# AZ-500 - Microsoft Azure Security Technologies

Nel corso AZ-500 – Microsoft Azure Security Technologies gli allievi apprendono conoscenze e competenze necessarie ad implementare e mantenere la sicurezza di una infrastruttura Azure. Imparano inoltre ad identificare e neutralizzare le vulnerabilità mediante i tool dedicati alla sicurezza. Il corso tratta anche aspetti relativi allo scripting e alla automazione, alla virtualizzazione e alla architettura cloud N-tier.

Durata corso 4 giorni

**Lingua**: Lingua utilizzata nel corso/dal docente: Italiano. Il materiale didattico e l'ambiente di laboratorio sono in lingua Inglese

**Destinatari**: Professionisti It

## Prerequisiti

Per partecipare con profitto al corso è necessario avere conseguito la certificazione Microsoft Azure Administrator Associate oppure possedere competenze equivalenti.

## Moduli

### Module 1: Manage Identity and Access

Azure Active Directory
Azure Identity Protection
Enterprise Governance
Azure AD Privileged Identity Management
Hybrid Identity
Lab: Role-Based Access Control
Lab: Azure Policy
Lab: Resource Manager Locks
Lab: MFA, Conditional Access and AAD Identity Protection
Lab: Azure AD Privileged Identity Management
Lab: Implement Directory Synchronization

### Module 2: Implement Platform Protection

Perimeter Security
Network Security
Host Security
Container Security
Lab: Network Security Groups and Application Security Groups
Lab: Azure Firewall
Lab: Configuring and Securing ACR and AKS

### Module 3: Secure Data and Applications

Azure Key Vault
Application Security
Storage Security
SQL Database Security
Lab: Key Vault (Implementing Secure Data by setting up Always Encrypted)
Lab: Securing Azure SQL Database
Lab: Service Endpoints and Securing Storage

## Module 4: Manage Security Operations

Azure Monitor
Azure Security Center
Azure Sentinel

## Al termine del corso AZ-500 – Microsoft Azure Security Technologies gli allievi saranno in grado di implementare:

- strategie di governance aziendale tra cui il controllo dell'accesso basato sui ruoli, le policy Azure e i blocchi delle risorse;
- un'infrastruttura Azure AD, compresi utenti, gruppi e autenticazione a più fattori;
- Azure AD Identity Protection, comprese le politiche di rischio, l'accesso condizionato e le revisioni degli accessi;
- strategie di sicurezza perimetrale, compreso Azure Firewall;
- Azure AD Privileged Identity Management, compresi i ruoli Azure AD e le risorse Azure;
- Azure AD Connect, compresi i metodi di autenticazione e la sincronizzazione delle directory on-premises;
- le strategie di sicurezza della rete, compresi Network Security Groups e Application Security Groups;
- le strategie di sicurezza dell'host tra cui la protezione degli endpoint, la gestione dell'accesso remoto, la gestione degli aggiornamenti e la crittografia del disco;
- le strategie di sicurezza dei container, tra cui Azure Container Instances, Azure Container Registry e Azure Kubernetes;
- Azure Key Vault compresi certificati, chiavi e segreti;
- le strategie di sicurezza delle applicazioni, tra cui la registrazione delle app, le identità gestite e gli endpoint dei servizi;
- Azure Monitor, comprese le fonti collegate, l'analisi dei log e gli avvisi;
- le strategie di sicurezza dello storage, comprese le firme di accesso condivise, le politiche di conservazione dei blob e l'autenticazione di Azure Files;
- le strategie di sicurezza del database, tra cui autenticazione, classificazione dei dati, mascheramento dinamico dei dati e sempre criptato;
- Azure Security Center, comprese le politiche, le raccomandazioni e l'accesso alle macchine virtuali just in time;
- Azure Sentinel, comprese cartelle di lavoro, incidenti e playbook.