

MS-101: Microsoft 365 Mobility and Security

- **Formato do curso:** Presencial e Live Training
- **Localidade:** Lisboa
- **Data:** 18 Abr. 2022 a 22 Abr. 2022
- **Preço:** 1810€
- **Horário:** Laboral - das 9h00 às 17h00
- **Duração:** 35 horas

This course covers three central elements of Microsoft 365 enterprise administration – Microsoft 365 security management, Microsoft 365 compliance management, and Microsoft 365 device management.

In **Microsoft 365 security management**, you will examine all the common types of threat vectors and data breaches facing organizations today, and you will learn how Microsoft 365's security solutions address these security threats. You will be introduced to the Microsoft Secure Score, as well as to Azure Active Directory Identity Protection. You will then learn how to manage the Microsoft 365 security services, including Exchange Online Protection, Advanced Threat Protection, Safe Attachments, and Safe Links.

Finally, you will be introduced to the various reports that monitor your security health. You will then transition from security services to threat intelligence; specifically, using the Security Dashboard and Advanced Threat Analytics to stay ahead of potential security breaches. With your Microsoft 365 security components now firmly in place, you will examine the key components of Microsoft 365 compliance management. This begins with an overview of all key aspects of data governance, including data archiving and retention, Information Rights Management, Secure Multipurpose Internet Mail Extension (S/MIME), Office 365 message encryption, and data loss prevention (DLP). You will then delve deeper into archiving and retention, paying particular attention to in-place records management in SharePoint, archiving and retention in Exchange, and Retention policies in the Security and Compliance Center. Now that you understand the key aspects of data governance, you will examine how to implement them, including the building of ethical walls in Exchange Online, creating DLP policies from built-in templates, creating custom DLP policies, creating DLP policies to protect documents, and creating policy tips. You will then focus on managing data governance in Microsoft 365, including managing retention in email, troubleshooting retention policies and policy tips that fail, as well as troubleshooting sensitive data.

You will then learn how to implement Azure Information Protection and Windows Information Protection. You will conclude this section by learning how to manage search and investigation, including searching for content in the Security and Compliance Center, auditing log investigations, and managing advanced eDiscovery.

The course concludes with an in-depth examination of Microsoft 365 device management. You will begin by planning for various aspects of device management, including preparing your Windows 10 devices for co-management. You will learn how to transition from Configuration Manager to Intune, and you will be introduced

to the Microsoft Store for Business and Mobile Application Management. At this point, you will transition from planning to implementing device management; specifically, your Windows 10 deployment strategy. This includes learning how to implement Windows Autopilot, Windows Analytics, and Mobile Device Management (MDM). When examining MDM, you will learn how to deploy it, how to enroll devices to MDM, and how to manage device compliance.

O valor do curso não inclui o valor do exame.

Destinatários

This course is designed for persons who are aspiring to the Microsoft 365 Enterprise Admin role and have completed one of the Microsoft 365 role-based administrator certification paths.

Pré-requisitos

Before attending this course, students must have:

- Completed a role-based administrator course such as Messaging, Teamwork, Security and Compliance, or Collaboration.
- A proficient understanding of DNS and basic functional experience with Microsoft 365 services.
- A proficient understanding of general IT practices.

Objetivos

- Examine the threat vectors and data breaches organizations face today in their cybersecurity landscape, and the wide range of security solutions that Microsoft 365 provides to combat those threats
- Manage the Microsoft 365 security services
- Manage the Microsoft 365 threat intelligence features that provide organizations
- Introduce you to the data governance features of Microsoft 365
- Calculate your compliance readiness, implement compliance solutions, and create information barriers, DLP policies, and policy tips
- Implement retention in email, sensitivity labels, and Windows Information Protection, and how to troubleshoot data loss prevention issues
- Manage content search and investigations in Microsoft 365
- Prepare for device management in Microsoft 365
- Examine the Microsoft 365 features an organization must plan for to implement its Windows devices deployment strategy, including Windows Autopilot, its Windows device subscription activation strategy,

and Desktop Analytics

- Implement Mobile Device Management (MDM) in Microsoft 365
-

Programa

Explore security metrics in Microsoft 365 Defender

- Examine threat vectors and data breaches
- Explore the Zero Trust security model
- Explore security solutions in Microsoft 365 Defender
- Examine Microsoft Secure Score
- Examine Privileged Identity Management
- Examine Azure Identity Protection

Manage your security services in Microsoft 365 Defender

- Examine Exchange Online Protection
- Examine Microsoft Defender for Office 365
- Manage Safe Attachments
- Manage Safe Links

Implement threat protection by using Microsoft 365 Defender

- Explore threat intelligence in Microsoft 365 Defender
- 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

Explore data governance and compliance in Microsoft 365

- Examine governance and compliance solutions in Microsoft Purview
- Explore archiving and records management in Microsoft 365
- Explore retention in Microsoft 365
- Explore Microsoft Purview Message Encryption

Implement compliance in Microsoft 365

- Explore compliance in Microsoft 365
- Implement Microsoft Purview Insider Risk Management
- Create information barriers in Microsoft 365
- Explore Data Loss Prevention in Microsoft 365
- Implement Data Loss Prevention policies

Manage compliance in Microsoft 365

- Implement data classification of sensitive information
- Explore sensitivity labels

- Implement sensitivity labels

Manage content search and investigations in Microsoft 365

- Search for content in the Microsoft Purview compliance portal
- Manage Microsoft Purview Audit (Standard)
- Manage Microsoft Purview Audit (Premium)
- Manage Microsoft Purview eDiscovery (Standard)
- Manage Microsoft Purview eDiscovery (Premium)

Prepare for device management in Microsoft 365

- Explore device management using Microsoft Endpoint Manager
- Prepare your Windows devices for Co-management
- Plan for mobile application management in Microsoft Intune

Plan your deployment strategy for Windows devices

- Examine Windows client deployment scenarios
- Explore Windows Autopilot deployment models
- Plan your Windows client Subscription Activation strategy

Implement Mobile Device Management in Microsoft 365

- Explore Mobile Device Management
- Deploy Mobile Device Management
- Enroll devices to Mobile Device Management

- Manage device compliance
- Implement endpoint security in Microsoft Intune

Ao concluir com aproveitamento esta formação, cumprindo a percentagem mínima de 70% de assiduidade e após avaliação ao curso, o formando poderá receber o seu Certificado Microsoft de conclusão e o badge digital para partilhar com a sua rede profissional online.