MS-500A: Microsoft 365 Security Administration

32 HORAS

MS-500T01-A: Managing Microsoft 365 Identity and Access

INTRODUCTION

Help protect against credential compromise with identity and access management. In this course you will learn how to secure user access to your organization's resources. Specifically, this course covers user password protection, multi-factor authentication, how to enable Azure Identity Protection, how to configure Active Directory federation services, how to setup and use Azure AD Connect, and introduces you to Conditional Access. You will also learn about solutions for managing external access to your Microsoft 365 system.

AUDIENCE

This course is for the Microsoft 365 security administrator role. This role collaborates with the Microsoft 365 Enterprise Administrator, business stakeholders and other workload administrators to plan and implement security strategies and ensures 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 has strong skills and experience with identity protection, information protection, threat protection, security management and data governance. This role focuses on the Microsoft 365 environment and includes hybrid environments.

AT COURSE COMPLETION

After completing this course, students will be able to:

- Administer user and group security in Microsoft 365.
- Manage passwords in Microsoft 365.
- Describe Azure Identity Protection features.
- Plan and implement Azure AD Connect.
- Manage synchronized identities.
- Plan implement federated identities.
- Describe and use conditional access.

PREREQUISITES

Before attending this course, students must have:

- 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.

COURSE OUTLINE

Module 1: User and Group Security

- User Accounts in Microsoft 365
- Administrator Roles and Security Groups in Microsoft 365
- Password Management in Microsoft 365
- Azure AD Identity Protection

Module 2: Identity Synchronization

- Introduction to Identity Synchronization
- Planning for Azure AD Connect
- Implementing Azure AD Connect
- Managing Synchronized Identities

Module 3: Federated Identities

- Introduction to Federated Identities
- Planning an AD FS Deployment
- Implementing AD FS

Module 4: Access Management

- Conditional Access
- Managing Device Access
- Role Based Access Control (RBAC)
- Solutions for External Access

MS-500T02-A: Implementing Microsoft 365 Threat Protection

INTRODUCTION

Threat protection helps stop damaging attacks with integrated and automated security. In this course 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 for them. You will learn about Secure Score, Exchange Online protection, Azure Advanced Threat Protection, Windows Defender Advanced Threat Protection, and how to use Microsoft 365 Threat Intelligence. It also discusses securing mobile devices and applications. The goal of this course is to help you configure your Microsoft 365 deployment to achieve your desired security posture.

Teatinos 550, Santiago Centro – Mesa Central +56 22 6576300
www.sondatraining.com - contacto@sondatraining.com

MS-500A: Microsoft 365 Security Administration

AT COURSE COMPLETION

After completing this course, students will be able to:

- Describe cyber-attack threat vectors.
- Describe security solutions for Microsoft 365
- Use Microsoft Secure Score to evaluate your security posture.
- Use the Security Dashboard in the Microsoft Security & Compliance center.
- Configure various advanced threat protection services for Microsoft 365.
- Configure Advanced Threat Analytics.
- Plan and deploy Mobile Device Management.

COURSE OUTLINE

Module 1: Security in Microsoft 365

- Threat Vectors and Data Breaches
- Security Solutions for Microsoft 365
- Microsoft Secure Score

Module 2: Advanced Threat Protection

- Exchange Online Protection
- Office 365 Advanced Threat Protection
- Managing Safe Attachments
- Managing Safe Links
- Azure Advanced Threat Protection
- Windows Defender Advanced Threat Protection

Module 3: Threat Intelligence

- Microsoft 365 Threat Intelligence
- Using the Security Dashboard
- Configuring Advanced Threat Analytics

Module 4: Mobility

- Plan for Mobile Application Management
- Plan for Mobile Device Management
- Deploy Mobile Device Management
- Enroll Devices to Mobile Device Management

MS-500T03-A: Implementing Microsoft 365 Information Protection

INTRODUCTION

Information protection is the concept of locating and classifying data anywhere it lives. In this course you will learn about information protection technologies that help secure your Microsoft 365 environment. Specifically, this course discusses information rights managed content, message encryption, as well as labels, policies and rules that support data loss prevention and information protection. Lastly, the course explains the deployment of Microsoft Cloud App Security.

AT COURSE COMPLETION

After completing this course, students will be able to:

- Implement information rights management.
- Secure messages in Office 365.
- Configure Data Loss Prevention policies.
- Deploy and manage Cloud App Security.
- Implement Azure information protection for Microsoft 365.
- Implement Windows information protection for devices.

COURSE OUTLINE

Module 1: Information Protection

- Information Rights Management
- Secure Multipurpose Internet Mail Extension
- Office 365 Message Encryption
- Azure Information Protection
- Advanced Information Protection
- Windows Information Protection

Module 2: Data Loss Prevention

- Data Loss Prevention Explained
- Data Loss Prevention Policies
- Custom DLP Policies
- Creating a DLP Policy to Protect Documents
- Policy Tips

Module 3: Cloud Application Security

- Cloud Application Security Explained
- Using Cloud Application Security Information
- Office 365 Cloud App Security

MS-500T04-A: Administering Microsoft 365 Built-in Compliance

INTRODUCTION

Internal policies and external requirements for data retention and investigation may be necessary for your organization. In this course you will learn about archiving and retention in Microsoft 365 as well as data governance and how to conduct content searches and investigations. Specifically, 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. The course also helps your organization prepare for Global Data Protection Regulation (GDPR).

Teatinos 550, Santiago Centro – Mesa Central +56 22 6576300
www.sondatraining.com - contacto@sondatraining.com

AT COURSE COMPLETION

After completing this course, students will be able to:

- Plan and deploy a data archiving and retention system.
- Perform assessments in Compliance Manager.
- Manage email retention through Exchange.
- Conduct an audit log investigation.
- Create and manage an eDiscovery investigation.
- Manage GDPR data subject requests.

COURSE OUTLINE

Module 1: Archiving and Retention

- Archiving in Microsoft 365
- Retention in Microsoft 365
- Retention Policies in the Security and Compliance Center
- Archiving and Retention in Exchange
- In-place Records Management in SharePoint

Module 2: Data Governance in Microsoft 365

- Planning Security and Compliance Needs
- Building Ethical Walls in Exchange Online
- Manage Retention in Email
- Troubleshooting Data Governance
- Analytics and Telemetry

Module 3: Managing Search and Investigations

- Searching for Content in the Security and Compliance Center
- Audit Log Investigations
- Advanced eDiscovery