CCN
centro criptológico nacional

Guía de Seguridad de las TIC

IMPLEMENTACIÓN DE SEGURIDAD EN SERVIDOR DE IMPRESIÓN SOBRE MICROSOFT WINDOWS SERVER 2016

NOVIEMBRE 2018

MINISTERIO DE DEFENSA

Edita:

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=S2800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2018.11.29 15:30:14 +01'00'

NIPO: 083-19-034-0
Fecha de Edición: noviembre de 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).

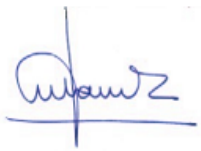
Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad 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

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 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 Server 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 Server 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 la implementación, establecer la configuración y realizar tareas de administración maximizando las condiciones de seguridad del servidor de impresión de Microsoft Windows Server 2016 en un servidor miembro de una infraestructura de dominio.

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 la guía codificada como CCN-STIC-570A para realizar los pasos adecuados.

Esta guía asume que el servidor de impresión se va a implementar sobre un equipo con Windows Server 2016 Standard de 64 Bits donde se ha seguido el proceso de implantación de seguridad definido en el documento codificado como “CCN-STIC-570A”.

Cumpliendo con estos requisitos previos, puede iniciar la instalación del servidor de impresión basado en Microsoft Windows Server 2016 Standard.

Así mismo, no se contempla en esta guía la instalación del servicio de impresión en clúster, ni se han aplicado características de alta disponibilidad o protección ante fallos del servicio.

4. ALCANCE

La guía se ha elaborado para proporcionar información específica para realizar una implementación del servidor de impresión sobre Microsoft Windows Server 2016 Standard en una configuración restrictiva de seguridad. Se incluyen, además, operaciones básicas de administración como la gestión de impresoras, colas de impresión, implementación de políticas y delegación de la administración, entre otros aspectos, además de aquellas acciones que deben ser llevadas a cabo para el adecuado mantenimiento del servicio.

El escenario en el cual está basada la presente guía tiene las siguientes características técnicas:

a) Un único bosque de Directorio Activo.

b) Un único dominio dentro del bosque de Directorio Activo.

c) Nivel funcional del bosque y del dominio en Windows Server 2016.

d) Un controlador de dominio basado en Windows Server 2016 Standard.

e) Un servidor miembro del dominio basado en Windows Server 2016 Standard.

f) La instalación del servicio de impresión se realiza en modo limpio, es decir, no se contemplan procedimientos de migración desde versiones anteriores.

g) No se contemplan mecanismos de alta disponibilidad ni balanceo de carga en el escenario planteado.

Este documento incluye:

a) **Mecanismos para la aplicación de configuraciones**. Se incorporan mecanismos para la implementación de forma automática de las configuraciones de seguridad susceptibles de ello.

b) **Mecanismos para la creación de cuentas necesarias para la funcionalidad de la solución**. Tanto los procesos de implementación como de instalación requieren de cuentas específicas; se ha automatizado el proceso de creación de dichas cuentas.

c) **Descripción de la seguridad en el servicio de impresión**. Completa la descripción de los mecanismos de seguridad, autenticación y autorización utilizados en el servicio de impresión de Windows Server 2016, así como las medidas para reforzar dicha seguridad.

d) **Guía paso a paso**. Va a permitir implantar y establecer las configuraciones de seguridad de un servidor de impresión de Windows Server 2016.

e) **Guía de administración**. Va a permitir realizar tareas de administración en el entorno de seguridad establecido.

f) **Lista de comprobación**. Permitirá verificar el grado de cumplimiento de un servidor 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 refuerzo de la seguridad que describe y los recursos que proporciona. Este procedimiento constará, a grandes rasgos, de los siguientes pasos:

a) Antes de comenzar a aplicar la guía, además de los requisitos para la instalación del servicio de impresión, será necesario cumplir los requisitos definidos para Windows Server 2016.

b) Así mismo, antes de instalar el rol de servidor de impresión, será necesario aplicar la guía de seguridad codificada como CCN-STIC-570A.

c) A continuación, se deberá instalar y configurar el rol de servidor de impresión de Windows Server 2016 tal y como se describe en la presente guía.

5.1 AVISOS IMPORTANTES A LOS USUARIOS DE ESTA GUÍA

Los contenidos de esta guía son de aplicación a equipos de tipo puesto servidor con Sistema Operativo Windows Server 2016, en castellano, planteando como objetivo la reducción de la superficie de exposición a ataques que plantea la instalación predeterminada. 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 de Windows Server 2016 Standard de 64 bits, con los parámetros por defecto de instalación y aplicando la guía CCN-STIC-570A para su configuración. No se ha verificado en otros tipos de instalaciones como pudiera ser Windows Server 2016 Datacenter. No obstante, y teniendo en consideración las funcionalidades de ambas versiones de sistema operativo servidor podría llegar a implementarse la siguiente guía sobre la versión Datacenter. La presente guía no será funcional con las versiones Windows Server 2016 Essentials.

Esta guía se ha diseñado para reducir la superficie de exposición de los equipos servidores que cuenten con una implementación de rol de servidor de impresión en un entorno de dominio de Directorio Activo.

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

a) Servidor Dell PowerEdge™ T320:

   i. Intel Pentium Xeom 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 de seguridad mínimos de Windows Server 2016 Standard de 64 bits. Esto quiere decir que se requieren equipos con procesadores Intel o AMD de 64 bits (x64), con más de 2048 MB de memoria RAM.

Así mismo, hay que tener en cuenta que el rol de servidor de impresión requiere, para un entorno de producción, un mínimo de 2 GB de memoria RAM para funcionar adecuadamente, aunque se recomiendan 4 GB.

Se espera, por tanto, que el rendimiento de Windows Server 2016 pueda exceder dichos límites. Es por ello que se recomienda al menos disponer de 6 GB de memoria RAM en entornos en producción.

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 o características deseadas en Microsoft Windows Server 2016.

Para garantizar la seguridad de los servidores, deberán instalarse las actualizaciones recomendadas por el fabricante, disponibles a través del servicio de Windows 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 donde se han aplicado los test y cambios en la configuración, que se ajustan 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.

5.2 ESTRUCTURA DE LA GUÍA

Esta guía dispone de una estructura que diferencia la implementación del Servidor de impresión sobre 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 el Servidor de impresión de Microsoft sobre Windows Server 2016 a las necesidades requeridas por el Esquema Nacional de Seguridad (ENS).

b) **Anexo B**: En este anexo se define la configuración necesaria para adaptar el Servidor de impresión de Microsoft sobre Windows Server 2016 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) que se aplica.

6. ARQUITECTURA Y SEGURIDAD DEL SERVIDOR DE IMPRESIÓN

Los servicios de impresión de Microsoft Windows Server 2016 permiten compartir impresoras en una red y centralizar las tareas de administración del servidor de impresión y las impresoras de red mediante el complemento de administración de impresión, que ayuda a supervisar las colas de impresión y a recibir notificaciones cuando dichas colas interrumpen el procesamiento de los trabajos de impresión.

Además, permite migrar los servidores de impresión e implementar conexiones de impresora con directivas de grupo.

En Windows Server 2016 se mantienen algunas de las mejoras relacionada con el servidor de impresión, que ya se incorporaron en Windows Server 2012 R2, las cuales se describen a continuación:

a) **Capacidad integrada para la implementación de impresoras con la directiva de grupo**. Puede usar la consola de administración de impresión con directivas de grupo para implementar automáticamente conexiones de impresora para usuarios o equipos e instalar los controladores de impresoras apropiados. Esta función apareció por primera vez en Windows Server 2003 R2, pero requería el uso de la herramienta “PushPrinterConnections.exe” en un script de inicio (en conexiones por equipo) o en un script de inicio de sesión (en conexiones por usuario). Ahora esta funcionalidad está incluida en los equipos cliente que ejecutan Windows 10 y Windows Server 2016 y superior. Asimismo, estos sistemas operativos ahora pueden recibir conexiones de impresora por usuario durante las operaciones de actualización de la directiva de grupo en segundo plano.

b) **Capacidad de importación y exportación de las colas de impresión**. Puede usar el asistente para migración de impresoras o la herramienta de línea de comandos "Printbrm.exe" para exportar colas de impresión, configuraciones de impresora, puertos de impresora y monitores de idioma y, después, importarlos en otro servidor de impresión que ejecute un sistema operativo Windows Server 2016. Este procedimiento es una forma eficaz de consolidar varios servidores de impresión o reemplazar un servidor de impresión antiguo. El Asistente para migración de impresoras y la herramienta de línea de comandos "PrintBrmUi.exe" sustituye a "Print Migrator 3.1".

c) **Mejora de las descripciones de los eventos del Visor de eventos y de la información de la resolución**. Se han redactado de nuevo todas las descripciones de los eventos relacionados con la impresión que aparecen en el visor de eventos con objeto de aumentar su utilidad para la comprensión y la solución de problemas de impresión. Además, si se hace clic en el vínculo "ayuda en línea" del registro de eventos mientras se está viendo un evento, aparece en un explorador web información detallada del evento referente a cómo diagnosticar un problema y resolverlo, y también acerca de cómo comprobar si el problema se corrigió correctamente.

d) **Mejoras de la seguridad en la instalación de controladores de impresora**. La configuración de seguridad predeterminada de Windows Server 2016 permite a los usuarios que no sean miembros del grupo local Administradores instalar solamente controladores de impresora de confianza, como los que se incluyen en Windows o en paquetes de controladores de impresoras firmados digitalmente. Esto ayuda a garantizar que los usuarios no puedan instalar controladores de impresora no probados o no confiables, o en los que se haya incorporado código dañino.

   No obstante, este aumento de seguridad implica que algunos usuarios no podrán instalar el controlador apropiado para una impresora compartida, incluso si el controlador ha sido probado y aprobado en su entorno. Para permitir que usuarios que no sean miembros del grupo local Administradores puedan conectarse a un servidor de impresión e instalar controladores de impresora hospedadas en el servidor, puede usar uno de estos métodos:

   i. Instalar paquetes de controladores de impresoras en el servidor de impresión.

   ii. Usar la directiva de grupo para implementar conexiones de impresora en usuarios o equipos.

   iii. Usar la directiva de grupo para modificar la configuración de seguridad del controlador de impresora.

e) **Mejoras de los filtros de impresora en Administración de impresión**. En la consola de administración de impresión, los filtros permiten mostrar solamente aquellas impresoras que cumplan un conjunto concreto de criterios. Por ejemplo, puede resultarle conveniente filtrar las impresoras que cumplan determinadas condiciones de error o las impresoras de un grupo de edificios, con independencia del servidor de impresión que usen. Los filtros se almacenan en la carpeta "Filtros personalizados" de impresora del árbol de "Administración de impresión" y son dinámicos, por lo que los datos siempre están actualizados.

f) Los filtros se han mejorado en Windows Server 2016 en dos sentidos:

   i. Filtro personalizado "Todos los controladores". Se trata de un filtro predeterminado nuevo que presenta todos los controladores instalados en el servidor seleccionado, así como sus versiones.

   ii. Aumento del número de criterios de filtrado a seis. Al aumentar el número de criterios de filtrado desde el límite anterior de tres, ahora es posible crear filtros más específicos.

g) **Integración del "Administrador del servidor"**. En Windows Server 2016, se puede usar el administrador del servidor para instalar la función del servidor "Servicios de impresión", servicios de funciones opcionales y otras características. El administrador del servidor también muestra eventos relacionados con la impresión desde el visor de eventos e incluye una instancia del complemento administración de impresión que solamente puede administrar el servidor local.

Los servicios de impresión se implementan en Windows Server 2016 como una función de servidor del administrador del servidor con los siguientes servicios de función secundarios:

   i. Servidor de impresión.

   ii. Servicio Line Printer Daemon (LPD).

   iii. Impresión en Internet.

h) A partir de Windows Server 2012 R2 se desusa el protocolo Line Printer Daemon (LPR/LPD). Con el tiempo se quitará esta característica, los clientes que imprimen en un servidor que usa este protocolo, como los clientes de UNIX, no podrán conectarse ni imprimir. En su lugar, los clientes de UNIX deberían usar el IPP. Los clientes de Windows se pueden conectar con impresoras UNIX compartidas mediante el Monitor de puerto estándar de Windows.

i) **Aislamiento de controladores de impresora**. Antes de Windows 7 y Windows Server 2008 R2, el error de los componentes de controladores de impresora era un problema principal en la compatibilidad con servidores de impresión. El error de un controlador de impresora cargado en un proceso de administrador de trabajos de impresión producía un error en el proceso, lo que llevaba a una interrupción de todo el sistema de impresión. El impacto de un error en el administrador de trabajos de impresión en un servidor de impresión es particularmente significativo por el gran número de usuarios e impresoras a los que afecta.

j) Desde Windows 7 y Window Server 2008 R2 se pueden configurar los componentes de controlador de impresora para que se ejecuten en un proceso aislado independiente del proceso del administrador de trabajos de impresión. Windows Server 2016 mantiene esta característica de seguridad. Al aislar el controlador de impresora se evita que un controlador de impresora defectuoso detenga todas las operaciones de impresión en un servidor de impresión, lo que resulta en una mayor confiabilidad del servidor.

   Además del beneficio de mejorar toda la estabilidad del sistema de impresión, esta nueva característica ofrece un medio para aislar nuevos controladores de prueba y de depuración, así como para identificar los controladores de impresora que están causando problemas en el administrador de trabajos de impresión.

k) **Impresión con reconocimiento de ubicación de red**. A partir de Windows 7, el valor Impresora predeterminada reconoce la ubicación de red. Un usuario de portátil o teléfono móvil puede establecer una impresora predeterminada diferente para cada red a la que se conecte. Es posible tener una impresora predeterminada para el hogar y otra impresora predeterminada para la oficina. Su portátil puede seleccionar automáticamente la impresora predeterminada correcta, según la ubicación actual del usuario.

Para usar la consola de "Administración de impresión" en Windows Server 2016, se debe instalar la función servidor de impresión en el equipo donde la desee usar.

Para implementar conexiones de impresora con la directiva de grupo, el entorno debe cumplir los siguientes requisitos:

a) El esquema de servicios de dominio de Directorio Activo (AD DS) debe usar una versión de esquema de Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 o Windows Server 2016.

Requisitos de seguridad:

b) Para administrar un servidor de impresión remoto, debe ser miembro de los grupos "Opers. de impresión" u "Opers. de servidores", o del grupo local "Administradores" en el servidor de impresión remoto. Estas credenciales no son necesarias para supervisar los servidores de impresión remotos, aunque algunas funciones estarán deshabilitadas.

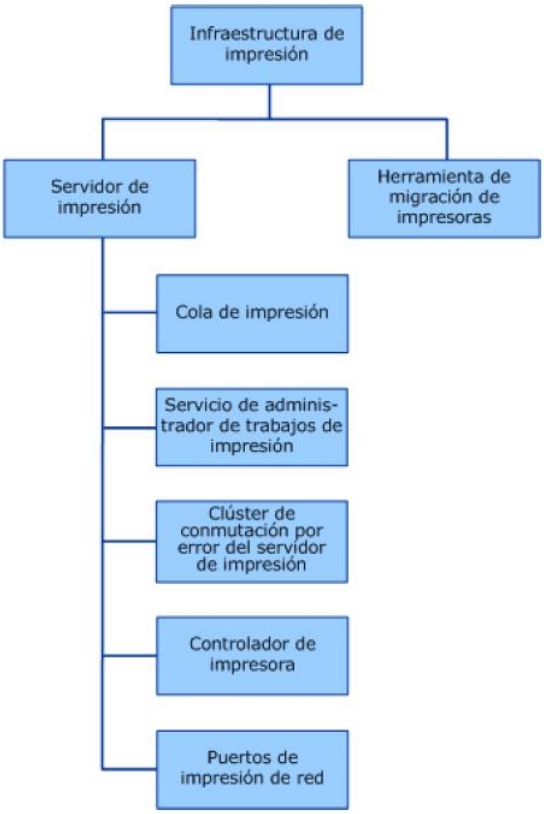
c) Para usar la consola de administración de impresión (Printmanagement.msc) con la directiva de grupo, debe ser miembro del grupo local Administradores y tener acceso de escritura a los objetos de directiva de grupo (GPO) en el dominio de AD DS o la unidad organizativa donde desea implementar las conexiones de impresora.

d) Se recomienda a los administradores que usen una cuenta con permisos restrictivos para realizar tareas rutinarias no administrativas, y usar una cuenta con más permisos sólo cuando realicen tareas administrativas específicas.

6.1 COMPONENTES Y ENTIDADES DE LOS SERVICIOS DE IMPRESIÓN

La infraestructura de impresión de un servidor permite que usuarios locales y remotos ejecuten trabajos de impresión en el propio servidor, así como administrar las impresoras y todos sus aspectos relacionados con la impresión.

A continuación, se muestra una estructura jerárquica de las entidades administradas en los servicios de impresión de Windows Server 2016.



Cola de impresión (Print Queue). Una cola de impresión es una representación de un dispositivo de impresión o impresora física en Microsoft Windows. Cuando se abre la cola de impresión se muestran todos los trabajos activos y su estado.

Servicio de cola de impresión (Print Spooler Service). Cada servidor de impresión dispone de un único servicio de cola de impresión, el cual gestiona todos los trabajos de impresión y las colas que están configuradas en dicho servidor.

Clúster de conmutación por error de servicios de impresión (Print Server Failover Clúster). Un clúster es un grupo de servidores independientes que funcionan en conjunto para incrementar la disponibilidad del servicio de impresión u otros servicios. Si uno de los servidores falla, otro de los miembros del clúster asume la responsabilidad del servicio. En esta guía no se contempla la instalación de un clúster de conmutación por error para los servicios de impresión.

Controlador de impresora (Printer Driver). El controlador de impresora es el software del fabricante que permite que Windows Server 2016 interactúe con el hardware de impresión. Cada impresora que se instale requiere de un controlador de impresora asociado al fabricante, modelo y versión de dicha impresora.

6.2 AISLAMIENTO DE CONTROLADORES DE IMPRESIÓN

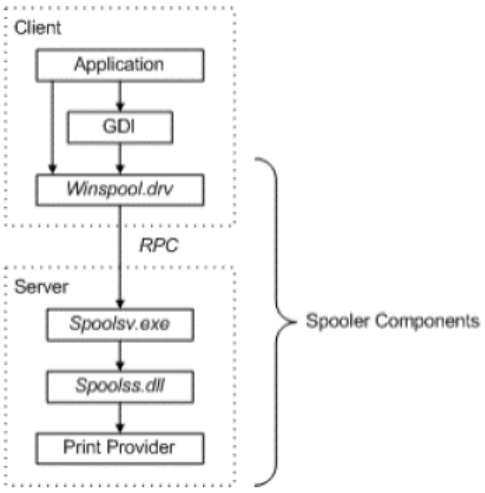
Como su nombre indica, el aislamiento de controladores de impresión en Windows Server 2016 permite que algunos de los componentes del controlador se ejecuten en un proceso o procesos separados de la cola de impresión. En versiones anteriores los controladores de impresión siempre se ejecutaban en el mismo proceso que la cola de impresión.

De esta forma, cualquier problema o error asociado con controladores defectuosos se aíslan del servicio de cola de impresión y no afecta al resto de los procesos.

En Windows Server, el servicio de impresión se compone de dos elementos básicos, la cola de impresión y los controladores de impresoras.

La cola de impresión es el componente principal y se ejecuta en el proceso “spoolsvc.exe”, el cual se inicia junto con el sistema y continúa en ejecución hasta que el sistema se apaga.

A continuación, se muestra un diagrama de los dos componentes mencionados.



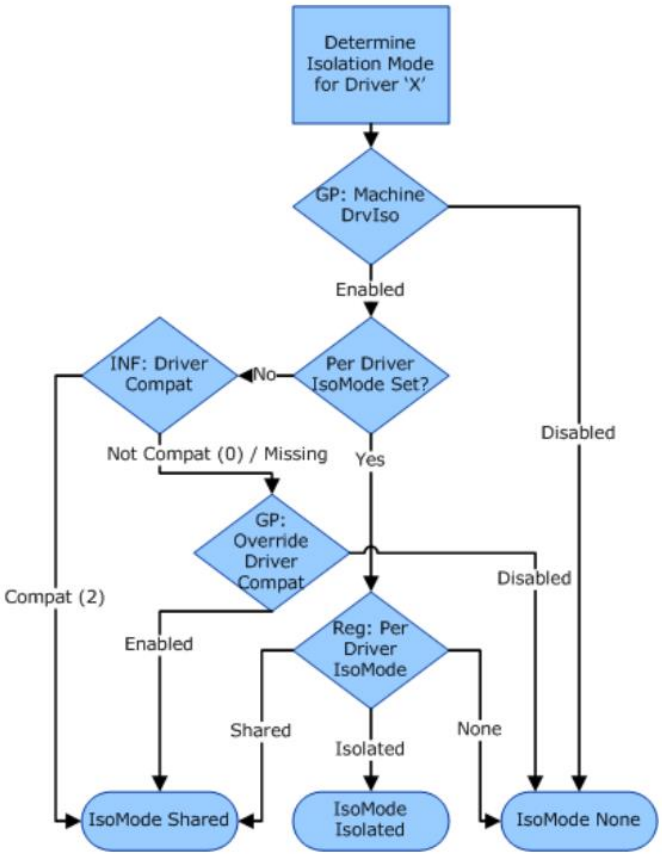
Con respecto al aislamiento de controladores, existen tres modos básicos de aislamiento que se pueden configurar para controladores individuales:

a) **Ninguno**. En este modo, los componentes del controlador de impresión se cargan en el proceso de cola de impresión. Este modo es el que se encontraba en versiones anteriores de Windows Server.

b) **Compartido**. En este modo, múltiples controladores se configuran para el aislamiento y se cargan en el mismo proceso compartido, el cual está a su vez separado del proceso de cola de impresión. Aunque esta arquitectura protege el proceso de cola de impresión, los controladores compartidos pueden verse afectados unos con otros.

c) **Aislado**. En este modo, cada controlador se carga de forma completamente aislada en su propio espacio de ejecución. Esta arquitectura protege tanto al proceso de cola de impresión como a los controladores de impresión entre sí.

El siguiente diagrama de flujo muestra un mapa de decisiones para elegir el modo de aislamiento del controlador:



Los modos de aislamiento se deben configurar por cada uno de los controladores de forma individual, no a nivel de todo el sistema.

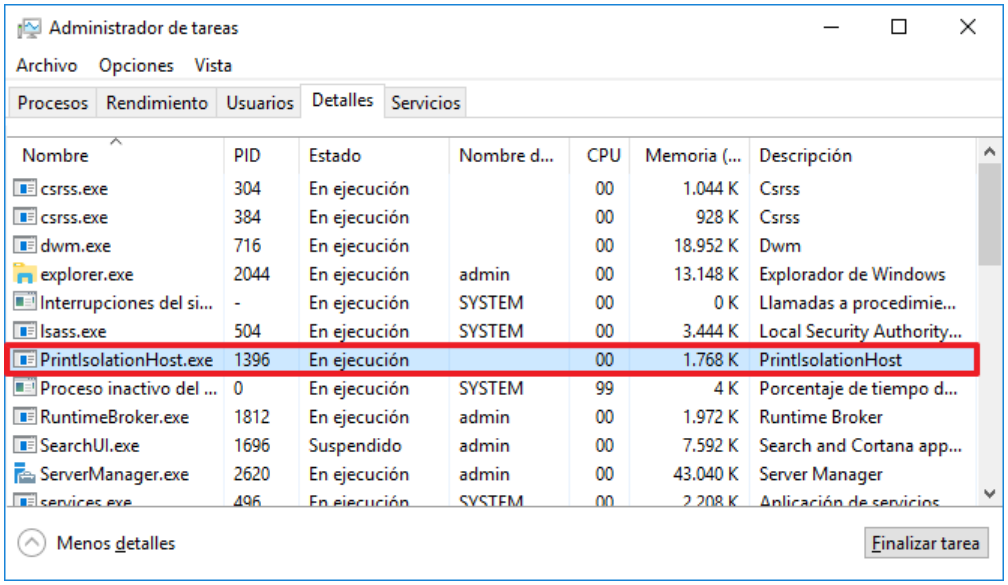
Así mismo, es posible que ciertos controladores de impresión no puedan ejecutarse en modo de aislamiento debido a que hacen llamadas directamente a la cola de impresión o a otros módulos de configuración de la impresora.

Cuando se utiliza el modo de aislamiento, cada vez que se realiza una impresión se lanza un proceso denominado “PrintIsolationHost.exe”.

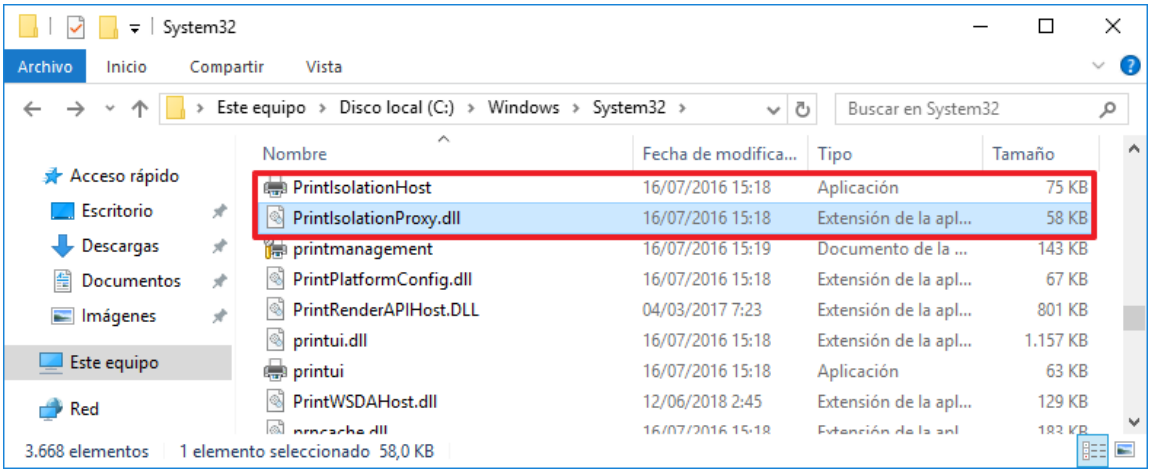
De esta forma, el proceso de cola de impresión únicamente se limita a actuar de proxy para las llamadas del procesador de impresión y otros componentes del controlador.

Dentro de los procesos “spoolsv.exe” y “PrintIsolationHost.exe” se carga una librería denominada “PrintIsolationProxy.dll” que redirige las llamadas a impresoras específicas entre los procesos.

A continuación, se muestra un ejemplo de la ejecución en modo de aislamiento de los controladores de impresión.



Como se puede observar, por cada proceso de impresión se carga la librería de redirección de llamadas “PrintIsolationProxy.dll”.



La configuración del aislamiento de controladores de impresión se puede realizar mediante el registro de Windows directamente o mediante directivas de grupo (GPO), encontrándose éstas en la ruta **"Configuración de equipo → Directivas → Plantillas administrativas → Impresoras"**. A continuación, se indican las directivas relacionadas:

a) **Ejecutar controladores de impresión en procesos aislados**. Esta configuración de directiva determina si el administrador de trabajos de impresión ejecutará controladores de impresión en un proceso aislado o separado. Cuando se carguen controladores de impresión en un proceso aislado (o procesos aislados), si aparece un error de controlador de impresión no provocará un error del servicio del administrador de trabajos de impresión. Si se habilita o no establece esta configuración de directiva, de forma predeterminada el administrador de trabajos de impresión ejecutará controladores de impresión en un proceso aislado. Si se deshabilita esta configuración de directiva, el administrador de trabajos de impresión ejecutará controladores de impresión en el proceso del administrador de trabajos de impresión.

b) **Invalidar la configuración de compatibilidad de ejecución de controlador de impresión notificada por el controlador de impresión**. Esta configuración de directiva determina si el administrador de trabajos de impresión invalidará la compatibilidad del aislamiento del controlador notificada por el controlador de impresión. Esto permite ejecutar controladores de impresión en un proceso aislado, aunque el controlador no notifique una incompatibilidad. Si habilita esta configuración de directiva, el administrador de trabajos de impresión aislará todos los controladores de impresión que no renuncien a participar explícitamente en el aislamiento de controladores. Si deshabilita o no establece esta configuración de directiva, el administrador de trabajos de impresión usará el valor de la marca de compatibilidad del aislamiento de controladores notificado por el controlador de impresión.

Los valores de estas directivas se reflejan en los siguientes valores del registro:

a) HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Printers\
   i. PrintDriverIsolationExecutionPolicy
   ii. PrintDriverIsolationOverrideCompat

Además de los valores indicados, se pueden controlar otros aspectos relacionados con el comportamiento del aislamiento desde los siguientes valores del registro de Windows:

a) HKLM\SYSTEM\CurrentControlSet\Control\Print\
   i. PrintDriverIsolationIdleTimeout
   ii. PrintDriverIsolationTimeBeforeRecycle
   iii. PrintDriverIsolationMaxobjsBeforeRecycle

6.3 CONFIGURACIÓN DE LA SEGURIDAD DEL SERVIDOR DE IMPRESIÓN

Planear la seguridad de los servidores de impresión y determinar cómo restringir el acceso a ellos es una parte importante de la administración de los servidores de impresión.

En Windows Server 2016, puede delegar tareas de administración de impresión directamente a usuarios que no son administradores del sistema al igual que sucedía en versiones anteriores.

También puede definir la configuración de seguridad predeterminada de la impresora que se hereda al agregar nuevas impresoras al servidor de impresión.

Estos cambios hacen posibles las siguientes mejoras en la administración de impresoras y servidores de impresión:

a) Puede controlar el acceso a recursos y equilibrar cargas de trabajo delegando determinadas tareas administrativas de impresión a usuarios sin agregarlos al grupo de seguridad Administradores.

b) Puede administrar la configuración de permisos mediante la interfaz de usuario mejorada de la pestaña seguridad en el cuadro de diálogo “Propiedades del servidor de impresión”.

c) Puede administrar la infraestructura de impresoras configurando las opciones de seguridad de impresora predeterminadas que las nuevas impresoras heredan automáticamente al agregarlas. Puede configurar las opciones por servidor para que no tenga que configurar las impresoras individualmente.

Los permisos del servidor de impresión controlan los niveles de acceso para los usuarios de un servidor de impresión determinado. Los permisos de impresora controlan qué tareas de impresión pueden realizar los usuarios en las impresoras agregadas recientemente que están administradas por el servidor de impresión.

Los administradores deben asignar estos permisos cuando sea necesario a los usuarios que no sean administradores del sistema.

Una vez que un administrador personaliza la configuración de seguridad para el servidor de impresión, todas las impresoras recién agregadas a este servidor de impresión heredan esta configuración de seguridad automáticamente, es decir, no se modifica la configuración de seguridad para las impresoras existentes en el servidor.

Los niveles de permisos se diferencian en:

a) Permisos del servidor de impresión.

b) Permisos de impresora.

Los dos niveles de permisos del servidor de impresión son:

a) **Ver servidor**. El permiso “Ver servidor” asigna la capacidad de ver el servidor de impresión. Sin este permiso, los usuarios no pueden ver las impresoras administradas por el servidor. De forma predeterminada este permiso se concede a los miembros del grupo “Todos”.

b) **Administrar servidor**. El permiso “Administrar servidor” asigna la capacidad para crear y eliminar colas de impresión (con controladores ya instalados), agregar o eliminar puertos y agregar o eliminar formularios. Un usuario estándar con este permiso se denomina "administrador de impresión delegado".

Los tres niveles de permisos de impresora son los siguientes:

a) **Imprimir.** El permiso "Imprimir" asigna a los usuarios la posibilidad de conectarse a impresoras e imprimir, pausar, reanudar, iniciar y cancelar sus propios documentos. De forma predeterminada, este permiso se concede a los miembros del grupo "Todos" cuando se crea una cola de impresión.

b) **Administrar documentos.** El permiso "Administrar documentos" asigna la posibilidad de controlar la configuración del trabajo para todos los documentos, así como pausar, reiniciar y eliminar todos los documentos.

c) **Administrar impresoras**. El permiso "Administrar impresora" asigna la posibilidad de pausar y reiniciar la impresora, cambiar la configuración del administrador de trabajos en cola, compartir una impresora, ajustar los permisos de la impresora y cambiar las propiedades de la impresora.

En Windows Server 2016, la configuración de seguridad predeterminada para el servidor de impresión y la impresora es la siguiente.

Nivel de permisos	Todos	Propietario de creadores	Administradores
Imprimir	Permitir		Permitir
Administrar documentos		Permitir	Permitir
Administrar impresoras			Permitir
Ver servidor	Permitir		Permitir
Administrar servidor			Permitir

Los miembros del grupo "Administradores" pueden crear un administrador de impresión delegado completo asignando el permiso "Administrar servidor" a un usuario.

Cuando se asigna el permiso "Administrar servidor", también se asigna automáticamente el permiso "Ver servidor".

También puede delegar un subconjunto de estos permisos para crear un administrador de impresión delegado parcial.

Nota: Antes de agregar cualquier impresora al servidor, debe crear un grupo de usuarios que pueden realizar tareas de impresión delegadas y, a continuación, configurar los permisos apropiados. Si lo hace, todas las impresoras recién agregadas heredan automáticamente esta configuración y no tiene que configurar individualmente las impresoras existentes para el servidor de impresión.

En la tabla siguiente se enumeran las tareas de impresión que un usuario puede realizar cuando tiene asignados los permisos correspondientes en la pestaña "Seguridad" de las "Propiedades" del servidor de impresión.

Nivel de permisos	Imprimir	Administrar impresoras	Administrar documentos	Ver servidor	Administrar servidor
Ver la cola de impresión (en el servidor local)				Sí	
Imprimir documentos propios en la cola	Sí				

Nivel de permisos	Imprimir	Administrar impresoras	Administrar documentos	Ver servidor	Administrar servidor
Ver, pausar, reiniciar y cancelar todos los trabajos de impresión de una cola			Sí		
Actualizar controladores instalados o incluidos, y controladores disponibles en Windows Update, en una cola existente.		Sí			
Nota: Esto no se aplica a los entornos de impresión en clúster.					
Agregar o eliminar un formulario en una cola		Sí			
Ver las propiedades de impresora				Sí	
Ver las propiedades del servidor de impresión				Sí	
Configurar los permisos de seguridad de impresora en una cola de impresión		Sí			
Administrar el descriptor de seguridad marca setServerSecurity Descriptor del servidor de impresión					
Agregar una cola de impresión a un servidor de impresión					Sí, cuando los controladores ya están instalados.
Eliminar una cola de impresión de un servidor de impresión		Sí, pero solo la cola para la que tiene permisos.			
Agregar un controlador de impresión a un servidor de impresión					Sí, pero solo localmente. El usuario debe ser miembro del grupo “Administradores” para poder agregar controladores (incluso de forma remota) al servidor de impresión.
Eliminar un controlador de impresión de un servidor de impresión					Sí, pero solo para los controladores (no los paquetes de controladores)
Agregar, eliminar y configurar puertos en un servidor de impresión					Sí

Nivel de permisos	Imprimir	Administrar impresoras	Administrar documentos	Ver servidor	Administrar servidor
Agregar y eliminar un formulario en un servidor de impresión		Un usuario que tiene asignados los permisos Administrar impresoras, pero no Administrar servidor, puede agregar un formulario cuando AllowUserManageForms está establecido en el Registro de Windows en un valor distinto de cero. Un usuario puede agregar formularios hasta el valor especificado para AllowUserManageForms. Un usuario solo puede agregar y eliminar formularios de usuario. Sin embargo, un usuario con el permiso SERVER_ACCESS_ADMINISTER puede agregar y eliminar formularios de impresora y de usuario sin ninguna limitación.			Sí
Compartir la impresora		Sí, si tiene los permisos Administrar impresora en el servidor de impresión y se han habilitado las excepciones Compartir impresoras y archivos en Firewall de Windows con seguridad avanzada			Sí, si tiene los permisos Administrar impresora en el servidor de impresión y se han habilitado las excepciones Compartir impresoras y archivos en Firewall de Windows con seguridad avanzada

A continuación, se muestra una lista de grupos de seguridad de impresión sugeridos y sus permisos asociados:

a) Grupo "Administradores del sistema". Consta de los miembros del grupo de seguridad Administradores.

b) Grupo "Administradores de impresión". Consta de los miembros del grupo Administradores del sistema y los usuarios a los que se ha asignado algún conjunto de derechos de administrador de impresión delegado. Dependiendo de los derechos que asigne, los miembros de este grupo se pueden considerar administradores delegados completos o administradores delegados parciales.

En la tabla siguiente se muestra qué acciones se pueden realizar dependiendo de los permisos asignados:

	Usuarios estándar: pueden conectarse a impresoras e imprimir sus documentos (Permisos: Imprimir, Ver servidor)	Administradores delegados parciales: pueden agregar impresoras (Permisos: Imprimir, Ver servidor, Administrar servidor)	Administradores delegados parciales: pueden administrar colas existentes (Permisos: Imprimir, Ver servidor, Administrar impresoras, Administrar documentos)	Administradores delegados completos: pueden realizar todas las tareas de impresión administrativas (Permisos: Imprimir, Administrar documentos, Administrar impresoras, Ver servidor, Administrar servidor)	Administradores del sistema: pueden administrar el sistema totalmente (Permisos: Imprimir, Administrar documentos, Administrar impresoras, Ver servidor, Administrar servidor)
Ver la cola de impresión en el servidor local	Sí	Sí	Sí	Sí	Sí
Imprimir en la cola	Sí	Sí	Sí	Sí	Sí
Ver, pausar, reiniciar o cancelar trabajos de impresión que sean propiedad del usuario en una cola	Sí	Sí	Sí	Sí	Sí
Modificar todos los trabajos de impresión de una cola			Sí	Sí	Sí

	Usuarios estándar: pueden conectarse a impresoras e imprimir sus documentos (Permisos: Imprimir, Ver servidor)	Administradores delegados parciales: pueden agregar impresoras (Permisos: Imprimir, Ver servidor, Administrar servidor)	Administradores delegados parciales: pueden administrar colas existentes (Permisos: Imprimir, Ver servidor, Administrar impresoras, Administrar documentos)	Administradores delegados completos: pueden realizar todas las tareas de impresión administrativas (Permisos: Imprimir, Administrar documentos, Administrar impresoras, Ver servidor, Administrar servidor)	Administradores del sistema: pueden administrar el sistema totalmente (Permisos: Imprimir, Administrar documentos, Administrar impresoras, Ver servidor, Administrar servidor)
Actualizar un controlador instalado o incluido en una cola existente			Sí	Sí	Sí
Agregar o eliminar un formulario en la cola			Sí	Sí	Sí
Ver las propiedades de impresora	Sí	Sí	Sí	Sí	Sí
Ver las propiedades del servidor de impresión	Sí	Sí	Sí	Sí	Sí
Administrar el permiso de seguridad en la cola de impresión			Sí	Sí	Sí
Administrar el descriptor de seguridad marca setServerSecurityDescirptor del servidor de impresión					Sí

	Usuarios estándar: pueden conectarse a impresoras e imprimir sus documentos (Permisos: Imprimir, Ver servidor)	Administradores delegados parciales: pueden agregar impresoras (Permisos: Imprimir, Ver servidor, Administrar servidor)	Administradores delegados parciales: pueden administrar colas existentes (Permisos: Imprimir, Ver servidor, Administrar impresoras, Administrar documentos)	Administradores delegados completos: pueden realizar todas las tareas de impresión administrativas (Permisos: Imprimir, Administrar documentos, Administrar impresoras, Ver servidor, Administrar servidor)	Administradores del sistema: pueden administrar el sistema totalmente (Permisos: Imprimir, Administrar documentos, Administrar impresoras, Ver servidor, Administrar servidor)
Agregar y eliminar la cola de impresión en un servidor		Sí, pero puede agregar una impresora usando solo un controlador preinstalado.	Sí, pero solo puede eliminar la cola de impresión con el permiso Administrar impresora.	Sí, pero puede agregar una impresora usando solo un controlador preinstalado.	Sí
Agregar y eliminar un controlador de impresión en un servidor		Sí, pero solo localmente. El usuario debe ser miembro del grupo Administradores para poder agregar controladores no incluidos o para agregar controladores al servidor de impresión de forma remota.		Sí, pero solo localmente. El usuario debe ser miembro del grupo Administradores para poder agregar controladores no incluidos o para agregar controladores al servidor de impresión de forma remota.	Sí
Agregar, eliminar y configurar puertos en un servidor de impresión		Sí		Sí	Sí
Agregar y eliminar un formulario en un servidor de impresión		Sí		Sí	Sí

	Usuarios estándar: pueden conectarse a impresoras e imprimir sus documentos (Permisos: Imprimir, Ver servidor)	Administradores delegados parciales: pueden agregar impresoras (Permisos: Imprimir, Ver servidor, Administrar servidor)	Administradores delegados parciales: pueden administrar colas existentes (Permisos: Imprimir, Ver servidor, Administrar impresoras, Administrar documentos)	Administradores delegados completos: pueden realizar todas las tareas de impresión administrativas (Permisos: Imprimir, Administrar documentos, Administrar impresoras, Ver servidor, Administrar servidor)	Administradores del sistema: pueden administrar el sistema totalmente (Permisos: Imprimir, Administrar documentos, Administrar impresoras, Ver servidor, Administrar servidor)
Compartir la impresora			Sí, si tiene los permisos Administrar impresora en el servidor de impresión y se han habilitado las excepciones Compartir impresoras y archivos* en Firewall de Windows con seguridad avanzada.	Sí, si se han habilitado las excepciones Compartir impresoras y archivos* en Firewall de Windows con seguridad avanzada.	Sí

Nota: Se recomienda que solo un miembro del grupo Administradores del sistema instale controladores. Si un administrador de impresión delegado piensa agregar o administrar colas de forma remota, el Administrador del sistema debe instalar el controlador en el siguiente directorio mediante scripts o manualmente: \Windows\System32\spool\drivers\x64\3

Más adelante en esta guía se indicarán los procedimientos para crear administradores delegados y gestionar adecuadamente los permisos de impresión en cada una de las impresoras instaladas en un servidor de impresión basado en Windows Server 2016.

6.4 DIRECTIVA DE GRUPO PARA MODIFICAR LA CONFIGURACIÓN DE SEGURIDAD DEL CONTROLADOR DE IMPRESORA

Tal y como se ha indicado anteriormente, la configuración de seguridad predeterminada de Windows 10 y Windows Server 2016 permite que usuarios que no sean miembros del grupo local "Administradores" solo puedan instalar controladores de impresoras de confianza, como las ofrecidas con Windows o en paquetes de controladores de impresoras firmados digitalmente.

Puede usar la configuración de la directiva de grupo “Restricciones de apuntar e imprimir” para controlar la forma en que los usuarios instalan controladores de impresoras desde los servidores de impresión.

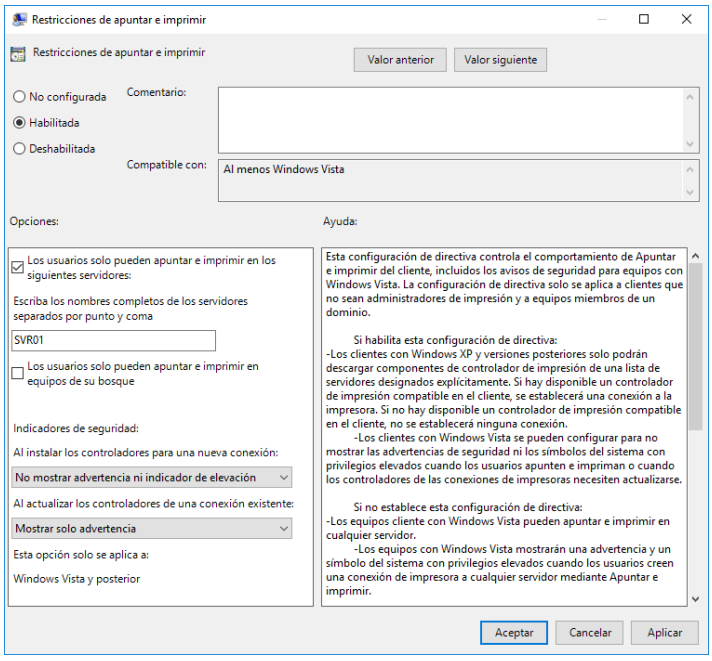
Esta configuración se puede usar para permitir a los usuarios conectarse únicamente a determinados servidores de impresión que sean de confianza. Puesto que este valor evita que los usuarios se conecten a otros servidores de impresión que pueden hospedar potencialmente controladores de impresión, no probados o dañinos, puede desactivar los mensajes de advertencia de instalación de controladores de impresión sin poner en riesgo la seguridad.

Se recomienda evaluar cuidadosamente las necesidades de impresión de los usuarios antes de establecer los servidores de impresión a los que podrán conectarse. Si los usuarios necesitan conectarse de forma ocasional a impresoras compartidas de una sucursal u otro departamento, asegúrese de que se incluyen estos servidores de impresión en la lista (si cree que los controladores de impresión instalados en los servidores son de confianza).

Además, puede usar la opción “Restricciones de punto y de impresión” para desactivar completamente los indicadores de advertencia, aunque este valor deshabilitará la seguridad mejorada en la instalación de controladores de impresoras de Windows 10 y Windows Server 2016 para los usuarios.

Para permitir que los usuarios se conecten únicamente a determinados servidores de impresión en los que confía, la directiva “Restricciones de apuntar e imprimir” se debe habilitar y activar la casilla “Los usuarios solo pueden apuntar e imprimir en los siguientes servidores”. A continuación, se pueden escribir los nombres completos de los servidores a los cuales desea que los usuarios puedan conectarse. Separe cada nombre con un punto y coma.

Además, se pueden ocultar las advertencias de seguridad, para ello, en el cuadro “Al instalar los controladores para una nueva conexión” se debe seleccionar la opción “No mostrar advertencia ni indicador de elevación” y en el cuadro “Al actualizar los controladores de una conexión existente”, escoja la opción “Mostrar solo advertencia”.



6.5 DESPLIEGUE DE IMPRESORAS CON DIRECTIVAS DE GRUPO

Se puede utilizar el complemento **"**Administración de impresión con directiva de grupo**"** para implementar automáticamente conexiones de impresora para usuarios o equipos e instalar los controladores de impresora apropiados.

Este método de instalación de una impresora resulta útil en lugares como laboratorios, clases u oficinas sucursales, donde la mayoría de los equipos o usuarios necesitan obtener acceso a las mismas impresoras.

También es un método útil para la implementación de controladores de impresoras para usuarios que no son miembros del grupo local "Administradores" y ejecutan Windows 10.

Para implementar conexiones de impresora con directivas de grupo, el entorno debe cumplir el siguiente requisito:

a) El esquema de servicios de dominio de Directorio Activo (AD DS) debe usar una versión de esquema Windows Server 2016.

En las conexiones por equipo, Windows agrega las conexiones de impresora cuando el usuario inicia sesión (o cuando el equipo se reinicia si se usa la utilidad "PushPrinterConnections.exe").

En las conexiones por usuario, Windows agrega las conexiones de impresora durante la actualización de la directiva en segundo plano (o cuando el usuario inicia sesión si se usa la utilidad "PushPrinterConnections.exe").

Si se quita la configuración de conexión de impresora desde la GPO, Windows quita las impresoras correspondientes del equipo cliente durante la siguiente actualización de directiva en segundo plano o en el inicio de sesión del usuario (o en el siguiente reinicio o inicio de sesión si se usa la utilidad "PushPrinterConnections.exe").

La utilidad "PushPrinterConnections.exe" lee la configuración de la conexión de impresora de la directiva de grupo y agrega las conexiones de impresora adecuadas al equipo o a la cuenta de usuario (o actualiza las conexiones existentes).

El archivo "PushPrinterConnections.exe" detecta el sistema operativo y finaliza automáticamente en los equipos que ejecutan Windows 10 o Windows Server 2016. Estos equipos tienen compatibilidad integrada para las conexiones de impresora que se implementan con directivas de grupo, de modo que puede implementar correctamente este archivo en todos los equipos cliente de su organización.

7. SISTEMAS DE TRAZABILIDAD Y AUDITORÍA

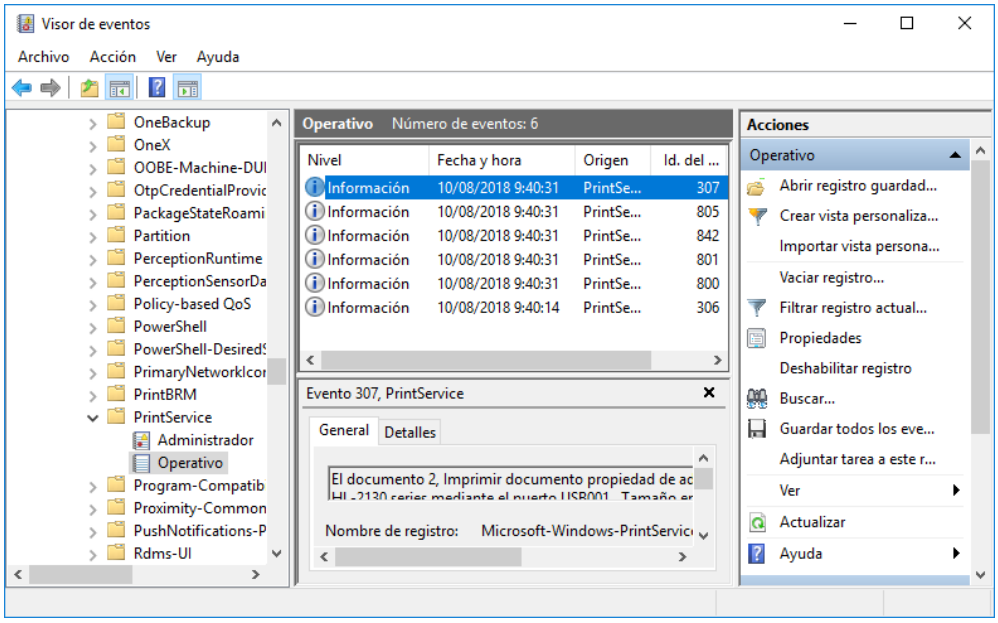
7.1 REGISTRO DE TRABAJOS DE IMPRESIÓN

Debido al cumplimiento de normativas o legislación, se requiere en muchos casos dejar registrado que usuario ha ejecutado un trabajo de impresión con todos sus detalles.

Para ello, Windows Server 2016 permite habilitar el registro de operaciones con un alto nivel de detalle de los diferentes trabajos de impresión que se están ejecutando en dicho servidor.

Sin embargo, este registro de operaciones de impresión, por defecto no está habilitado.

El registro de operaciones se localiza en la consola administrativa del visor de eventos en la ruta **"Inicio → Herramientas administrativas → Visor de eventos"**, una vez dentro, se debe acceder al nodo **"Visor de eventos (local) → Registros de aplicaciones y servicios → Microsoft → Windows → PrintService → Operativo"**.



El evento con identificador 307 es el que indica la operación de impresión, así como el dueño del documento y la impresora donde ha sido ejecutado.