

MS-102T00

Microsoft 365 Administrator Essentials

40 horas

Microsoft 365

Microsoft

INTRODUÇÃO

This course covers the following key elements of Microsoft 365 administration: Microsoft 365 tenant management, Microsoft 365 identity synchronization, and Microsoft 365 security and compliance.

In Microsoft 365 tenant management, you learn how to configure your Microsoft 365 tenant, including your organizational profile, tenant subscription options, component services, user accounts and licenses, security groups, and administrative roles. You then transition to configuring Microsoft 365, with a primary focus on configuring Office client connectivity. Finally, you explore how to manage user-driven client installations of Microsoft 365 Apps for enterprise deployments.

The course then transitions to an in-depth examination of Microsoft 365 identity synchronization, with a focus on Azure Active Directory Connect and Connect Cloud Sync. You learn how to plan for and implement each of these directory synchronization options, how to manage synchronized identities, and how to implement password management in Microsoft 365 using multifactor authentication and self-service password management.

In Microsoft 365 security management, you begin examining the common types of threat vectors and data breaches facing organizations today. You then learn how Microsoft 365's security solutions address each of these threats. You are introduced to the Microsoft Secure Score, as well as to Azure Active Directory Identity Protection. You then learn how to manage the Microsoft 365 security services, including Exchange Online Protection, Safe Attachments, and Safe Links. Finally, you are introduced to the various reports that monitor an organization's security health. You then transition from security services to threat intelligence; specifically, using Microsoft 365 Defender, Microsoft Defender for Cloud Apps, and Microsoft Defender for Endpoint.

Once you have this understanding of Microsoft 365's security suite, you then 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, Microsoft Purview message encryption, and data loss prevention (DLP). You then delve deeper into archiving and retention, paying particular attention to Microsoft Purview insider risk management, information barriers, and DLP policies. You then examine how to implement these compliance features by using data classification and sensitivity labels.

OBJETIVO DO CURSO

-

PÚBLICO-ALVO

Audience profile

This course is designed for persons aspiring to the Microsoft 365 Administrator role and have completed at least one of the Microsoft 365 role-based administrator certification paths.

PRÉ-REQUISITOS

Prerequisites

Before attending this course, students must have:

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

OUTLINE COURSE

Module 1: MS-102 Configure your Microsoft 365 tenant

This learning path provides instruction on how to configure your Microsoft 365 tenant, including your organizational profile, tenant subscriptions, user accounts and licenses, groups, custom domains, and client connectivity.

Module 2: MS-102 Manage your Microsoft 365 tenant

This learning path provides instruction on how to manage your Microsoft 365 tenant, including administrative roles, tenant health and services, Microsoft 365 Apps for enterprise, and workplace analytics using Microsoft Viva Insights.

Module 3: MS-102 Implement identity synchronization

This learning path examines how to plan for and implement identity synchronization in a hybrid Microsoft 365 deployment, including how to implement Azure AD Connect and how to manage synchronized identities.

Module 4: MS-102 Explore security metrics in Microsoft 365 Defender

This learning path examines 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.

Module 5: MS-102 Manage your security services in Microsoft 365 Defender

This learning path examines how to manage the Microsoft 365 security services, with a special focus on security reporting and managing the Safe Attachments and Safe Links features in Microsoft Defender for Office 365.

Module 6: MS-102 Implement threat protection by using Microsoft 365 Defender

This learning path examines how to manage the Microsoft 365 threat intelligence features that provide organizations with insight and protection against the internal and external cyber-attacks that threaten their tenants.

Module 7: MS-102 Explore data governance in Microsoft 365

This learning path introduces you to the data governance features of Microsoft 365, which serve regulatory compliance, can facilitate eDiscovery, and are part of a business strategy to protect the integrity of the data estate.

Module 8: MS-102 Implement compliance in Microsoft 365

This learning path provides instruction on implementing the Microsoft 365 data governance features, including how to calculate your compliance readiness, implement compliance solutions, and create information barriers, DLP policies, and policy tips.

Module 9: MS-102 Manage compliance in Microsoft 365

This learning path provides instruction on managing the Microsoft 365 data governance features, including how to implement retention in email, sensitivity labels, and Windows Information Protection, and how to troubleshoot data loss prevention issues.