Curso: Academia Administrador Microsoft 365

Duração: 148h
Área formativa: Cursos

Sobre o curso

A **Academia Administrador Microsoft 365** prepara profissionais com as competências para lidar com aspetos inerentes à administração, gestão e segurança de sistemas de informação tanto on-premises como em Cloud, nomeadamente Microsoft 365.

O programa desta Academia aposta na preparação teórico-prática de profissionais especializados em Sistemas Microsoft, simultaneamente, na certificação técnica de competências, que possibilitam alcançar 2 certificações.

Porque quero frequentar esta Academia ?

:: 2 Certificações Microsoft reconhecidas internacionalmente.

:: A Academia Administrador Microsoft 365 conta com os melhores profissionais certificados do mercado como formadores.

:: Formação qualificada, através da Rumos. Uma das empresas lideres na área da formação.

:: 2nd Shot Gratuito Têm direito a uma segunda oportunidade de exame de forma gratuita os formandos que, após terem efectuado o exame, tenham reprovado com nota inferior a 10% em relação à nota mínima exigida e que façam os exames nas datas propostas no calendário da Academia.

:: Acesso ao **Employability Hub**, um serviço dedicado a apoiar a integração e a progressão de carreira dos formandos das Academias da FLAG. Oferecemos um acompanhamento personalizado, focado na maximização do teu posicionamento no mercado de trabalho. Descobre mais sobre o Employability Hub aqui.

Que certificações vou obter?

:: Microsoft 365 Certified: Enterprise Administrator Expert

:: Microsoft 365 Certified: Teams Administrator Associate

Que profissões me esperam?

:: Administrador de Sistemas;

:: Gestor de Sistemas TI;

:: Administrador de Redes;

:: Consultor Microsoft 365.

> Ao concluíres com aproveitamento esta formação, receberás um badge digital para partilhares com a tua rede profissional online.
>
> Sabe mais sobre os badges digitais aqui.

Objectivos

A **Academia Administrador Microsoft 365** tem como objectivos:

:: Oferecer uma formação teórico-prática avançada, sólida, especializada e atualizada, que prepare os formandos para uma carreira de sucesso na área de Administração do Microsoft 365;

:: Dotar os formandos com o know-how e a qualificação necessários para exercer com sucesso uma atividade de Administração, Suporte a utilizadores e Segurança em Microsoft 365, assim como nas ferramentas que nelas estão integradas nomeadamente o Microsoft Teams e o Microsoft 365 Copilot

:: Potenciar a produtividade, o reconhecimento profissional e a empregabilidade dos formandos, através das mais elevadas Certificações Microsoft, reconhecidas internacionalmente.

Metodologia

Constituído por módulos de formação, integrados numa ótica de sessões mistas de teoria e prática. Serão elaborados exercícios e simulações de situações práticas garantindo uma aprendizagem mais eficaz. Os conteúdos ministrados durante a academia foram desenvolvidos pela Rumos, em consulta a organizações parceiras, e são devidamente acompanhados por material didático, distribuídos aos participantes.

Composição

:: 148 Horas de Formação

:: 5 Ações de Formação TI

:: 3 Cursos em B-learning

:: 2 Ações de Preparação para Exame

:: 2 Exames de Certificação

Pré-requisitos

A **Academia Administrador Microsoft 365** tem como pré-requisitos:

:: Conhecimentos de Inglês técnico: é aconselhável que o formando seja capaz de compreender manuais técnicos na língua inglesa;

:: O formando deverá conhecimentos de informática na ótica do utilizador ao nível dos transmitidos na Academia Técnico de Informática, nomeadamente em Networking, Sistemas Operativos e Servidores;

:: Não apresenta quaisquer pré-requisitos a nível de habilitações académicas ou experiência profissional.

Destinatários

A **Academia Administrador Microsoft 365** destina-se a:

:: Técnicos e Administradores de Sistemas que pretendam especializar-se em Microsoft 365;

:: Interessados em ter conhecimentos integrados de administração e apoio aos utilizadores em 365;

:: Técnicos de Helpdesk e Administradores de Sistemas que ambicionem alcançar uma Certificação Internacional.

Programa

Microsoft Azure Fundamentals (E-Learning)

- Cloud Concepts
- Core Azure Services
- Security, Privacy, Compliance, and Trust
- Azure Pricing and Support
- Sessão Q&A Azure Fundamentals

Sessão Q&A: Microsoft Azure Fundamentals (3h)

Microsoft 365 Fundamentals (E-Learning)

- Microsoft 365 core services
- Microsoft on-premise services and cloud services in Microsoft 365
- Unified endpoint management in Microsoft 365
- Teamwork in Microsoft 365
- Security, Compliance and Collaboration

Sessão Q&A: Microsoft 365 Fundamentals (3h)

MS-102: Microsoft 365 Administrator Essentials (35h)

- Configure your Microsoft 365 experience
- Manage users, licenses, and mail contacts in Microsoft 365
- Manage groups in Microsoft 365
- Add a custom domain in Microsoft 365
- Configure client connectivity to Microsoft 365
- Configure administrative roles in Microsoft 365
- Manage tenant health and services in Microsoft 365
- Deploy Microsoft 365 Apps for enterprise
- Analyze your Microsoft 365 workplace data using Microsoft Viva Insights
- Explore identity synchronization
- Prepare for identity synchronization to Microsoft 365
- Implement directory synchronization tools
- Manage synchronized identities
- Manage secure user access in Microsoft 365
- Examine threat vectors and data breaches
- Explore the Zero Trust security model
- Explore security solutions in Microsoft Defender XDR
- Examine Microsoft Secure Score
- Examine Privileged Identity Management
- Examine Microsoft Entra ID Protection
- Examine email protection in Microsoft 365
- Enhance your email protection using Microsoft Defender for Office 365
- Manage Safe Attachments
- Manage Safe Links
- Explore threat intelligence in Microsoft Defender XDR
- Implement app protection by using Microsoft Defender for Cloud Apps
- Implement endpoint protection by using Microsoft Defender for Endpoint
- Implement threat protection by using Microsoft Defender for Office 365
- Examine data governance solutions in Microsoft Purview
- Explore archiving and records management in Microsoft 365
- Explore retention in Microsoft 365
- Explore Microsoft Purview Message Encryption
- Explore compliance in Microsoft 365
- Implement Microsoft Purview Insider Risk Management
- Implement Microsoft Purview Information Barriers
- Explore Microsoft Purview Data Loss Prevention
- Implement Microsoft Purview Data Loss Prevention
- Implement data classification of sensitive information

- Explore sensitivity labels
- Implement sensitivity labels

APE – Ação de preparação para exame MS-102 (3h)

- Preparação para exames
- Esclarecimento de dúvidas

MS-700: Managing Microsoft Teams (28h)

- Explore Microsoft Teams
- Plan and deploy Microsoft Teams
- Implement lifecycle management and governance for Microsoft Teams
- Monitor your Microsoft Teams environment
- Manage access for external users
- Implement security for Microsoft Teams
- Implement compliance for Microsoft Teams
- Plan and configure network settings for Microsoft Teams
- Create and manage teams
- Manage collaboration experiences for chat and channels
- Manage apps for Microsoft Teams
- Introduction to Teams meetings and calling
- Manage meetings and events experiences
- Plan for Microsoft Teams Rooms and Surface Hub
- Configure, deploy, and manage Teams devices
- Plan for Teams Phone
- Configure and deploy Teams Phone
- Configure and manage voice users
- Configure auto attendants and call queues
- Troubleshoot audio, video, and client issues

APE – Ação de preparação para exame MS-700 (3h)

- Preparação para exames
- Esclarecimento de dúvidas

Microsoft 365 Copilot for Administrators (7h)

- Get started
- Design and prerequisites
- Administrative roles and Tenant health
- Threat protection
- Protecting sensitive data

MD-102: Microsoft 365 Endpoint Administrator (35h)

- Explore the Enterprise Desktop
- Explore Windows Editions
- Understand Microsoft Entra ID
- Manage Microsoft Entra identities
- Manage device authentication
- Enroll devices using Microsoft Configuration Manager
- Enroll devices using Microsoft Intune
- Execute device profiles
- Oversee device profiles
- Maintain user profiles
- Execute mobile application management
- Deploy and update applications
- Administer endpoint applications
- Protect identities in Microsoft Entra ID
- Enable organizational access
- Implement device compliance
- Generate inventory and compliance reports
- Deploy device data protection
- Manage Microsoft Defender for Endpoint
- Manage Microsoft Defender in Windows client
- Manage Microsoft Defender for Cloud Apps
- Assess deployment readiness
- Deploy using the Microsoft Deployment Toolkit
- Deploy using Microsoft Configuration Manager
- Deploy Devices using Windows Autopilot
- Implement dynamic deployment methods
- Plan a transition to modern endpoint management
- Manage Windows 365
- Manage Azure Virtual Desktop

Microsoft Security, Compliance, and Identity Fundamentals (E-Learning)

- Describe security and compliance concepts
- Describe identity concepts
- Describe the function and identity types of Microsoft Entra ID
- Describe the authentication capabilities of Microsoft Entra ID
- Describe access management capabilities of Microsoft Entra ID
- Describe the identity protection and governance capabilities of Azure AD
- Describe core infrastructure security services in Azure
- Describe the security management capabilities in Azure
- Describe security capabilities of Microsoft Sentinel
- Describe threat protection with Microsoft Defender XDR
- Describe Microsoft’s Service Trust portal and privacy capabilities
- Describe the compliance management capabilities in Microsoft Purview
- Describe information protection, data lifecycle management, and data governance capabilities in Microsoft Purview
- Describe the insider risk capabilities in Microsoft Purview
- Describe the eDiscovery and Audit capabilities in Microsoft Purview

Sessão Q&A: Microsoft Security, Compliance, and Identity Fundamentals (3h)

SC-200: Microsoft Security Operations Analyst (28h)

- Introduction to Microsoft 365 threat protection
- Mitigate incidents using Microsoft 365 Defender
- Protect your identities with Microsoft Entra ID Protection
- Remediate risks with Microsoft Defender for Office 365
- Safeguard your environment with Microsoft Defender for Identity
- Secure your cloud apps and services with Microsoft Defender for Cloud Apps
- Respond to data loss prevention alerts using Microsoft 365
- Manage insider risk in Microsoft Purview
- Investigate threats by using audit features in Microsoft Defender XDR and Microsoft Purview Standard
- Investigate threats using audit in Microsoft Defender XDR and Microsoft Purview (Premium)
- Investigate threats with Content search in Microsoft Purview
- Protect against threats with Microsoft Defender for Endpoint
- Deploy the Microsoft Defender for Endpoint environment
- Implement Windows security enhancements with Microsoft Defender for Endpoint
- Perform device investigations in Microsoft Defender for Endpoint
- Perform actions on a device using Microsoft Defender for Endpoint
- Perform evidence and entities investigations using Microsoft Defender for Endpoint
- Configure and manage automation using Microsoft Defender for Endpoint
- Configure for alerts and detections in Microsoft Defender for Endpoint
- Utilize Vulnerability Management in Microsoft Defender for Endpoint
- Plan for cloud workload protections using Microsoft Defender for Cloud
- Connect Azure assets to Microsoft Defender for Cloud
- Connect non-Azure resources to Microsoft Defender for Cloud
- Manage your cloud security posture management
- Explain cloud workload protections in Microsoft Defender for Cloud
- Remediate security alerts using Microsoft Defender for Cloud
- Construct KQL statements for Microsoft Sentinel
- Analyze query results using KQL
- Build multi-table statements using KQL
- Work with data in Microsoft Sentinel using Kusto Query Language
- Introduction to Microsoft Sentinel
- Create and manage Microsoft Sentinel workspaces
- Query logs in Microsoft Sentinel
- Use watchlists in Microsoft Sentinel
- Utilize threat intelligence in Microsoft Sentinel
- Connect data to Microsoft Sentinel using data connectors
- Connect Microsoft services to Microsoft Sentinel
- Connect Microsoft Defender XDR to Microsoft Sentinel
- Connect Windows hosts to Microsoft Sentinel
- Connect Common Event Format logs to Microsoft Sentinel
- Connect syslog data sources to Microsoft Sentinel
- Connect threat indicators to Microsoft Sentinel
- Threat detection with Microsoft Sentinel analytics

- Automation in Microsoft Sentinel
- Security incident management in Microsoft Sentinel
- Identify threats with Behavioral Analytics
- Data normalization in Microsoft Sentinel
- Query, visualize, and monitor data in Microsoft Sentinel
- Manage content in Microsoft Sentinel
- Explain threat hunting concepts in Microsoft Sentinel
- Threat hunting with Microsoft Sentinel
- Use Search jobs in Microsoft Sentinel
- Hunt for threats using notebooks in Microsoft Sentinel