centro criptológico nacional

## Guía de Seguridad de las TIC

# IMPLEMENTACIÓN DE SEGURIDAD EN CITRIX VIRTUAL APPS AND DESKTOPS SOBRE WINDOWS SERVER 2016

FEBRERO 2020

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES


NIPO: 083-20-089-7

Fecha de Edición: febrero de 2020
Sidertia Solutions S.L. ha participado en la realización y modificación del presente documento y sus anexos.

# PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

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 y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del 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, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, 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 la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

Febrero de 2020

Paz Esteban López
Secretaria de Estado
Directora 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 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 2016, 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 la implementación y garantía de la seguridad para Citrix Virtual Apps and Desktops 7.15 CU5 LTSR, instalado en los servidores miembro MS Windows Server 2016 perteneciente a un dominio Windows de Directorio Activo.

La presente guía tiene como objeto la implementación de todos los roles necesarios para el funcionamiento de una infraestructura básica con los roles, Citrix Delivery Controller, Citrix Storefront, Citrix Director y Citrix Licensing. Se establecerán también los procesos y tareas administrativas para hacer una administración segura de los mismos.

La instalación y configuración de la solución se ha diseñado de tal forma que la implementación sea lo más restrictiva posible, minimizando la superficie de ataque y por lo tanto los riesgos que pudieran existir. Es posible que para el uso de determinadas funcionalidades de Windows Server 2016 requiera modificar las configuraciones que se plantean con la presente guía. También puede darse el caso que la implementación de otros servicios o aplicaciones, no objeto de esta guía, conlleven la modificación de las configuraciones aquí definidas.

No obstante, se tiene en consideración que los ámbitos de aplicación son muy variados, y por ello, su aplicación dependerá de 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 esta guía 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”.

Esta guía asume que los roles de Citrix Virtual Apps and Desktops se van a instalar sobre equipos con sistema operativo Windows Server 2016 Standard de 64 Bits, donde previamente se ha seguido el proceso de implantación definido en la guía “CCN-STIC-570A”. De la misma forma, para la aplicación de los roles Citrix Director y Citrix Storefront es de necesidad la aplicación, además, de las medidas de seguridad descritas en la guía “CCN-STIC-574” en sus configuraciones para un servidor web dinámico.

Así mismo, no se contempla en esta guía la instalación de ninguno de los roles en alta disponibilidad, 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 de una infraestructura con todos los roles del producto sobre Microsoft Windows Server 2016 en una configuración restrictiva de seguridad. La guía se ha elaborado para proporcionar información específica sobre cómo implementar las distintas configuraciones para los escenarios planteados en servidores miembro de un dominio bajo el Sistema Operativo Microsoft Windows Server 2016.

Este documento incluye:

a) **Características de los roles Citrix Virtual Apps and Desktops.** Completa descripción de los roles que componen una infraestructura con esta tecnología.

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

c) **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.

d) **Guía paso a paso.** Permite implantar y establecer las configuraciones de seguridad en un servidor (una para cada rol descrito en la presente guía).

e) **Lista de comprobación.** Ayuda a verificar el grado de cumplimiento de un servidor con respecto a las condiciones de seguridad que se establecen en esta guía.

## 5. DESCRIPCIÓN DE 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 la guía, además de los requisitos para la instalación de cada uno de los roles, será necesario cumplir los requisitos definidos para Windows Server 2016, en concreto, para los roles Citrix Director y Citrix Storefront será de necesidad cumplir con los requisitos definidos para el rol IIS 10.

b) Si el entorno en el que está aplicando seguridad, pertenece a una red clasificada, se deberá realizar la securización del sistema antes de instalar cada uno de los productos. Para ello, será necesario aplicar la guía de seguridad codificada como CCN-STIC-570A en todos los servidores, y a continuación, para los servidores que ejecuten los roles Citrix Director y Citrix Storefront, se deberá aplicar la guía “CCN-STIC-574”, que instala y configura el rol de IIS 10 de Windows Server 2016. Una vez aplicadas las medidas de seguridad, puede proceder con la aplicación de la presente guía.

c) En aquellos sistemas que les sea de aplicación el ENS estas medidas deberán adaptarse a las necesidades de cada organización.

## 5.1 AVISOS IMPORTANTES A LOS USUARIOS DE ESTA GUÍA

El contenido de esta guía es de aplicación sobre equipos tipo puesto servidor, con Sistema Operativo Windows Server 2016, en castellano, con una instalación por defecto.

El objetivo de la guía es el 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 de Windows Server 2016 Standard, con los parámetros por defecto de instalación con la guía “CCN-STIC-570A” aplicada. 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 la versión 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 los roles contenidos en el producto Citrix Virtual Apps and Desktops 7.15 CU5 en un entorno de dominio de Active Directory.

La guía de seguridad ha sido elaborada utilizando un laboratorio basado en una plataforma de virtualización tipo Hyper-V de Windows Server 2016 con las siguientes características técnicas:

a) Servidor Dell PowerEdgeTM T320:
   i. Intel Pentium Xeon Quad Core.
   ii. HDD 80 GB.
   iii. 32 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. 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 IIS 10 requiere, para un entorno de producción, un mínimo de requerimientos (2 GB de RAM y 32 GB de espacio de almacenamiento en disco). Oficialmente no se indica ningún requerimiento adicional.

Para la aplicación de la presente guía debe contar con los requerimientos mínimos de cada rol del producto que indica el fabricante de forma oficial adicionalmente a los requisitos del sistema operativo.

a) Citrix Delivery Controller
   i. 5GB de RAM
   ii. 800MB espacio libre en disco
b) Citrix Director
   i. 2GB de RAM
   ii. 200MB espacio libre en disco
c) Citrix Storefront
   i. 2GB de RAM
d) Citrix Licensing
   i. 2GB de RAM

**Nota:** Puede consultar el resto de requisito a través del siguiente enlace: https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/system-requirements.html

Para determinar el dimensionamiento hardware de su infraestructura, se deberá tener en cuenta las recomendaciones oficiales del fabricante indicadas en la documentación del producto, ya que, en función del número de conexiones que vayan a gestionar sus servidores, las recomendaciones necesarias variarán de un entorno a otro.

La guía ha sido desarrollada con el objetivo de dotar a la infraestructura de la seguridad máxima en caso de redes clasificadas y la seguridad mínima siguiendo las normas descritas en el ENS. 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 reemplazar políticas consolidadas y probadas de las organizaciones sino a servir como la 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 de cada uno de los roles del producto Citrix Virtual Apps and Desktops 7.15 CU5 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 los sistemas Microsoft Windows Server 2016 en su versión Standard con cualquiera de los roles Citrix 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 donde se quiera instalar cualquiera de los roles Citrix.

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.

# 6. DESCRIPCIÓN DE CITRIX VIRTUAL APPS AND DESKTOPS

Citrix Virtual Apps and Desktops es una solución de virtualización que permite tener un control de las máquinas virtuales y aplicaciones de una organización a la vez que se proporciona un acceso seguro a las mismas desde cualquier dispositivo.

La arquitectura de Citrix Virtual Apps and Desktops permite:

a) Proporcionar aplicaciones y escritorios a los usuarios independientemente del sistema operativo que utilicen.

b) Administrar y tener un control de acceso a los recursos de la organización

c) Administrar una red entera desde un único centro de datos

d) Aislar y centralizar el acceso a la información desde equipos de confianza

Citrix Virtual Apps and Desktops comparte un modelo de arquitectura unificado llamado Flexcast Management Architecture que permite mantener en una misma implementación distintas versiones de un mismo producto controlando los recursos que ofrece cada uno de ellos.

## 6.1 COMPONENTES DE CITRIX VIRTUAL APPS AND DESKTOPS

### 6.1.1 CITRIX DELIVERY CONTROLLER

El rol Citrix Delivery Controller, coloquialmente conocido también como “bróker”, es el componente principal de la infraestructura, permite realizar el mantenimiento del Sitio.

Un Sitio es la unidad lógica que compone una implementación, puede estar compuesto por uno o más Delivery Controllers, dependiendo del entorno y las necesidades de alta disponibilidad.

El rol Delivery Controler realiza la labor de control de las máquinas virtuales, coordinando, y autenticando la distribución de las aplicaciones y escritorios, gestionando y optimizando las conexiones a recursos publicados, entre los servidores disponibles.

A su vez, el rol Delivery Controller se encarga de realizar un seguimiento de que usuarios están utilizando que recursos, guardando toda la información en las bases de datos.

Otra de las funcionalidades del rol es la capacidad de controlar la energía de las máquinas virtuales bajo demanda o mediante configuraciones administrativas, permitiendo, por ejemplo, que el escritorio de un usuario se encienda a la vez que el usuario inicia sesión en Citrix.

### 6.1.2 CITRIX STOREFRONT

El rol Citrix Storefront es el encargado de la autenticación de los usuarios en los recursos de la organización. Gestiona las subscripciones de los usuarios y ofrece una experiencia consistente entre múltiples dispositivos. Controla la implementación de la aplicación Citrix Receiver y permite su autoconfiguración basándose en las configuraciones de las tiendas implementadas.

Cuando un usuario completa su autenticación, este rol contacta con el Sitio, o Sitios definidos para presentar los recursos disponibles a los que tiene acceso. Este rol emplea la tecnología Microsoft .NET ejecutándose sobre Microsoft Internet Information Services.

Citrix Storefront cuenta principalmente con los siguientes tres componentes:

a) Servicio de autenticación: autentica a los usuarios en un dominio de Directorio Activo, permitiendo que los usuarios no tengan que autenticarse de nuevo en cada uno de sus escritorios o aplicaciones.

b) Servicio de enumeración de escritorios y aplicaciones: contacta con las implementaciones de Citrix Virtual Apps and Desktops y presenta al usuario los recursos obtenidos.

c) Servicio de subscripciones: recoge los detalles de las aplicaciones favoritas de los usuarios y actualiza los múltiples dispositivos para presentar una experiencia unificada entre ellos.

El rol Citrix Storefront se puede implementar en varios servidores, para lograr mayor capacidad de gestión de conexiones y para mejorar la disponibilidad del servicio.

### 6.1.3 CITRIX DIRECTOR

Citrix Director es la herramienta web que permite realizar tareas de soporte sobre la infraestructura y a su vez realizar una monitorización del entorno. Este rol permite la configuración de múltiples sitios bajo una única implementación.

Entre los datos que Citrix Director muestra en su web de administración, se encuentra la siguiente información:

a) Datos de sesiones en tiempo real.

b) Estado y métricas del tráfico HDX.

También permite la visualización e interacción con sesiones de usuarios, utilizando la funcionalidad de Asistencia Remota de Windows.

Al igual que el resto de roles, permite su implementación en alta disponibilidad utilizando un servicio de balanceo externo.

### 6.1.4 CITRIX LICENSING

Este rol es el encargado de administrar las licencias para todos los productos Citrix, comunica continuamente con el rol Citrix Delivery Controller para gestionar las licencias para cada una de las sesiones de los usuarios y con la consola Citrix Studio para asignar archivos de licencia. Es obligatoria la implementación de al menos un servidor de licencias para almacenar y controlar las licencias del entorno.

## 6.2 SERVICIOS INSTALADOS POR CADA ROL

Durante la instalación de los roles de Citrix Virtual Apps and Desktops se realiza la configuración de varios de los servicios que se encargaran de proporcionar las funcionalidades a la implementación.

El objetivo de este apartado es indicar que servicios se configuran durante la instalación de los distintos roles de Citrix, así como los permisos necesarios para que los servicios de los distintos roles se ejecuten correctamente.

### 6.2.1 SERVICIOS CITRIX DELIVERY CONTROLLER

A continuación, se detallan los servicios utilizados por el rol Citrix Controller, junto con su descripción funcional y el estado de configuración que se aplica en la presente guía.

Se deben diferenciar los servicios propios de Citrix de los servicios del sistema con los que interactúa.

| Nombre | Descripción | Valor de inicio |
|---|---|---|
| Asignador de extremos de RPC | Resuelve identificadores de interfaces RPC de transporte. Si se detiene o deshabilita este servicio los programas que usen servicios de llamada a procedimiento remoto (RPC) no funcionarán correctamente. | Automático |
| Estación de trabajo | Herramientas de registro proporciona una infraestructura para administrar los registros del servidor web y automatizar las tareas de registro comunes. | Automático |

| Nombre | Descripción | Valor de inicio |
|---|---|---|
| Iniciador de procesos de servidor DCOM | El servicio DCOMLAUNCH inicia los servidores COM y DCOM en respuesta a las solicitudes de activación de objetos. Si se detiene los programas que utilicen COM o DCOM no funcionarán correctamente. | Automático |
| Llamada a procedimiento remoto (RPC) | El servicio RPCSS es el administrador de control de servicios para servidores COM y DCOM. Realiza solicitudes de activación de objetos, resoluciones del exportador de objetos y recolección distribuida de elementos no usados para servidores COM y DCOM. | Automático |
| Servicio Interfaz de almacenamiento en red | Este servicio entrega notificaciones de red a los clientes en modo usuario. | Automático |
| Citrix AD Identity Service | Administra las cuentas de equipo de Active Directory. | Automático |
| Citrix Analytics | Servicio de analíticas de Citrix. | Automático |
| Citrix App Library | Guarda información acerca de las aplicaciones del Sitio. | Automático |
| Citrix Broker Service | Proporciona servicios de configuración e intermediación en las conexiones con escritorios y aplicaciones. | Automático |
| Citrix ConfifSyncService | Copia la configuración del Sitio de forma local para LocalHostCache. | Automático |
| CitrixConfiguration Logging | Registra los cambios de configuración y la actividad de los administradores en los entornos Citrix. | Automático |
| CitrixConfiguration Service | Servicio principal que almacena información sobre el resto de servicios de la implementación. | Automático |
| CitrixConnector | Coordina la implementación de software y transmite los registros de implementación. | Deshabilitado |
| CitrixDelegatedAdmin | Administra la configuración de permisos de administración delegada. | Automático |
| CitrixEnvTest | Administra las pruebas para evaluar el estado de un sitio de la implementación. | Automático |
| CitrixHigh AvailavilityService | Ofrece continuidad de servicio cuando se producen interrupciones del sitio central. | Automático |
| CitrixHostService | Servicio que permite la administración de conexiones de hipervisor y hosts. | Automático |
| CitrixMachine CreationService | Servicio para la creación de máquinas virtuales utilizando MCS. | Automático |
| CitrixMonitor | Servicio de monitorización de la infraestructura FMA. | Automático |
| CitrixOrchestration | API de alto nivel para Citrix Virtual Apps and Desktops. | Automático |
| CitrixPrivileged Service | Administra las operaciones con privilegios en Storefront. | Automático |
| CitrixStorefront | Servicio para administrar la implementación de Storefront. | Automático |

| Nombre | Descripción | Valor de inicio |
|---|---|---|
| CitrixTelemetry Service | Servicio de la funcionalidad “Call Home” que recopila datos de diagnóstico y carga periódicamente paquetes de telemetría con esos datos directamente en Citrix Insight Services para el análisis y la solución de problemas. | Deshabilitado |
| CitrixTrust | Servicio de la infraestructura FMA para las relaciones de confianza. | Automático |
| XaXdCloudProxy | Habilita la comunicaciones desde servidores VDA y servidores Storefront. | Automático |
| Monitor Agent | Agente de monitorización de entornos. | Deshabilitado |

### 6.2.2 SERVICIOS CITRIX STOREFRONT

En el presente apartado, se describen los servicios que se configuran durante la instalación del rol Citrix Storefront, junto con los servicios del sistema necesarios para su correcto funcionamiento.

| Nombre | Descripción | Valor de inicio |
|---|---|---|
| Aislamiento de claves CNG | El servicio Aislamiento de claves CNG se hospeda en el proceso LSA. Proporciona aislamiento de proceso de claves para las claves privadas y las operaciones criptográficas asociadas según lo requiere el Criterio Común. | Automático |
| Servidor | Ofrece compatibilidad con uso compartido de archivos, impresoras y canalizaciones con nombre en la red para este equipo. | Automático |
| Citrix Peer Resolution Service | Resuelve nombres de nodos del mismo nivel dentro de mallas de nodo a nodo. | Automático |
| CitrixConfiguration Replication | Brinda acceso a la información de configuración de Delivery Services. | Automático |
| CitrixCredentialWallet | Ofrece un almacén seguro para las credenciales. | Automático |
| CitrixDefaultDomain Service | Proporciona autenticación, cambio de contraseñas y otros servicios de dominio. | Automático |
| CitrixServiceMonitor | Proporciona un estado de salud de los servicios de Storefront. | Automático |
| CitrixSubscriptions Store | Proporciona almacenamiento y capacidad de replicación para las suscripciones de los usuarios. | Automático |
| CitrixTelemetryService | Servicio de telemetría de Citrix para el rol Storefront. | Automático |
| NetTcpPortSharing | Ofrece la posibilidad de compartir puertos TCP a través del protocolo Net.TCP. | Automático |
| CitrixClusterService | Brinda servicios necesarios para la incorporación a un grupo de servidores. | Deshabilitado |

### 6.2.3 SERVICIOS CITRIX LICENSING

En la siguiente tabla puede encontrar una descripción de los servicios utilizados por el rol Citrix Licensing para la gestión de las licencias del entorno.

| Nombre | Descripción | Valor de inicio |
|---|---|---|
| Citrix Licensing | Proporciona servicios de licencia para los productos Citrix. | Automático |
| CtxLSPortSvc | Este servicio controla la lectura de los archivos de licencia y la actualización de cadenas con comentarios de licencia. | Automático |
| Citrix_GT_ LicensingProv | Servicio WMI para el licenciamiento de productos. | Manual |

### 6.2.4 SERVICIOS CITRIX DIRECTOR

El componente de soporte Citrix Director, al ser puramente una consola web de gestión, soporte y monitorización del entorno, cuenta únicamente con los mismos servicios que el rol Internet Information Services (IIS).

| Nombre | Descripción | Valor de inicio |
|---|---|---|
| Servicio de publicación World Wide Web | Proporciona conectividad y administración web mediante el Administrador de Internet Information Services. | Automático |
| Servicio de administración IIS | Habilita este servidor para administrar la metabase de IIS. La metabase de IIS almacena la configuración de los servicios IIS. | Automático |

## 6.3 MEDIOS DE INSTALACIÓN Y ADMINISTRACIÓN

En el siguiente punto se detallan los elementos necesarios para los distintos casos de uso del sistema, entre los que se contemplan la instalación, la configuración y la administración de los sistemas de la infraestructura Citrix Virtual Apps and Desktops.

Dentro de los componentes necesarios para realizar la instalación usted debe contar con al menos los siguientes requisitos:

a) Medios de instalación (.iso) de Windows Server 2016.

b) Medios de instalación (.iso) de SQL Server 2016 SP2.

c) Medios de actualización acumulativa a SQL Server 2016 SP2 CU11 o posterior.

d) Medios de instalación (.iso) de la versión Citrix Virtual Apps and Desktops 7.15 CU5.

e) Archivo de licencias de Citrix que haya descargado y asignado desde la web del fabricante.

De no contar con alguno de los anteriores, deberá obtenerlo antes de dar comienzo a la instalación del software.

Para realizar la administración de la infraestructura, deberá utilizar un equipo aislado, con las siguientes herramientas disponibles:

a) Administración de directivas de grupo.

b) Usuarios y equipos de Active Directory.

c) Citrix Studio.

d) Acceso web a Citrix Licensing.

e) Acceso web a Citrix Director.

f) Administrador de Internet Information Services

g) SQL Server Management Studio.

Debido a la importancia que conlleva la administración del entorno, las herramientas administrativas serán accesibles desde cada uno de los servidores adicionalmente a las máquinas de administración que destine en su infraestructura.

**Nota:** La herramienta de administración Citrix Storefront debido a una limitación de producto solo puede utilizarse desde cualquiera de los servidores con el rol Citrix Storefront de su infraestructura.

La siguiente tabla detalla las herramientas de administración disponibles desde cada tipo de servidor siguiendo las indicaciones marcadas en la presente guía.

| Rol Instalado | Herramientas administrativas |
|---|---|
| Citrix Delivery Controller | Citrix Studio |
| | Citrix Scout |
| Citrix Storefront | Administrador de Internet Information Services |
| | Citrix Storefront |
| Citrix Licensing | Citrix License Administration Console (acceso web) |
| | Citrix Licensing Manager (acceso web) |
| Citrix Director | Administrador de Internet Information Services |
| | Citrix Director (acceso web) |

**Nota:** Pese a detallar en la tabla anterior la herramienta administrativa "Citrix License Administration Console" su funcionamiento y uso está restringido en la presente guía de seguridad debido a que utiliza protocolos no seguros para realizar la autenticación de los usuarios administradores. Si por algún motivo administrativo necesita hacer uso de dicha utilidad, deberá permitir la comunicación utilizando el protocolo NTLM entre su controlador de dominio y el servidor con el rol Citrix Licensing.

Adicionalmente a las herramientas administrativas anteriores, para realizar algunas configuraciones sobre el entorno, tiene disponible cmdlets de Powershell, con los que se pueden realizar algunas de las siguientes tareas:

a) Revisar y gestionar configuraciones del Sitio.

b) Cambiar la base de datos a la que apuntan cada uno de los servicios de la infraestructura.

c) Ver las tareas en segundo plano pendientes por realizar en los hipervisores.

d) Administración de las propiedades de los catálogos de máquinas y grupos de entrega.

## 7. SEGURIDAD EN CITRIX VIRTUAL APPS AND DESKTOPS

Una infraestructura de Citrix Virtual Apps and Desktops, puede presentar los recursos configurados dentro de la red corporativa, intranet o añadiendo elementos adicionales hacia internet. En cualquiera de los tres casos, se deben tomar medidas para asegurar el servicio, puesto que los ataques pueden originarse desde usuarios, equipos en la red LAN o desde redes públicas.

Para ofrecer una seguridad completa para los escritorios y las aplicaciones virtuales de la intranet de una organización, cada servidor de la infraestructura debe protegerse de:

a) Los equipos o clientes ligeros que puedan conectarse al entorno, principalmente hacia el servidor Citrix Storefront que realiza las funciones de frontal web en la red corporativa.

b) Otros servidores ubicados en la misma subred que alberga los servidores de la infraestructura, y que puedan tener comunicación con servicios de la red intranet o internet directamente.

c) Posibles accesos no autorizados, o anónimos, desde redes públicas no confiables, controlando en todo momento los permisos de acceso, tanto a recursos de la organización, como a los propios servidores.

En la presente guía se aplica el principio de segregación de roles, por lo que se implementa cada rol de la infraestructura sobre un servidor aislado, y procura que las redes estén lo suficientemente segmentadas en función de los servicios que prestan.

Una parte de las medidas de seguridad en el entorno se debe a una configuración adecuada de las reglas del firewall de Microsoft Windows Server 2016, limitando la comunicación que tienen los servidores y servicios entre ellos, el proceso de instalación de Citrix Virtual Apps and Desktops configura de forma automática las reglas necesarias para mantener comunicación con el resto de servidores de la infraestructura. Todas las reglas necesarias, han sido implementadas mediante directivas de grupo utilizando Directorio Activo.

Para tomar una posición proactiva contra los usuarios maliciosos y atacantes, todos los roles de la infraestructura se instalan siguiendo directivas de seguridad, que permitan tener controles de acceso, trazabilidad y segmentación de los servicios. Por defecto, tras realizar la instalación y configuración del Sitio, se configuran los siguientes roles administrativos, que contarán con visibilidad y capacidad de administración de la infraestructura.

| Rol administrativo | Descripción del rol |
|---|---|
| Administrador total | Puede realizar cualquier tarea y operación dentro del Sitio. |
| Administrador de solo lectura | Puede ver todos los objetos especificados para su ámbito, pero no puede realizar ningún cambio sobre las configuraciones. |
| Administrador de asistencia técnica | Puede ver los grupos de entrega y administrar las sesiones junto con las maquinas asociadas a dichos grupos de entrega, puede realizar tareas de administración de sesiones y administración de energía de los equipos. |
| Administrador de catálogos de maquinas | Puede crear y administrar catálogos de máquinas y aprovisionar maquinas en ellos. Puede crear catálogos de máquinas a partir de la infraestructura de virtualización, este rol puede administrar las imágenes base e instalar software, pero no puede asignar las aplicaciones o los escritorios a los usuarios. |
| Administrador de grupos de entrega | Puede entregar aplicaciones, escritorios y máquinas, además de administrar las sesiones asociadas. También puede administrar las configuraciones de aplicaciones y escritorios tales como las configuraciones de directivas y de administración de energía. |
| Administrador de host | Puede administrar conexiones de host y sus parámetros de recursos asociados. No puede entregar maquinas, aplicaciones ni escritorios a los usuarios. |

Como parte de las tareas de su infraestructura, se deberá otorgar a cada administrador los mínimos privilegios necesarios para realizar la administración del entorno, en las indicaciones de instalación y configuración, se preparará un grupo de seguridad para el rol de administrador total, adicionalmente usted puede crear grupos adicionales en función del número y tipo de administradores con los que cuente.

Cuando Citrix Virtual Apps and Desktops es parte de un sistema completo de servicio en alta disponibilidad, se deberá evaluar la posibilidad de utilizar la característica balanceo de carga en red (NLB) de Windows server 2016, o bien, implementar el componente de red Citrix ADC, ninguno de ellos contemplados en esta guía.

Otro de los mecanismos de seguridad utilizados para la protección de los sistemas web, consiste en la configuración del módulo de filtrado de solicitudes. En la presente guía de seguridad se realiza la configuración de aquellas solicitudes necesarias en el sistema. Los roles Citrix Storefront y Citrix Director presentan las siguientes configuraciones a nivel de IIS.

| Rol administrativo | Extensión | Estado |
|---|---|---|
| Citrix Director | .dll | Habilitada |
| | .exe | Habilitada |
| | .js | Habilitada |
| | .original | Habilitada |
| | .pspimage | Habilitada |
| | .svc | Habilitada |
| | .xml | Habilitada |
| Citrix Storefront | .appcache | Habilitada |
| | .cr | Habilitada |
| | .dtd | Habilitada |
| | .ica | Habilitada |
| | .ico | Habilitada |
| | .js | Habilitada |
| | .svg | Habilitada |
| | .xml | Habilitada |

**Nota:** La anterior tabla detalla las extensiones necesarias para el correcto funcionamiento de Citrix Storefront y Citrix Director, utilizando la implementación web por defecto, si usted desea modificar el sitio web puede que sea necesario añadir nuevas extensiones al módulo de filtrado de solicitudes.

Adicionalmente, si la descarga o actualización de Citrix Workspace App/Citrix Receiver está habilitada, se deberá permitir en Citrix Storefront las extensiones ".dmg" y ".exe"

De la misma forma, si sobre su implementación se desea configurar la funcionalidad de HTML5, Citrix Storefront requiere que las extensiones ".eot", ".ttf" y ".woff".

Para el correcto funcionamiento del sistema, se debe conocer que, tanto Citrix Storefront, como Citrix Director, hacen uso de los verbos HTTP "GET", "POST" y "HEAD", que se puede configurar en el apartado de filtrado de solicitudes.

## 7.1 AUDITORIA Y REGISTRO

La auditoría y el registro de la actividad son indispensables para poder realizar tareas de análisis de uso, análisis forense y obtener resultados en pruebas. Para estas tareas dispone de muchas herramientas. Entre otras:

a) Registro de aplicaciones y servicios de Windows.

b) Registro de solicitudes del servidor IIS.

c) Registros de Windows (aplicación, seguridad, sistemas, etc.).

d) Base de datos CitrixLogging.

e) Auditoría de ficheros y objetos.

Se entiende que el registro de actividad debe separarse en dos niveles principales:

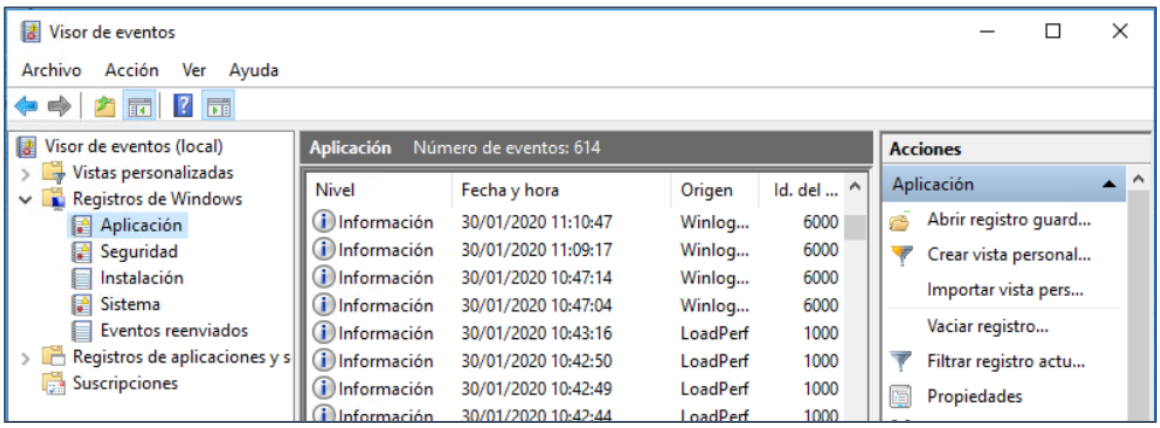
a) Actividad del servicio.

b) Actividad de los usuarios en su interacción con el servidor.

Cada una de ellas se configuran y almacenan de forma independiente.

**Nota:** No es posible crear un modelo genérico para todos los servidores, sino que será necesario adaptar la configuración a los contenidos, uso y rol del servidor.

El mecanismo de registros de servicios y aplicaciones en Windows Server 2016 a través del sistema ETW (Event Tracing for Windows) incorpora un módulo específico para los servicios de los roles Citrix Virtual Apps and Desktops. Durante la implementación de la presente guía todos los eventos se recopilan en el visor de eventos de aplicación.



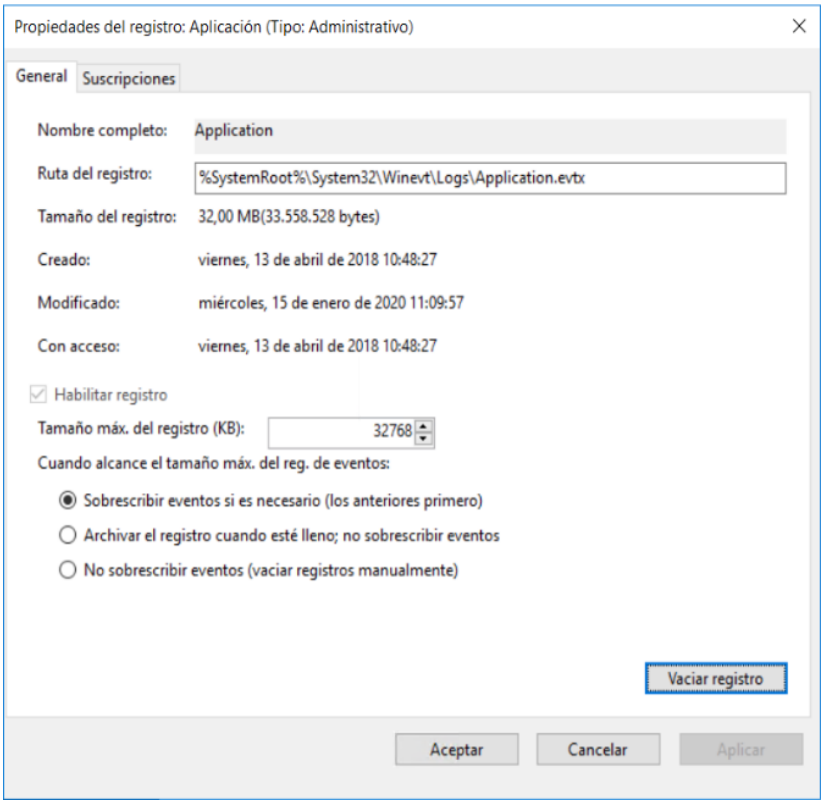

*Vista del registro de Windows Aplicación.*

El registro de aplicación queda activado, por defecto, en el sistema tras su instalación, por lo que se recomienda no desactivar el registro de aplicación o se perderá información relevante ante un error en el sistema.

Los eventos administrativos indicarán actuaciones que el administrador tendrá que atender necesariamente, mientras que los operacionales recogerán aquellos habituales, como pueden ser inicios o paradas del servidor, gestión de sesiones o disponibilidad de recursos.

Todos los eventos que muestra cada vista personalizada son eventos guardados en el Registro de Aplicación del Sistema. Se deberá ajustar la configuración de rotación de dicho registro en función de las necesidades de su organización.

a) %SystemRoot%\System32\Winevt\Logs\Application.evtx




*Propiedades del registro de aplicación*

Uno de los principales beneficios de la tecnología Citrix Virtual Apps and Desktops es la salvaguarda de todas las tareas administrativas realizadas desde la consola Citrix Studio, toda esta información se almacena en una de las bases de datos del Sistema "CitrixLogging" y permite ver en todo momento las acciones llevadas a cabo en el sistema.

Durante el paso a paso de implementación se insta al administrador a realizar una modificación sobre las preferencias de registro, para evitar que se puedan realizar cambios sobre el entorno si la base de datos de inicios de sesión no está disponible. Esto protegerá al sistema de cambios no trazados.

En función de su tipo de licenciamiento, la base de datos "CitrixLogging" guardará los cambios administrativos durante más o menos días, por ejemplo, el tiempo de retención de logs y eventos administrativos para una licencia Premium asciende a un año.

## 7.2 IDENTIDADES Y GRUPOS LOCALES

Como parte de la implementación del rol Citrix Storefront, el asistente realiza la creación de varios grupos locales utilizados para el correcto funcionamiento del servicio.

El propio rol Citrix Storefront se encarga de la gestión de los grupos de seguridad locales y de los miembros que pertenecen a ellos por lo que no debe modificarlos manualmente.

Durante el proceso de instalación, Citrix Storefront añade los siguientes usuarios al grupo de Administradores locales:

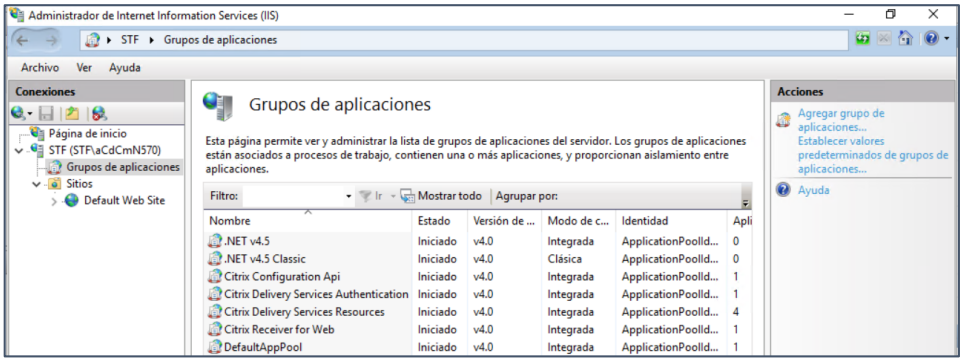
a) Citrix Configuration Replicatión (NT SERVICE\CitrixConfigurationReplication)

b) Citrix Cluster Join (NT SERVICE\CitrixClusterService

Adicionalmente, durante el proceso de instalación y configuración de Citrix Storefront, se realiza la creación de los siguientes grupos locales y grupos de aplicaciones a nivel de Internet Information Services:

| Grupo local | Descripción del grupo | Miembros |
|---|---|---|
| CitrixClusterMembers | La pertenencia de un equipo a este grupo denota la pertenencia al Cluster de Citrix Storefront. | Todos los servidores Storefront de la implementación |
| CitrixCWServiceRead Users | Usuarios autorizados para leer en Citrix Credential Wallet. | IIS APPPOOL\Citrix Delivery Services Authentication<br>IIS APPPOOL\Citrix Delivery Services Resources |
| CitrixCWServiceWrite Users | Usuarios autorizados para escribir en Citrix Credential Wallet. | IIS APPPOOL\Citrix Delivery Services Authentication |
| CitrixDelegated AuthenticatorUsers | Conceder acceso a los servicios de autenticación de dominio. | IIS APPPOOL\Citrix Delivery Services Authentication<br>IIS APPPOOL\Citrix Delivery Services Resources<br>IIS APPPOOL\Citrix Receiver for Web |
| CitrixDelegated DirectoryClaimFactory Users | Conceder acceso a la fábrica de notificaciones de directorio del dominio. | IIS APPPOOL\Citrix Delivery Services Authentication |
| CitrixPNRSUsers | Los miembros tienen acceso concedido a Citrix Peer Resolution Service. | NT SERVICE\CitrixCredentialWallet<br>NT SERVICE\CitrixSubscriptionsStore |
| CitrixSubscription ServerUsers | Los miembros de este grupo pueden acceder a Citrix Delivery Services Workflow Subscription Service. | |
| CitrixSubscriptions StoreServiceUsers | Usuarios autorizados para acceder a Citrix Subscriptions Store. | IIS APPPOOL\Citrix Delivery Services Resources |
| CitrixSubscriptions SyncUsers | La pertenencia al grupo denota permisos para sincronizar. | |

A nivel del sitio web, por defecto, dentro de la consola de administración de Internet Information Services, bajo el nodo de configuración Grupos de Aplicaciones, se pueden apreciar las aplicaciones creadas durante la instalación del producto.




*Grupos de aplicaciones creados durante la instalación*

**Nota:** Los grupos de aplicaciones utilizan, por defecto, el valor ApplicationPoolIdentity para aislarse unos de otros.

Existe la posibilidad de usar cuentas distintas a las generadas durante la instalación del producto, si se opta por esta posibilidad y se utiliza una de las cuentas integradas, que no sea la ApplicationPoolIdentity, se debe tener en cuenta que:

a) La cuenta Servicio de red (Networkservice) tiene derechos de usuario de bajo nivel.

b) La cuenta de usuario Sistema local tiene derechos de usuario de nivel superior que las otras dos cuentas de usuario integradas, Servicio de red o Servicio local.

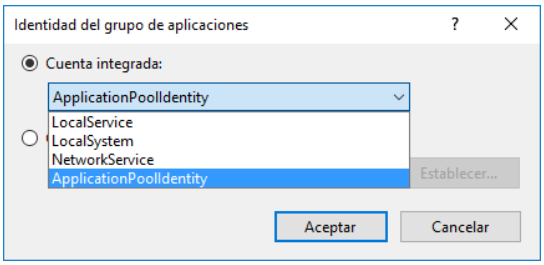
c) La ejecución de un grupo de aplicaciones con una cuenta que tiene derechos de usuario de alto nivel supone un grave riesgo para la seguridad.

**Nota:** Las identidades de grupo de aplicaciones no requieren de gestión alguna y no tienen contraseña, lo que facilita su administración y evita problemas de seguridad por falta de mantenimiento.

El aislamiento logrado al utilizar cuentas individuales para cada una de las aplicaciones ofrece una garantía de independencia, que aumenta cuando se aíslan las carpetas con permisos individualizados, aunque sigue siendo inferior a utilizar ApplicationPoolIdentity.

La seguridad aumenta con el aislamiento entre aplicaciones de sitio, ya que, en caso de vulnerarse la seguridad de una de ellas, no serán accesibles las otras aplicaciones.

Al crearse un sitio web, automáticamente se crea su aplicación de forma aislada y se asigna la cuenta integrada ApplicationPoolIdentity, a no ser que se fuerce el uso de una cuenta existente.




*Cuentas integradas disponibles para el uso del grupo de aplicaciones.*

**Nota:** No modifique los permisos de ninguno de los grupos de aplicaciones creados por Citrix, de lo contrario puede experimentar errores de funcionamiento.

## 7.3 AUTENTICACIÓN

Gran parte de las tareas de mantenimiento e implementación de una infraestructura Citrix Virtual Apps and Desktops se dedican a asegurar los contenidos. No se debe olvidar que servir a través de una red un recurso siempre es aumentar la superficie de exposición, pero hacerlo en una extranet o incluso públicamente en Internet, lleva a extremos la probabilidad de ataque.

Siempre hay que evaluar y ponderar entre seguridad y servicio, de no hacerlo, puede terminar en cualquiera de los extremos:

a) Exposición total sin seguridad a cambio de servicio.

b) Recursos casi inaccesibles al preponderar la seguridad.

En el término medio debe estar la solución al servicio que se desea prestar, con una seguridad adecuada que no impida el trabajo para el que se sirve el recurso.

La presente guía de seguridad define que, como mínimo, se deben habilitar los métodos de autenticación:

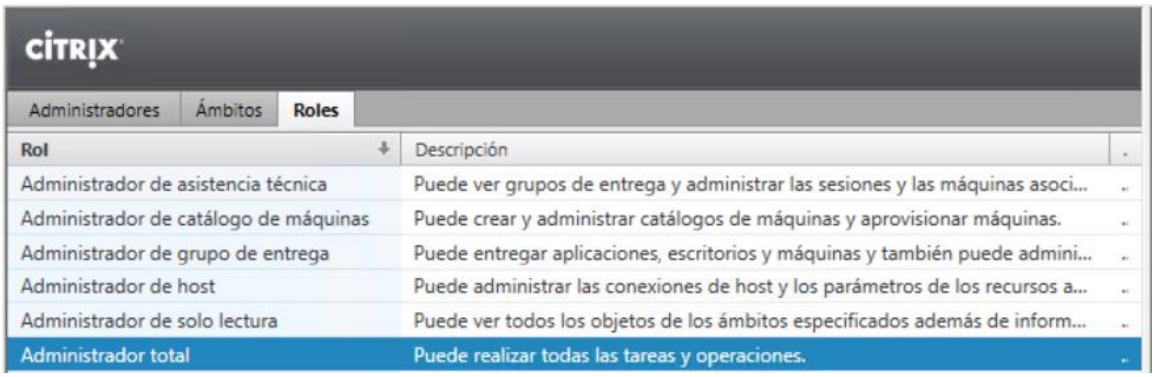
a) Usuario y contraseña.

b) PassThrough de dominio.

Esto permitirá que un usuario de dominio con el inicio de sesión único configurado, podrá disponer de los recursos que le asigne su organización.

## 7.4 AUTORIZACIONES

Una de las líneas base de la presente guía define al grupo de dominio “Administradores de Citrix” con permisos de control total sobre la infraestructura, basándose en los permisos detallados anteriormente. Se recomienda que, en el caso de querer otorgar algún otro permiso sobre acciones administrativas del sistema, lo realice utilizando grupos de seguridad para cada rol utilizado, para ello, dentro de la consola Citrix Studio, se pueden definir autorizaciones de acceso a ciertos nodos de la configuración.




*Puede crear varios grupos de seguridad en función de los roles que desee utilizar.*

## 7.5 RESTRICCIONES

Durante la aplicación de la guía de seguridad CCN-STIC-574 IIS 10, se debe haber realizado el paso que indica que se deben restringir las conexiones al servidor Citrix Storefront desde una subred específica. Para el correcto funcionamiento de la infraestructura.

Dichas restricciones deben corresponderse con:

a) La red de servidores, sobre las que implemente la infraestructura de servidores Citrix Virtual Apps and Desktops.

b) La red de usuarios que vayan a hacer uso de Citrix Virtual Apps and Desktops.

## 7.6 PERMISOS

El nivel de permisos NTFS en ficheros y carpetas aumenta la administración de una forma considerable ya que exige un gran esfuerzo y grandes dotes de organización para evitar problemas de aperturas indiscriminadas o la imposibilidad de servir el recurso por falta de permisos adecuados.

Los permisos NTFS son atributos propios de los elementos que protegen. Este punto de partida ayuda a entender mejor la seguridad de ficheros en Windows. El usuario debe recibir de forma directa o por pertenencia a un grupo el acceso al fichero.

Como para cualquier otro recurso, Microsoft recomienda la utilización del modo de asignación estándar: **Cuentas de usuarios → Grupos del dominio → Grupos locales → Permisos**. Este método evita las reescrituras constantes de permisos que hacen pesadas las tareas de mantenimiento.

Existe la posibilidad de habilitar la suplantación de usuario, que proporciona la capacidad de controlar la identidad bajo la que se ejecuta el código de la aplicación, de esta forma no hay por qué conceder permisos a un usuario de forma específica.

Por ejemplo, si se ha habilitado la suplantación de usuarios en el grupo de aplicaciones y se ejecuta utilizando una cuenta que tiene los permisos de acceso adecuados, el usuario no tendrá la restricción de acceso.

Cuando los accesos son desde fuera del dominio la gestión del acceso por medio de permisos NTFS suele ser difícil y deficiente al no poder distinguir usuarios, por lo que se debería combinar con otros niveles de seguridad o no utilizarlo. Lo mismo se puede decir de la auditoría de objetos.

## 7.7 CERTIFICADOS

Los servidores seguros que utilizan cifrado SSL/TLS permiten el intercambio de información entre ellos y los clientes sin que pueda ser capturado de forma directa y logra que el ataque sea mucho más improbable y complejo que sin usar técnicas criptográficas.

La presente guía de seguridad ofrecerá los pasos necesarios para asegurar, mediante la instalación de certificados, todos y cada uno de los roles de Citrix Virtual Apps and Desktops.

Es de vital importancia asegurar las comunicaciones establecidas desde los equipos cliente hacia los servidores Citrix Storefront y Citrix Director, pero también se deberá asegurar las comunicaciones realizadas entre servidores de la infraestructura.

Los servidores contemplados son:

a) Citrix Delivery Controller

b) Citrix Storefront

c) Citrix Director

d) Citrix Licensing

Los certificados pueden ser emitidos por:

a) El propio servidor IIS (autofirmado).

b) Por una autoridad certificadora (CA) dentro del bosque/dominio.

c) Una CA pública (FNMT, Verisign, Chamberts of Commerce, etc.).

**Nota:** Cada uno de los certificados estará pensado para un ámbito determinado.

### 7.7.1 CERTIFICADOS AUTOFIRMADOS

En esta guía se han utilizado certificados autofirmados para asegurar las comunicaciones con SSL. Su administración es la más sencilla y no requiere ninguna instalación adicional o compra de certificado externo.

De manera general, se recomienda limitar el uso de certificados autofirmados a las siguientes situaciones:

a) Entornos de prueba o completamente cerrados.

b) Acceso desde la LAN propia y con usuarios conocedores del entorno, que pueden confiar en un acceso sin entidad certificadora raíz conocida.

### 7.7.2 AUTORIDAD CERTIFICADORA (CA)

Los certificados gestionados por el dominio requieren instalar una autoridad certificadora (CA) integrada con el Directorio activo.

La gestión es, de las tres opciones, la más compleja y con mayor carga administrativa.

Como ventaja tienen la no limitación de emisión de certificados y la ausencia de coste en la emisión. Se debe utilizar esta opción para proteger comunicaciones en redes propias y con clientes del dominio o bosque propios.

### 7.7.3 AUTORIDADES DE CERTIFICACIÓN PÚBLICA

Los certificados emitidos por autoridades certificadoras de raíz públicas permiten asegurar sitios que están presentes en Internet, y cuyos clientes solo tienen este certificado para comprobar la veracidad del sitio.

La gestión es fácil, solo debe alojarse en el repositorio de certificados y darle uso. En algunos casos es necesario alojar el certificado de la entidad raíz en los navegadores, si bien no es necesario en los principales proveedores de seguridad del mercado, en los que los navegadores de más uso ya los llevan integrados (no es el caso de la FNMT, que sí requiere dicha instalación).

La renovación de certificados cuando aún no han caducado suele ser una tarea fácil ya que se puede utilizar el certificado todavía válido como medio de certificar nuestra identidad y para cifrar las comunicaciones, sin embargo, cuando un certificado ha caducado se debe proceder a su sustitución por uno nuevo.

Como penalización, el uso de este tipo de certificados tiene un coste económico para la empresa que los solicite.