# ExecuTrain

Impulsamos tu talento tecnológico

| | | |
|---|---|---|
| MICROSOFT | RED HAT | VIRTUALIZACIÓN |
| CIBERSEGURIDAD | DESARROLLO | OFFICE |
| BIG DATA | BLOCK CHAIN | BASES DE DATOS |
| GESTIÓN DE SERVICIOS IT | CLOUD COMPUTING | METODOLOGÍAS EN PROYECTOS |
| SISTEMAS OPERATIVOS | Y MÁS... | |

www.executrain.com.mx

# ¿Por qué ExecuTrain?

ExecuTrain es un proveedor de entrenamiento corporativo a nivel internacional y líder mundial en la capacitación empresarial. Contamos con más de 30 años de Experiencia y con más de 75 mil personas capacitadas a nivel Nacional.

Te guiamos en la definición de tus requerimientos de capacitación, en las diferentes etapas:

- ✓ Detección de necesidades, evaluación de conocimientos, plan de capacitación y seguimiento posterior para elegir el plan de capacitación como tú lo necesitas.
- ✓ El **más amplio catálogo de cursos**, desde un nivel básico hasta los niveles de conocimientos más especializados.
- ✓ En ExecuTrain el material y la **metodología están diseñados por expertos en aprendizaje humano**. Lo que te garantiza un mejor conocimiento en menor tiempo.
- ✓ Tú puedes confiar y estar seguro del aprendizaje porque nuestro **staff de instructores es de primer nivel**, algunos de los cuales son consultores en reconocidas empresas.
- ✓ No pierdas tu tiempo, los cursos están diseñados para un aprendizaje práctico.

**Nuestro compromiso es que tú aprendas, si no quedas satisfecho con los resultados del programa, podrás volver a tomar los cursos hasta tu entera satisfacción o la devolución de tu dinero.**

# Modalidad de Servicio

### Cursos en Fecha Calendario

Súmate a nuestros grupos en fechas públicas.

### Cursos Privados

On site, en nuestras instalaciones o en línea con instructor en vivo.

### Autoestudio con soporte de instructor

Cursos en modalidad autoestudio, con acceso 24/7 a la plataforma de estudio, con soporte de instructor y foros de ayuda

ExecuTrain
Impulsamos tu talento tecnológico

**Duración: 28 horas**

# AZ-500 / Microsoft Azure Security Technologies

Este curso proporciona a los profesionales de seguridad de TI el conocimiento y las habilidades necesarias para implementar controles de seguridad, mantener la postura de seguridad de una organización e identificar y remediar las vulnerabilidades de seguridad. Este curso incluye seguridad para la identidad y el acceso, protección de la plataforma, datos y aplicaciones, y operaciones de seguridad.

## Perfil del Público

Este curso está dirigido a ingenieros de seguridad de Azure que planean realizar el examen de certificación asociado o que realizan tareas de seguridad en su trabajo diario. Este curso también sería útil para un ingeniero que quiera especializarse en brindar seguridad para plataformas digitales basadas en Azure y desempeñar un papel integral en la protección de los datos de una organización.

**Rol de trabajo: Ingeniero de Seguridad**
**Preparación para el examen: AZ-500**

## Requisitos Previos

Los alumnos que superan la prueba tendrán conocimientos previos y comprensión de:

- ✓ Procedimientos recomendados y requisitos de seguridad del sector, como defensa en profundidad, acceso con privilegios mínimos, control de acceso basado en roles, autenticación multifactor, responsabilidad compartida y modelo de confianza cero.
- ✓ Protocolos de seguridad, como las redes privadas virtuales (VPN), el protocolo de seguridad de Internet (IPSec), la capa de sockets seguros (SSL), y los métodos de cifrado de discos y datos.
- ✓ Tener cierta experiencia en la implementación de cargas de trabajo de Azure En este curso no se cubren los conceptos básicos de la administración de Azure, sino que el contenido se basa en ese conocimiento al agregar información específica de seguridad.
- ✓ Tener experiencia con sistemas Windows y Linux, así como lenguajes de scripting. Los laboratorios del curso pueden usar PowerShell y la CLI..

## Módulos

### Protección de soluciones de Azure con Azure Active Directory

Explore cómo configurar y administrar su instancia de Azure Active Directory de forma segura.

Al final de este módulo, podrá:

- Configuración de Azure AD y Azure AD Domain Services para la seguridad
- Creación de usuarios y grupos que habilitan el uso seguro del inquilino
- Uso de MFA para proteger las identidades del usuario
- Configuración de opciones de seguridad sin contraseña

ExecuTrain
Impulsamos tu talento tecnológico

## Implementación de la identidad híbrida

Explore cómo implementar y configurar Azure AD Connect para crear una solución de identidad híbrida para su empresa.

Al final de este módulo, podrá:

- Implementación de Azure AD Connect
- Selección y configuración de la mejor opción de autenticación para sus necesidades de seguridad
- Configurar la escritura diferida de contraseñas

## Implementación de Azure AD Identity Protection

Proteger las identidades de Azure AD mediante el acceso condicional, MFA, las revisiones de acceso y otras funcionalidades.

Al final de este módulo, podrá:

- Implementar y configurar Identity Protection
- Configurar MFA para usuarios, grupos y aplicaciones
- Crear directivas de acceso condicional para garantizar la seguridad
- Crear y seguir un proceso de revisión de acceso

## Configuración de Azure AD Privileged Identity Management

Asegúrese de que las identidades con privilegios tengan protección adicional y proporcione el mínimo acceso necesario a estas para poder realizar el trabajo.

Al final de este módulo, sabrá hacer lo siguiente:

- Describir la Confianza cero y cómo afecta a la seguridad
- Configurar e implementar roles con Privileged Identity Management (PIM)
- Evaluar la utilidad de cada configuración de PIM en relación con los objetivos de seguridad

## Diseño de una estrategia de gobernanza empresarial

Aprenda a usar RBAC y Azure Policy para limitar el acceso a las soluciones de Azure y determinar qué método es adecuado para sus objetivos de seguridad.

Al final de este módulo, podrá:

- Explicación del modelo de responsabilidad compartida y cómo afecta a la configuración de seguridad
- Creación de directivas de Azure para proteger las soluciones
- Configuración e implementación del acceso a servicios mediante RBAC

## Implementación de la seguridad perimetral

Evite los ataques antes de que lleguen a las soluciones de Azure. Use los conceptos de Defensa en profundidad y Confianza cero para proteger el perímetro de Azure.

Al final de este módulo, podrá:

- Definir la defensa en profundidad
- Proteger el entorno de ataque por denegación de servicio
- Proteger las soluciones con firewalls y VPN
- Explorar la configuración de la seguridad perimetral de un extremo a otro en función de la posición de seguridad

## Configuración de la seguridad de red

Use las funcionalidades de red de Azure para proteger la red y las aplicaciones de ataques externos e internos.

Al final de este módulo, podrá:

- Implementación y configuración de grupos de seguridad de red para proteger las soluciones de Azure
- Configuración y bloqueo de puntos de conexión de servicio y vínculos privados

- Protección de las aplicaciones con Application Gateway, firewall de aplicaciones web y Front Door
- Configuración de ExpressRoute para ayudar a proteger el tráfico de red

## Configuración y administración de la seguridad del host

Aprenda a bloquear los dispositivos, las máquinas virtuales y otros componentes que ejecutan las aplicaciones en Azure.

Al final de este módulo, podrá:

- Configuración e implementación de Endpoint Protection
- Implementación de una estrategia de acceso con privilegios para dispositivos y estaciones de trabajo con privilegios
- Protección de las máquinas virtuales y acceso a ellas
- Implementación de Windows Defender
- Práctica de la seguridad por capas mediante la revisión e implementación de Security Center y pruebas comparativas de seguridad

## Habilitación de la seguridad de contenedores

Explore cómo proteger las aplicaciones que se ejecutan en contenedores y cómo conectarse a ellas de forma segura.

Al final de este módulo, podrá:

- Definir las herramientas de seguridad disponibles para contenedores en Azure
- Configurar la seguridad de contenedores y servicios de Kubernetes
- Bloquear los recursos de red, almacenamiento e identidad conectados a sus contenedores
- Implementar RBAC para controlar el acceso a los contenedores

## Implementación y protección de Azure Key Vault

Proteja sus claves, certificados y secretos en Azure Key Vault. Aprenda a configurar el almacén de claves para la implementación más segura.

Al final de este módulo, podrá:

- Definición de lo que es un almacén de claves y cómo protege certificados y secretos
- Implementar y configurar Azure Key Vault
- Proteger el acceso y la administración del almacén de claves
- Almacenar claves y secretos en el almacén de claves
- Exploración de consideraciones de seguridad clave, como la rotación de claves y la copia de seguridad o recuperación

## Configuración de las características de seguridad de una aplicación

Registre las aplicaciones de la empresa y, a continuación, use las características de seguridad de Azure para configurar y supervisar un acceso seguro a la aplicación.

Al final de este módulo, podrá:

- Registrar una aplicación en Azure mediante el registro de aplicaciones
- Seleccionar y configurar los usuarios de Azure AD que pueden acceder a cada aplicación
- Configurar e implementar certificados de aplicación web

## Implementación de la seguridad de almacenamiento

Asegúrese de que el almacenamiento y la transferencia de los datos, así como el acceso a los mismos, se realiza de forma segura mediante las características de seguridad de archivos y almacenamiento de Azure.

Al final de este módulo, podrá:

- Definición de la soberanía de datos y cómo se logra en Azure
- Configuración del acceso de Azure Storage de forma segura y administrada
- Cifrado de los datos mientras están en reposo y en tránsito
- Aplicación de reglas para la retención de datos

## Configuración y administración de la seguridad de bases de datos SQL

Configure y bloquee la base de datos SQL en Azure para proteger los datos corporativos mientras están almacenados.

Al final de este módulo, podrá:

- Configurar qué usuarios y aplicaciones tienen acceso a las bases de datos SQL.
- Bloquear el acceso a los servidores mediante firewalls.
- Detectar, clasificar y auditar el uso de los datos.
- Cifrar y proteger los datos mientras están almacenados en la base de datos.de bases de datos SQL

## Configuración y administración de Azure Monitor

Use Azure Monitor, Log Analytics y otras herramientas de Azure para supervisar el funcionamiento seguro de las soluciones de Azure.

Al final de este módulo, podrá:

- Configurar y supervisar Azure Sentinel
- Definir las métricas y los registros de los que quiera realizar un seguimiento para las aplicaciones de Azure
- Conectar orígenes de datos a Log Analytics y configurar el servicio
- Crear y supervisar alertas asociadas a la seguridad de las soluciones

## Habilitar y administrar Microsoft Defender para la nube

Use Azure Security Center, Azure Defender y Puntuación de seguridad para realizar un seguimiento de su posición de seguridad en Azure y mejorarlo.

Al final de este módulo, podrá:

- Definir los tipos más comunes de ciberataques
- Configurar Azure Security Center en función de la posición de seguridad
- Revisar la Puntuación de seguridad y elevarla
- Bloquear las soluciones mediante Security Center y Defender
- Habilitar el acceso Just-In-Time y otras características de seguridad

## Configuración y supervisión de Microsoft Sentinel

Use Azure Sentinel para detectar, realizar un seguimiento y responder a las infracciones de seguridad dentro del entorno de Azure.

Al final de este módulo, podrá:

- Explicación de qué es Azure Sentinel y cómo se usa
- Implementación de Azure Sentinel
- Conectar datos a Azure Sentinel, como registros de Azure, Azure AD y otros
- Seguimiento de incidentes mediante libros, cuadernos de estrategias y técnicas de búsqueda