

# Securing Windows Server 2016 (Seguridad con Windows Server 2016)

Código: MS-20744

**Propuesta de Valor:** MICROSOFT

**Duración:** 40 Horas



Este curso impartido por un instructor, enseña a los profesionales de TI cómo pueden mejorar la seguridad de la infraestructura de TI que administran. Este curso comienza haciendo hincapié en la importancia de asumir que las infracciones de red ya han ocurrido ya, y luego le enseña cómo proteger las credenciales administrativas y los derechos para garantizar que los administradores pueden realizar sólo las tareas que necesitan, cuando lo necesitan.



## AUDIENCIA

- Este curso es para profesionales de TI que necesitan administrar las redes de Windows Server 2016 de forma segura. Normalmente, estos profesionales trabajan con redes configuradas como entornos basados en dominios de Windows Server, con acceso administrado a Internet y servicios en la nube.



## PRE REQUISITOS

Los estudiantes deben tener por lo menos dos años de experiencia en el campo de TI y deben tener:

- Una sólida y práctica comprensión de los fundamentos de la red, incluyendo TCP / IP, Protocolo de Datagrama de Usuario (UDP) y Sistema de Nombres de Dominio (DNS).
- Una comprensión sólida y práctica de los principios de los Servicios de dominio de Active Directory (AD DS).
- Una sólida y práctica comprensión de los fundamentos de virtualización de Microsoft Hyper-V.
- Comprensión de los principios de seguridad de Windows Server.



## OBJETIVOS

- Asegurar Windows Server.
- Desarrollo seguro de aplicaciones y una infraestructura de carga de trabajo de servidor.

- Administrar líneas de base de seguridad.
- Configurar y administrar la administración justa y justo a tiempo (JIT).
- Administrar la seguridad de los datos.
- Configurar Firewall de Windows y un firewall distribuido definido por software.
- Tráfico de red seguro.
- Proteger su infraestructura de virtualización.
- Administrar malware y amenazas.
- Configurar la auditoría avanzada.
- Administrar actualizaciones de software.
- Administrar las amenazas con ATA (Advanced Threat Analytics) y Microsoft Operations Management Suite (OMS).

---

 **CERTIFICACIÓN DISPONIBLE**

- Certificado Oficial de **MICROSOFT**

---

 **CONTENIDO**

1. DETECCIÓN DE VIOLACIÓN Y USO DE LAS HERRAMIENTAS DE SYS INTERNALS
2. PROTECCIÓN DE CREDENCIALES Y ACCESO PRIVILEGIADO
3. LIMITAR LOS DERECHOS DE ADMINISTRADOR CON JUST ENOUGH ADMINISTRATION
4. GESTIÓN DE ACCESO PRIVILEGIADO Y BOSQUES ADMINISTRATIVOS
5. MITIGACIÓN DE MALWARE Y AMENAZAS
6. ANÁLISIS DE LA ACTIVIDAD MEDIANTE AUDITORIAS AVANZADAS Y ANÁLISIS DE LOG
7. ANALIZAR LA ACTIVIDAD CON LA CARACTERÍSTICA DE MICROSOFT ADVANCED THREAT ANALYTICS Y OPERATIONS MANAGEMENT SUITE
8. ASEGURAR LA VIRTUALIZACIÓN DE UNA INFRAESTRUCTURA
9. ASEGURAR EL DESARROLLO DE APLICACIONES Y LA INFRAESTRUCTURA DE CARGA DE TRABAJO DEL SERVIDOR
10. PROTECCIÓN DE DATOS CON CIFRADO
11. LIMITAR EL ACCESO A ARCHIVOS Y CARPETAS
12. USO DE FIREWALLS PARA CONTROLAR EL FLUJO DE TRÁFICO DE LA RED
13. ASEGURAR EL TRÁFICO DE RED
14. ACTUALIZACIÓN DE WINDOWS SERVER

---

## BENEFICIOS

- Los candidatos están familiarizados con los métodos, tecnologías utilizados para fortalecer los entornos de servidor y proteger las infraestructuras de las máquinas virtuales mediante el uso de máquinas virtuales protegidas, con cifrado y estructura protegida.