centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 684

PUBLICACIÓN SEGURA DE APLICACIONES Y ESCRITORIOS VIRTUALES CON CITRIX

SEPTIEMBRE 2020

MINISTERIO DE DEFENSA

Edita:

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

© Centro Criptológico Nacional, 2020
NIPO: 083-20-200-X

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

LIMITACIÓN DE RESPONSABILIDAD
El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL
Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

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.

septiembre de 2020

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL 5
2. INTRODUCCIÓN 5
3. OBJETO 6
4. ALCANCE 7
5. DESCRIPCIÓN DE USO DE ESTA GUÍA 8
5.1 AVISOS IMPORTANTES A LOS USUARIOS DE ESTA GUÍA 8
5.2 ESTRUCTURA DE LA GUÍA 10
6. DESCRIPCIÓN DE CITRIX VIRTUAL APPS AND DESKTOPS 10
6.1 VIRTUAL DELIVERY AGENT COMO COMPONENTE DE CITRIX VIRTUAL APPS AND DESKTOPS 11
6.2 SERVICIOS INSTALADOS POR EL ROL CITRIX VIRTUAL DELIVERY AGENT 11
6.3 MEDIOS DE INSTALACIÓN Y ADMINISTRACIÓN 14
6.4 CITRIX WORKSPACE APP Y CITRIX RECEIVER 15
7. SEGURIDAD EN APLICACIONES Y ESCRITORIOS VIRTUALES CON CITRIX 16
7.1 AUDITORIA Y REGISTRO 17
7.2 IDENTIDADES Y GRUPOS LOCALES 18
7.3 AUTENTICACIÓN 19
7.4 AUTORIZACIONES 20
7.5 RESTRICCIONES 20

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 la publicación de aplicaciones y escritorios virtuales mediante Citrix Virtual Apps and Desktops 7.15 CU5 LTSR, sobre clientes MS Windows 10 y servidores miembro MS Windows Server 2016, ambos pertenecientes a un dominio Windows de Directorio Activo.

La presente guía tiene como objeto la implementación del rol Citrix Virtual Delivery Agent. Se establecerán también los procesos y tareas administrativas para hacer una administración segura del mismo.

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 del cliente sobre el que instale la solución, 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 las guías codificadas como “CCN-STIC-570A” y “CCN-STIC-599A”.

Esta guía asume que el rol Citrix Virtual Delivery Agent se va a instalar sobre equipos con los siguientes sistemas operativos:

a) Windows Server 2016 Standard de 64 Bits, donde previamente se ha seguido el proceso de implantación definido en la guía “CCN-STIC-570A”.

b) Windows 10 Enterprise LTSC (versión 1809) de 64 Bits, donde previamente se ha seguido el proceso de implantación definido en la guía “CCN-STIC-599A19”.

4. ALCANCE

La guía ha sido elaborada con el propósito de proporcionar información específica para realizar la implementación del rol del producto sobre Microsoft Windows Server 2016 y Microsoft Windows 10 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 y equipos cliente de un dominio bajo el Sistema Operativo Microsoft Windows 10.

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.

e) Un servidor miembro del dominio basado en Windows Server 2016 con la instalación de Microsoft SQL Server 2016.

f) Un servidor miembro del dominio basado en Windows Server 2016 con el rol Citrix Controller.

g) Un servidor miembro del dominio basado en Windows Server 2016 con el rol Citrix Storefront.

h) Un servidor miembro del dominio basado en Windows Server 2016 con el rol Citrix Licensing.

i) Un servidor miembro del dominio basado en Windows Server 2016 Standard con el rol Citrix Director.

j) Un servidor miembro del dominio basado en Windows Server 2016 con el rol Citrix Virtual Delivery Agent.

k) Un equipo miembro del dominio basado en Windows 10 Enterprise LTSC con el rol Citrix Virtual Delivery Agent.

l) Un equipo miembro del dominio basado en Windows 10 Enterprise LTSC el cual actuará como cliente de conexión a la infraestructura de Citrix.

m) La instalación del rol Citrix Virtual Delivery Agent se realiza en modo limpio, es decir, no se contemplan procedimientos de migración desde versiones anteriores.

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

Este documento incluye:

a) **Características del rol Citrix Virtual Delivery Agent.** Completa descripción del rol necesario para la virtualización de aplicaciones y escritorios.

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

c) **Mecanismos para la aplicación 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).

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

f) **Lista de comprobación.** Ayuda a verificar el grado de cumplimiento de los equipos 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 del rol Citrix Virtual Delivery Agent, será necesario cumplir los requisitos definidos para Windows Server 2016 o Windows 10 dependiendo de su implementación.

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 el producto. Para ello, será necesario aplicar la guía de seguridad codificada como CCN-STIC-570A en todos los servidores y la guía de seguridad codificada como CCN-STIC-599A19 en todos los equipos clientes. 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.

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

5.1 AVISOS IMPORTANTES A LOS USUARIOS DE ESTA GUÍA

El contenido de esta guía es de aplicación tanto para equipos tipo puesto servidor, con Sistema Operativo Windows Server 2016, como para equipos tipo puesto cliente, con Sistema Operativo Windows 10; ambos 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 las siguientes versiones:

a) **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.

b) **Windows 10 Enterprise LTSC (versión 1809)**: con los parámetros por defecto de instalación con la guía "CCN-STIC-599A19" aplicada. La versión es común en características básicas a distintas versiones y ediciones del sistema operativo y, si bien, lo expresado aquí podría valer de forma genérica para todas ellas, se ha centrado y asegurado exclusivamente para esta versión.

Esta guía se ha diseñado para reducir la superficie de exposición de los equipos que cuenten con una implementación del rol Citrix Virtual Delivery Agent contenido 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.

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.

Para garantizar la seguridad de los equipos, 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.

Para poder realizar las configuraciones contempladas en esta guía, deberá tener en funcionamiento la infraestructura necesaria para el producto Citrix Virtual Apps and Desktops 7.15 CU5 LTSR con sus respectivas configuraciones de seguridad contempladas en la guía codificada como "CCN-STIC-683 Implementación de seguridad en Citrix Virtual Apps and Desktops sobre Windows Server 2016".

Del mismo modo, tenga en consideración que los sistemas operativos (y productos desplegados en ellos) correspondientes a los equipos sobre los que se instale el rol Citrix Virtual Delivery Agent deberán poseer un nivel de seguridad adecuado a su propósito teniendo en consideración la normativa aplicable. A modo de ejemplo, si procede a instalar el rol Citrix Virtual Delivery Agent sobre equipo MS Windows 10 para su virtualización, éste deberá poseer la configuración de seguridad de la guía codificada como "CCN-STIC-599A19".

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 del rol Citrix Virtual Delivery Agent del producto Citrix Virtual Apps and Desktops 7.15 CU5 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 y Microsoft Windows 10 en su versión Enterprise con el rol Citrix Virtual Delivery Agent 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 su versión Standard y Microsoft Windows 10 en su versión Enterprise a las necesidades requeridas en los entornos clasificados donde se quiera instalar el rol Citrix Virtual Delivery Agent.

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 VIRTUAL DELIVERY AGENT COMO COMPONENTE DE CITRIX VIRTUAL APPS AND DESKTOPS

El rol Citrix Virtual Delivery Agent, coloquialmente conocido también como "VDA", es el agente necesario de la infraestructura que realiza la comunicación con los Delivery Controller y ofrecer los recursos (aplicaciones o escritorios) a los usuarios finales.

Durante la inicialización de la sesión (después de que un usuario inicia sesión) también verifica si hay una licencia válida de Citrix disponible y aplicará las políticas que se hayan configurado para esa sesión en particular.

En un servidor Windows permite que varios usuarios se conecten a la vez. En un escritorio Windows permite la conexión de un solo usuario.

6.2 SERVICIOS INSTALADOS POR EL ROL CITRIX VIRTUAL DELIVERY AGENT

Durante la instalación del rol Citrix Virtual Delivery Agent se realiza la configuración de varios de los servicios que se encargarán de proporcionar las funcionalidades a la implementación.

A continuación, se detallan los servicios utilizados por el rol Citrix Virtual Delivery Agent, 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
Citrix Audio Redirection Service	Ofrece redirección de sonido entre el dispositivo de punto final y el escritorio virtual.	Automático
Citrix CEIP Service for Vda	Servicio del programa Customer Experience Improvement Program de Citrix para VDA	Deshabilitado
Citrix Desktop Service	Gestiona la comunicación entre Delivery Controller y los escritorios virtuales. Se ocupa de la intermediación inicial (brokering) de las conexiones e interacción con las sesiones.	Automático
Citrix Device Redirector Service	Servicio para administrar dispositivos remotos de Citrix.	Automático
Citrix Diagnostic Facility COM Server	Administra y controla las sesiones de seguimiento de la central de diagnóstico de Citrix en el sistema.	Automático
Citrix Dynamic Virtual Channel Service	Ofrece respaldo para canal virtual dinámico entre el dispositivo de punto final y el escritorio virtual.	Automático
Citrix Encryption Service	Permite una comunicación segura con el cifrado de 128 bits de RC5 entre Citrix Delivery Clients y el servidor Citrix XenApp.	Automático

Nombre	Descripción	Valor de inicio
Citrix End User Experience Monitoring Service	Servicio para recopilar y ordenar mediciones de la experiencia del usuario final.	Automático
Citrix Group Policy Engine	Responsable de aplicar los parámetros configurados por los administradores de Citrix para el equipo y los usuarios mediante el componente de Directiva de grupo.	Automático
Citrix HDX HTML5 Video Redirection Service	Citrix HDX HTML5 Video Redirection Service.	Automático
Citrix ICA Service	Administra la comunicación entre el dispositivo de punto final y el escritorio virtual.	Automático
Citrix Location and Sensor Virtual Channel Service	Permite a una aplicación del lado del servidor aprovechar las capacidades de Ubicación y sensores.	Automático
Citrix Mobile Receiver Virtual Channel Service	Permite a una aplicación del lado del servidor utilizar las capacidades de dispositivo móvil.	Automático
Citrix Multi Touch Redirection Service	Ofrece redirección de multitoque entre el dispositivo de punto final y el escritorio virtual.	Automático
Citrix Print Manager Service	Este servicio da respaldo a la arquitectura de impresión universal avanzada de Citrix.	Automático
Citrix Profile Management	Administra los parámetros de personalización de los usuarios.	Automático
Citrix Pvs for VMs agent	Servicio de actualización de contraseñas de máquina del agente de Pvs para VMs.	Automático
Citrix Services Manager	Citrix Services Manager	Automático
Citrix Smart Card Certificate Propagation Service	Propaga certificados desde tarjetas inteligentes.	Automático
Citrix Smart Card Removal Policy Service	Aplica una directiva de retirada de tarjetas inteligentes al sacar una tarjeta inteligente.	Automático
Citrix Smart Card Service	Ofrece redirección de tarjeta inteligente entre el dispositivo de punto final y el escritorio virtual.	Automático
Citrix Stack Control Service	Servicio de traducción RPC/COM	Automático
Citrix Telemetry Service	Servicio de telemetría de Citrix	Deshabilitado
Citrix UWA Cache Service	Administra una caché privada de aplicaciones de Universal Windows Platform y sus iconos para su uso por parte de Citrix. Broker Agent envía la información de esta caché al Delivery Controller.	Automático
Servicio Citrix HDX MediaStream para Flash	Suministra la función HDX MediaStream para Flash a las aplicaciones publicadas y los escritorios virtuales. HDX MediaStream para Flash permite que Adobe Flash Player se ejecute en el dispositivo cliente en lugar de ejecutarse en la sesión del servidor.	Automático

Adicionalmente, se indican aquellos servicios del sistema que son necesarios para el correcto funcionamiento de la implementación. Si bien, estos servicios son configurados previamente mediante la aplicación de diferentes guías de seguridad, es necesario modificar sus valores durante la aplicación de esta guía.

Estos servicios se detallan, junto con su descripción funcional y el estado de configuración que se aplica en la presente guía.

Nombre	Descripción	Valor de inicio
Aislamiento de claves CNG	Proporciona aislamiento de proceso de claves para las claves privadas y las operaciones criptográficas asociadas según lo requiere el Criterio común. El servicio almacena y usa claves de larga duración en un proceso seguro que cumple los requisitos del Criterio común.	Automático
Asignador de extremos de RPC	Resuelve identificadores de interfaces RPC en extremos de transporte. Si se detiene o deshabilita este servicio, los programas que usen servicios de llamada a procedimiento remoto (RPC) no funcionarán correctamente.	Automático
Cola de Impresión	Este servicio pone en cola los trabajos de impresión y administra la interacción con la impresora. Si lo desactiva no podrá imprimir ni verlas impresoras.	Automático
Estación de trabajo	Crea y mantiene conexiones de red cliente con servidores remotos con el protocolo SMB. Si se detiene este servicio, las conexiones dejarán de estar disponibles. Si se deshabilita, no podrá iniciarse ningún servicio que dependa explícitamente de él.	Automático
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 este servicio se detiene o deshabilita, los programas que usen COM o DCOM no funcionarán correctamente. Por ello, es muy recomendable que ejecute el servicio DCOMLAUNCH.	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. Si este servicio se detiene o deshabilita, los programas que usen COM o DCOM no funcionarán correctamente. Por ello, es muy recomendable que ejecute el servicio RPCSS.	Automático

Nombre	Descripción	Valor de inicio
Servicio Informe de errores de Windows	Permite informar de errores cuando los programas dejan de funcionar o responder y proporcionar las soluciones existentes. También permite generar registros para servicios de diagnóstico y reparación. Si se detiene este servicio, es posible que los informes de errores no funcionen correctamente y que los resultados de los servicios de diagnóstico y las reparaciones no se muestren.	Automático
Servicio Interfaz de almacenamiento en red	Este servicio entrega notificaciones de red (por ejemplo, interfaces agregadas/eliminadas, etc.) a los clientes en modo usuario. Si se detiene este servicio, se perderá la conectividad desde la red. Si se deshabilita este servicio no se iniciará ningún servicio que dependa de él de forma explícita.	Automático
Servicios de Escritorio Remoto	Permite a los usuarios conectarse de forma interactiva a un equipo remoto. Escritorio remoto y el servidor host de sesión de Escritorio remoto dependen de este servicio.	Manual
Solicitante de instantáneas de volumen de Hyper-V	Coordina las comunicaciones que requieren el uso del Servicio de instantáneas de volumen para realizar copias de seguridad de las aplicaciones y los datos de esta máquina virtual desde el sistema operativo del equipo físico.	Manual

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 Windows 10.

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

d) Medios de instalación (.iso) de la versión Citrix Workspace App 1912 LTSR.

e) Medios de instalación (.iso) de la versión Citrix Receiver 14.9.7000

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 Storefront.

6.4 CITRIX WORKSPACE APP Y CITRIX RECEIVER

Citrix Workspace App y Citrix Receiver son dos productos de Citrix que permiten a los dispositivos de los clientes:

a) Acceder a la infraestructura donde están alojados los recursos publicados.

b) Enumerar los diferentes recursos que tiene a su disposición un usuario.

c) Lanzar el recurso (aplicación o escritorio).

Tanto Citrix Receiver como Citrix Workspace App se tratan del mismo producto, siendo este último la evolución del primero. Si bien es cierto que la versión del producto Citrix Virtual Apps and Desktops 7.15 LTSR CU5 incluye el producto Citrix Receiver, esta guía permite la instalación de la nueva versión denominada Citrix Workspace App.

La instalación de la versión queda a criterio de elección de los administradores de la implementación.

La aplicación Citrix Workspace se puede usar en PC, tabletas y clientes ligeros con dominio y sin dominio. Proporciona un uso de alto rendimiento de aplicaciones virtualizadas y así mismo, ofrece acceso a aplicaciones locales de equipos remotos.

Para la aplicación de la presente guía debe contar con los requerimientos mínimos de los productos Citrix Workspace App o Citrix Receiver (en función del elegido para su instalación) que indica el fabricante de forma oficial adicionalmente a los requisitos del sistema operativo.

a) Citrix Workspace App

   i. 1GB de RAM

   ii. 572MB espacio libre en disco

b) Citrix Receiver

   i. 1GB de RAM

   ii. 500MB espacio libre en disco

Nota: Puede consultar el resto de requisitos a través del siguiente enlace: https://docs.citrix.com/en-us/citrix-workspace-app-for-windows/system-requirements.html

7. SEGURIDAD EN APLICACIONES Y ESCRITORIOS VIRTUALES CON CITRIX

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 equipo de la implementación 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 equipos.

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

Nombre	Habilitado	Protocolo	Puerto local
Asistencia remota (TCP de entrada)	Sí	TCP	Cualquiera
Citrix Audio Redirection Service	Sí	UDP	16500-16509
Citrix CGP Server Service	Sí	TCP	2598
Citrix Desktop Service	Sí	TCP	80
Citrix ICA FrameHawk Service	Sí	UDP	3224-3324
Citrix ICA Service	Sí	TCP	1494
Citrix Websocket Service	Sí	TCP	8008
UDP de Citrix CGP	Sí	UDP	2598
UDP de Citrix ICA	Sí	UDP	1494

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.

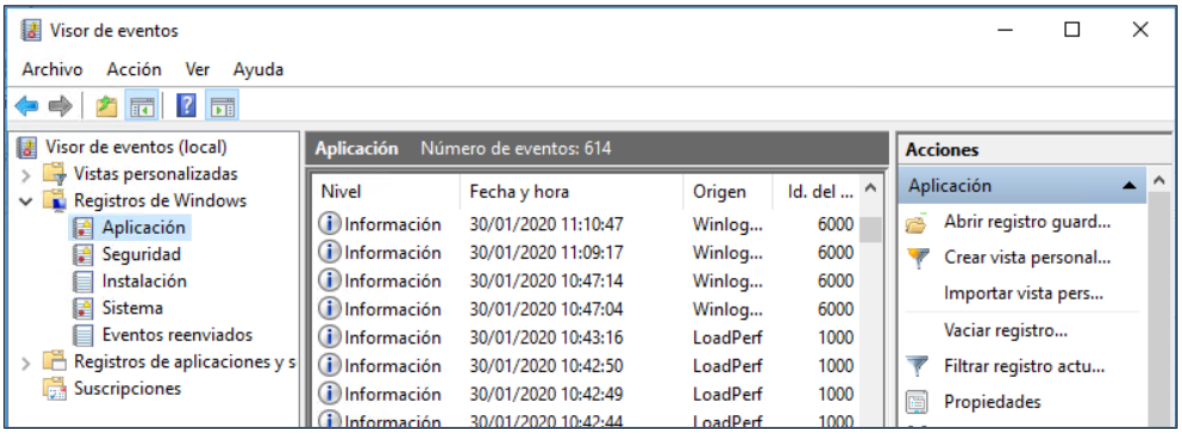
Se entiende que el registro de actividad debe separarse en dos niveles principales:

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.

El mecanismo de registros de servicios y aplicaciones en Windows 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.



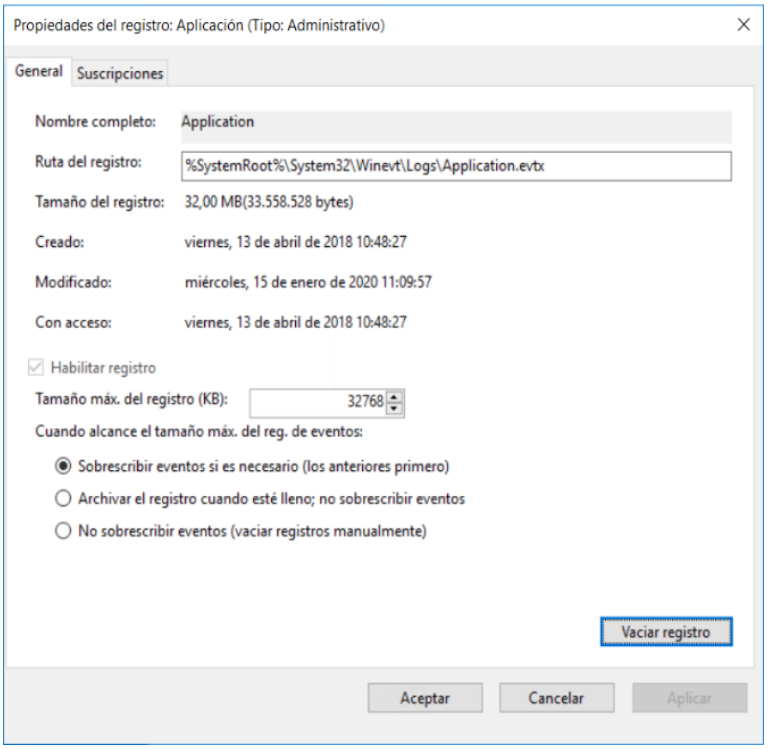
Vista del registro de Windows Aplicación.

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 la aplicación de la guía "CCN-STIC-683 Implementación de seguridad en Citrix Virtual Apps and Desktops sobre Windows Server 2016" 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 Virtual Delivery Agent, el asistente realiza la creación y modificación de varios grupos locales utilizados para el correcto funcionamiento del servicio.

El propio rol Citrix Virtual Delivery Agent 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.

El resultado de las adiciones y modificaciones resultantes se muestra en la siguiente tabla.

Grupo local	Descripción del grupo	Miembros
Usuarios de escritorio remoto	A los miembros de este grupo se les concede el derecho de iniciar sesión remotamente.	DOMINIO\Usuarios del dominio NT AUTHORITY\Usuarios autentificados
Usuarios del monitor del sistema	Los miembros de este grupo tienen acceso a los datos del contador de rendimiento de forma local y remota.	NT SERVICE\BrokerAgent
Usuarios del registro de rendimiento	Los miembros de este grupo pueden programar contadores de registro y rendimiento, habilitar proveedores de seguimiento y recopilar seguimientos de eventos localmente y a través del acceso remoto a este equipo.	NT SERVICE\CitrixTelemetryService
Direct Access Users	A los miembros de este grupo se les concede el derecho de iniciar sesiones remotas directamente, sin un broker para la conexión.	

7.3 AUTENTICACIÓN

Gran parte de las tareas de 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 los usuarios que harán uso de los recursos publicados mediante la infraestructura de Citrix Virtual Apps and Desktops, deberán ser generados específicamente para tal fin. Diferenciando para ello dos tipos de usuarios:

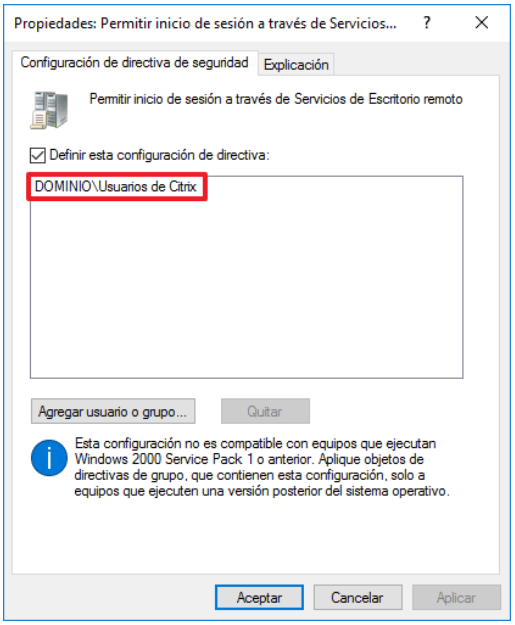
a) Usuarios de cliente final: Usuario de Dominio con acceso a un equipo a través del cual se accederá a la infraestructura de Citrix.

b) Usuarios de Citrix: Usuario con el que se autenticará en la infraestructura de Citrix y el cual tendrá acceso a los recursos publicados.

7.4 AUTORIZACIONES

Una de las líneas base de la presente guía define al grupo de dominio “Usuarios de Citrix” con permisos de uso de la infraestructura de Citrix y el cual englobará a todos los usuarios que harán uso de los servicios de los servicios de Escritorio remoto.

Para ello, mediante directiva de asignación de derechos de acceso se permite el inicio de sesión a través de Servicios de Escritorio remoto al grupo de seguridad “Usuarios de Citrix”.



Directiva de seguridad de inicio de sesión a través de Servicios de Escritorio remoto

7.5 RESTRICCIONES

Durante la aplicación de la guía de seguridad CCN-STIC-684 se insta a los administradores a restringir, mediante grupos de seguridad, el acceso de los usuarios que harán uso de los recursos publicados mediante la infraestructura de Citrix.

Estas restricciones, se aplican a nivel de “grupos de entrega” mediante la consola de Citrix Studio.

Un grupo de entrega es un conjunto de máquinas seleccionadas de uno o varios catálogos de máquinas. El grupo de entrega especifica los usuarios que pueden usar esas máquinas y las aplicaciones y/o escritorios disponibles para esos usuarios.

Las restricciones de acceso a recursos, mediante la consola de Citrix Studio tienen dos niveles de seguridad:

a) Restringir el uso de un grupo de entrega a un grupo de usuarios específico.

b) Restringir la visibilidad de una aplicación dentro de un grupo de entrega a un grupo de usuarios específico.

Para cumplir este doble factor de seguridad se indicará, a lo largo de la guía, a los administradores del entorno la necesidad de crear grupos de usuarios diferenciados para ambos roles pues que un mismo grupo de entrega de aplicaciones puede contener diferentes aplicaciones que entregará a grupos de usuarios diferentes.