiva de contraseñas	14
Definición de una directiva de bloqueo de cuentas	15
Control de acceso	16
Permisos	16
Propiedad de los objetos	16
Herencia de permisos	16
Derechos de usuario	17
Auditoría de objetos	17
Prácticas recomendadas de control de acceso	17
Servidor de seguridad externo	18
ISA Server 2006	18
Directivas de ISA Server	19

Protección antivirus.....	19
Tipos de virus.....	19
Virus del sector de inicio	19
Virus de infección de archivos.....	19
Programas troyanos	20
Prácticas recomendadas de protección antivirus	20
Estrategias de seguridad de red.....	21
Redes inalámbricas	22
Escenarios de seguridad de red.....	23
Sin servidor de seguridad.....	23
Un servidor de seguridad sencillo.....	23
Servidor de seguridad existente	24
Dos servidores de seguridad existentes.....	26
Administración de actualizaciones de seguridad.....	27
Configuración de seguridad de SQL Server	29
Apéndice	30
Vínculos en este documento	30

Introducción

Microsoft® proporciona sistemas operativos con seguridad de redes basada en sofisticados estándares. En el sentido más amplio, la seguridad incluye planeamiento y consideración de ventajas e inconvenientes. Por ejemplo, un equipo se puede encerrar en una cámara acorazada a la que sólo tiene acceso un administrador de sistemas. Puede que este equipo tenga la máxima seguridad, pero no es útil porque no está conectado a ningún otro equipo. Debe considerar cómo proporcionar seguridad a la red sin sacrificar la capacidad de uso.

La mayoría de las organizaciones se preparan para ataques externos y establecen barreras de seguridad, pero muchas empresas no tienen en cuenta cómo mitigar una infracción de seguridad cuando un usuario malintencionado consigue traspasar el servidor de seguridad. Las medidas de seguridad sólo funcionarán correctamente si los usuarios no tienen que llevar a cabo muchos procedimientos y pasos para hacer su trabajo de manera segura. La implementación de directivas de seguridad debe ser lo más sencilla posible para los usuarios. De lo contrario, tenderán a buscar formas menos seguras de hacer las cosas.

Recomendaciones de seguridad para Microsoft Dynamics™ NAV

En esta sección se explican las recomendaciones que se deben adoptar al ejecutar Microsoft Dynamics NAV. Las siguientes reglas generales pueden ayudar a aumentar la seguridad del entorno Dynamics NAV.

Microsoft Dynamics NAV puede utilizar tanto Microsoft® SQL Server y C/SIDE Database Server para Dynamics NAV como el servidor de base de datos. Se recomienda utilizar Windows Server™ 2003 R2 como sistema operativo para el servidor de base de datos en una instalación de cliente/servidor de Dynamics NAV. También puede utilizar Windows Vista™ y Windows™ XP como el sistema operativo de servidor de base de datos para instalaciones más pequeñas.

C/SIDE Database Server para Dynamics NAV y TCPS

Se recomienda utilizar el protocolo de seguridad TCPS para la comunicación entre los clientes de Dynamics NAV y C/SIDE Database Server. TCPS es una versión segura de TCP/IP que utiliza la Interfaz de proveedor de compatibilidad de seguridad (SSPI, *Security Support Provider Interface*) con cifrado habilitado y autenticación Kerberos.

TCPS es el protocolo predeterminado para C/SIDE Database Server.

TCPS es un protocolo estricto y sólo le permitirá iniciar sesión en C/SIDE Database Server si:

- el equipo que está utilizando pertenece al mismo dominio que el servidor.
- la cuenta de usuario que está usando es una cuenta de dominio de Windows del mismo dominio que el servidor y tiene asignadas funciones en la base de datos.

Si ejecuta C/SIDE Database Server como un servicio en el equipo servidor, **debe** ejecutar el servicio como la cuenta NT Authority\Network Service (en Windows Vista esta cuenta se llama Servicio de red) o la cuenta del sistema local. Esto significa que no puede ejecutar el servidor desde el indicador de comandos si está utilizando TCPS como protocolo de red.

Al ejecutar C/SIDE Database Server como un servicio en Windows™2000, **sólo** puede utilizar la cuenta de sistema local.

Para obtener el nivel de seguridad más alto y aprovechar los beneficios del protocolo TCPS, recomendamos que ejecute C/SIDE Database Server en Windows Server 2003, Windows Vista o en Windows XP y utilice TCPS como el protocolo de red.

Hacer que el servicio de servidor sea seguro

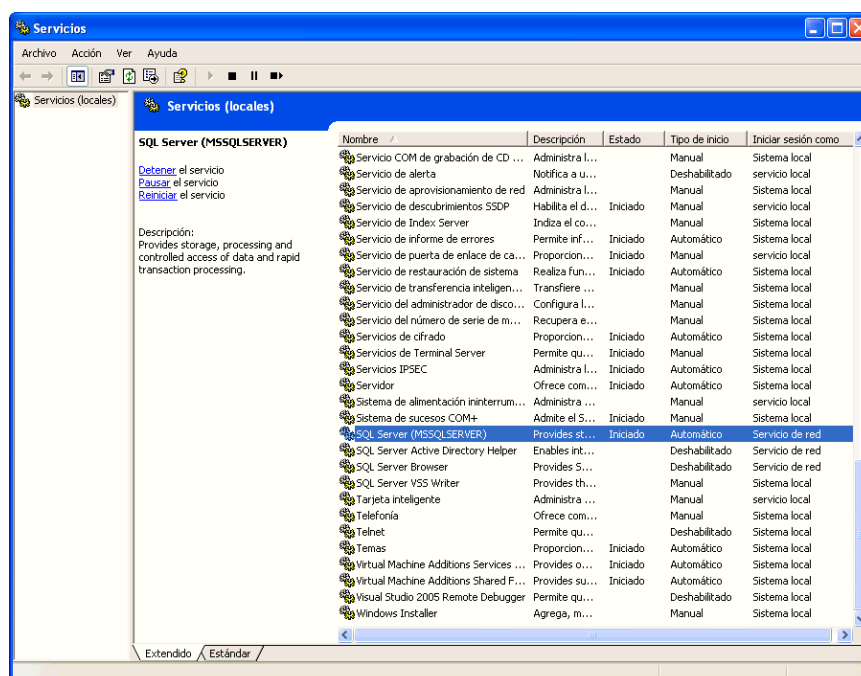
Al ejecutar Dynamics NAV en una instalación de cliente/servidor, el servidor de base de datos generalmente se ejecuta como un servicio y **debe** asegurarse de que este servicio se configura de manera segura.

SQL Server

Si está ejecutando Dynamics NAV en SQL Server, SQL Server se ejecuta como un servicio. De manera predeterminada, el servicio SQL Server utiliza la cuenta de sistema local. Sin embargo, se recomienda ejecutar el servicio SQL Server como la cuenta NT Authority\Network Service.

Para asegurarse de que el servicio se ejecuta como NT Authority\Network Service:

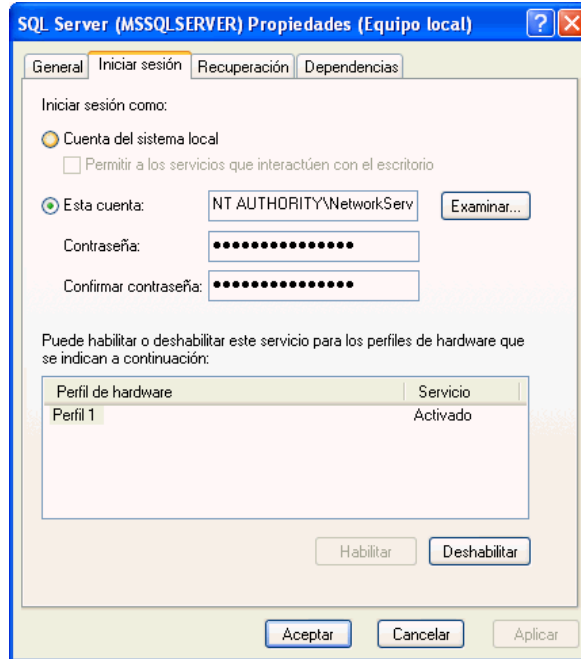
1. En el equipo SQL Server, haga clic en Inicio, Panel de control, Herramientas administrativas, Servicios para abrir la ventana **Servicios**.



Ventana Servicios

2. Desplácese hacia abajo y seleccione el servicio. Si sólo hay una instancia de SQL Server, el servicio se llama MSSQLSERVER. Haga clic en el servicio con el botón secundario del Mouse (ratón) y seleccione Propiedades para abrir la ventana **Propiedades**.

3. En la ventana **Propiedades**, haga clic en la ficha **Iniciar sesión**:



Ventana Propiedades del Servicio SQL Server

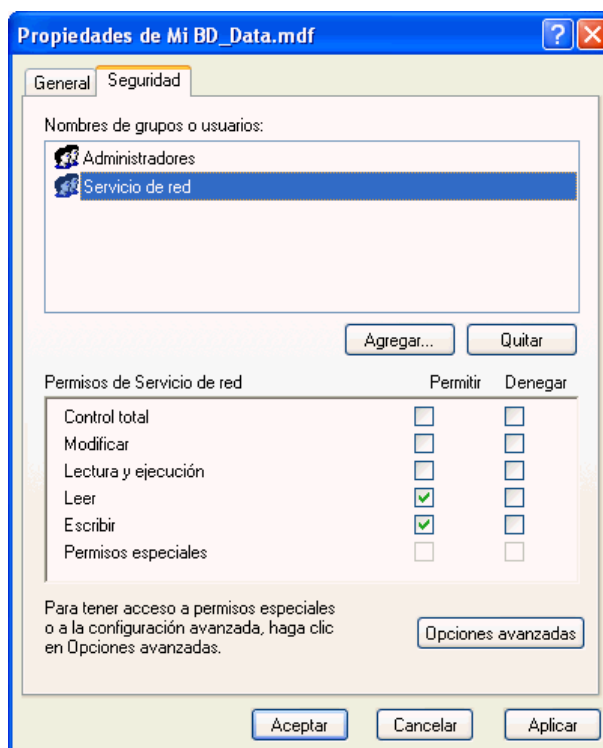
4. En la ficha **Iniciar sesión**, en Iniciar sesión como; haga clic en Esta cuenta; escriba *NT Authority\Network Service* y haga clic en Aceptar. En Windows Vista, escriba Servicio de red y haga clic en Aceptar.

Para garantizar que los usuarios se pueden conectar a la base de datos, **debe** proporcionar a la cuenta NT Authority\Network Service bajo la que el servidor se está ejecutando permiso de lectura y escritura a los archivos de la base de datos.

Para proporcionar a la cuenta NT Authority\Network Service permiso de lectura y escritura a los archivos de la base de datos de un servidor de base de datos:

1. Abra el Explorador de Windows y vaya a la carpeta que contiene el archivo de base de datos.
2. Seleccione el archivo, haga clic en él con el botón secundario del *mouse* y haga clic en Propiedades.
3. En la ventana **Propiedades**, haga clic en la ficha **Seguridad** y, en el campo **Nombres de usuario y grupo**, haga clic en Agregar.
4. En la ventana *Seleccionar usuarios, equipos o grupos*, escriba *Servicio de red* y haga clic en Aceptar.
5. **SERVICIO DE RED** se ha agregado al campo **Nombres de usuario y grupo** de la ventana **Propiedades**.

6. Seleccione **SERVICIO DE RED** y, en el campo **Permisos**, seleccione los permisos de lectura y escritura.



Ventana Propiedades de la base de datos

Para obtener más información sobre la seguridad, visite el [sitio web sobre seguridad de SQL Server](#) y TechNet para obtener más [información sobre seguridad de SQL Server](#).

C/SIDE Database Server para Microsoft Dynamics NAV

Al instalar C/SIDE Database Server o utilizar el parámetro de la línea de comandos `installservice` para configurar el servidor, el servicio del servidor se ejecuta como la cuenta NT Authority\Network Service de manera predeterminada. La cuenta NT Authority\Network Service sólo existe en Windows Server 2003 y Windows XP. En Windows Vista, esta cuenta se llama Servicio de red.

Si utiliza Windows 2000 Server el servicio de servidor se ejecuta como la cuenta Sistema local.

Si no está usando TCPS, es recomendable que cree una cuenta con los mínimos privilegios para el servicio. Como máximo, esta cuenta debe tener los mismos privilegios que la cuenta Usuarios normal o ser una cuenta de dominio que no sea un administrador del dominio ni de ningún equipo local. En la sección anterior se explica el procedimiento para asegurarse de que el servicio se ejecuta como la cuenta NT Authority\Network Service.

Debe recordar que tiene que otorgar a la cuenta NT Authority\Network Service, o a la cuenta de usuario con la que se ejecuta el servidor, acceso de lectura y escritura a los archivos de base de datos para asegurar que los usuarios pueden conectar a la base de datos. También se explica en la sección anterior cómo hacerlo.

Servidor de aplicaciones para Microsoft Dynamics NAV

El servicio Dynamics NAV Application Server se ejecuta como la cuenta NT Authority\Network Service de manera predeterminada y esto permite obtener acceso a C/SIDE Database Server de manera local. Sin embargo, en una red debe asegurarse de que el servicio Dynamics NAV Application Server se está ejecutando como una cuenta de dominio de Windows reconocida por C/SIDE Database Server si desea que obtenga acceso al servidor de base de datos. Esta cuenta no debe ser un administrador del dominio ni de ningún equipo local.

Automated Data Capture System para Microsoft Dynamics NAV

Si está utilizando el sistema de captura de datos automatizada Automatic Data Capture System de Dynamics NAV, utilícelo en redes inalámbricas cifradas.

Dynamics NAV Employee Portal

Si está ejecutando Dynamics NAV Employee Portal, utilice HTTPS como el protocolo de red para la instalación de NEP y obtener así un más seguridad.

HTTPS (HyperText Transport Protocol Secure) es el protocolo para obtener acceso a un servidor Web seguro. Si se utiliza HTTPS en la dirección URL en lugar de HTTP, se reenvía el mensaje a un número de puerto seguro en lugar de al número de puerto web predeterminado 80. A continuación, un protocolo de seguridad como SSL administra la sesión.

Contraseñas y acceso a la base de datos

Utilice siempre contraseñas seguras. Para obtener más información sobre contraseñas seguras, consulte la sección Contraseñas seguras.

Las contraseñas no se deben reutilizar. Es una práctica habitual reutilizar las contraseñas entre sistemas y dominios. Por ejemplo, un administrador encargado de dos dominios puede crear cuentas de Administrador de dominio en cada uno que utilicen la misma contraseña e incluso establecer contraseñas de administrador local en equipos del dominio que sean iguales en el dominio. En ese caso, si se produce una situación de riesgo con una cuenta o un equipo, puede poner en peligro el dominio entero.

Una vez que Dynamics NAV está instalado y la base de datos se ha adjuntado, cree un inicio de sesión de Windows para el administrador de la base de datos y asígnele el rol SUPER en Dynamics NAV. El usuario SUPER se encargará de la administración de bases de datos, la seguridad, etc. En Dynamics NAV sólo se debe asignar el rol SUPER a los usuarios que necesiten realizar este tipo de tareas administrativas.

El resto de usuarios con acceso a la base de datos Dynamics NAV deben ejecutar la aplicación con menos privilegios. Esto significa que se les deben asignar roles en Dynamics NAV para obtener acceso a características y a funcionalidad con la que puedan realizar sus tareas en la compañía.

Asegúrese de que sólo los usuarios cuya función en la empresa lo requiera pueden importar archivos FOB así como crear y restaurar copias de seguridad de base de datos.

Copias de seguridad

Realice copias de seguridad frecuentemente de la base de datos de Dynamics NAV y recuerde comprobar dichas copias para asegurarse de que se pueden restaurar correctamente.

Almacene las copias de seguridad en un lugar seguro para salvaguardarlas de robos y modificaciones así como para limitar el impacto de peligros como fuego, humo, polvo, altas temperaturas, descargas eléctricas y desastres medioambientales (por ejemplo terremotos).

Sistema operativo y actualizaciones

Aunque Dynamics NAV se puede ejecutar en varias versiones de Windows, se recomienda utilizar los sistemas operativos más recientes con las características de seguridad más actualizadas. Los sistemas operativos más recientes son Server 2003 R2, Windows Vista y el Service Pack 2 de Windows XP.

Utilice el servicio de Windows Update proporcionado por Microsoft para aplicar las actualizaciones de seguridad más recientes. Utilice la característica de actualización automática de Windows para mantener actualizados todos los equipos cliente con las actualizaciones de seguridad y los Service Pack más recientes.

Archivos de licencia

Si está ejecutando C/SIDE Database Server para Dynamics NAV, guarde el archivo de licencia en lugar seguro donde no se pueda modificar ni sustraer fácilmente.

Si está ejecutando la Opción SQL Server, la licencia se almacena de manera segura en el servidor.

Plan de recuperación

Debe disponer de un plan de recuperación de desastres que asegure la reanudación rápida de los servicios tras un desastre. Un plan de recuperación debe incluir aspectos como los siguientes:

- Adquisición de equipamiento nuevo o temporal
- Restauración de copias de seguridad en los nuevos sistemas
- Comprobación de que el plan de recuperación funciona realmente

Seguridad física

La seguridad física es absolutamente esencial, ya que no hay ninguna forma de complementarla con seguridad de software. Por ejemplo, si se roba una unidad de disco duro, también se robarán los datos que contiene. Teniendo esto en cuenta:

- Mantenga los equipos fuera del alcance de los usuarios no autorizados.
- Asegúrese de instalar alarmas antirrobo, con independencia del nivel de confidencialidad de los datos.
- Asegúrese de que las copias de seguridad de los datos cruciales se almacenan fuera del sitio y que las copias de seguridad se guardan en contenedores ignífugos.

Empleados

Es conveniente limitar los derechos administrativos en todos los productos y características. De forma predeterminada, la empresa sólo deben conceder a los empleados acceso de lectura a las funciones del sistema, salvo que requieran otros privilegios para realizar su trabajo. Microsoft recomienda seguir el principio de privilegios mínimos: conceder a los usuarios sólo los privilegios necesarios para tener acceso a los datos y la funcionalidad.

Los empleados descontentos y los que ya no trabajan en la empresa son una amenaza para la seguridad de la red. Teniendo esto en cuenta:

- Lleve a cabo investigaciones de antecedentes laborales.
- Prevea "venganzas" de los empleados descontentos y los que ya no trabajan en la empresa.
- Asegúrese de que deshabilita todas las cuentas de Windows y contraseñas asociadas cuando un empleado abandona la empresa. A efectos de informes, no elimine los usuarios. No reutilice las cuentas.
- Proporcione entrenamiento a los usuarios para que estén alerta ante actividades sospechosas e informen de ellas.
- No conceda privilegios de forma automática. Si los usuarios no necesitan tener acceso a determinados equipos, salas de equipos o conjuntos de archivos, asegúrese de que no lo tengan.
- Proporcione entrenamiento a los supervisores para identificar y responder ante posibles problemas con los empleados.
- Asegúrese de que los empleados conocen su función en el mantenimiento de la seguridad de la red.
- Dé una copia de las directivas de la compañía a todos los empleados.
- No permita que los usuarios instalen software que no esté autorizado por los responsables.

Administrador

Se recomienda que los administradores del sistema se mantengan informados de las correcciones de seguridad más recientes disponibles en Microsoft. Los atacantes son muy hábiles en la combinación de pequeños errores para realizar intrusiones a gran escala en una red. En primer lugar, los administradores deben asegurarse de que cada equipo es lo más seguro posible y, después, deben agregar las actualizaciones de seguridad y utilizar software antivirus. En esta guía se ofrecen multitud de vínculos y recursos para ayudarle a buscar información valiosa y prácticas recomendadas.

La complejidad es otro de los inconvenientes para proteger la red. Cuanto más compleja sea la red, más difícil será protegerla o solucionar los problemas después de que un intruso haya conseguido obtener acceso. El administrador debe crear documentos de la topografía completa de la red, con el objetivo de mantener la máxima sencillez posible.

La seguridad está principalmente relacionada con la administración del riesgo. Como la tecnología no es la solución a todos los problemas, la seguridad exige una combinación de tecnología y directivas. Dicho de otra forma, nunca habrá un producto que simplemente pueda desempaquetar e instalar en la red, y que proporcione al instante una seguridad perfecta. La seguridad es el resultado de combinar tecnología y directivas, es decir, es la *manera* en que se utiliza la tecnología que determina en última instancia el nivel de seguridad de una red. Microsoft proporciona tecnología y características que tienen en cuenta la seguridad, pero sólo el administrador puede determinar las directivas correctas para cada organización. Asegúrese de planear la seguridad al principio del proceso de implementación. Debe conocer qué desea proteger y qué está dispuesto a hacer para protegerlo.

Por último, desarrolle planes de contingencias para posibles emergencias antes de que sucedan. Combine planes exhaustivos con tecnología sólida para disfrutar de la máxima seguridad.

Para obtener más información sobre seguridad en general, consulte el artículo [10 leyes inmutables de la seguridad](#) (en inglés) y los artículos sobre administración de seguridad en las columnas de [Microsoft Technet – Viewpoint](#) (en inglés).

Protección del sistema operativo de servidor

Aunque es posible que muchos pequeños clientes no tengan un sistema operativo de servidor, es importante que conozca las prácticas recomendadas de seguridad que utilizan los grandes clientes que tienen entornos de red más complejos. Tenga en cuenta que muchas de las directivas y prácticas descritas en este documento se pueden aplicar fácilmente incluso si sólo tiene sistemas operativos cliente.

Los conceptos que se describen en esta sección se aplican tanto a productos de Microsoft Windows Server 2003 como a productos de Microsoft Windows 2000 Server, aunque esta información se ha extraído principalmente de la ayuda en línea de Windows Server 2003. Windows Server 2003 ofrece un conjunto sólido de características de seguridad. La ayuda en línea de Windows Server 2003 contiene información completa acerca de todas las características y todos los procedimientos de seguridad.

Para obtener información adicional acerca de Windows Server 2003, visite [Windows Server TechCenter](#).

Para obtener información adicional acerca de Windows 2000 Server, visite [Windows 2000 Server en TechNet](#).

Las características principales del modelo de seguridad de servidor de Windows son la autenticación, el control de acceso y el inicio de sesión único:

- La autenticación es el proceso mediante el cual el sistema valida la identidad de un usuario utilizando sus credenciales de inicio de sesión. El nombre y la contraseña del usuario se comparan con los datos de una lista autorizada. Si el sistema detecta una coincidencia, la autorización concede acceso al usuario en la medida especificada en la lista de permisos para dicho usuario.
- El control de acceso limita el acceso del usuario a información o recursos informáticos en función de su identidad y su pertenencia a varios grupos predefinidos. En general, el control de acceso lo utilizan los administradores de sistemas para controlar el acceso de los usuarios a los recursos de la red, como servidores, directorios y archivos. Generalmente se implementa mediante la concesión de permiso a usuarios y grupos para tener acceso a objetos específicos.
- El inicio de sesión único permite que un usuario inicie sesión en el dominio de Windows una vez, con una sola contraseña, y se autentique en cualquier equipo del dominio de Windows. El inicio de sesión único permite a los administradores implementar la autenticación mediante contraseña en toda la red Windows, al tiempo que proporciona a los usuarios finales facilidad de acceso.

En las siguientes secciones se ofrece una descripción más detallada de estas tres características clave.

Autenticación

La autenticación es un aspecto fundamental de la seguridad del sistema y se utiliza para confirmar la identidad de cualquier usuario que intenta iniciar sesión en un dominio o tener acceso a los recursos de la red. El punto más débil de la mayoría de los sistemas de autenticación es la contraseña del usuario.

Las contraseñas proporcionan la primera línea de defensa contra el acceso no autorizado al dominio y los equipos locales. Es conveniente usar las siguientes prácticas recomendadas:

- Utilice siempre contraseñas seguras.
- Si las contraseñas deben escribirse en un papel, guarde el papel en un lugar seguro y destrúyalo cuando ya no sea necesario.
- No revele nunca las contraseñas a nadie.
- Utilice diferentes contraseñas para todas las cuentas de usuario.
- Cambie las contraseñas periódicamente.
- Tenga cuidado de dónde se guardan las contraseñas en los equipos.

Contraseñas seguras

La función que desempeñan las contraseñas en la protección de la red de una organización suele subestimarse y pasarse por alto. Como se mencionó anteriormente, las contraseñas proporcionan la primera línea de defensa contra el acceso no autorizado a la red. Por lo tanto, debe indicar a sus empleados que utilicen contraseñas seguras.

Sin embargo, las herramientas para descubrir contraseñas son cada vez mejores y los equipos que se utilizan para ello son más eficaces que nunca. Si se le da tiempo suficiente, una herramienta automatizada puede descubrir cualquier contraseña. No obstante, las contraseñas seguras son mucho más difíciles de descubrir que las no seguras.

Para conocer las instrucciones acerca de cómo crear contraseñas seguras, consulte [Contraseñas seguras: cómo crearlas y utilizarlas](#) (en inglés) y las [normas para crear contraseñas seguras](#) (en inglés).

Definición de la directiva de contraseñas

Cuando defina su directiva de contraseñas, asegúrese de crear una directiva que exija que todas las cuentas de usuario tengan contraseñas seguras. Para la mayoría de los sistemas, bastan las siguientes recomendaciones de la Guía de seguridad de Windows Server 2003:

- Defina la configuración de directiva **Forzar el historial de contraseñas** para que se recuerden varias contraseñas anteriores. Con esta configuración de directiva, los usuarios no pueden utilizar la misma contraseña cuando ésta caduca.
Configuración recomendada: 24
- Defina la configuración de directiva **Vigencia máxima de la contraseña** para que las contraseñas caduquen con la frecuencia necesaria en el entorno del cliente.
Configuración recomendada: entre 42 (predeterminado) y 90.

- Defina la configuración de directiva **Vigencia mínima de la contraseña** para que las contraseñas no se puedan cambiar hasta que transcurra un determinado número de días. Esta configuración de directiva funciona en combinación con la configuración de directiva **Forzar el historial de contraseñas**. Si se define una vigencia mínima de la contraseña, los usuarios no pueden cambiar repetidamente sus contraseñas para eludir la configuración de directiva **Forzar el historial de contraseñas** y, después, utilizar sus contraseñas originales. Los usuarios deben esperar el número de días especificado para cambiar su contraseña.
Configuración recomendada: 2
- Defina una configuración de directiva **Longitud mínima de la contraseña** de forma que las contraseñas deban estar formadas por un número mínimo de caracteres especificado. Las contraseñas largas, de siete caracteres o más, suelen ser más seguras que las cortas. Con esta configuración de directiva, los usuarios no pueden utilizar contraseñas en blanco y deben crear contraseñas que tengan al menos un determinado número de caracteres de longitud.
Configuración recomendada: 8
- Habilite la configuración de directiva **Las contraseñas deben cumplir los requerimientos de complejidad**. Esta configuración de directiva comprueba todas las contraseñas nuevas para asegurar que se cumplen los requisitos básicos de seguridad de las contraseñas. Este valor garantiza que las contraseñas tengan al menos tres símbolos de las cuatro categorías (mayúsculas, minúsculas, números y símbolos no alfanuméricos) y que no contenga ninguna porción del nombre de usuario ni los apellidos del mismo.
Configuración recomendada: Sí

Nota

Las contraseñas que cumplen estos requisitos no son necesariamente muy seguras. Por ejemplo, la contraseña "Contraseña1" cumple estos requisitos.

Para ver una lista de estos requisitos, consulte "Las contraseñas deben cumplir los requerimientos de complejidad" en la Ayuda en pantalla de Windows Server.

- **Almacene contraseñas con cifrado reversible:** el cifrado reversible se utiliza en sistemas donde una aplicación necesita obtener acceso a contraseñas no cifradas. En la mayoría de las implementaciones no es necesario.
Configuración recomendada: No

Definición de una directiva de bloqueo de cuentas

Tenga cuidado al definir la directiva de bloqueo de cuentas. Esta directiva no debe establecerse nunca en una pequeña empresa, ya que es bastante probable que bloquee a los usuarios autorizados, lo que puede resultar muy costoso.

Si decide aplicar una directiva de bloqueo de cuentas, establezca la configuración **Umbral de bloqueos de la cuenta** en un número alto para que las cuentas de los usuarios autorizados no se queden bloqueadas simplemente por escribir incorrectamente su contraseña varias veces.

Para obtener más información acerca de la directiva de bloqueo de cuentas, consulte "Introducción a la directiva de bloqueo de cuentas" en la Ayuda en pantalla de Windows Server.

Para obtener información acerca de cómo aplicar o modificar la directiva de bloqueo de cuentas, consulte "Para aplicar o modificar la directiva de bloqueo de cuentas" en la Ayuda en pantalla de Windows Server.

Control de acceso

Una red de Windows y sus recursos (incluido Dynamics NAV) se pueden asegurar si se tienen en cuenta los derechos que tienen usuarios, grupos de usuarios y otros equipos en la red. Puede proteger un equipo o varios concediendo derechos de usuario específicos a los usuarios o grupos. Puede proteger un objeto, como un archivo o una carpeta, mediante la asignación de permisos con los que los usuarios o grupos puedan realizar acciones específicas en dicho objeto. Los conceptos clave que componen el control de acceso incluyen:

- Permisos
- Propiedad de los objetos
- Herencia de permisos
- Derechos de usuario
- Auditoría de objetos

Permisos

Los permisos definen el tipo de acceso que se concede a un usuario o grupo para un objeto o propiedad de objeto, como archivos, carpetas y objetos del Registro. Los permisos se aplican a cualquier objeto protegido, como los archivos y los objetos del Registro. Los permisos se pueden conceder a cualquier usuario, grupo o equipo. Es conveniente asignar permisos a los grupos.

Propiedad de los objetos

Cuando se crea un objeto se le asigna un propietario. De forma predeterminada en Windows 2000 Server, el propietario es el creador del objeto. Esto ha cambiado en Windows Server 2003 para objetos creados por miembros en el grupo Administradores.

Cuando un miembro del grupo Administradores crea un objeto en Windows Server 2004, dicho grupo pasa a ser el propietario en lugar de la cuenta individual que creó el objeto. Este comportamiento se puede modificar mediante el complemento MMC (Microsoft Management Console) Configuración de seguridad local, utilizando la configuración **Objetos de sistema: propietario predeterminado para objetos creados por miembros del grupo de administradores**. Con independencia de qué permisos se establezcan en un objeto, su propietario siempre puede cambiarlos.

Para obtener más información, consulte "Posesión" en la Ayuda en pantalla de Windows Server.

Herencia de permisos

La herencia permite que los administradores asignen y administren de forma sencilla los permisos. Esta característica causa automáticamente que los objetos de un contenedor hereden todos los permisos posibles de ese contenedor. Por ejemplo, al crear archivos en una carpeta, heredan los permisos de la carpeta. Sólo se heredan los permisos marcados para herencia.

Derechos de usuario

Los derechos de usuario conceden privilegios y derechos de inicio de sesión específicos a usuarios y grupos del entorno informático.

Para obtener información acerca de los derechos de usuario, consulte "Derechos de usuario" en la Ayuda en pantalla de Windows Server.

Auditoría de objetos

El acceso de los usuarios a los objetos se puede auditar. Después, puede ver los sucesos relacionados con la seguridad en el registro de seguridad mediante el Visor de sucesos.

Para obtener más información, consulte "Auditoría" en la Ayuda en pantalla de Windows Server.

Prácticas recomendadas de control de acceso

- Asigne permisos a los grupos en lugar de a los usuarios. Puesto que no es eficaz mantener directamente las cuentas de usuario, la asignación de permisos por usuario debe llevarse a cabo excepcionalmente.
- Utilice permisos Denegar en casos especiales. Por ejemplo, puede utilizarlos para excluir un subconjunto de un grupo que tiene permisos Permitir.
- Nunca deniegue al grupo Todos el acceso a un objeto. Si deniega a todos el permiso para un objeto, incluirá también a los administradores. Una solución mejor sería quitar el grupo Todos, a condición de que conceda a otros usuarios, grupos o equipos los permisos para ese objeto. Recuerde que si no hay definidos permisos, no se permite el acceso.
- Asigne los permisos para un objeto en la parte más alta posible del árbol y, después, aplique la herencia para propagar la configuración de seguridad por el árbol. Puede aplicar de forma rápida y eficaz la configuración de control de acceso a todos los elementos secundarios o a un subárbol de un objeto principal. De esa manera, obtendrá el máximo efecto con el mínimo esfuerzo. La configuración de permisos que establezca debe ser adecuada para la mayoría de los usuarios, grupos y equipos.
- En ocasiones, los permisos explícitos pueden reemplazar a los permisos heredados. Los permisos Denegar heredados no impiden el acceso a un objeto si éste tiene una entrada de permiso explícito Permitir. Los permisos explícitos tienen preferencia sobre los permisos heredados, incluidos los permisos Denegar heredados.
- Para los permisos en objetos de Active Directory® asegúrese de que comprende las recomendaciones específicas para objetos de Active Directory.

Para obtener más información, consulte la sección sobre recomendaciones para asignar permisos en objetos de Active Directory de la ayuda en línea de Windows Server 2003.

Servidor de seguridad externo

Un servidor de seguridad es hardware o software que impide que los paquetes de datos entren o salgan de una red determinada. Para controlar el flujo de tráfico, los puertos del servidor de seguridad están abiertos o cerrados para los paquetes de información. El servidor de seguridad examina diversas partes de información en cada paquete de datos: el protocolo mediante el que el paquete se va a entregar, el destino o el remitente del paquete, el tipo de contenido del paquete y el número de puerto al que se envía. Si el servidor de seguridad está configurado para aceptar el protocolo especificado a través del puerto de destino, se permite el paso del paquete. Microsoft Windows Small Business Server 2003 Premium Edition incluye Microsoft Internet Security and Acceleration (ISA) Server 2000 como su solución de firewall. Small Business Server Standard Edition también incluye un firewall.

ISA Server 2006

Internet Security and Acceleration (ISA) Server 2006 enruta de forma segura las solicitudes y respuestas entre Internet y los equipos cliente de la red interna.

El servidor ISA Server actúa como una puerta de enlace de seguridad con Internet para los clientes de la red local. El equipo con ISA Server es transparente para las otras partes de la ruta de comunicación. El usuario de Internet no debería saber si hay un servidor de seguridad presente, salvo que intente tener acceso a un servicio o ir a un sitio al que el equipo con ISA Server le deniega el acceso. El servidor de Internet al que se tiene acceso interpreta las solicitudes del equipo ISA Server como si éstas tuvieran origen en la aplicación cliente.

Al elegir el filtrado de fragmentos de Protocolo Internet (IP) se permite que los servicios Proxy Web y Servidor de seguridad filtren fragmentos de paquetes. Mediante el filtrado de fragmentos de paquetes, todos los paquetes IP fragmentados se descartan. Un "ataque" muy conocido utiliza el envío de paquetes fragmentados que luego se ensamblan de nuevo de forma que pueden causar daños en el sistema.

ISA Server incluye un mecanismo de detección de intrusiones que identifica la hora en que se intenta un ataque contra una red y lleva a cabo un conjunto de acciones (o alertas) configuradas por si se produce un ataque.

Si Servicios de Internet Information Server (IIS) está instalado en el equipo con ISA Server, debe configurarlo para que no use los puertos que ISA Server utiliza para las solicitudes Web salientes (de forma predeterminada, 8080) y entrantes (de forma predeterminada, 80). Por ejemplo, puede modificar IIS para que supervise el puerto 81 y, después, configurar el equipo con ISA Server para dirigir las solicitudes Web entrantes al puerto 81 del equipo local en el que se ejecuta IIS.

Si se produce un conflicto entre los puertos que ISA Server e IIS utilizan, el programa de configuración detiene el servicio de publicación de IIS. Después, puede modificar IIS para que supervise un puerto diferente y reiniciar el servicio de publicación de IIS.

Directivas de ISA Server

Puede definir una directiva de ISA Server que determine el acceso de entrada y salida. Las reglas de sitio y contenido especifican a qué sitios y a qué contenido se puede tener acceso. Las reglas de protocolo indican si se puede tener acceso a un protocolo determinado para la comunicación entrante y saliente.

Puede crear reglas de sitio y contenido, reglas de protocolo, reglas de publicación en Web y filtros de paquetes IP. Estas directivas determinan cómo se comunican los clientes de ISA Server con Internet y qué comunicación se permite.

Protección antivirus

Un virus informático es un archivo ejecutable diseñado para replicarse a sí mismo, borrar o dañar archivos de datos y programas, y evitar su detección. De hecho, los virus suelen reescribirse y ajustarse para que no se puedan detectar. Es frecuente que los virus se envíen como datos adjuntos de correo electrónico. Los programas antivirus deben actualizarse constantemente para poder buscar virus nuevos y modificados. Los virus son el principal método de vandalismo informático.

El software antivirus está especialmente diseñado para la detección y prevención de los programas de virus. Como se crean continuamente nuevos programas de virus, muchos fabricantes de productos antivirus ofrecen a los clientes actualizaciones periódicas de su software. Microsoft recomienda encarecidamente el uso de software antivirus en todos los equipos.

El software antivirus suele instalarse en estos tres lugares: las estaciones de trabajo de los usuarios, los servidores y la red donde el correo electrónico entra (y, en algunos casos, sale) en la organización.

Tipos de virus

Existen tres tipos principales de virus que infectan los equipos: virus del sector de inicio, virus de infección de archivos y programas troyanos.

Virus del sector de inicio

Al iniciar un equipo, se analiza el sector de inicio del disco duro antes de cargar el sistema operativo o los archivos de inicio. Los virus del sector de inicio están diseñados para reemplazar la información del sector de inicio de los discos duros por su propio código. Cuando un equipo se infecta con este tipo de virus, el código del virus se lee en la memoria antes que todo lo demás. Una vez que el virus está en la memoria, puede replicarse en cualquier otro disco que esté en uso en el equipo infectado.

Virus de infección de archivos

El tipo más común de virus, el virus de infección de archivos, se adjunta a un archivo de programa ejecutable agregando su propio código. El código del virus suele agregarse de forma que evita la detección. Cuando se ejecuta el archivo infectado, el virus puede adjuntarse a otros archivos ejecutables. Los archivos que se infectan con este tipo de virus suelen tener la extensión .com, .exe o .sys.

Algunos virus de infección de archivos están diseñados para programas específicos. Los tipos de programas que suelen ser objeto de ataques son los archivos de superposición (.ovl) y los archivos de biblioteca de vínculos dinámicos (.dll). Aunque estos archivos no se ejecutan, los ejecutables los llaman. El virus se transmite cuando se realiza la llamada.

Los daños en los datos tienen lugar cuando se activa el virus. Un virus puede activarse al ejecutar un archivo infectado o cuando se cumple una condición determinada en el entorno (por ejemplo, una fecha específica del sistema).

Programas troyanos

En realidad, un programa troyano no es un virus. La distinción fundamental entre un virus y un programa troyano es que el troyano no se replica a sí mismo, sólo destruye información en el disco duro. El troyano se disfraza como un programa legítimo, por ejemplo un juego o una utilidad. Sin embargo, al ejecutarse puede destruir o estropear datos.

Prácticas recomendadas de protección antivirus

La difusión de un virus de macro se puede impedir. A continuación se ofrecen algunas sugerencias para evitar las infecciones:

- Instale una solución de protección antivirus que busque virus en los mensajes entrantes de Internet antes de que éstos pasen por el enrutador. De esta forma se asegura que se han analizado los mensajes de correo electrónico en busca de virus conocidos.
- Observe el origen de los documentos que se reciben. Los documentos no deben abrirse salvo que procedan de un remitente que considere de confianza.
- Hable con la persona que ha creado el documento. Si los usuarios no están totalmente convencidos de que el documento sea seguro, deben ponerse en contacto con la persona que ha creado el documento.
- Use la protección antivirus en macros de Microsoft Office. En Office, las aplicaciones alertan al usuario si un documento contiene macros. Esta característica permite que el usuario habilite o deshabilite las macros al abrir el documento.
- Utilice software de detección de virus para detectar y eliminar los virus de macro. El software de detección de virus puede detectar y generalmente eliminar los virus de macro de los documentos. Microsoft recomienda el uso de software antivirus que esté certificado por ICSA (*International Computer Security Association*).

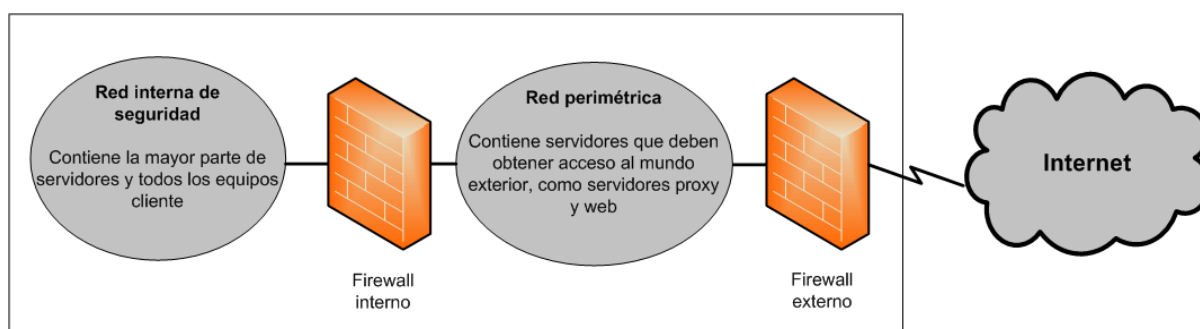
Para obtener más información sobre virus y seguridad en el equipo en general, visite:

- Microsoft Security en [Security Central](#)
- Seguridad en [Microsoft TechNet](#)

Estrategias de seguridad de red

Como el diseño y la implementación de un entorno de trabajo en redes IP requieren un equilibrio entre posibles problemas de redes públicas y privadas, el servidor de seguridad se ha convertido en un componente clave para salvaguardar la integridad de la red. Un servidor de seguridad no es un solo componente. La definición de servidor de seguridad de NCSA (*National Computer Security Association*) es "un sistema o combinación de sistemas que impone un límite entre dos o más redes". Aunque se utilizan diferentes términos, dicho límite se conoce habitualmente como "red perimetral". La red perimetral protege la intranet o la red de área local (LAN) contra intrusiones mediante el control del acceso desde Internet u otras redes de gran tamaño. A una red perimetral se la conoce a menudo como DMZ (la zona desmilitarizada).

En el siguiente diagrama se muestra una red perimetral flanqueada por servidores de seguridad y situada entre una red privada e Internet con el fin de proteger la red privada:



El enfoque del uso de servidores de seguridad como medida de protección varía según la organización. El filtrado de paquetes IP ofrece una seguridad deficiente, es complicado de administrar y se puede vencer con facilidad. Las puertas de enlace de aplicación son más seguras que los filtros de paquetes y más sencillas de administrar porque sólo pertenecen a unas pocas aplicaciones específicas, por ejemplo un sistema determinado de correo electrónico. Las puertas de enlace de circuitos son muy eficaces cuando el usuario de una aplicación de red es una preocupación mayor que los datos que transfiere dicha aplicación. El servidor proxy es una herramienta de seguridad completa que incluye una puerta de enlace de aplicación y acceso seguro para los usuarios anónimos, entre otros servicios. A continuación se ofrece información sobre las diferentes opciones:

- **Filtrado de paquetes IP**

El filtrado de paquetes IP es la primera implementación de la tecnología firewall.

Los encabezados de los paquetes se examinan en busca de las direcciones de origen y destino, y los puertos de Protocolo de control de transporte (TCP) y de Protocolo de datagramas de usuario (UDP) así como otro tipo de información. El filtrado de paquetes es una tecnología limitada que funciona correctamente en entornos de seguridad clara en los que, por ejemplo, todo lo que está fuera de la red perimetral no es de confianza y todo lo que está dentro sí. En los últimos años, varios proveedores han mejorado el método de filtrado de paquetes al agregar características de decisión inteligentes a la base de filtrado de paquetes; así se crea una nueva forma de filtrado de paquetes denominada inspección de protocolo con estado. Puede configurar el filtrado de paquetes para aceptar tipos específicos de paquetes a la vez que se rechazan todos los demás o para rechazar tipos específicos de paquetes y aceptar todos los demás.

- **Puertas de enlace de aplicaciones**

Las puertas de enlace de las aplicaciones se utilizan cuando el contenido real de una aplicación es muy importante. El hecho de que son específicas de aplicaciones es a la vez una ventaja y un inconveniente, ya que no se adaptan fácilmente a los cambios en la tecnología.

- **Puertas de enlace de circuitos**

Las puertas de enlace de circuitos son túneles creados a través de un firewall que conecta procesos o sistemas específicos por un lado con procesos o sistemas específicos por el otro. Las puertas de enlace de circuitos son muy útiles en situaciones en las que la persona que utiliza una aplicación es un riesgo potencialmente mayor que la información que transporta la aplicación. La puerta de enlace de circuitos se distingue del filtro de paquetes por su capacidad para conectar a un esquema de aplicación fuera de banda que puede agregar información.

- **Servidores proxy**

Los servidores proxy son herramientas de seguridad completas que incluyen firewall y puerta de enlace de aplicaciones que administran el tráfico de Internet que entra y sale de una LAN. Los servidores proxy también proporcionan almacenamiento en caché de documentos y control de acceso. Un servidor proxy puede mejorar el rendimiento mediante el almacenamiento en caché y el suministro directo de datos solicitados con frecuencia, por ejemplo una página Web popular. El servidor proxy también puede filtrar y descartar solicitudes que el propietario no considera apropiadas, como las solicitudes de acceso no autorizado a los archivos de propiedad exclusiva.

Asegúrese de que aprovecha esas características de protección del servidor de seguridad. Coloque una red perimetral en un punto de la topología de la red donde todo el tráfico de fuera de la red empresarial deba pasar a través del perímetro mantenido por el servidor de seguridad externo. Puede ajustar el control de acceso del servidor de seguridad para cubrir sus cliente y configurar los servidores de seguridad para que informen de todos los intentos de acceso no autorizado.

Para minimizar el número de puertos que deben abrirse en el servidor de seguridad interno, puede utilizar un servidor de seguridad de nivel de aplicación, como ISA Server 2000.

Para obtener más información acerca de TCP/IP, consulte "[Diseño de una red TCP/IP](#)" (en inglés).

Redes inalámbricas

De forma predeterminada, las redes inalámbricas están en general configuradas de manera que se pueden escuchar las señales inalámbricas. Pueden ser vulnerables a un intruso malintencionado que obtenga acceso gracias a la configuración predeterminada de algunos dispositivos de hardware inalámbrico, la accesibilidad que ofrecen las redes inalámbricas y los actuales métodos de cifrado. Hay opciones y herramientas de configuración que pueden proteger de la escucha, pero debe tenerse en cuenta que no sirven para proteger los equipos contra los intrusos y los virus que entran a través de la conexión de Internet. Por lo tanto, es extremadamente importante incluir un servidor de seguridad para proteger los equipos de intrusos no deseados en Internet.

Para obtener más información sobre cómo proteger una red inalámbrica, consulte "[Cómo aumentar la seguridad de la red doméstica inalámbrica 802.11b](#)" (en inglés).

Escenarios de seguridad de red

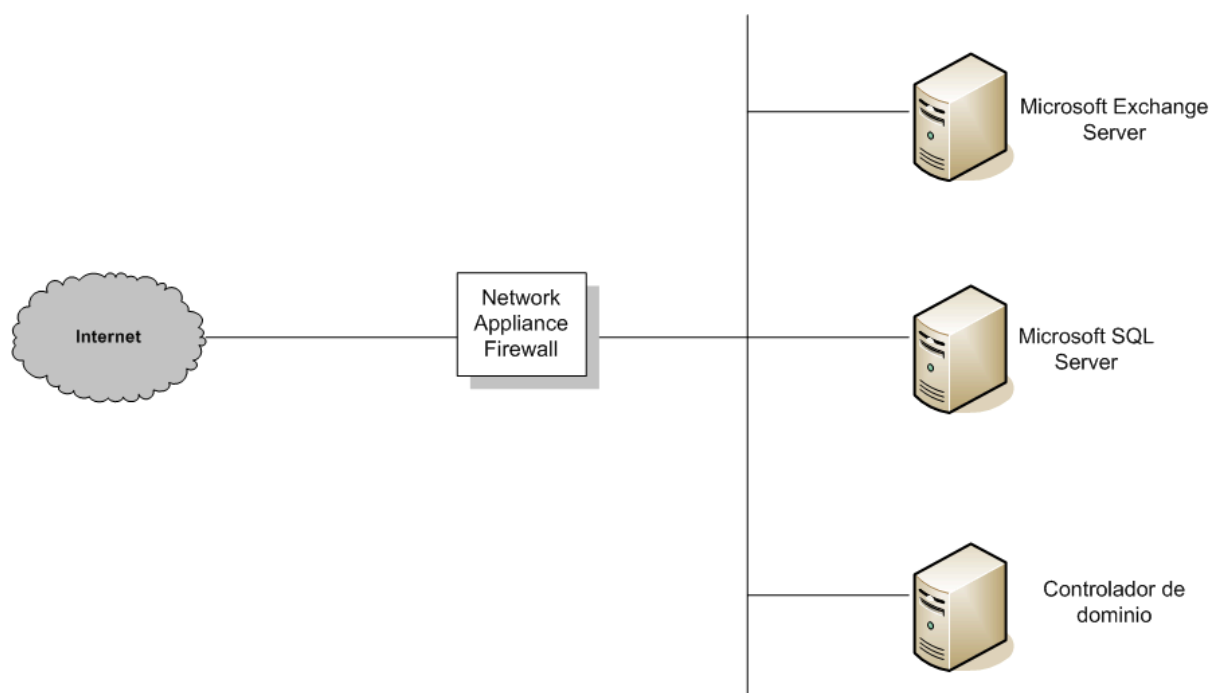
El nivel de seguridad de red que requiere su organización depende de varios factores. Suele reducirse a un equilibrio entre el presupuesto y la necesidad de mantener la seguridad de los datos de la empresa. Una pequeña empresa puede tener una estructura de seguridad muy compleja que proporcione el nivel más alto posible de seguridad de red, pero es probable que no se lo pueda permitir. En esta sección, se examinan cuatro escenarios y se ofrecen recomendaciones en cada uno que proporcionan diferentes niveles de seguridad.

Sin servidor de seguridad

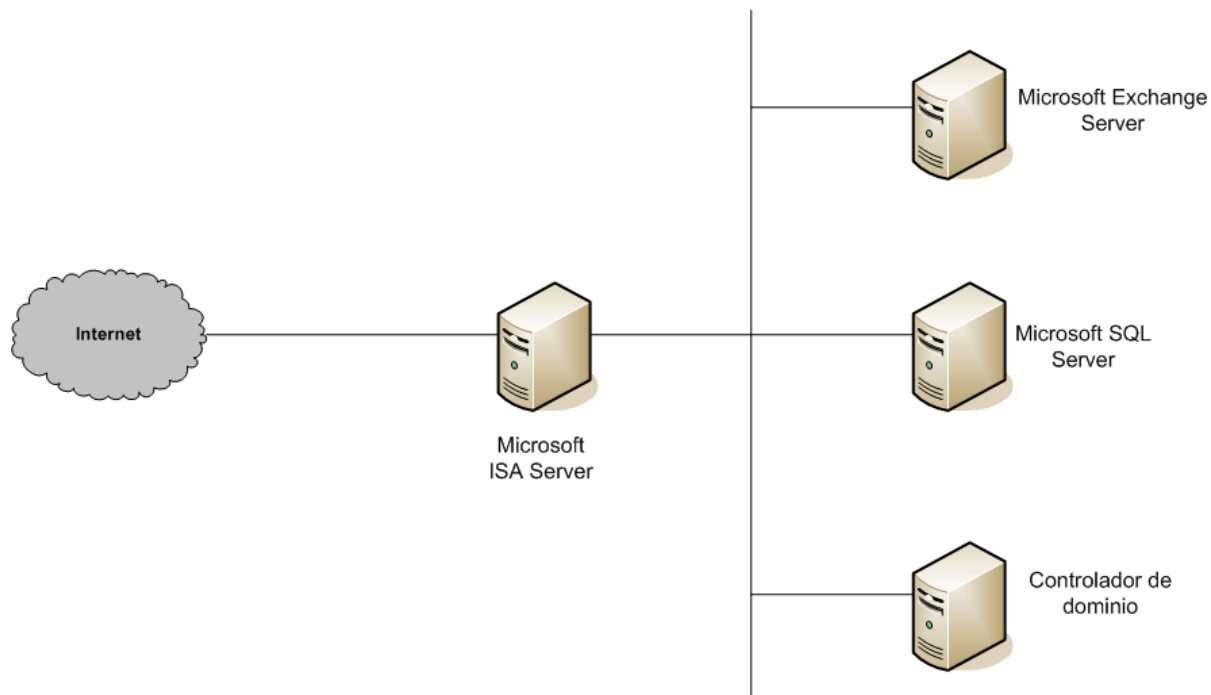
Si tiene una conexión a Internet pero no tiene un servidor de seguridad, debe implementarse alguna medida de seguridad de red. Hay dispositivos sencillos de servidor de seguridad de red que proporcionan suficiente seguridad para disuadir a la mayoría de los aspirantes a intrusos.

Un servidor de seguridad sencillo

El nivel mínimo de seguridad recomendado es un solo servidor de seguridad entre Internet y sus datos. Este servidor de seguridad no proporciona seguridad avanzada y no debe considerarse muy seguro. Pero es mejor que nada.



Es deseable que su presupuesto permita una solución más segura para proteger los datos. Una de esas soluciones es ISA Server. El costo adicional de este servidor proporciona mucha más seguridad que el servidor de seguridad medio, que en general sólo proporciona traducción de direcciones de red (NAT) y filtrado de paquetes.



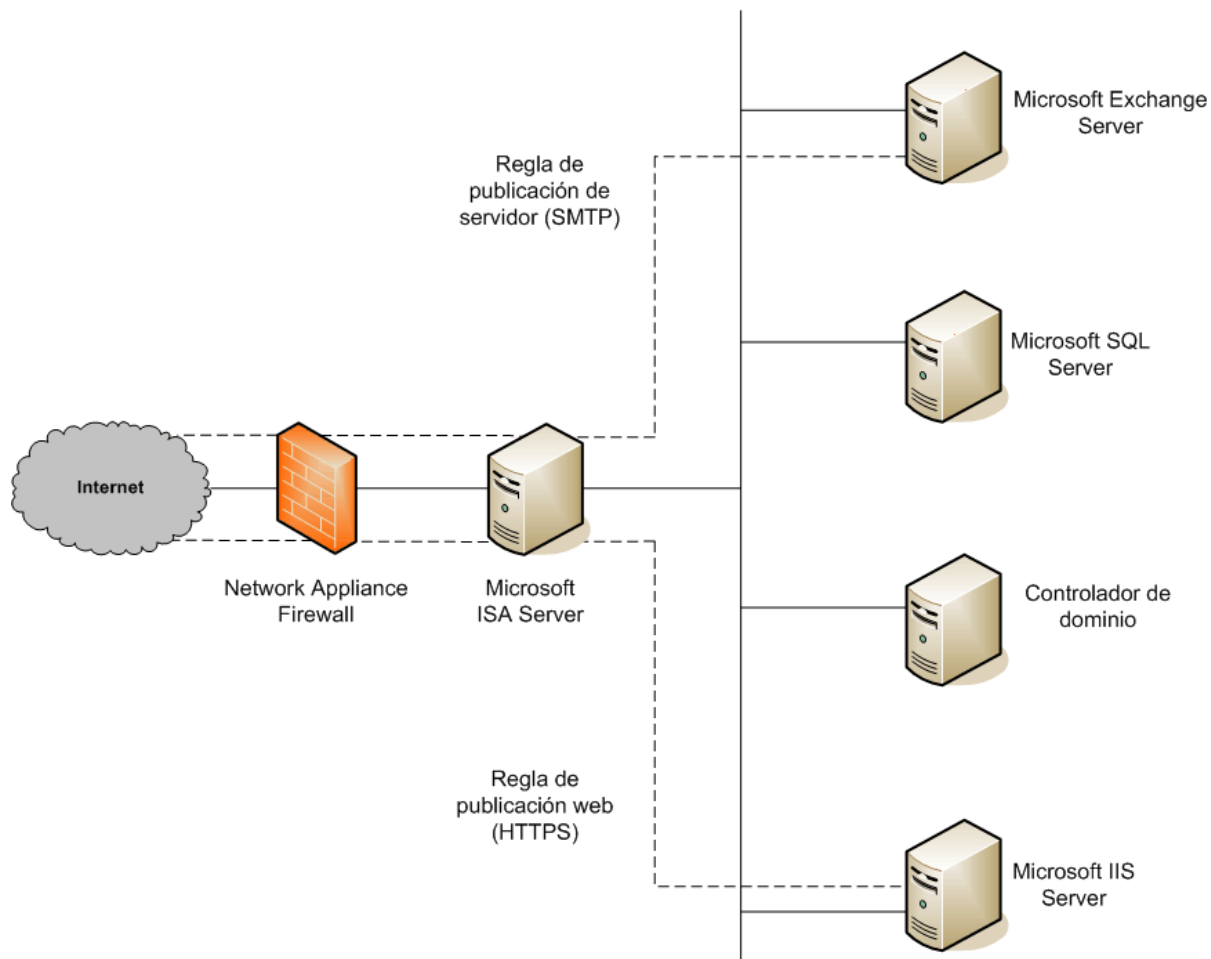
La solución de firewall único es más segura que el dispositivo básico de firewall y proporciona servicios de seguridad específicos de Windows.

Servidor de seguridad existente

Si dispone de un servidor de seguridad que separa su intranet de Internet, puede ser conveniente considerar la posibilidad de utilizar un servidor de seguridad adicional que proporcione varias maneras de configurar los recursos internos para Internet.

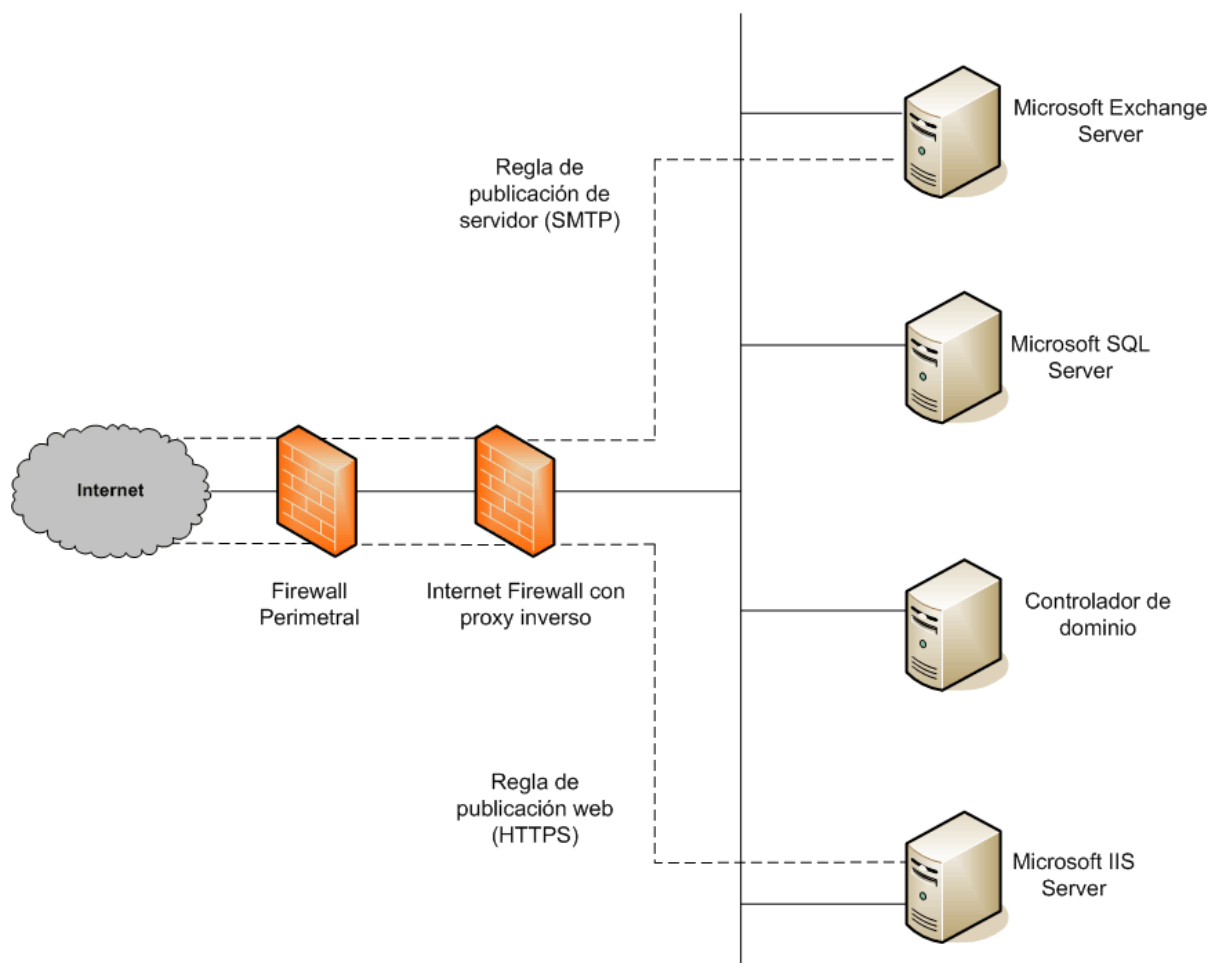
Uno de esos métodos es la publicación en Web. En este caso, ISA Server se implementa delante del servidor Web de una organización que proporciona acceso a los usuarios de Internet. En el caso de las solicitudes Web entrantes, ISA Server puede suplantar a un servidor Web en el exterior para atender desde la caché las solicitudes cliente de contenido Web. ISA Server reenvía las solicitudes al servidor Web únicamente cuando éstas no se pueden atender desde la caché.

Otro método es la publicación de servidor. ISA Server permite la publicación de servidores internos en Internet sin arriesgar la seguridad de la red interna. Puede configurar reglas de publicación en Web y publicación de servidor que determinen qué solicitudes se deben enviar a un servidor de la red local, lo que proporciona un nivel mayor de seguridad para los servidores internos.



Dos servidores de seguridad existentes

El cuarto escenario es aquel en el que la organización cuenta con dos servidores de seguridad y una red perimetral establecida (DMZ). Uno o varios de estos servidores proporcionan servicios de Proxy inverso de forma que los clientes de Internet no tienen acceso directamente a los servidores de la intranet. En su lugar, uno de los servidores de seguridad, preferentemente el servidor interno, intercepta las solicitudes de red para los servidores internos, comprueba los paquetes y, después, los reenvía en nombre del host de Internet.



Este escenario es similar al anterior tras agregar el segundo servidor de seguridad. La única diferencia es que el servidor de seguridad interno que admite el proxy inverso no es un servidor ISA Server. En este escenario, debe trabajar estrechamente con los responsables de cada servidor de seguridad para definir las reglas de publicación en servidor que se ajusten a la directiva de seguridad.

Administración de actualizaciones de seguridad

Los sistemas operativos y las aplicaciones suelen ser enormemente complejos. Pueden constar de millones de líneas de código escritas por muchos programadores diferentes. Es fundamental que el software funcione de manera confiable y no ponga en riesgo la seguridad o estabilidad del entorno de IT. Para minimizar los problemas, los programas se prueban exhaustivamente antes de su lanzamiento. Sin embargo, los atacantes no cesan en su empeño de buscar vulnerabilidades en el software, por lo que no es posible prever todos los ataques futuros.

Para muchas organizaciones, la administración de actualizaciones forma parte de su cambio general y de la estrategia de administración de la configuración. Sin embargo, independientemente de la naturaleza y el tamaño de la organización, es vital contar con una buena estrategia de administración de actualizaciones, incluso si la organización no ha hecho los cambios efectivos ni ha establecido la administración de la configuración. La gran mayoría de los ataques contra sistemas informáticos tienen lugar en aquellos sistemas donde las actualizaciones de seguridad no se han instalado.

Las actualizaciones de seguridad son un reto específico para la mayoría de las organizaciones. Una vez expuesta una vulnerabilidad en el software, los atacantes difundirán en general información acerca de ella rápidamente entre la comunidad de intrusos. Cuando el software presenta una debilidad, Microsoft se esfuerza por lanzar una actualización de seguridad tan pronto sea posible. Hasta que se implementa la actualización, la seguridad de la que depende el cliente y que éste mismo espera se ve seriamente disminuida.

En el entorno de Dynamics NAV, debe asegurarse de que los clientes tienen las actualizaciones de seguridad más recientes instaladas en el sistema. Asegúrese de que el cliente utiliza una de las tecnologías de Microsoft que están disponibles. Entre ellas se incluyen:

- **Microsoft Security Notification Service**
Security Notification Service es una lista de correo electrónico que distribuye avisos siempre que hay una actualización disponible. Estos avisos son un componente valioso de una estrategia de seguridad activa. También están disponibles en el sitio web sobre [notificación de seguridad de productos de TechNet](#) (en inglés).
- **Actualizaciones automáticas de Microsoft**
Windows puede aplicar automáticamente actualizaciones de seguridad a las máquinas.
- **Herramienta de búsqueda de boletines de seguridad de Microsoft**
La herramienta de búsqueda de boletines de seguridad está disponible en el [sitio web del servicio de boletines de seguridad](#) (en inglés). El cliente puede determinar qué actualizaciones necesita en función del sistema operativo, aplicaciones y Service Packs que ejecute.

- Microsoft Baseline Security Analyzer (MBSA)
Esta herramienta gráfica está disponible en el [sitio web de Microsoft Baseline Security Analyze](#) (en inglés). La herramienta compara el estado actual de un equipo con una lista de actualizaciones mantenida por Microsoft. Además, MBSA lleva a cabo comprobaciones básicas de seguridad de contraseñas y configuración de caducidad, directivas de cuentas de invitado y varias otras áreas. MBSA también busca vulnerabilidades en Microsoft Internet Information Services (IIS), SQL Server™ 2000, Exchange 5.5, Exchange 2000 y Exchange Server 2003.
- Microsoft Systems Management Server (SMS) Software Update Services Feature Pack
SMS Software Update Services Feature Pack contiene una serie de herramientas diseñadas para facilitar el proceso de distribución de actualizaciones de software en la compañía. Entre las herramientas están Security Update Inventory Tool, Microsoft Office Inventory Tool for Updates, Distribute Software Updates Wizard y SMS Web Reporting Tool con un complemento de informes web para las actualizaciones de software. Para obtener más información sobre cada herramienta, consulte el sitio web [Software Update Services Feature Pack](#) (en inglés).

Piense en utilizar cada una de estas herramientas. Es muy importante que los problemas de seguridad se traten lo más rápidamente posible, sin que se resienta la estabilidad del entorno.

Configuración de seguridad de SQL Server

Microsoft Dynamics NAV puede ejecutarse en SQL Server y las instalaciones más pequeñas también pueden ejecutarse en SQL Server Express.

Los siguientes pasos ayudarán a aumentar la seguridad de SQL Server:

- Asegúrese de que están instalados el sistema operativo, los Service Pack y las actualizaciones más recientes. Para obtener la información más reciente, compruebe el sitio web de [seguridad de Microsoft](#).
- Para la seguridad de nivel de sistema de archivos, asegúrese de que todos los datos y archivos de sistema de SQL Server están instalados en particiones NTFS. Los archivos sólo deben ser accesibles para los usuarios administrativos o de nivel del sistema mediante permisos NTFS. De esta forma, los archivos estarán protegidos del acceso de los usuarios cuando el Servicio MSSQLSERVER no esté en ejecución.
- Utilice una cuenta de dominio de bajos privilegios como cuenta NT Authority\Network Service (recomendada) o la cuenta de sistema local para el servicio SQL Server (MSSQLSERVER o SQLEXPRESS). Esta cuenta debe tener derechos mínimos en el dominio y contribuirá a resistir (pero no detener) un ataque al servidor en caso de riesgo. Dicho de otra forma, esta cuenta sólo debe tener permisos de usuario locales en el dominio. Si SQL Server está utilizando una cuenta de administrador de dominio para ejecutar los servicios, un compromiso del servidor llevará a un compromiso de todo el dominio. Para cambiar esta configuración, utilice SQL Server Management Studio. Las listas de control de acceso (ACL) de los archivos, el Registro y los derechos de usuario se modificarán automáticamente.
- La mayoría de las ediciones de SQL Server están instaladas con algunas bases de datos predeterminadas. Estas bases de datos son ejemplos utilizados para la comprobación, aprendizaje y ejemplos generales. No deben implementarse en un sistema de producción. El conocimiento de la presencia de estas bases de datos puede originar que un intruso intente llevar a cabo un ataque que afecte a la configuración predeterminada. Si las bases de datos de ejemplo se encuentran en el equipo de producción de SQL Server, deben eliminarse.
- La auditoría del sistema SQL Server está deshabilitada de manera predeterminada, por lo que no se audita ninguna condición. Esto dificulta la detección de intrusiones y ayuda a los atacantes a pasar inadvertidos. Como mínimo, debe habilitarse la auditoría de inicios de sesión erróneos.

Para obtener la información de seguridad de SQL Server más actualizada, visite el [sitio web de seguridad de SQL Server](#).

Apéndice

Vínculos en este documento

<i>Tema</i>	<i>Dirección URL</i>
Seguridad de SQL Server	http://go.microsoft.com/fwlink/?LinkId=80204
Instrucciones de seguridad para SQL Server	http://go.microsoft.com/fwlink/?LinkId=80205
Las diez leyes inmutables de la seguridad	http://go.microsoft.com/fwlink/?LinkId=80206
Microsoft Technet – Viewpoint	http://go.microsoft.com/fwlink/?LinkId=80207
Windows Server TechCenter	http://go.microsoft.com/fwlink/?LinkId=80209
Windows 2000 Server en TechNet	http://go.microsoft.com/fwlink/?LinkId=80208
Contraseñas seguras: cómo crearlas y utilizarlas	http://go.microsoft.com/fwlink/?LinkId=80117
Microsoft Security en Security Central	http://go.microsoft.com/fwlink/?LinkId=80211
Seguridad en Microsoft TechNet	http://go.microsoft.com/fwlink/?LinkId=80212
Diseño de una red TCP/IP	http://go.microsoft.com/fwlink/?LinkId=80214
Cómo aumentar la seguridad de la red doméstica inalámbrica 802.11b	http://go.microsoft.com/fwlink/?LinkId=80215
Notificación de seguridad de productos de TechNet	http://go.microsoft.com/fwlink/?LinkId=80216
Servicio de boletines de seguridad	http://go.microsoft.com/fwlink/?LinkId=80217
Microsoft Baseline Security Analyzer	http://go.microsoft.com/fwlink/?LinkId=80218
Software Update Services Feature Pack	http://go.microsoft.com/fwlink/?LinkId=80218

La información contenida en este documento representa la visión actual de Microsoft Corporation en la fecha de publicación acerca de las cuestiones que se tratan. Puesto que Microsoft debe responder a los cambios en las condiciones del mercado, no debe interpretarse como un compromiso por parte de Microsoft, y Microsoft no puede garantizar la precisión de la información presentada con posterioridad a la fecha de publicación.

Las notas del producto sólo tienen fines informativos. MICROSOFT NO OFRECE NINGUNA GARANTÍA EXPRESA, IMPLÍCITA O LEGAL EN CUANTO A LA INFORMACIÓN DE ESTE DOCUMENTO.

Es responsabilidad del usuario el cumplimiento de todas las leyes aplicables de derechos de autor. Sin perjuicio de tales derechos, ninguna parte de este documento se podrá reproducir, almacenar o introducir en un sistema de recuperación, ni transmitir en forma alguna ni por ningún medio (ya sea electrónico, mecánico, de fotocopia, grabación, etc.), ni con ningún fin, sin el permiso expreso por escrito de Microsoft Corporation.

Microsoft puede ser titular de patentes, solicitudes de patentes, marcas comerciales, derechos de autor y otros derechos de propiedad intelectual sobre el contenido de este documento. El suministro de este documento no le otorga ninguna licencia sobre dichas patentes, marcas, derechos de autor u otro tipo de propiedad intelectual, salvo que se prevea en un contrato por escrito de licencia de Microsoft.

© 2007 Microsoft Corporation. Reservados todos los derechos.

Microsoft, MS-DOS, Windows, Windows Server, Windows Vista, Windows XP, Windows 2000 Server, Windows Server 2003, C/SIDE, Microsoft Internet Security & Acceleration Server 2006, Microsoft Dynamics, Microsoft Dynamics NAV, Microsoft Exchange Server, Microsoft SQL Server son marcas registradas o marcas comerciales de Microsoft Corporation en Estados Unidos y en otros países.

El resto de marcas comerciales son propiedad de sus respectivos dueños.

