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**

# SC-300 / Microsoft Identity and Access Administrator

El curso Microsoft Identity and Access Administrator explora cómo diseñar, implementar y operar los sistemas de administración de identidades y acceso de una organización mediante Azure AD. Aprenda a administrar tareas, como proporcionar acceso seguro con autenticación y autorización a las aplicaciones empresariales. También aprenderá a proporcionar experiencias sencillas y funcionalidades de administración de autoservicio para todos los usuarios. Por último, aprenda a crear el acceso adaptable y la gobernanza de las soluciones de administración de identidades y acceso, lo que garantiza que puede solucionar problemas, supervisar e informar sobre su entorno. El administrador de identidades y acceso puede ser una sola persona o un miembro de un equipo más grande. Obtenga información sobre cómo este rol colabora con muchos otros roles de la organización para impulsar proyectos de identidad estratégicos. El objetivo final es proporcionar conocimientos para modernizar las soluciones de identidad, implementar soluciones de identidad híbrida e implementar la gobernanza de identidades.

## Perfil del Público

Este curso está pensado para los administradores de identidad y acceso que planean realizar el examen de certificación asociado o que realizan tareas de administración de identidades y acceso en su trabajo diario. Este curso también sería útil para un administrador o ingeniero que quiera especializarse en proporcionar soluciones de identidad y sistemas de administración de acceso para soluciones basadas en Azure; desempeñando un papel integral en la protección de una organización.

**Rol de trabajo: Ingeniero de Seguridad**
**Preparación para el examen: SC-300**

## Requisitos Previos

Antes de asistir a este curso, los estudiantes deben tener conocimientos en:

- ✓ Procedimientos recomendados de seguridad y requisitos de seguridad del sector, como la defensa en profundidad, el acceso con privilegios mínimos, la responsabilidad compartida y el modelo de confianza cero
- ✓ Familiarizarse con conceptos de identidad como autenticación, autorización y Active Directory
- ✓ Tener cierta experiencia en la implementación de cargas de trabajo de Azure Este curso no cubre los conceptos básicos de la administración de Azure, sino que el contenido del curso se basa en ese conocimiento al agregar información específica de seguridad.
- ✓ Cierta experiencia con Windows y sistemas operativos Linux y lenguajes de scripting es útil, pero no es necesario. Los laboratorios del curso pueden usar PowerShell y la CLI.

# Módulos

## Exploración de la identidad y Azure AD

En este módulo se tratarán las definiciones y los servicios disponibles para la identidad proporcionada en Azure AD para Microsoft 365. Comenzará con la autenticación, la autorización y los tokens de acceso y, a continuación, creará en soluciones de identidad completas.

Objetivos de aprendizaje

Al final de este módulo, podrá:

- Definición de términos de identidad comunes y explicación de cómo se usan en Microsoft Cloud
- Exploración de herramientas de administración comunes y las necesidades de una solución de identidad
- Revisión del objetivo de confianza cero y cómo se aplica en la nube de Microsoft
- Exploración de los servicios de identidad disponibles en Microsoft Cloud

## Implementación de la configuración inicial de Azure Active Directory

Aprenda a crear una configuración de Azure Active Directory inicial para asegurarse de que todas las soluciones de identidad disponibles en Azure están listas para su uso. En este módulo se explora cómo crear y configurar un sistema de Azure AD.

Objetivos de aprendizaje

Al final de este módulo, podrá:

- Implementar la configuración inicial de Azure Active Directory
- Crear, configurar y administrar identidades
- Implementar y administrar identidades externas (excepto escenarios B2C)
- Implementar y administrar una identidad híbrida

## Crear, configurar y administrar identidades

El acceso a las cargas de trabajo basadas en la nube debe controlarse de forma centralizada al proporcionar una identidad definitiva para cada usuario y recurso. Puede asegurarse de que los empleados y los proveedores tengan el acceso suficiente para realizar su trabajo.

Objetivos de aprendizaje

Al término de este módulo, podrá:

- Crear, configurar y administrar usuarios.
- Crear, configurar y administrar grupos.
- Administrar licencias
- Explicación de los atributos de seguridad personalizados y el aprovisionamiento automático de usuarios

## Implementación y administración de identidades externas

La posibilidad de invitar a usuarios externos a usar los recursos de Azure de la empresa es una gran ventaja, pero debe hacerlo de manera segura. Explore cómo habilitar la colaboración externa segura.

Objetivos de aprendizaje

Al final de este módulo, podrá:

- Administrar la configuración de colaboración externa en Azure Active Directory.
- Invitar a usuarios externos (de forma individual o masiva).
- Administrar cuentas de usuario externas en Azure Active Directory.
- Configurar proveedores de identidades (sociales y SAML/WS-Fed).

## Implementación y administración de una identidad híbrida

Crear una solución de identidad híbrida para usar su instancia local de Active Directory puede ser todo un desafío. Consulte cómo puede implementar una solución de identidad híbrida segura.

Objetivos de aprendizaje

Al final de este módulo, podrá hacer lo siguiente:

- Planeación, diseño e implementación de Azure Active Directory Connect (AADC)
- Administración de Azure Active Directory Connect (AADC)
- Administración de la sincronización de hash de contraseña (PHS)
- Administración de la autenticación de tránsito (PTA)
- Administración del inicio de sesión único de conexión directa (SSO de conexión directa)
- Administración de la federación excluyendo las implementaciones manuales de ADFS
- Solución de errores de sincronización
- Implementación y administración de Azure Active Directory Connect Health

## Protección de usuarios de Azure Active Directory con Multi-Factor Authentication

Obtenga información sobre cómo usar la autenticación multifactor con Azure AD para proteger las cuentas de usuario.

Objetivos de aprendizaje

En este módulo, aprenderá a:

- Entender Azure AD Multi-Factor Authentication (Azure AD MFA)
- Crear un plan para implementar Azure AD MFA
- Activar Azure AD MFA para usuarios y aplicaciones específicas

## Administrar la autenticación de usuarios

Hay varias opciones para la autenticación en Azure AD. Aprenda a implementar y administrar las autenticaciones correctas para los usuarios en función de las necesidades empresariales

Objetivos de aprendizaje

Al final de este módulo, podrá:

- Administrar métodos de autenticación (FIDO2/sin contraseña)
- Implementar una solución de autenticación basada en Windows Hello para empresas
- Configurar e implementar el autoservicio de restablecimiento de contraseña
- Implementación y administración de la protección de contraseñas
- Implementación y administración de restricciones de inquilino

## Planificación, implementación y administración del acceso condicional

El acceso condicional proporciona una gran granularidad de control sobre qué usuarios pueden realizar actividades concretas, acceder a recursos y garantizar que los datos y los sistemas sean seguros.

Objetivos de aprendizaje

Al final de este módulo, podrá:

- Planear e implementar los valores predeterminados de seguridad.
- Planear directivas de acceso condicional.
- Implementar controles y asignaciones de directivas de acceso condicional (destino, aplicaciones y condiciones).
- Probar las directivas de acceso condicional y solucionar los problemas relacionados.
- Implementar controles de aplicación.
- Implementar la administración de sesiones.

- Configurar umbrales de bloqueo inteligente.

## Administración de Azure AD Identity Protection

La protección de la identidad de un usuario mediante la supervisión de sus patrones de uso e inicio de sesión garantizará una solución de nube segura. Explore cómo diseñar e implementar Azure AD Identity Protection.

Objetivos de aprendizaje

Al final de este módulo, podrá hacer lo siguiente:

- Implementar y administrar directivas de riesgo de usuario
- Implementar y administrar directivas de riesgo de inicio de sesión
- Implementar y administrar una directiva de registro de autenticación multifactor
- Supervisar, investigar y solucionar los problemas con los usuarios de riesgo elevado

## Implementación de la administración del acceso para recursos de Azure

Explore cómo usar roles integrados de Azure, identidades administradas y directivas de RBAC para controlar el acceso a recursos de Azure. La identidad es la clave para proteger las soluciones.

Objetivos de aprendizaje

Al final de este módulo, podrá:

- Configuración y uso de roles de Azure en Azure AD
- Configuración de una identidad administrada y asignación a recursos de Azure
- Análisis de los permisos de rol concedidos o heredados por un usuario
- Configuración del acceso a los datos en Azure Key Vault mediante la directiva de RBAC

## Planeación y diseño de la integración de aplicaciones empresariales para SSO

La implementación de aplicaciones empresariales permite controlar qué usuarios pueden acceder a las aplicaciones, iniciar sesión fácilmente en las aplicaciones con inicio de sesión único y proporcionar informes de uso integrados.

Objetivos de aprendizaje

Al final de este módulo, podrá:

- Descubrir aplicaciones mediante MCAS o el informe de aplicación de ADFS
- Diseñar e implementar la administración de acceso para las aplicaciones
- Diseñar e implementar roles de administración de aplicaciones
- Configurar aplicaciones SaaS integradas previamente (Galería)

## Implementación y supervisión de la integración de aplicaciones empresariales para el inicio de sesión único

La implementación y supervisión de las aplicaciones empresariales en las soluciones de Azure puede garantizar la seguridad. Vea cómo implementar aplicaciones locales y basadas en la nube para los usuarios.

Objetivos de aprendizaje

Al final de este módulo, podrá:

- Implementar personalizaciones de tokens
- Implementación y configuración de las opciones de consentimiento
- Integrar las aplicaciones locales con Azure AD Application Proxy
- Integrar las aplicaciones SaaS personalizadas para el inicio de sesión único
- Implementar el aprovisionamiento de usuarios de aplicaciones
- Supervisar y auditar el acceso a las aplicaciones empresariales de Azure

Active Directory o el inicio de sesión en ellas

## Implementación del registro de aplicaciones

La línea de negocio que se desarrolló internamente debe registrarse en Azure AD y asignarse a los usuarios para obtener una solución segura de Azure. Explore cómo implementar el registro de aplicaciones.

Objetivos de aprendizaje

Al final de este módulo, podrá hacer lo siguiente:

- Planear la estrategia de registro de la aplicación de línea de negocio.
- Implementar registros de aplicaciones.
- Configuración de los permisos de la aplicación
- Planear y configurar permisos de aplicación de varios niveles.

## Planificación e implementación de la administración de derechos

Cuando usuarios nuevos o usuarios externos se unen a su sitio, es necesario asignarles rápidamente acceso a las soluciones de Azure. Explore cómo autorizar a los usuarios para que accedan a su sitio y sus recursos.

Objetivos de aprendizaje

Al final de este módulo, podrá:

- Definir catálogos.
- Revisar paquetes de acceso.
- Planear, implementar y administrar los derechos.
- Implementar y administrar las condiciones de uso.
- Administrar el ciclo de vida de los usuarios externos en la configuración de Azure AD Identity Governance.

## Planeamiento, implementación y administración de la revisión de acceso

Una vez implementada la identidad, es necesario un control adecuado con revisiones de acceso para conseguir una solución segura. Explore cómo planear e implementar revisiones de acceso.

Objetivos de aprendizaje

Al final de este módulo, podrá:

- Planear revisiones de acceso
- Crear revisiones de acceso para grupos y aplicaciones
- Supervisar los resultados de la revisión de acceso
- Administrar licencias para revisiones de acceso
- Automatizar tareas de administración para la revisión de acceso
- Configurar revisiones de acceso periódicas

## Planificación e implementación de acceso con privilegios

Es necesario asegurarse de que los roles administrativos están protegidos y administrados para aumentar la seguridad de la solución de Azure. Explore cómo usar PIM para proteger sus datos y recursos.

Objetivos de aprendizaje

Al final de este módulo, podrá:

- Definir una estrategia de acceso con privilegios para usuarios administrativos (recursos, roles, aprobaciones y umbrales)
- Configuración de Privileged Identity Management para roles de Azure AD
- Configurar Privileged Identity Management para recursos de Azure
- Asignación de roles
- Administrar solicitudes de PIM
- Analizar el historial de auditorías y los informes de PIM

- Crear y administrar cuentas de acceso de emergencia

**Supervisión y mantenimiento de Azure Active Directory**

Los registros de auditoría y diagnóstico de Azure AD proporcionan una vista completa de cómo los usuarios obtienen acceso a la solución de Azure. Obtenga información sobre cómo supervisar, solucionar problemas y analizar los datos de inicio de sesión.

Objetivos de aprendizaje

Al término de este módulo, sabrá hacer lo siguiente:

- Análisis e investigación de los registros de inicio de sesión para solucionar problemas de acceso
- Revisar y supervisar los registros de auditoría de Azure AD
- Habilitar e integrar los registros de diagnóstico de Azure AD con Log Analytics o Azure Sentinel
- Exportación del inicio de sesión y de registros de auditoría a un SIEM (administración de eventos e información de seguridad) de terceros
- Revisión de la actividad de Azure AD mediante Log Analytics o Azure Sentinel, excepto el uso de KQL (Lenguaje de consulta Kusto)
- Analizar libros o informes de Azure Active Directory
- Configuración de notificaciones