

MS-500: Microsoft 365 Security Administrator

- **Formato do curso:** Presencial e Live Training
- **Preço:** 1510€
- **Duração:** 28 horas

In this course you will learn how to secure user access to your organization's resources.

The course covers user password protection, multi-factor authentication, how to enable Azure Identity Protection, how to setup and use Azure AD Connect, and introduces you to conditional access in Microsoft 365. You will learn about threat protection technologies that help protect your Microsoft 365 environment. Specifically, you will learn about threat vectors and Microsoft's security solutions to mitigate threats. You will learn about Secure Score, Exchange Online protection, Azure Advanced Threat Protection, Windows Defender Advanced Threat Protection, and threat management. In the course you will learn about information protection technologies that help secure your Microsoft 365 environment. The course discusses information rights managed content, message encryption, as well as labels, policies and rules that support data loss prevention and information protection. Lastly, you will learn about archiving and retention in Microsoft 365 as well as data governance and how to conduct content searches and investigations. This course covers data retention policies and tags, in-place records management for SharePoint, email retention, and how to conduct content searches that support eDiscovery investigations.

Destinatários

This course is for the Microsoft 365 security administrator role:

- The Microsoft 365 Security administrator collaborates with the Microsoft 365 Enterprise Administrator, business stakeholders and other workload administrators to plan and implement security strategies and to ensure that the solutions comply with the policies and regulations of the organization.
- This role proactively secures Microsoft 365 enterprise environments. Responsibilities include responding to threats, implementing, managing and monitoring security and compliance solutions for the Microsoft 365 environment. They respond to incidents, investigations and enforcement of data governance. The Microsoft 365 Security administrator is familiar with Microsoft 365 workloads and hybrid environments.
- This role has strong skills and experience with identity protection, information protection, threat protection, security management and data governance.

Pré-requisitos

Learners should start this course already having the following skills:

- Basic conceptual understanding of Microsoft Azure.
 - Experience with Windows 10 devices.
 - Experience with Office 365.
 - Basic understanding of authorization and authentication.
 - Basic understanding of computer networks.
 - Working knowledge of managing mobile devices.
-

Objetivos

- Prepare for skills evaluated on the MS-500 Microsoft 365 Security Administrator certification exam
 - Plan, implement, and manage threat protection technologies in Microsoft 365
 - Plan, implement, and manage information protection technologies in Microsoft 365
 - Plan, implement, and manage government and compliance features in Microsoft 365
-

Programa

Implement and manage identity and access

- Create, configure, and manage identities
- Explore identity synchronization
- Implement and manage hybrid identity
- Implement and manage external identities
- Manage secure user access in Microsoft 365
- Manage user authentication
- Plan, implement, and administer Conditional Access
- Plan and implement privileged access
- Plan and implement entitlement management
- Manage Azure AD Identity Protection

Implement and manage threat protection

- Protect against threats with Microsoft Defender for Endpoint
- Deploy the Microsoft Defender for Endpoint environment
- Protect against malicious attacks and unauthorized access with Microsoft Edge
- Understand Microsoft 365 encryption
- Understand app management using Microsoft Endpoint Manager
- Manage device compliance
- Remediate risks with Microsoft Defender for Office 365
- Query, visualize, and monitor data in Microsoft Sentinel

Implement and manage information protection

- Create and manage sensitive information types
- Apply and manage sensitivity labels
- Prevent data loss in Microsoft Purview
- Manage data loss prevention policies and reports in Microsoft 365
- Manage the data lifecycle in Microsoft Purview
- Manage data retention in Microsoft 365 workloads
- Manage records in Microsoft Purview

Manage Governance and Compliance Features in Microsoft 365

- Manage compliance in Microsoft 365 and Exchange Online
- Manage Microsoft Purview eDiscovery (Premium)
- Manage regulatory and privacy requirements with Microsoft Priva
- Prepare Microsoft Purview Communication Compliance
- Manage insider risk in Microsoft Purview
- Plan information barriers
- Implement privileged access management
- Manage Customer Lockbox

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.