CCN
centro criptológico nacional

Guía de Seguridad de las TIC

IMPLEMENTACIÓN DE SEGURIDAD SOBRE MICROSOFT WINDOWS SERVER 2016 (CONTROLADOR DE DOMINIO O SERVIDOR MIEMBRO)

NOVIEMBRE 2018

MINISTERIO DE DEFENSA

Edita:

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2019.05.08 16:37:13 +02'00'

NIPO: 083-19-032-X
Fecha de Edición: noviembre 2018

Sidertia Solutions S.L. ha participado en la realización y modificación del presente documento y sus anexos.

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, actualizado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

noviembre de 2018

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL 6
2. INTRODUCCIÓN 6
3. OBJETO 7
4. ALCANCE 7
5. DESCRIPCIÓN DEL USO DE ESTA GUÍA 8
5.1 AVISOS IMPORTANTES A LOS USUARIOS DE ESTA GUÍA 9
5.2 ESTRUCTURA DE LA GUÍA 10
6. WINDOWS SERVER 2016 NOVEDADES 10
6.1 VERSIONES 11
6.2 INTERFAZ 12
6.3 DIRECTORIO ACTIVO 13
6.4 ADMINISTRACIÓN 14
6.5 SEGURIDAD Y CONTROL 15
6.6 SERVICIOS DE RED 16
7. DOMINIO DE DIRECTORIO ACTIVO 18
7.1 INFRAESTRUCTURA DE UNIDADES ORGANIZATIVAS 18
7.2 DIRECTIVAS DE DOMINIO 20
7.2.1 DIRECTIVA DE CUENTA 20
7.2.1.1 DIRECTIVA DE CONTRASEÑAS 20
7.2.1.2 DIRECTIVA DE BLOQUEO DE CUENTA 21
7.2.1.3 DIRECTIVA KERBEROS 22
7.2.2 DIRECTIVAS LOCALES 22
7.2.2.1 OPCIONES DE SEGURIDAD 22
7.2.2.2 REGISTRO DE EVENTOS 23
8. CONTROLADOR DE DOMINIO Y SERVIDOR MIEMBRO 24
8.1 PLANTILLA DE SEGURIDAD 24
8.1.1 DIRECTIVAS DE CUENTA 25
8.1.2 DIRECTIVAS LOCALES 25
8.1.2.1 DIRECTIVAS DE AUDITORÍA 25
8.1.2.2 ASIGNACIÓN DE DERECHOS DE USUARIO 25
8.1.2.3 OPCIONES DE SEGURIDAD 27
8.1.3 SERVICIOS DEL SISTEMA 30
8.1.4 REGISTRO 32
8.1.5 SISTEMA DE FICHEROS 32
8.2 CONFIGURACIONES ESPECÍFICAS DEL CONTROLADOR DE DOMINIO 32
8.2.1 ASIGNACIÓN DE PERMISOS A CUENTAS CONCRETAS DEL DOMINIO 32
8.2.2 NIVEL FUNCIONAL DEL DOMINIO 33
8.2.3 SERVICIOS DE DIRECTORIO ACTIVO 34
8.2.3.1 ALMACENAMIENTO DE LOS FICHEROS ASOCIADOS AL DIRECTORIO ACTIVO 34
8.2.3.2 CONTROLADORES DE DOMINIO DE SOLO LECTURA 34
8.2.3.3 LIMITACIÓN DE RANGO DE PUERTOS DE TCP PARA RPC 35
9.1 FIREWALL DE WINDOWS CON SEGURIDAD AVANZADA 36
9.2 PLANTILLAS ADMINISTRATIVAS 37
9.3 CUENTAS DE SERVICIO 37

9.4 DESACTIVACIÓN DE PROTOCOLOS INNECESARIOS 38
9.5 APLICACIÓN DE LAS PLANTILLAS DE SEGURIDAD 38

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como CERT Gubernamental Nacional español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

2. INTRODUCCIÓN

Este documento forma parte del conjunto de normas desarrolladas por el Centro Criptológico Nacional para entornos basados en los productos y sistemas operativos de Microsoft (CCN STIC 500), siendo de aplicación para la Administración pública en el cumplimiento del Esquema Nacional de Seguridad (ENS) y de obligado cumplimiento para los sistemas que manejen información clasificada nacional.

La serie CCN STIC 500 se ha diseñado de manera incremental. Así, dependiendo del sistema, se aplicarán consecutivamente varias de estas guías. En este sentido se deberán aplicar las guías correspondientes dependiendo del entorno que se esté asegurando.

Por ejemplo, en el caso de un entorno que le sea de aplicación el ENS, para un servidor miembro de un dominio con Microsoft Windows Server 2012 R2, en el que se instale Microsoft Exchange Server 2013, deberán aplicarse las siguientes guías:

a) Guía CCN STIC 870A en el servidor miembro con Windows Server 2012 R2.

b) Guía CCN-STIC-873 Internet Information Services (IIS) 8.5.

c) Guía CCN STIC 880 Microsoft Exchange Server 2013 en Windows 2012 R2.

Por ejemplo, en el caso de un entorno de red clasificada, para un servidor con Microsoft Windows Server 2012 R2, en el que se instale Microsoft Exchange Server 2013, deberán aplicarse las siguientes guías:

a) Guía CCN STIC 560A en el servidor miembro con Windows Server 2012 R2.

b) Guía CCN-STIC-563 Internet Information Services (IIS) 8.5.

c) Guía CCN STIC 552 Microsoft Exchange Server 2013 en Windows 2012 R2.

Nota: Estas guías están pensadas y diseñadas para entornos de máxima seguridad donde no existirá conexión con redes no seguras como puede ser Internet.

3. OBJETO

El propósito de este documento consiste en proporcionar los procedimientos para implementar y garantizar la seguridad para una instalación completa (no core) del sistema "Windows Server 2016" actuando bien como servidor controlador de dominio o bien como servidor miembro de un dominio. Otras configuraciones, como servidores instalados en modo Core o bien como servidores independientes a un dominio, son tratados en otras guías de esta misma serie.

La configuración que se aplica a través de la presente guía se ha diseñado para ser lo más restrictiva posible, minimizando la superficie de ataque y por lo tanto los riesgos que pudieran existir. En algunos casos y dependiendo de la funcionalidad requerida del servidor, podría ser necesario modificar la configuración, que aquí se plantea, para permitir que el equipo proporcione servicios adicionales.

No obstante, se tiene en consideración que los ámbitos de aplicación son muy variados y por lo tanto dependerán de su aplicación, las peculiaridades y funcionalidades de los servicios prestados por las diferentes organizaciones. Por lo tanto, las plantillas y normas de seguridad se han generado definiendo unas pautas generales de seguridad que permitan el cumplimiento de los mínimos establecidos en el ENS y las condiciones de seguridad necesarias en un entorno clasificado.

En el caso de la aplicación de seguridad sobre un entorno perteneciente a una red clasificada, se establece la máxima seguridad posible teniendo en consideración la guía CCN-STIC-301 – Requisitos STIC. Si su sistema requiere de otra configuración menos restrictiva, y está autorizado para ello, consulte el apartado "APLICACIÓN DE NIVELES DE CLASIFICACIÓN" del "ANEXO B" de esta guía para realizar los pasos adecuados.

4. ALCANCE

La guía se ha elaborado para proporcionar información específica sobre cómo implementar las distintas configuraciones para los escenarios planteados. En particular, se incluirá la configuración para asegurar un servidor con "Windows Server 2016", instalado en español con la versión completa del producto, bien actuando con el rol de controlador de dominio o bien como servidor miembro de un dominio.

Este documento incluye:

a) **Descripción de las nuevas funcionalidades** para todos aquellos operadores que tengan experiencia en la versión previa de Windows Server 2016.

b) **Descripción del Directorio Activo.** Completa descripción del servicio de Directorio Activo como soporte a una infraestructura y todos aquellos elementos anexos al mismo.

c) **Funcionalidades de seguridad local adicionales.** Completa descripción de aquellas características y servicios que, no encontrándose definidos por defecto, agregan seguridad adicional a una infraestructura de Windows Server 2016.

d) **Mecanismos para la implementación de la solución.** Se incorporan mecanismos para la implementación de la solución de forma automatizada.

e) **Mecanismos para la planificación de configuraciones.** Se incorporan mecanismos para la planificación de las configuraciones de seguridad susceptibles de ello, tales como las plantillas de seguridad.

f) **Guía paso a paso.** Permitirá implantar y establecer las configuraciones de seguridad en servidores controladores de dominio y en servidores miembros del dominio.

g) **Tareas de administración sobre el Directorio Activo**. Conjunto de operaciones que podrán ser aplicadas por una organización para las mejoras de seguridad en la administración de un servicio de Directorio Activo.

h) **Lista de comprobación.** Permitirá verificar el grado de cumplimiento de los servidores con respecto a las condiciones de seguridad que se establecen en esta guía.

5. DESCRIPCIÓN DEL USO DE ESTA GUÍA

Para entender esta guía de seguridad, es conveniente explicar el proceso de aplicación de seguridad que describe y los recursos que proporciona. Este proceso constará de los siguientes pasos:

a) Antes de comenzar a aplicar esta guía, debe tenerse en cuenta que, además de los requisitos a cumplir para la instalación de Windows Server 2016, puede ser necesario comprobar los requisitos de otros servicios y aplicaciones que se vayan a aplicar posteriormente, especialmente requisitos relacionados con el particionamiento de los discos. En la mayoría de los productos y/o servicios se recomienda tener en particiones distintas el sistema operativo y el resto de ficheros de la aplicación.

b) Si el servidor va a ser un controlador de dominio, se debe proceder de la siguiente manera:

   i. Revisar e implementar el apartado correspondiente a la aplicación de seguridad sobre un controlador de dominio.

   ii. Además, debido a la existencia de un dominio, será necesario revisar y aplicar el apartado correspondiente a la seguridad de Directorio Activo.

c) Si el servidor es un servidor miembro del dominio, se debe proceder de la siguiente forma:

   i. Revisar y aplicar, si no se ha realizado previamente, el apartado correspondiente a la seguridad del Directorio Activo.

   ii. Revisar e implementar el apartado correspondiente a la aplicación de seguridad sobre un servidor miembro.

d) Si el entorno que el que está aplicando seguridad pertenece a una red clasificada, se deberá realizar la securización de Microsoft Internet Explorer 11 a través de la implementación de las políticas de seguridad definidas en la guía CCN-STIC-520 Internet Explorer 11 para un servidor perteneciente a un dominio.

e) Esta guía de seguridad está enfocada a sistemas clasificados, aunque puede ser tomada como base para la securización de IE 11 en aquellos sistemas que les sea de aplicación el ENS. En este último caso, estas medidas deberán adaptarse a las necesidades de cada organización.

5.1 AVISOS IMPORTANTES A LOS USUARIOS DE ESTA GUÍA

Los contenidos de esta guía son de aplicación a equipos tipo puesto servidor con Sistema Operativo Windows Server 2016, en castellano, con el objetivo de reducir la superficie de exposición a ataques posibles con una instalación por defecto, manteniendo los principios de máxima seguridad, mínima exposición y servicios y mínimos privilegios que emanan de la CCN-STIC-301. En el caso de llevar a cabo la aplicación de esta guía sobre el Sistema Operativo con una configuración de idioma diferente al castellano, es posible que deba incorporar nuevos recursos y/o realizar ciertas modificaciones sobre los recursos que se adjuntan con este documento para permitir la correcta aplicación y uso del documento.

La guía ha sido probada y verificada con la versión Windows Server 2016 Standard. También sería válida para una versión de Windows Server 2016 Datacenter. Las diferencias entre estas versiones serán tratadas en el punto “6.1 VERSIONES” de la presente guía.

La guía de seguridad ha sido elaborada utilizando un laboratorio basado en una plataforma de virtualización tipo Hyper-V de Windows Server 2012 R2 Datacenter con las siguientes características técnicas:

a) Servidor Dell PowerEdge™ T320:
   i. Intel Pentium Xeon CPU ES 2430 2.20GHz.
   ii. HDD 1TB.
   iii. 64 GB de RAM.
   iv. Interfaz de Red 1 GB.

Esta guía de seguridad no funcionará con *hardware* que no cumpla con los requisitos mínimos de Windows Server 2016 Standard. Esto quiere decir que se requieren equipos con procesadores Intel o AMD de 64 bits (x64), con más de 2048 MB (2GB) de memoria RAM para la opción de instalación “Servidor con Experiencia de escritorio”.

Nota: Puede comprobar los requisitos del sistema de Windows Server 2016 en el siguiente enlace: https://docs.microsoft.com/en-us/windows-server/get-started/system-requirements

La guía ha sido desarrollada con el objetivo de dotar a la infraestructura de la seguridad máxima. Es posible que algunas de las funcionalidades esperadas hayan sido desactivadas y por lo tanto pueda ser necesario aplicar acciones adicionales para habilitar servicios, roles o características deseadas.

Para garantizar la seguridad de los clientes y servidores, deberán instalarse las actualizaciones recomendadas por el fabricante, disponibles a través del servicio de Microsoft Update. Las actualizaciones, por lo general, se liberan los segundos martes de cada mes, no obstante, hay que tener presente que determinadas actualizaciones, por su criticidad, pueden ser liberadas en cualquier momento.

Dependiendo de la naturaleza de estas actualizaciones, el lector podrá encontrarse con algunas diferencias respecto a lo descrito en esta guía. Esto viene motivado por los cambios que, en ocasiones, se realizan para las distintas actualizaciones de seguridad.

Antes de aplicar esta guía en producción, deberá asegurarse de haber probado en un entorno aislado y controlado, en el cual se habrán aplicado las pruebas y posteriores cambios en la configuración que se ajusten a los criterios específicos de cada organización.

El espíritu de estas guías no está dirigido a remplazar políticas consolidadas y probadas de las organizaciones, sino a servir como línea base de seguridad que deberá ser adaptada a las necesidades propias de cada organización.

El procedimiento establecido en este documento asume que está configurando un sistema a partir de un entorno limpio (formateado) en el caso de una red clasificada y un entorno ya en producción en el caso del ENS.

5.2 ESTRUCTURA DE LA GUÍA

Esta guía dispone de una estructura que diferencia la implementación del sistema Microsoft Windows Server 2016 dependiendo del entorno sobre el que vaya a ser aplicado.

La guía dispone de las siguientes configuraciones divididas en dos grandes anexos, los cuales se definen a continuación:

a) **Anexo A:** En este anexo se define la configuración necesaria para adaptar los sistemas Microsoft Windows Server 2016 en sus versiones Standard y Datacenter a las necesidades requeridas por el Esquema Nacional de Seguridad (ENS).

b) **Anexo B:** En este anexo se define la configuración necesaria para adaptar los sistemas Microsoft Windows Server 2016 en sus versiones Standard y Datacenter a las necesidades requeridas en los entornos clasificados.

Cabe remarcar que en sus respectivos anexos se dotará de la información necesaria y concreta para cada tipo de implementación.

De manera adicional, en cada una de las carpetas “Scripts” que se adjuntan a los documentos, existe un directorio que almacena un informe en formato HTML con cada objeto de directiva de grupo (GPO) o directiva de grupo local (GPL) que se aplica durante el paso a paso de la guía.

6. WINDOWS SERVER 2016 NOVEDADES

Windows Server 2016 constituye la última evolución de la versión Windows Server 2012 R2. Para todos aquellos operadores que ya hayan implementado guías anteriores y se encuentren familiarizados con Windows Server 2012 R2 se exponen, a continuación, aquellos cambios significativos que bien a efectos de seguridad, de implementación o de experiencia en su manejo suponen un cambio en la versión Windows Server 2016. También es importante la lectura de este punto para el resto de operadores que nunca hayan trabajado con sistemas Windows y necesiten hacer una implementación en sus infraestructuras de Windows Server 2016.

Como es evidente, en todos los lanzamientos de un nuevo sistema operativo suelen aparecer novedades respecto a versiones anteriores. En esta ocasión, una de las muchas novedades que incorpora Windows Server 2016 es una seguridad avanzada multi-capa, que ofrece a los administradores una serie de herramientas avanzadas, que permiten detectar y bloquear toda la actividad sospechosa antes de que ésta pueda ser capaz de causar daños en el

servidor, ayudando con ello a proteger tanto la maquina local, como las máquinas virtuales alojadas en ese servidor.

Otra de las grandes novedades que trae Windows Server 2016 es la integración de la última tecnología de Azure para hacer más flexible esa combinación del entorno virtual con el entorno físico. Muchas de las mejoras que ofrece este sistema operativo están orientadas a las soluciones de nube o entornos híbridos.

Windows Server 2016 ofrece una nueva opción de implementación denominada Nano Server. El cual es un sistema operativo de servidor administrado de forma remota y optimizado para centros de datos y nubes privadas.

Es muy similar a Windows Server en modo Server Core ya disponible en ediciones anteriores, pero más reducido, no tiene capacidad de inicio de sesión local y solo es compatible con agentes, herramientas y aplicaciones de 64 bits. La opción de instalación de Nano Server está disponible para las ediciones Standard y Datacenter de Windows Server 2016. Al tratarse de un modo de instalación aún más reducido que la versión Server Core, se minimiza la superficie de ataque disponible aumentando con ello la seguridad.

La instalación de la opción de Nano Server se recomienda para una serie de escenarios:

a) Como un host para las máquinas virtuales de Hyper-V.

b) Como un host de almacenamiento para el servidor de archivos de escalabilidad horizontal

c) Como un servidor DNS.

d) Como un servidor web que ejecuta Internet Information Services (IIS).

Nano Server también tiene una serie de limitaciones:

a) Nano Server no puede actuar como un controlador de dominio de Directorio Activo y no se admiten directivas de grupo.

b) No puede configurarse para utilizar un servidor proxy para el acceso a Internet.

c) No se admiten ni System Center Configuration Manager ni System Center Data Protection Manager.

6.1 VERSIONES

En Windows Server 2016 no existe un cambio en lo que respecta a las ediciones frente a lo ya existente en Windows Server 2012 R2, ya que posee las mismas ediciones que poseía el anterior sistema operativo. Debe recordarse que en las versiones previas de Windows Server 2008 R2 existía adicionalmente la versión Enterprise que desapareció con la salida de Windows Server 2012.

Nota: Existe la versión Essentials diseñada para empresas con un máximo de 25 usuarios y 50 dispositivos. Essentials es una buena opción para clientes que usan Foundation Edition, la cual no está disponible con Windows Server 2016.

Ambas versiones presentan las mismas funcionalidades y servicios que se pueden implementar sin embargo existen diferencias que son necesarias comentar para decidir qué tipo de edición implementar.

La diferencia fundamental entre ambas versiones reside en el número de Entornos de Sistema Operativo (OSE) y contenedores de Hyper-V que cubren:

a) La versión Windows Server 2016 Standard permite ejecutar hasta dos instancias de máquinas virtuales en un máximo de dos procesadores.

b) La versión Windows Server 2016 Datacenter permite ejecutar un número ilimitado de máquinas virtuales en un máximo de dos procesadores.

Nota: La edición Standard permite el uso de una instancia del software del servidor en el OSE físico en el servidor con licencia (además de dos OSE virtuales), si el OSE físico se usa únicamente para hospedar y administrar los OSE virtuales.

Por lo tanto, para aquellos entornos de servidor donde se vaya a realizar una alta implementación de máquinas virtuales, deberá emplearse la versión de Windows Server 2016 Datacenter. Para el resto de sistemas donde el servidor físico no vaya a realizar implementaciones de máquinas virtuales o la implementación vaya a ser en un número no superior a 2, deberán instalar la versión Windows Server 2016 Standard.

Además de esta diferencia principal la versión Datacenter incluye la funcionalidad "Shielded Virtual Machines" (blindado de máquinas virtuales) la cual proporciona una protección adicional contra código malicioso.

La versión Datacenter dispone de redes definidas de software, espacios de almacenamiento directo y réplica de almacenamiento, cualidades de las que no dispone la edición Standard.

Para más información sobre versiones, licenciamiento y características consulte los siguientes enlaces:

a) Licencias de ediciones:

https://www.microsoft.com/es-xl/licensing/product-licensing/windows-server-2016.aspx

b) Comparativa entre Windows Server 2016 Datacenter y Standard:

https://docs.microsoft.com/en-us/windows-server/get-started/2016-edition-comparison

Con respecto a las versiones previas del Sistema Operativo, Windows Server 2016 presenta una serie de características que bien han desaparecido o bien se encuentran en desuso.

A continuación, se proporciona un enlace donde se enumeran las características y funcionalidades de Windows Server 2016 eliminadas o pendientes de eliminación por desuso.

https://docs.microsoft.com/en-us/windows-server/get-started/deprecated-features

6.2 INTERFAZ

Uno de los cambios que trajo de vuelta Windows 10 y al que se une Windows Server 2016 es el uso del menú tal y como era conocido antes de Windows 8 y Windows Server 2012 lo que supone una vuelta al estilo antiguo, pero con una personalización totalmente nueva, al igual que sucedía en Windows 10.

El "Administrador del servidor" (Server Manager) mantiene las funcionalidades y el estilo implementado en Windows Server 2012 R2, permitiendo gestionar tanto las características y los roles del propio servidor como realizar la gestión centralizada de otros servidores existentes dentro de la infraestructura.

6.3 DIRECTORIO ACTIVO

Los servicios de certificados de Active Directory en Windows Server 2016 aumenta la compatibilidad para la identificación de la clave de TPM.

Ahora es posible usar el KSP de tarjeta inteligente para el acceso a la clave almacenada en el TPM para los usuarios unidos al dominio, y los dispositivos que no están unidos al dominio pueden utilizar la inscripción NDES para obtener los certificados que permitan el uso de las claves almacenadas en el TPM.

Los Servicios de dominio de Active Directory incluyen mejoras que ayudan a las organizaciones a proteger los entornos de Active Directory y mejoran la administración de identidades, tanto para dispositivos corporativos como personales.

La Administración de Acceso Privilegiado (Privileged Access Management – PAM) ayuda a mitigar los problemas de seguridad de Active Directory provocados por técnicas de robo de credenciales como pass-the-hash, suplantación de identidad u otros tipos de ataque. Debido a esto se proporciona una nueva solución de acceso que se configura mediante el Administrador de Identidad de Microsoft (Microsoft Identity Manager – MIM).

La Administración de Acceso Privilegiado introduce las siguientes características detalladas a continuación:

a) Un bosque aprovisionado con PAM (Privileged Access Management) posee una confianza especial con otro bosque existente que permite determinar que el entorno está libre de una actividad maliciosa y es posible hacer uso de cuentas con privilegios.

b) Se crean nuevos procesos en MIM (Microsoft Identity Manager) para solicitar privilegios administrativos, junto con nuevos flujos de trabajo basados en la aprobación de solicitudes.

c) Existen entidades de seguridad ocultas (grupos) aprovisionadas por MIM (Microsoft Identity Manager) para atender a las solicitudes de privilegios administrativos. Dichas entidades de seguridad poseen un atributo que hace referencia al SID de un grupo administrativo conocido dentro de un bosque existente. Esto permite acceder a dichos grupos a recursos dentro de un bosque conocido sin necesidad de realizar un cambio en ninguna lista de control de acceso (ACL).

d) Característica de caducidad de vinculo la cual permite establecer un tiempo límite de pertenencia a un grupo. El usuario puede ser agregado al grupo con un tiempo determinado para realizar la tarea administrativa correspondiente y después ser eliminado del grupo lo que le impedirá seguir teniendo los permisos administrativos concedidos anteriormente. El límite de tiempo de pertenencia se establece con un valor de tiempo de vida (Time To Live – TTL) que se propaga a la duración de un vale de Kerberos.

Nota: Esta característica se permite para todos los atributos sin embargo la relación de grupo y usuario es el único ejemplo en el que la característica de caducidad de vínculo funciona de forma completa.

e) Se han implementado mejoras de KDC para los controladores de dominio de Active Directory que permiten restringir la duración del ticket Kerberos al valor más bajo posible de tiempo de vida en los casos en los que un usuario tiene múltiples pertenencias con límite de tiempo en grupos administrativos.

f) Nuevas herramientas de monitorización para ayudar a identificar la solicitud de acceso, los accesos otorgados y las acciones realizadas con ese acceso.

Nota: Para más información acerca de PAM (Privileged Access Management) consulte el siguiente enlace:
https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/privileged-identity-management-for-active-directory-domain-services

Microsoft Passport es un nuevo formato de autenticación basado en claves dedicado a organizaciones que van más allá del uso de contraseñas.

El usuario inicia sesión en el dispositivo con una información de inicio de sesión biométrica o PIN que está vinculada a un certificado o un par de claves asimétricas. Los proveedores de identidad (IDP) validan al usuario asignando la clave pública del usuario a IDLocker y proporciona información de inicio de sesión mediante autenticación con contraseña de un solo uso (One Time Password - OTP), Phonefactor o un mecanismo de notificación diferente.

Nota: Para más información acerca de Microsoft Passport consulte el siguiente enlace:
https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-identity-verification

Los Servicios de federación de Active Directory (ADFS) en Windows Server 2016 incluyen nuevas características que le permiten configurar ADFS para la autenticación de usuarios almacenados en directorios de protocolo ligero de acceso a directorios (LDAP).

Nota: Para más información acerca de los servicios de federación consulte el siguiente enlace:
https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/overview/whats-new-active-directory-federation-services-windows-server

6.4 ADMINISTRACIÓN

El área Administración y Automatización se centra en la información de referencia y las herramientas para profesionales de TI que desean ejecutar y administrar Windows Server 2016, incluido Windows PowerShell.

Windows PowerShell 5.1 incluye nuevas e importantes características, entre las que se incluyen el soporte para el desarrollo con clases y las nuevas características de seguridad, que amplían y mejoran su uso, y permiten controlar y administrar entornos basados en Windows de manera más sencilla y completa.

A continuación, se detallan algunas de las nuevas características que se incluyen en Windows Server 2016:

a) Posibilidad de ejecución de PowerShell localmente en Nano Server.

b) Nuevos cmdlets (command-let) de usuarios y grupos locales para reemplazar la GUI (Interfaz gráfica de usuario).

c) Incorporación de compatibilidad con la depuración de PowerShell.

d) Windows Server 2016 y Windows 10 incluyen la nueva característica PackageManagement (anteriormente denominada OneGet) que permite a profesionales de TI o de DevOps automatizar la detección de software, la instalación y el inventario, de manera local o remota, con independencia de la tecnología del instalador y de dónde se encuentra el software.

Nota: Para más información consulte el siguiente enlace: https://github.com/OneGet/oneget/wiki

e) Just in Time Administration: Permite limitar el tiempo de duración de los privilegios concedidos, evitando con ello que existan usuarios con privilegios administrativos que se olviden con el paso del tiempo que fueron concedidos.

6.5 SEGURIDAD Y CONTROL

Windows Server 2016 incluye nuevas herramientas integradas para contrarrestar las posibles vulnerabilidades de seguridad, permitiendo frustrar ataques en sus sistemas. Además, en caso de que un usuario no autorizado lograse entrar en su infraestructura, las nuevas capas de seguridad, que se integran en el nuevo sistema operativo, limitarán los daños que pueden causar y ayudarán a detectar las actividades sospechosas.

Una de las principales novedades en cuanto a la seguridad es la característica exclusiva de Microsoft denominada "Máquinas virtuales blindadas", que permite cifrar las máquinas virtuales con BitLocker y asegurarse con ello que se ejecutan sólo en hosts autorizados por el Servicio de protección de host.

Otra nueva característica de Windows Server 2016 es el entorno protegido que se conoce como Virtual Secure Mode (VSM), utilizado por una serie de componentes, incluyendo la protección de credenciales. Virtual Secure Mode es un entorno de ejecución seguro donde se mantienen claves y procesos críticos de seguridad. Se ejecutan como Trustlets en una partición virtualizada segura.

Otras novedades de seguridad que se implementan con Windows Server 2016 son:

a) Just Enough Administration: Permite conceder permisos granulares a las cuentas de usuarios para limitar sus acciones a las estrictamente necesarias. También es posible reducir el número de administradores de las maquinas con la ayuda de las cuentas virtuales o cuentas de servicio que realizan acciones con privilegios en nombre de usuarios normales.

b) Just in Time Administration: Permite limitar el tiempo de duración de los privilegios concedidos, evitando con ello que existan usuarios con privilegios administrativos que se olviden con el paso del tiempo que fueron concedidos.

c) Credential Guard utiliza la seguridad basada en la virtualización para aislar las claves de usuario para que únicamente el software del sistema con privilegios pueda acceder a ellos. El acceso no autorizado a estos datos puede desencadenar en la sustracción de información con ataques como "Pass-the-Hash" o "Pass-The-Ticket". Credential Guard frena estos ataques mediante la protección de hash de contraseña NTLM y vales de concesión de autenticación Kerberos.

d) Credential Guard remoto ofrece un inicio de sesión único para las sesiones de escritorio remoto (RDP), redirigiendo las solicitudes de Kerberos al dispositivo que está solicitando la conexión. lo que elimina la necesidad de pasar credenciales al host de escritorio remoto (RDP).

e) Device Guard es una combinación de características de seguridad de hardware y software que, configuradas conjuntamente, bloquean un dispositivo para que solo pueda ejecutar aplicaciones de confianza que se definen en la integridad de código. Si la aplicación no es de confianza, no se podrá ejecutar.

f) Control Flow Guard (CFG) es una característica de seguridad de plataforma optimizada para combatir vulnerabilidades de corrupción de memoria.

g) La protección de flujo de control es otra característica de seguridad que viene configurada de forma nativa para bloquear vectores de ataque comunes.

Por último, Windows Defender ayuda a protegerse frente a vulnerabilidades desconocidas sin que ello afecte a los roles de servidor. Windows Defender no es una novedad como tal, pero para los usuarios que desconozcan esta característica, Windows Defender es una protección activa contra malware conocido y actualiza las definiciones de antimalware mediante Windows Update. Windows Defender está instalado de manera predeterminada y funcional en Windows Server 2016.

A continuación, se muestra una tabla comparando las características de seguridad que posee Windows Server 2016 frente a Windows Server 2012 R2.

Nombre del Parámetro	Windows Server 2012 R2	Windows Server 2016
Máquinas virtuales blindadas	○	●
Servicio de protección de host	○	●
Administración Just Enough	●	●
Administración Just in Time	●	●
Credential Guard	○	●
Credential Guard Remoto	○	●
Device Guard	○	●
Integridad de código	○	●
Windows Defender	◐	●
Protección de flujo de control	○	●
Detección de amenazas mejoradas	◐	●

6.6 SERVICIOS DE RED

Las funciones de red son una parte fundamental de la plataforma de Software definido Datacenter (SDDC) y en Windows Server 2016 se proporcionan nuevas y mejoradas tecnologías de redes definidas por software (SDN) para proporcionar una solución SDDC completamente personalizada.

Nota: Para más información acerca de redes definidas por software consulte el siguiente enlace: https://docs.microsoft.com/es-es/windows-server/networking/sdn/plan/plan-a-software-defined-network-infrastructure

A continuación, se detallan las nuevas o mejoradas características de red en Windows Server 2016:

a) Una novedad en Windows Server 2016 se encuentra en el controlador de red el cual proporciona un punto centralizado, programable de la automatización para administrar, configurar, supervisar y solucionar problemas de infraestructura de red físicas y virtuales en el centro de datos.

b) La virtualización de las funciones de red (NFV). El objetivo de NFV es disgregar las funciones de red de dispositivos de hardware y permitir que los servicios de red que ahora son llevados a cabo por routers, firewalls, balanceadores de carga y otros dispositivos de hardware dedicado sean hospedados en máquinas virtuales (VM).

c) Datacenter Firewall. Cuando se implementa y ofrece como un servicio por el proveedor de servicios, los administradores pueden instalar y configurar las directivas de firewall para ayudar a proteger sus redes virtuales de tráfico no deseado que se origina desde Internet y redes de intranet.

d) Puerta de enlace RAS. Es un protocolo de puerta de enlace de borde (BGP) basado en software, compatible con el enrutador de Windows Server 2016 y que se encuentra diseñada para proveedores de servicios de nube (CSP) y las empresas que alojan varias redes virtuales usando la virtualización de Hyper-V. En Windows Server 2016, la puerta de enlace de RAS enruta el tráfico de la red entre la interface de red física y los recursos de red de las máquinas virtuales, con independencia de dónde se encuentren los recursos. Es posible usar la puerta de enlace RAS para enrutar el tráfico de red entre las redes físicas y virtuales en la misma ubicación física o en varias ubicaciones físicas diferentes en Internet.

e) Equilibrador de carga por software (SLB). Es usado para distribuir uniformemente el tráfico de red entre los recursos virtuales.

f) Tecnologías de encapsulación flexible. Es otra de las características incluidas con el conmutador de red, esta tecnología de encapsulación funciona en el plano de datos y admiten LAN Extensible Virtual (VxLAN) y la virtualización de red para la encapsulación de enrutamiento genérico (NVGRE) como mecanismo para virtualizar la dirección IP.

En Windows Server 2016 el rol de servidor DHCP ya no admite NAP, la compatibilidad con NAP se introdujo en el rol de servidor DHCP con Windows Server 2008 y se admite en sistemas operativos anteriores a Windows 10 y Windows Server 2016 del cliente y servidor del Windows. En Windows Server 2016, servidores DHCP no aplica directivas NAP y los ámbitos de DHCP no pueden estar habilitado para NAP.

Ahora, el servidor DNS ofrece una compatibilidad mejorada en las siguientes áreas. Es posible usar la directiva de DNS para la ubicación geográfica a través de la administración del tráfico, las respuestas de DNS inteligentes en función de la hora, o la aplicación de filtros en las consultas DNS entre otras características.

También es posible configurar RRL (Response Rate Limiting) para administrar la respuesta a las solicitudes de un cliente DNS cuando el servidor recibe varias solicitudes de selección del destino al mismo cliente.

Se han mejorado las funcionalidades IPAM para arquitecturas como el control de subredes /32 IPv4 e IPv6 /128 y encontrar subredes con direcciones IP e intervalos en un bloque de direcciones IP, además, es posible usar IPAM para administrar los servidores DNS y DHCP de varios bosques de Active Directory cuando existe entre ellos una relación de confianza bidireccional entre el bosque donde se encuentra implementado IPAM.

Se han incluido mejoras en el rendimiento TCP aumentando el intervalo de congestión inicial (Initial Congestion Window – ICW) se ha aumentado de 4 a 10 y se ha implementado a su vez TCP Fast Open (TFO).

Esta última característica permite reducir la cantidad de tiempo necesario para establecer una conexión TCP que junto con el aumento del ICW permite la transferencia de objetos más grandes.

Para mejorar el comportamiento TCP al realizar una recuperación de pérdida de paquetes, se han implementado las características Tail Loss Probe (TLP) y Recent Acknowledgement (RACK). TLP ayuda a convertir los tiempos de espera de retransmisión (RTO) para recuperaciones rápidas y RACK reduce el tiempo necesario para que la recuperación rápida retransmita un paquete perdido.

7. DOMINIO DE DIRECTORIO ACTIVO

El directorio activo es el servicio de directorio de la plataforma Windows que permite que las aplicaciones encuentren, utilicen y administren recursos de la Organización. Dentro de la planificación y diseño de la infraestructura de "Active Directory", se deben tener en cuenta las medidas de seguridad que se puedan adoptar en la infraestructura. En particular, hay dos aspectos que tienen especial importancia a la hora de aplicar estas guías de configuración: las unidades organizativas y las directivas de dominio agrupadas en GPO.

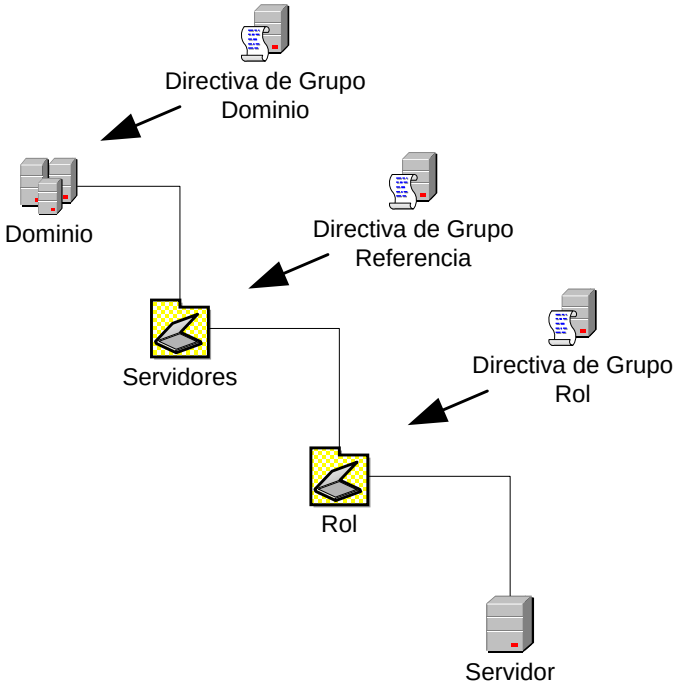
7.1 INFRAESTRUCTURA DE UNIDADES ORGANIZATIVAS

El objetivo del diseño de unidades organizativas, que se describe a continuación, consiste en crear una directiva de grupo homogénea que abarque todos los servidores y que asegure, al mismo tiempo, que los que residan dentro del servicio de directorio satisfagan los estándares de seguridad de su entorno. Con este diseño, cada servidor recibirá las configuraciones de seguridad a través de directivas de grupo en los tres niveles jerárquicos siguientes:

a) **Nivel de Dominio**. Para cumplir los requisitos comunes de seguridad, tales como directivas de cuenta y de contraseñas que deben ejecutarse en todos los servidores del dominio.

b) **Nivel de Referencia**. Para cumplir los requisitos de seguridad específicos del servidor que son comunes a todos los servidores miembros del dominio.

c) **Nivel de Rol**. Para cumplir los requisitos de seguridad de los roles específicos del servidor. Por ejemplo, los requisitos de seguridad de los servidores de infraestructura son distintos de los de los servidores que ejecutan Internet Information Services (IIS).



Este tipo de diseño de unidades organizativas y directivas de grupo permite que todos los servidores y puestos de trabajo de su organización dispongan de una referencia consistente para las configuraciones estándar de seguridad. Además, la estructura de unidades organizativas y la aplicación de directivas de grupo deben proporcionar, mediante un diseño granular, configuraciones de seguridad para tipos específicos de servidores dentro de una Organización.

Un primer paso consiste en establecer Unidades Organizativas (OU) para los distintos roles de servidor. Estas OUs se encontrarán anidadas dentro de una OU para todos los servidores miembro, con excepción de los controladores de dominio quienes poseen su propia OU.

A continuación, y a modo de ejemplo, se describe como realizar esta configuración en un entorno de red clasificada. En primer lugar, se debe crear una directiva de grupo de referencia. Para hacer esto, deberá utilizarse la plantilla de seguridad de referencia "CCN-STIC-570A Servidor Miembro.inf" y vincularla a una directiva de seguridad (objeto de directiva de grupo (GPO)) que se aplique en la unidad organizativa "Servidores Miembro". La directiva de grupo de referencia debe definir las configuraciones deseadas para todos los servidores en una Organización. Esta directiva de grupo de referencia deberá ser tan restrictiva como sea posible en las configuraciones que sean generales. Cualquier rol de servidor que necesite ser diferente de esta política deberá incluirse en OUs específicas de servidor por separado.

Continuando con lo indicado en el apartado anterior, será necesario crear una directiva de grupo distinta para los cambios graduales en las directivas que se ajusten a los distintos roles de servidor que puedan existir en la Organización. Asignando estos roles a unidades organizativas de niveles, que cuelgan de la OU de servidores miembro, los cambios serán acumulativos, simplificando la gestión de directivas de seguridad y asegurando la existencia de una configuración de seguridad consistente, aplicada a todos los equipos miembros de la Organización.

Hay múltiples modos de generar estructuras lógicas del Directorio Activo. No obstante, será necesario familiarizarse con este modo, ya que será la referencia empleada en todas las guías de la serie CCN-STIC-500. En el conjunto de guías desarrollado para los distintos productos, se

espera que todos los archivos de plantillas incrementales se apliquen a OUs situadas debajo de la OU de los servidores miembro. Por esta razón y siguiendo el ejemplo, cada una de estas OUs de nivel inferior requiere que se aplique el archivo "CCN-STIC-570A Servidor Miembro.inf" y el archivo incremental específico a éstas para definir el rol que cada una llevará a cabo en la organización, ya que los requisitos de seguridad para cada uno de los roles de servidor son diferentes.

Nota: Esta guía asume que los servidores que ejecutan Windows Server 2016 realizarán roles específicamente definidos. Si los servidores en la organización no corresponden a estos roles o dispone de servidores multipropósito, se deben utilizar las configuraciones definidas aquí como una guía para crear plantillas de seguridad propias. Sin embargo, debe tenerse en cuenta que cuantas más funciones realicen los servidores, más compleja será su configuración, más servicios quedarán expuestos y más vulnerables serán a un posible ataque.

De los diferentes roles que puede tener un servidor, el de controlador de dominio es especial. Las cuentas de estos servidores no estarán situadas en una unidad organizativa por debajo de la OU de los servidores miembro; sino que residirán en el contenedor especial "Domain Controllers". Por esta razón, se creará una política incremental específica para controladores de dominio y, en esta política, se implantará la plantilla "CCN-STIC-570A Controlador Dominio.inf" en el caso del ejemplo de una red clasificada.

7.2 DIRECTIVAS DE DOMINIO

Es importante resaltar que cuando un equipo pertenece a un dominio, las cuentas de usuarios, servicios y administradores de ese dominio se rigen por las políticas de cuentas que estén definidas en el dominio y las políticas de cuentas locales del servidor sólo afectarán a las cuentas locales. Por lo tanto, para establecer directivas de contraseñas, bloqueo de cuentas, etc., será necesario realizarlo a nivel de dominio.

La mayoría de las configuraciones de seguridad tratadas en este apartado son para contraseñas y cuentas de usuarios. Cuando revise estas configuraciones y recomendaciones, tenga presente que todas las configuraciones se aplican a todos los usuarios que están dentro de los límites del dominio.

7.2.1 DIRECTIVA DE CUENTA

Las directivas de cuenta definidas a continuación afectan a todas las cuentas de usuarios, servicios y administradores pertenecientes al dominio.

7.2.1.1 DIRECTIVA DE CONTRASEÑAS

Las contraseñas complejas que cambian regularmente reducen la posibilidad de que un ataque de contraseñas tenga éxito. Las configuraciones de las políticas de contraseñas controlan la complejidad y la vida útil de las contraseñas. Esta sección analiza cada configuración de la política de contraseñas específica.

Estas pautas también se deben utilizar para todas las contraseñas de cuentas de servicio en la Organización. Es importante recalcar que las políticas de contraseñas definidas en la directiva de dominio afectan a las cuentas de usuarios de ese dominio de "Active Directory". Estos valores se establecen dentro del complemento "Plantillas de Seguridad" en la siguiente ubicación.

a) Directivas de cuenta\Directiva de contraseñas

Crear requisitos estrictos para la longitud y complejidad de las contraseñas no necesariamente se traduce en usuarios y administradores que utilizan contraseñas robustas.

Con las políticas de contraseñas activadas, los usuarios del sistema pueden satisfacer los requisitos de complejidad técnica para una contraseña definida por el sistema, pero se requieren políticas de seguridad sólidas adicionales para cambiar los malos hábitos relacionados con el uso de las contraseñas. Por ejemplo, “Clasificado1” podría satisfacer los requisitos de complejidad de las contraseñas, pero esta no es una contraseña muy difícil de determinar.

Toda Organización debe establecer unas pautas de seguridad para crear contraseñas adecuadas, que incluyan:

a) Evitar el uso de palabras que figuren en un diccionario, palabras con faltas de ortografía comunes o juegos de palabras y palabras extranjeras.

b) Evitar utilizar contraseñas a las que se le añade un dígito simplemente.

c) Evitar utilizar contraseñas que otros puedan adivinar fácilmente viendo su escritorio o bien por ingeniería social (como los nombres de sus mascotas, equipos deportivos y familiares).

d) Evitar pensar en las contraseñas como palabras propiamente dichas, hay que pensar en códigos secretos.

e) Deben emplearse contraseñas que requieran escribir con ambas manos en el teclado.

f) Deben usarse letras mayúsculas y minúsculas, números y símbolos en todas las contraseñas.

g) Deben usarse espacios y caracteres que sólo se pueden producir utilizando la tecla "Alt".

Además de las políticas de contraseñas anteriores, algunas organizaciones requieren un control centralizado sobre todos los usuarios. A continuación, se describe cómo evitar que los usuarios cambien sus contraseñas excepto cuando se les pide que lo hagan. Los usuarios pueden cambiar sus contraseñas durante los periodos mínimo y máximo de las contraseñas. Sin embargo, el diseño de un entorno de Alta Seguridad requiere que los usuarios cambien sus contraseñas sólo cuando el sistema operativo se lo indica pasados los días, según está configurado en el parámetro "Tiempo máximo de las contraseñas".

Para evitar que los usuarios cambien sus contraseñas (excepto cuando se requiera), puede deshabilitar la opción "Cambiar una contraseña..." de las opciones que se muestran cuando se presiona CTRL+ALT+SUPR. Puede implementar esta configuración para todo un dominio utilizando una Política de Grupo o editando el registro para uno o más usuarios específicos.

En la presente guía, se mostrará también como hacer uso de la funcionalidad de FGPP (directiva de contraseña específica) para establecer criterios de contraseñas diferentes en función del tipo de usuario o rol.

7.2.1.2 DIRECTIVA DE BLOQUEO DE CUENTA

La directiva de bloqueo de cuentas es una característica de seguridad de Windows Server 2016 que bloquea la cuenta de un usuario después de varios intentos de inicio de sesión fallidos durante un periodo de tiempo específico. El usuario no puede iniciar sesión con una cuenta que

se encuentre bloqueada y el servidor puede configurarse para responder a este tipo de posible ataque deshabilitando la cuenta para un número predeterminado de intentos fallidos de iniciar una sesión.

Estos parámetros de la política de seguridad ayudan a evitar que los atacantes adivinen las contraseñas de un usuario, reduciendo así la probabilidad de que un ataque contra su entorno de red tenga éxito.

Los valores de directiva de bloqueo de cuentas se establecen dentro del complemento "Plantillas de seguridad" en la siguiente ubicación:

a) Directivas de cuenta\Directiva de bloqueo de cuenta

Establecer una política de bloqueo de cuentas tan restrictiva incrementa la seguridad del entorno, pero, como contrapartida, también puede incrementar la carga administrativa asociada a desbloquear las cuentas de usuarios.

Además, también se debe tener en cuenta que esta política de bloqueo de cuentas puede permitir un ataque por denegación de servicio a un atacante que, conociendo los nombres de las cuentas, ejecute varios intentos incorrectos de inicio de sesión, impidiendo así el acceso al usuario legítimo.

Debe tener en consideración que la única cuenta que no se encuentra supeditada a esta protección es la del Administrador. Para evitar ataques de código malicioso sobre dicha cuenta es requerimiento el cambio del nombre de la misma.

Al igual que con las contraseñas, es posible hacer uso de la funcionalidad de FGPP (directiva de contraseña específica) para un mejor control de los sistemas de bloqueo de cuenta.

7.2.1.3 DIRECTIVA KERBEROS

Las directivas de Kerberos se utilizan para las cuentas de usuarios del dominio. Estas políticas determinan los parámetros relacionados con el protocolo Kerberos versión 5, como la vida útil de los tickets y su ejecución. Las directivas Kerberos no existen en las directivas locales.

Disminuir la vida útil de los tickets Kerberos reduce el riesgo de que un atacante robe las contraseñas y después se haga pasar por una cuenta legítima de usuario. Sin embargo, mantener estas políticas aumenta los costos de autorización. En la mayoría de los entornos, no se deben cambiar los valores predeterminados para estas políticas. Las configuraciones Kerberos se incluyen en la directiva de dominio para que afecte a todo el conjunto. Estos valores se establecen dentro del complemento "Plantillas de Seguridad" en la siguiente ubicación:

a) Directivas de cuenta\Directiva Kerberos

7.2.2 DIRECTIVAS LOCALES

7.2.2.1 OPCIONES DE SEGURIDAD

Existen algunas directivas en las opciones de seguridad que también se comportan como políticas de cuenta y que se deben considerar a nivel dominio para que afecten a las cuentas del dominio (los ejemplos más significativos son: Seguridad de red: forzar el cierre de sesión cuando expire la hora de inicio de sesión y Servidor de red Microsoft: desconectar a los clientes cuando expire el tiempo de inicio de sesión).

Estos valores se establecen dentro del complemento "Plantillas de Seguridad" en la siguiente ubicación.

a) Directivas locales\Opciones de seguridad

Algunos de estos parámetros requieren explicaciones adicionales que se ofrecen en los siguientes apartados:

a) **Acceso de red: permitir traducción SID/nombre anónima.** Si esta directiva está activada en un controlador de dominio, un usuario que conozca los atributos SID de un administrador podría contactar con un equipo que también tenga esta directiva activada y usar el SID para obtener el nombre del administrador. Entonces, esa persona podría usar el nombre de cuenta para iniciar un ataque intentando adivinar la contraseña.

   No obstante, debe tenerse en cuenta que la desactivación de este parámetro puede provocar que los sistemas heredados sean incapaces de comunicarse con los dominios basados en Windows Server 2016. Algunos de los servicios heredados que pueden presentar este problema son:

   i. Servidores RAS basados en Windows NT 4.0.

   ii. Los servidores RAS que, ejecutándose en servidores Windows 2000, pertenecen a dominios Windows NT 3.X o Windows NT 4.0.

   iii. Servidores SQL basados en Windows NT 4.0.

   iv. Los servidores SQL que, ejecutándose en servidores Windows 2000, pertenecen a dominios Windows NT 3.X o Windows NT 4.0.

   v. Aplicaciones Web sobre IIS configuradas para usar autentificación básica y con acceso anónimo desactivado. En este caso, la cuenta de usuario Invitado no podrá acceder a la aplicación Web.

b) **Seguridad de red: configurar tipos de cifrado permitidos para Kerberos.** Esta configuración de directiva permite establecer los tipos de cifrado que puede usar Kerberos, y sólo se admite en versiones de Windows iguales o superiores a Windows 7 y Windows Server 2008 R2, incluyendo en ellos por lo tanto a Windows Server 2016.

   La configuración recomendada es la más segura de las disponibles en el momento de redactar la guía que permite el uso de los servicios más comunes. No obstante, debe tenerse en cuenta que el nivel de cifrado recomendado sólo podrá ser utilizado por equipos Windows Server 2008 R2 y Windows 7 o posteriores; si en el dominio existen equipos con versiones de Windows anteriores será necesario editar la configuración de este parámetro para permitir algún otro tipo de cifrado que pueda ser utilizado por esos equipos antiguos.

Nota: Tenga en consideración que debido a la aplicación de ciertas configuraciones de seguridad en cuanto a cifrado es posible que productos como Microsoft Exchange Server, Microsoft Sharepoint o Hyper-V no funcionen debido a dicha configuración.

7.2.3 REGISTRO DE EVENTOS

Los registros de eventos registran los eventos del sistema y de aplicaciones. El registro de seguridad captura y almacena los eventos de auditoría.

El contenedor “Registro de eventos”, en la plantilla de seguridad, se utiliza para definir atributos relacionados con los registros de eventos de aplicaciones, la seguridad y el registro de eventos del sistema, tales como el tamaño máximo del registro, derechos de acceso para cada registro y parámetros y métodos de retención. Las configuraciones para los registros de eventos de aplicaciones, de la seguridad y del sistema se configuran en la política de referencia con el fin de aplicarse a todos los miembros del dominio. Posteriormente, en cada unidad organizativa se podrá crear una directiva específica para los distintos roles de servidores.

Las configuraciones del registro de eventos se pueden modificar utilizando el complemento de "Plantillas de Seguridad" en la siguiente ubicación".

a) Registro de eventos

8. CONTROLADOR DE DOMINIO Y SERVIDOR MIEMBRO

El controlador de dominio es uno de los roles fundamentales, junto al servicio de DNS, que da funcionalidad a la infraestructura del Directorio Activo. De su seguridad depende en gran medida, la protección de una organización. La guía, por lo tanto, plantea la necesidad de establecer una elevada protección para estos roles.

Dentro de este apartado, se incluirán las configuraciones de seguridad que son necesarias para un controlador de dominio. Un dominio puede tener varios servidores actuando como controladores de dominio. La mayoría de las configuraciones que se establecen en este apartado se deberán crear una única vez, independientemente del número de controladores de dominio existentes.

Debido a su importancia y a la criticidad de los datos que almacenan, los controladores de dominio siempre deben estar almacenados en ubicaciones físicamente protegidas a las que sólo tenga acceso el personal administrativo cualificado. No se debe mezclar el rol de controlador de dominio con otros servicios que pueda prestar la organización, salvo que sea estrictamente necesario como, por ejemplo, cuando la infraestructura solo tenga un servidor.

Así mismo dentro de este apartado también se tratan las configuraciones que son necesarias para servidores miembro que, aunque no sean controladores de dominio cumplen otro rol dentro de la organización y por lo tanto deben poseer también seguridad.

8.1 PLANTILLA DE SEGURIDAD

Las directivas definidas anteriormente establecen la configuración general que debe aplicarse sobre todo el dominio. Sin embargo, ciertas configuraciones son recomendables establecerlas a nivel del rol que cumple cada sistema.

En este apartado, se definen los valores adicionales de seguridad para los controladores de dominio y servidores miembro que ejecutan Windows Server 2016.

Para los controladores de dominio se debe definir una nueva plantilla específica incremental para no alterar la GPO por defecto "Default Domain Controllers Policy" que proporciona Microsoft. No obstante, tal y como se establecerá en los diferentes paso a paso, la nueva GPO tendrá prioridad frente a la predefinida por Microsoft para los controladores de dominio. Se asume, en estas configuraciones, que el dominio se ha configurado conforme a lo descrito en el apartado de "Active Directory".

Los equipos definidos servidor miembro poseerán también un objeto GPO adicional al aplicado al nivel de dominio que permita establecer seguridad sobre los mismos al igual que sobre los controladores de dominio.

8.1.1 DIRECTIVAS DE CUENTA

Las directivas de cuenta que afectan a las cuentas de dominio se han definido a nivel de dominio por lo que no es necesario definir ninguna configuración dentro de este conjunto de directivas salvo que se requiera de una configuración adicional.

8.1.2 DIRECTIVAS LOCALES

8.1.2.1 DIRECTIVAS DE AUDITORÍA

La directiva de auditoría determina los sucesos de seguridad que se generan, de manera que se registre la actividad del usuario o del sistema. El administrador puede supervisar la actividad relacionada con la seguridad como, por ejemplo, quién accede a un objeto, si un usuario se conecta o desconecta de un equipo, o si se realizan cambios a una configuración de directiva de auditoría.

Antes de implementar las directivas de auditoría, se deberá decidir qué categorías de sucesos se deben auditar para el entorno corporativo. Las configuraciones de auditoría que elija un administrador, para las categorías de sucesos, definen la política de auditoría empresarial. Al definir las configuraciones de auditoría para las categorías específicas de sucesos, los administradores pueden crear una política de auditoría que se ajuste a las necesidades de seguridad de una Organización.

Si no se configura ninguna auditoría, será difícil, o imposible, determinar qué sucedió durante un incidente de seguridad. Sin embargo, si se configura la auditoría para que demasiadas actividades autorizadas generen sucesos, el registro de eventos de seguridad se llenará con datos inútiles. Por tanto, se deberá realizar una configuración para equilibrar aquello que se supervisa, de manera que los datos recopilados tengan relevancia.

Los valores de directiva de auditoría se establecen dentro del complemento "Plantillas de Seguridad" en la siguiente ubicación.

a) Directivas locales\Directiva de auditoría

8.1.2.2 ASIGNACIÓN DE DERECHOS DE USUARIO

La asignación de derechos de usuario determina qué usuarios o grupos tienen derechos o privilegios en el servidor tales como iniciar una sesión local, depurar programas o restaurar archivos y directorios. Los permisos o privilegios de usuarios controlan los permisos que los usuarios tienen en el sistema de destino. Se usan para conceder el permiso para realizar ciertas acciones como el inicio de una sesión en red o local, así como tareas administrativas como, por ejemplo, generar nuevos tokens de inicio de sesión.

Los valores de la asignación de derechos de usuario se establecen dentro del complemento "Plantillas de Seguridad" en la siguiente ubicación.

a) Directivas locales\Asignación de derechos de usuario

Nota: Algunas cuentas y grupos de seguridad no se pueden incluir en las plantillas debido a que sus identificadores de seguridad (SIDs) son específicos para cada dominio. Por ejemplo, un grupo creado "a mano" no posee un identificador único que permita añadirlo a la plantilla de seguridad por lo que se debe hacer manualmente.
Así mismo, debe tenerse en cuenta la distinción entre Administradores (grupo) y Administrador (usuario). Por ejemplo, si se agrega el grupo Administradores en lugar del usuario Administrador a los permisos de usuario de acceso denegado, se negará ese derecho a todos los usuarios del grupo Administradores.

Algunos parámetros requieren de explicaciones adicionales que se ofrecen en los siguientes apartados:

a) Denegar el acceso a este equipo desde la red. Este permiso de usuario denegará ciertos protocolos de red, incluidos los protocolos basados en SMB, NetBIOS, CIFS (Common Internet File System), HTTP y COM+ (Component Object Model Plus). La configuración de esta directiva reemplaza al permiso de usuario "Tener acceso a este ordenador desde la red" cuando una cuenta de usuario está sujeta a ambas directivas.

Nota: Algunas de las cuentas y grupos, incluidos en este permiso, tendrán SIDs únicos para cada dominio de la organización; por lo tanto, deben añadirse manualmente en las plantillas de seguridad.

b) **Denegar el inicio de sesión a través de Servicios de Escritorio remoto.** Deberán incluirse los usuarios y grupos a los que se quiere denegar el acceso mediante Terminal Services. En caso de que un usuario tenga el permiso "Permitir" asociado a esta denegación, prevalecerá la opción más restrictiva (la denegación de acceso).

Nota: Algunas de las cuentas y grupos, incluidos en este permiso, tendrán SIDs únicos para cada dominio de la organización; por lo tanto, deben añadirse manualmente en las plantillas de seguridad.

c) **Habilitar confianza con el equipo y las cuentas de usuario para delegación.** Esta configuración de seguridad determina qué usuarios pueden establecer la configuración "Se confía para delegación" en un objeto de equipo o usuario. Un proceso de servidor que se ejecuta en un equipo (o en un contexto de usuario) de confianza para la delegación puede obtener acceso a los recursos de otro equipo mediante credenciales delegadas de un cliente, siempre y cuando la cuenta de cliente no tenga establecido el marcador de control de cuenta que indica que la cuenta no se puede delegar.

   Un uso incorrecto de este derecho de usuario o de la configuración "Se confía para delegación" podría hacer que la red fuera vulnerable a ataques sofisticados mediante programas de caballo de Troya que suplantan a los clientes entrantes y usan sus credenciales para obtener acceso a los recursos de red.

   En controladores de dominio, el grupo Administradores, o aquellos usuarios que vayan a unir nuevos controladores de dominio al dominio, necesitan tener asignado este derecho de usuario. De lo contrario, fallará la promoción de nuevos servidores a controladores de dominio.

   En el resto de equipos (servidores miembros y estaciones de trabajo), en general, no es necesario asignar este derecho de usuario a ningún usuario o grupo.

d) **Omitir comprobación de recorrido.** La configuración errónea de esta directiva puede producir varios problemas. Para más información sobre estos problemas conocidos véase la sección "Saltarse la comprobación" del siguiente documento de Microsoft:

   http://support.microsoft.com/kb/823659#method3

e) **Tener acceso a este equipo desde la red.** Este permiso de usuario es requerido por varios protocolos de red, incluidos los protocolos basados en SMB, NetBIOS, CIFS, HTTP y COM+. Aunque en Windows Server 2016 los permisos concedidos al grupo de seguridad "Todos" ya no dan acceso a los usuarios anónimos, los grupos y cuentas invitados todavía pueden obtener acceso a través del grupo de seguridad "Todos". Por este motivo, debe limitarse el empleo de este grupo de seguridad.

Nota: Cuando se desee asignar un permiso o privilegio a un usuario no se debe hacer al grupo “Todos”. En su lugar se debe emplear el grupo “Usuarios del dominio” o el grupo “Usuarios autentificados”.

8.1.2.3 OPCIONES DE SEGURIDAD

Las directivas de opciones de seguridad permiten configurar un gran número de aspectos del sistema entre los que se encuentra los nombres de Administrador y de Cuenta de invitado, el acceso a unidades de disco y unidades de CD-ROM, la instalación de controladores, el inicio de sesión, etc. Más concretamente los aspectos que permiten modificar son los siguientes:

a) Cuentas: Configuraciones adicionales a las directivas de cuenta.
b) Auditoría: Configuraciones adicionales a las directivas de auditoría.
c) DCOM: Configuraciones para el modelo de objetos de componentes distribuidos.
d) Dispositivos: Configuraciones para la conexión y desconexión de dispositivos en el equipo, así como acciones realizadas sobre los mismos.
e) Controlador de dominio: Configuraciones específicas para los controladores de dominio.
f) Miembro de dominio: Configuraciones para equipos pertenecientes a un dominio.
g) Inicio de sesión: Configuraciones para definir acciones sobre el inicio de sesión en los equipos.
h) Cliente re red Microsoft: Configuraciones para establecer las comunicaciones entre equipos clientes.
i) Servidor de red Microsoft: Configuraciones para establecer las comunicaciones entre equipos servidores.
j) Acceso a la red: Configuraciones para definir acciones sobre los accesos a la red.
k) Seguridad de red: Configuraciones sobre aspectos de protocolos en red.
l) Consola de recuperación: Configuraciones para determinar acciones a poder realizar sobre la consola de recuperación.
m) Apagar: Configuraciones para definir el apagado del equipo.
n) Criptografía: Configuraciones acerca de algoritmos a utilizar.
o) Objetos del sistema: Configuración para distinción de mayúsculas y minúsculas, así como el refuerzo sobre los permisos de objetos de Windows.
p) Configuración del sistema: Configuración para compatibilidades y procesamiento de certificados.
q) Control de cuentas de usuario: Configuraciones para establecer el comportamiento de la UAC.

Los controladores de dominio reciben las opciones de seguridad de la política de controladores de dominio por defecto. Tal y como se ha descrito con anterioridad se debe definir una política de grupo que tenga prioridad sobre la que se establece por defecto. Estas

directivas deberán ser más restrictivas para no rebajar la seguridad establecida por la política por defecto

Los valores de las opciones de seguridad se establecen dentro del complemento "Plantillas de Seguridad" en la siguiente ubicación.

a) Directivas locales\Opciones de seguridad

Algunos de estos parámetros requieren explicaciones adicionales que se ofrecen en los siguientes apartados:

a) **Auditoría: apagar el sistema de inmediato si no se pueden registrar las auditorías de seguridad.** Además de apagar los servidores inmediatamente cuando no se pueden registrar más eventos de auditoría de seguridad, esta opción de seguridad podría afectar a la funcionalidad de los servicios.

b) **Auditoría: forzar la configuración de subcategorías de la directiva de auditoría (Windows Vista o posterior) para invalidar la configuración de la categoría de directiva de auditoría.** Windows Vista y las versiones posteriores de Windows permiten administrar la directiva de auditoría de una manera más precisa mediante subcategorías de directiva de auditoría. Las nuevas subcategorías de directiva de auditoría se pueden configurar mediante directivas de grupo en la ubicación "Configuración del equipo\Directivas\Configuración de Windows\Configuración de seguridad\Configuración de directiva de auditoría avanzada\Directivas de auditoría". Sin embargo, si se establece una directiva de auditoría en el nivel de categoría se invalida la nueva característica de directiva de auditoría de subcategorías, salvo que se habilite esta directiva.

   Las nuevas subcategorías incluyen las siguientes: Inicio de sesión de cuentas, Administración de cuentas, Seguimiento detallado, Acceso DS, Inicio y cierre de sesión, Acceso a objetos, Cambio en directivas, Uso de privilegios, Sistema, Auditoría de acceso a objetos global.

c) **Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (siempre).** Esta opción determina si el componente del cliente SMB requiere la firma de paquetes. Esta opción puede impedir la comunicación con servidores SMB que no soporten la firma de las comunicaciones o que no tengan habilitadas las opciones de servidor correspondientes: Servidor de red Microsoft; Firmar digitalmente las comunicaciones (si el servidor lo permite) o Servidor de red Microsoft: Firmar digitalmente las comunicaciones (siempre).

d) **Criptografía de sistema: usar algoritmos que cumplan FIPS para cifrado, firma y operaciones hash.** Aunque esta opción está deshabilitada en esta configuración, conviene aclarar que si se habilita sólo se utilizará el protocolo TLS 1.0 y dejarán de funcionar las conexiones con SSL 2.0 o SSL 3.0. Para más información sobre estos problemas conocidos:

   i. "PRB: Cannot visit SSL sites after you enable FIPS compliant cryptography"

      http://support.microsoft.com/kb/811834

e) **DCOM: restricciones de acceso al equipo en sintaxis de Lenguaje de definición de descriptores de seguridad (SDDL).** Esta configuración de directiva determina los usuarios o grupos que pueden tener acceso a las aplicaciones DCOM de forma local o remota. Esta configuración se usa para controlar la superficie expuesta a ataques del equipo en el uso de aplicaciones DCOM. Cuando se especifican los usuarios o grupos que deben obtener permiso, el campo del descriptor de seguridad se rellena con la representación del Lenguaje de definición de descriptores de seguridad de esos grupos y privilegios. Si el descriptor de seguridad se deja en blanco, la configuración de directiva se define en la plantilla, pero no se aplica. Los usuarios y grupos pueden obtener privilegios explícitos Permitir o Denegar para el acceso tanto local como remoto.

   Si un acceso es permitido por esta directiva, dicho acceso además tendrá que ser permitido por la propia aplicación DCOM (las aplicaciones DCOM pueden opcionalmente establecer sus propias listas de control de acceso) para que sea realmente admitido.

f) **DCOM: restricciones de inicio de equipo en sintaxis de Lenguaje de definición de descriptores de seguridad (SDDL).** Esta directiva es similar a la anterior, pero para iniciar o activar aplicaciones DCOM, en lugar de acceder a ellas.

g) **Seguridad de red: no almacenar valor de hash de LAN Manager en el próximo cambio de contraseña.** De forma predeterminada, los sistemas previos a Windows Vista empleaban LM como mecanismo para almacenar los hashes derivados de las contraseñas. No obstante, debe tenerse en consideración que dicho protocolo es muy débil y puede implicar riesgos de seguridad muy importantes. Esta configuración fuerza a que no se almacenen dichos hashes y, por lo tanto, no puedan emplearse en el entorno de dominio. Esto podría ocasionar problemas con servicios de red, ya obsoletos, que solo admiten autenticación con hashes de tipo LM. Si presenta alguno de esos servicios debería evaluarse su retirada de la infraestructura de la organización.

h) **Seguridad de red: restringir NTLM.** *(Varias opciones)*

   A continuación, se comentan, de forma conjunta, las diversas opciones de seguridad relativas a la restricción del uso del protocolo NTLM: aquellas cuya descripción comienza por "Seguridad de red: restringir NTLM:".

   Estas opciones de seguridad permiten eliminar el uso del protocolo de autenticación NTLM, de modo que sólo se puedan utilizar otros protocolos de autenticación que se consideren más seguros, como Kerberos.

   Desde el punto de vista de la seguridad, sería deseable eliminar la utilización del protocolo NTLM, pero no se puede obviar el hecho de que todavía muchas aplicaciones dependen de su uso.

   Por ello, la configuración recomendada permite todavía el uso de NTLM, pero, al mismo tiempo, activa las capacidades de auditoría de eventos de autenticación NTLM, para facilitar la transición a una futura configuración sin protocolo NTLM: los administradores, revisando esos eventos, podrán comprobar qué aplicaciones de su entorno utilizan NTLM y podrán, así, determinar si es posible desactivar NTLM. En el caso de encontrar aplicaciones utilizando NTLM, se podrá evaluar la sustitución de dichas aplicaciones por nuevas versiones o nuevas aplicaciones que no lo utilicen.

i) **Servidor de red Microsoft: nivel de validación de nombres de destino SPN del servidor.** Esta configuración de seguridad determina el nivel de validación que realiza un servidor

SMB en el nombre principal de servicio (SPN) proporcionado por el cliente SMB al intentar establecer una sesión en un servidor SMB.

La opción "Requerido del cliente" hace que el cliente deba enviar un nombre SPN en la configuración de sesión y que dicho nombre coincida con el servidor SMB al que se solicita establecer una conexión. Si el cliente no proporciona ningún SPN o el SPN proporcionado no coincide, se deniega la sesión.

Es posible que esta opción cause problemas con sistemas anteriores a Windows Server 2008 y Windows Vista. Si fuera necesario el uso de sistemas heredados en el dominio, podría ser necesario cambiar esta configuración a "Aceptar si lo proporciona el cliente" (preferido) o a "Deshabilitado" (opción menos segura).

j) **Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre).** Esta opción impide la comunicación con este servidor a los siguientes clientes:

i. Clientes de red de Microsoft MS-DOS (por ejemplo, Microsoft LAN Manager)

ii. Clientes de red de Microsoft Windows for Workgroups

iii. Equipos con Microsoft Windows 95 sin el componente "DS Client" instalado

iv. Equipos con Microsoft Windows NT 4.0 sin SP3 o superior

v. Clientes Novell Netware 6 CIFS

vi. Clientes SMB SAMBA que no tengan soporte para firma SMB

8.1.3 SERVICIOS DEL SISTEMA

Cuando se instala por primera vez Windows Server 2016, se crean los servicios predeterminados del sistema y se configuran para ejecutarse cuando se inicia el sistema. Algunos de estos servicios no necesitan ejecutarse en ciertos entornos.

Existen servicios opcionales adicionales con Windows Server 2016, como el servicio denominado "Servicios de certificados de Active Directory", que no se instala durante la instalación predeterminada de Windows Server 2016. Los servicios opcionales se pueden añadir a un sistema existente habilitando roles o características manualmente, utilizando la consola del Administrador del Servidor, o de manera automatizada utilizando cmdlets de PowerShell.

Cualquier servicio o aplicación es un punto potencial de ataque. Por lo tanto, todos los servicios o archivos ejecutables que no sean necesarios deben ser desactivados o eliminados en el entorno objetivo. Las plantillas de seguridad asociadas a esta guía tienen en consideración este hecho y, por lo tanto, deshabilitarán todos aquellos servicios que se consideran innecesarios en una red de máxima seguridad o bien no sean necesarios para un funcionamiento normal del entorno. Si en algunos de sus controladores de dominio o servidores miembro necesitara habilitar un servicio deshabilitado a través de las GPO de la presente guía deberá realizar la modificación en la plantilla incremental de controladores de dominio o del servidor miembro. Valore, no obstante, las repercusiones de habilitar dicho servicio y establezca medidas para garantizar que el servicio se encuentra siempre actualizado.

Se debe tener en consideración que Microsoft puede agregar nuevos servicios que deberán ser configurados adecuadamente.

Esta guía asume que el servidor controlador de dominio tendrá activos los roles "Servicios de dominio de Active Directory" y "Servidor DNS", porque el segundo suele ir unido al primero, como se comenta más adelante.

Las configuraciones de los servicios del sistema se pueden modificar utilizando el complemento de "Plantillas de seguridad" en la siguiente ubicación.

a) Servicios del sistema

Hay determinados servicios cuyo estado puede producir problemas, en este apartado se ofrecen explicaciones para algunos de estos servicios:

a) **Aplicación auxiliar de NetBIOS sobre TCP/IP.** Si se deshabilita este servicio el sistema no será capaz de acceder a las carpetas compartidas donde se encuentran los objetos de directiva de grupo (GPOs).

b) **Aplicación auxiliar IP.** Este servicio proporciona conectividad de túnel mediante tecnologías de transición IPv6 (6to4, ISATAP, Proxy de puerto y Teredo) e IP-HTTPS. Si se detiene este servicio, el equipo no contará con la conectividad de red para aplicaciones IPv6 que ofrecen estas tecnologías.

c) **Cliente DHCP.** El servicio cliente DHCP se utiliza para obtener direcciones IP dinámicas de un servidor DHCP y para realizar las actualizaciones automáticas en DNS, incluso cuando el servidor tiene una dirección IP estática. Si se deshabilita este servicio o se establece un arranque manual, se deberá utilizar otro mecanismo para el registro en DNS.

d) **Inicio de sesión en red.** Si se deshabilita el servicio Inicio de sesión en red (Netlogon), el servidor experimentará problemas al actuar como miembro de dominio, ocasionando fallos como la no aplicación de las políticas de grupo.

e) **Programador de tareas.** En Windows Server 2016 no se aconseja deshabilitar este servicio porque muchas tareas críticas del sistema se realizan como tareas programadas, incluso las anexas al administrador del servidor.

f) **Servicio de Registro Remoto.** El acceso remoto al registro se limita a los usuarios autorizados que, de forma predeterminada, son únicamente los administradores. Si se deshabilita o se detiene este servicio, no se podrán utilizar servicios de obtención de información remota como MBSA, STAT Scanner, ISS y otros. Además, de este servicio depende el servicio "Espacio de nombres DFS".

g) **Servicio de Transferencia Inteligente en Segundo Plano (BITS).** El servicio de actualizaciones automáticas (Windows Update) depende del servicio BITS para la descarga de actualizaciones, por lo tanto, si se deshabilita este servicio no será posible realizar las actualizaciones automáticas con Windows Update, Software Update Services o System Center Configuration Manager.

h) **Servidor.** Si se deshabilita este servicio, no se podrán utilizar directorios compartidos de archivos y de recursos administrativos como “C$”. Además, dejarán de funcionar aplicaciones que dependen de la existencia de algún recurso compartido administrativo (por ejemplo: “ADMIN$”).

i) **Servidor DNS.** El Directorio Activo se basa en las consultas DNS para localizar servicios y recursos en la red. Por lo tanto, para el correcto funcionamiento del servicio de directorio es necesario que exista una infraestructura DNS. Por simplicidad, se suele integrar el servicio DNS en los controladores de dominio, que es la solución recomendada.

j) **Windows Update** (Actualizaciones automáticas). Al deshabilitar el servicio Windows Update, el servidor no podrá recibir las actualizaciones automáticas de seguridad ni con Windows Update ni con Software Update Services. Por lo tanto, se debe establecer otro mecanismo para mantener actualizado el servidor. Si se necesita usar el servicio de actualizaciones automáticas entonces será necesario activar este servicio junto con el servicio "Servicio de Transferencia Inteligente en Segundo Plano (BITS)".

8.1.4 REGISTRO

La plantilla de seguridad permite aplicar permisos más restrictivos a las entradas del registro del servidor. En general, la seguridad por defecto de Windows Server 2016 en el registro es adecuada, aun así, se deben introducir modificaciones.

Las configuraciones de permisos sobre el registro se pueden configurar utilizando el complemento "Plantillas de Seguridad" en la siguiente ubicación.

a) Registro

8.1.5 SISTEMA DE FICHEROS

Generalmente no se recomienda modificar las listas de control de acceso existentes por defecto en un servidor Windows Server 2016 por las siguientes razones:

a) Windows Server 2016, como las versiones predecesoras, suprime la principal preocupación que había en versiones anteriores, la existencia de SID en las listas “Todos”. Así, ya no es necesario reemplazar “Todos” por “Usuarios autenticados”.

b) Las amplias modificaciones en las listas de control de acceso representan un aumento exponencial del coste en cuanto a mantenimiento.

c) Los efectos potenciales de excesivas modificaciones en ACLs cuando se proceda a la actualización del sistema y la adición (quizás impensable aún) de nuevos componentes.

No obstante, es recomendable establecer listas de control de acceso en rutas estratégicas con el fin de impedir la ejecución de ciertas acciones por parte de usuarios no administradores, asumiendo el coste de soporte adicional que es necesario en redes altamente críticas.

Las configuraciones de permisos sobre el sistema de ficheros se pueden configurar utilizando el complemento de "Plantillas de Seguridad" en la siguiente ubicación.

a) Sistema de archivos

8.2 CONFIGURACIONES ESPECÍFICAS DEL CONTROLADOR DE DOMINIO

Para completar la configuración de la plantilla de seguridad de un controlador de dominio se deberán revisar las configuraciones adicionales propuestas en el apartado “9 BLOQUEOS ADICIONALES”. Además, en este apartado se incluyen algunos bloqueos específicos del rol de controlador de dominio.

8.2.1 ASIGNACIÓN DE PERMISOS A CUENTAS CONCRETAS DEL DOMINIO

Para cada cuenta y grupos de seguridad de un dominio de "Active Directory", existirá un identificador de seguridad (SID) único dependiente del SID del dominio. Esto puede producir que, al editar plantillas de seguridad generadas en un entorno perteneciente a otro dominio,

aparezcan cadenas de números en las asignaciones de permisos, en ese caso se deben modificar para que hagan referencia a los usuarios y grupos específicos del dominio. La siguiente tabla tiene algunos de los identificadores de seguridad únicos para el dominio.

SID	Nombre de la cuenta
S-1-5-<SID del dominio>-500	DOMINIO\Administrador
S-1-5-<SID del dominio>-501	DOMINIO\Invitado
S-1-5-<SID del dominio>-512	DOMINIO\Administradores del dominio

Debe tener en consideración que durante el proceso de implementación se generarán nuevos grupos de usuarios que aun estando referenciados en la guía deberán crearse de forma específica. Esto es debido a que, al ser grupos no definidos por Microsoft de forma predeterminada, generarán SID de objetos diferentes para cada dominio. Por lo tanto y durante el proceso del paso a paso, además de la creación de estos grupos se solicitará la modificación de las plantillas para agregar a estos grupos si fuese necesario.

8.2.2 NIVEL FUNCIONAL DEL DOMINIO

El Directorio Activo proporciona varios niveles que activan funcionalidades diferentes tanto a nivel de dominio como de todo el bosque.

Estos niveles funcionales están diseñados para dar respuesta a las distintas necesidades de las Organizaciones en función de la infraestructura y funcionalidad que tienen implantada y con qué tecnologías deberá convivir un despliegue de "Windows Server 2016".

Si todos los controladores de dominio son equipos con "Windows Server 2016", el nivel funcional puede establecerse como "Windows Server 2016", que proporcionará las funcionalidades más ricas y nuevas. Sin embargo, si está migrando una infraestructura de versiones previas deberá mantener el nivel funcional hasta que la implementación de los nuevos controladores de Windows Server 2016, y la retirada de los controladores de dominio de versiones previas, se haya producido satisfactoriamente. Windows Server 2016 no permite la convivencia con controladores de dominio Windows Server 2000 y Windows Server 2003. Por lo tanto, no puede integrar controladores de dominio Windows Server 2016 en dominios con nivel funcional en modo Mixto o Windows 2003.

El nivel funcional debe ser de al menos 2008 y es necesario eliminar cualquier servidor con Windows Server 2003 de la organización:

Aunque el Servicio de replicación de archivos (FRS) y los niveles funcionales de Windows Server 2003 quedaron obsoletos en versiones anteriores de Windows Server, vale la pena repetir que el sistema operativo Windows Server 2003 ya no es compatible. Como resultado, cualquier controlador de dominio que ejecute Windows Server 2003 debe eliminarse del dominio. El nivel funcional de dominio y bosque debe elevarse al menos a Windows Server 2008 para evitar que un controlador de dominio que ejecuta una versión anterior de Windows Server se agregue al entorno.

Los otros niveles funcionales están diseñados para permitir la convivencia de distintas combinaciones de controladores de dominio (Windows Server 2003, Windows Server 2008, Windows Server 2008 R2). Se deberá seleccionar el nivel más adecuado en función de las necesidades de la Organización.

Puede obtener más información sobre la actualización de versiones y los niveles funcionales en la siguiente dirección URL.

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/upgrade-domain-controllers

8.2.3 SERVICIOS DE DIRECTORIO ACTIVO

Los controladores de dominio almacenan la base de datos de información del dominio, elemento clave a proteger en la infraestructura. Para incrementar la seguridad de esta información se recomiendan las siguientes configuraciones especificadas en los siguientes apartados.

8.2.3.1 ALMACENAMIENTO DE LOS FICHEROS ASOCIADOS AL DIRECTORIO ACTIVO

Para el correcto funcionamiento del servicio de directorio activo, se recomienda utilizar unidades de discos dedicados para el almacenamiento de los ficheros de la base de datos de Active Directory (AD) y los ficheros de registro (logs); de tal manera que en estos volúmenes exista espacio suficiente para almacenar la base de datos y sus registros correspondientes.

Además, si se quiere tener en cuenta el rendimiento y la tolerancia a fallos de discos físicos, se pueden utilizar diferentes soluciones de RAID para estos volúmenes. A modo de ejemplo se define a continuación una posible solución:

Contenido	Volumen
Sistema Operativo	C:
Base de datos de AD y SYSVOL	D:
Ficheros de Log	E:

8.2.3.2 CONTROLADORES DE DOMINIO DE SOLO LECTURA

Windows Server 2016 permite instalar controladores de dominio de sólo lectura (RODC, Read Only Domain Controller). Este tipo de controlador de dominio tiene la particularidad de que alberga una copia de sólo lectura de la base de datos de Active Directory, y está pensado para su despliegue en lugares donde no se puede garantizar la seguridad física del servidor.

El hecho de que sean de sólo lectura aumenta la seguridad del dominio porque, en el caso de que un atacante con acceso físico al mismo lograra modificar información de la copia que alberga de la base de datos de Active Directory, estas modificaciones no se propagarían hacia el resto de controladores de dominio.

No obstante, se recomienda garantizar la seguridad física de todos los controladores de dominio, incluidos los de sólo lectura si se optara por instalar alguno de este tipo. Si bien el hecho de que un controlador de dominio sea de sólo lectura puede reducir el impacto de una potencial toma de control por parte de un atacante con acceso físico al mismo, dicho impacto seguiría siendo muy grande, ya que el atacante tendría acceso a mucha información crítica contenida en la base de datos de Active Directory.

Por ello, no se incluyen recomendaciones en esta guía para el uso de controladores de dominio de sólo lectura, pero se comenta aquí su existencia por si los administradores optaran por utilizarlos.

Para más información se puede consultar la siguiente dirección URL.

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/rodc/install-a-windows-server-2012-active-directory-read-only-domain-controller--rodc---level-200-

Nota: Aunque el enlace se relaciona con Microsoft Windows Server 2012 R2 el proceso es similar en Windows Server 2016.

8.2.3.3 LIMITACIÓN DE RANGO DE PUERTOS DE TCP PARA RPC

Para simplificar las reglas de filtrado de los firewalls que gestionen las comunicaciones de los controladores de dominio, se recomienda limitar el rango de puertos TCP utilizados por aplicaciones RPC.

A continuación, se muestran los valores de los parámetros del registro que permiten limitar ese rango de puertos. Esos parámetros pueden localizarse en la ruta

HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc\Internet

Entrada del valor de registro de subclaves	Formato	Valor	Comentarios
Ports	REG_MULTI_SZ	57901-57950	Define el rango de puertos que será o no usado por RPC dependiendo del valor de la clave UseInternetPorts, explicada a continuación
PortsInternetAvailable	REG_SZ	Y	
UseInternetPorts	REG_SZ	Y	El valor "Y" indica que los puertos indicados en el parámetro "Ports" serán utilizados por aplicaciones RPC. Si el valor fuera "Y" indicaría que los puertos del parámetro "Ports" no serían utilizados por aplicaciones RPC.

Para más información sobre la limitación del rango de puertos TCP para RPC se puede consultar los siguientes documentos:

a) "Service overview and network port requirements for the Windows Server System":

http://support.microsoft.com/kb/832017

b) "Cómo configurar la asignación dinámica de puertos RPC para trabajar con firewall":

http://support.microsoft.com/kb/154596

c) "El intervalo de puertos dinámicos predeterminado para TCP/IP ha cambiado desde Windows Vista y en Windows Server 2008":

http://support.microsoft.com/kb/929851

Nota: Aunque los enlaces no corresponden con el sistema operativo tratado en esta guía es de igual aplicación.

9. BLOQUEOS ADICIONALES

Dentro de esta sección, se describen algunas configuraciones adicionales que no se pueden implementar mediante plantillas de seguridad. Algunas de ellas no se implementarán en las instrucciones paso a paso de la guía, pero se explican aquí por si los administradores deciden implementarlas.

9.1 FIREWALL DE WINDOWS CON SEGURIDAD AVANZADA

Windows Server 2016 incorpora un firewall propio que permite definir reglas de filtrado para definir el tráfico de red entrante y saliente del servidor que debe ser permitido o denegado.

Esta funcionalidad de firewall, denominada "Firewall de Windows con seguridad avanzada", es configurable desde línea de comando mediante la utilidad netsh (netsh advfirewall), desde la consola de administración "Administrador del servidor", bajo “Configuración → Firewall de Windows con seguridad avanzada”, y también es configurable utilizando GPOs (Configuración del equipo\Directivas\Configuración de Windows\Configuración de seguridad\Firewall de Windows con seguridad avanzada).

La explicación detallada de todas las opciones de configuración del Firewall de Windows con seguridad avanzada queda fuera del alcance de esta guía. No obstante, a continuación, se expone una breve descripción de las opciones de configuración principales y se ofrecen recomendaciones concretas para aplicar en un controlador de dominio.

Las reglas y políticas del firewall se agrupan en tres perfiles de modo que, para cada conexión de red, en cada momento, sólo se aplicarán las correspondientes a uno de los perfiles:

a) **Dominio:** Se aplica cuando el servidor tiene conectividad con un controlador de dominio a través de esa interfaz de red.

b) **Privado:** Se aplica cuando el servidor no tiene conectividad con un controlador de dominio y la red a la que está conectado ha sido categorizada como privada por el administrador.

c) **Público:** Se aplica cuando el servidor no tiene conectividad con un controlador de dominio y la red a la que está conectado no ha sido categorizada por el administrador, o ha sido categorizada como red pública.

Nota: En Windows Server 2016 dos o más perfiles pueden estar activos simultáneamente si el equipo dispone de varias conexiones de red y éstas están conectadas a redes de tipos distintos (dominio/privado/público). En cada interfaz de red puede estar activo un perfil distinto.

Cada perfil define una política por defecto que se aplicará a los paquetes de red a los que aplique ese perfil cuando no haya ninguna regla específica de filtrado para dichos paquetes. Se puede especificar una opción distinta a conexiones entrantes y salientes. Se recomienda utilizar la siguiente configuración para todos los perfiles:

a) Conexiones entrantes: Bloquear las conexiones entrantes que no coincidan con una regla.

b) Conexiones salientes: Permitir las conexiones salientes que no coincidan con una regla.

Con esta configuración se deberán definir reglas de filtrado para conexiones entrantes que permitan todas las conexiones de red que lleguen al servidor y vayan dirigidas a servicios que deban efectivamente ser accesibles a través de la red. Por ejemplo, para que los clientes

puedan realizar consultas DNS al servidor, si el servidor ejerce ese rol, una regla del firewall deberá permitir las conexiones entrantes dirigidas al puerto 53/UDP.

Windows Server 2016 incluye una serie de reglas por defecto cuando se instala sin roles ni características y, posteriormente, el propio proceso de instalación de un rol o característica incluye la creación automática de las reglas necesarias para los servicios de red ofrecidos por ese rol o características. Estas reglas generadas automáticamente son, en general, razonablemente seguras, pero aun así siempre es recomendable revisarlas y deshabilitar aquellas que no sean imprescindibles. Por ejemplo, si el servidor no va tener IPv6 habilitado, se pueden deshabilitar todas las reglas de firewall que permiten tráfico IPv6, si no va a utilizar DHCP, se pueden deshabilitar todas las reglas que permiten tráfico DHCP, y así sucesivamente.

En los informes adjuntos que contienen la configuración de las plantillas de seguridad, se muestra la configuración recomendada del firewall de Windows con seguridad avanzada para controladores de dominio y para servidores miembro en cada uno de los entornos.

Esas configuraciones recomendadas del firewall se incluyen en los ficheros adjuntos a esta guía en forma de directiva de firewall (ficheros con extensión ".wfw") que pueden ser importadas en un equipo o en un objeto GPO. En la guía paso a paso (ver anexos) se incluyen las instrucciones necesarias para aplicarlas a través de un GPO.

Para más información, sobre el firewall con seguridad avanzada, se puede consultar la siguiente dirección URL.

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/windows-firewall-with-advanced-security-design-guide

9.2 PLANTILLAS ADMINISTRATIVAS

Debido a las novedades de Windows Server 2016 con respecto a los sistemas operativos que le preceden, existen una serie de configuraciones a añadir en las plantillas de seguridad y que están contenidas dentro de los ficheros ADMX y ADML que se han añadido al conjunto de plantillas incluidas en el sistema.

Las carpetas de scripts que acompañan a la presente guía incluyen, a su vez, carpetas que contienen las diferentes configuraciones que se añadirán tanto a la plantilla de seguridad que configura los controladores de dominio como a la que configura los servidores miembros del dominio.

9.3 CUENTAS DE SERVICIO

No debe configurarse nunca un servicio para que se ejecute bajo el contexto de seguridad de una cuenta de dominio, a menos que sea absolutamente necesario. Si se pone en peligro físico a un servidor, se pueden obtener fácilmente las contraseñas de la cuenta de dominio al vaciar los secretos de la Autoridad de Seguridad Local (LSA).

En caso de que necesite emplear una cuenta de dominio para iniciar un servicio, se recomienda el empleo de cuentas de servicio administradas ya comentadas en el punto “6.5 SEGURIDAD Y CONTROL”.

9.4 DESACTIVACIÓN DE PROTOCOLOS INNECESARIOS

Con el objetivo de reducir aún más la superficie de ataque se deben deshabilitar todos aquellos protocolos de red que no sean estrictamente necesarios.

9.5 APLICACIÓN DE LAS PLANTILLAS DE SEGURIDAD

Esta guía incluye varias plantillas de seguridad para controladores de dominio y servidores miembro. Para aplicar esta plantilla existen diferentes métodos. En esta guía se recomienda automatizar su aplicación mediante objetos GPO.

Un método adicional que se puede usar es utilizar el complemento MMC "Configuración y análisis de seguridad". Para ello se deberían realizar los siguientes pasos:

a) Abra el complemento de MMC llamado "Configuración y Análisis de Seguridad".

b) Cree la base de datos.

c) Haga clic con el botón secundario del ratón en el objeto Configuración y Análisis de Seguridad.

d) Haga clic en “Abrir Base de Datos”.

e) Escriba un nuevo nombre para la base de datos y haga clic en “Abrir”.

f) Seleccione la plantilla de seguridad correspondiente y, a continuación, haga clic en “Abrir”.

Para aplicar las configuraciones de seguridad siga los siguientes pasos:

a) Haga clic con el botón secundario del ratón en el objeto “Configuración y Análisis de Seguridad”.

b) Seleccione “Configurar el Equipo Ahora”.

c) En el cuadro de diálogo “Configurar el Equipo Ahora”, escriba el nombre del archivo de registro que desea ver y haga clic en Aceptar.

La aplicación mediante objetos GPO está recomendada en un entorno de dominio porque la gestión y aplicación de las configuraciones es mucho más flexible y sencilla.