
TEMARIO DEL CURSO

Administrador Asociado de Identidad y Acceso Certificado por Microsoft (SC-300)

20 horas | Nivel Básico

Curso oficial orientado a administradores de identidad y acceso que necesitan diseñar, implementar y operar soluciones de identidad modernas con Microsoft Entra ID, alineadas con los principios de Confianza cero.

OBJETIVOS DEL CURSO

- Diseñar e implementar una solución completa de identidad y acceso con Microsoft Entra ID.
 - Administrar identidades de usuario, dispositivos, aplicaciones e identidades externas a lo largo de su ciclo de vida.
 - Configurar autenticación segura, autenticación multifactor y acceso condicional basado en riesgo.
 - Proteger el acceso a aplicaciones y cargas de trabajo mediante identidades administradas y control de permisos.
 - Planificar y aplicar la gobernanza de identidades, incluyendo revisiones de acceso y acceso con privilegios.
 - Supervisar y auditar la actividad de identidad para mejorar continuamente la seguridad y el cumplimiento.
-

A QUIÉN VA DIRIGIDO

- Administradores de Identidad y Acceso.
 - Administradores de Azure y Microsoft 365.
 - Ingenieros de Seguridad y responsables de control de acceso.
 - Arquitectos de identidad y profesionales de infraestructura cloud.
 - Técnicos y administradores que vayan a presentarse al examen de certificación SC-300 o que gestionen identidades en entornos híbridos y cloud.
-

EL CURSO INCLUYE

- Manuales digitales
- Diploma de asistencia
- Tramitación de FUNDAE incluida

TEMARIO

MÓDULO 01.

Explorar la Identidad en Azure AD (opcional)

- Este es un módulo opcional de nivel básico que cubre los conceptos fundamentales de identidad y gestión de acceso con Azure Active Directory (Microsoft Entra ID). Se estudian los principios de Confianza cero, autenticación, autorización, tokens y otros conceptos clave relacionados con la identidad moderna en entornos cloud e híbridos.
- Lecciones
- ¿Qué es la identidad en Azure?

MÓDULO 02.

Implementar una solución de gestión de identidad

- Aprende a crear y gestionar tu implementación de Azure Active Directory (Microsoft Entra ID) y a configurar los usuarios, grupos e identidades externas necesarios para operar la solución. También se aborda la implementación y administración de una solución de identidad híbrida con Active Directory local.
- Lecciones
- Configurar y gestionar Azure Active Directory.
- Crear, configurar y gestionar identidades.
- Implementar y gestionar identidades externas.
- Implementar y gestionar identidades híbridas.

MÓDULO 03.

Implementar una solución de autenticación y gestión de acceso

- Implementa y administra la gestión de acceso utilizando Azure AD (Microsoft Entra ID). Se utilizan autenticación multifactor, Acceso Condicional y protección de identidad para asegurar el acceso a usuarios, dispositivos y aplicaciones.
- Lecciones
- Planificar e implementar autenticación multifactor (MFA).
- Administrar la autenticación de usuarios y métodos modernos de autenticación.
- Planificar, implementar y administrar el acceso condicional.
- Administrar la protección de identidad.
- Implementar la administración de sesiones y la evaluación continua de acceso.

MÓDULO 04.

Implementar la gestión de acceso para aplicaciones

- Explora cómo las aplicaciones pueden integrarse en la solución de identidad y acceso mediante aplicaciones empresariales y registros de aplicaciones en Azure AD (Microsoft Entra ID). Se registran, integran y gestionan aplicaciones SaaS y locales.
- Lecciones
- Planificar y diseñar la integración de aplicaciones empresariales para SSO.
- Implementar y supervisar la integración de aplicaciones empresariales y configurarlas para SSO.
- Implementar el registro de aplicaciones.

MÓDULO 05.

Planificar e implementar una estrategia de gobernanza de identidad

- Diseña e implementa la gobernanza de identidades para la solución de identidad utilizando control de acceso, revisiones de acceso, acceso con privilegios y supervisión continua del Directorio Activo de Azure (Microsoft Entra ID).
- Lecciones
- Planificar e implementar la gestión de control de acceso.
- Planificar, implementar y gestionar revisiones de acceso.
- Planificar e implementar acceso privilegiado con Privileged Identity Management (PIM).
- Supervisar y mantener el Directorio Activo de Azure.