Rumos valorizamos profissionais!

SC-400: Microsoft Information Protection Administrator

- **Formato do curso:** Presencial e Live Training
- **Localidade:** Lisboa
- **Data:** 08 Mai. 2023 a 10 Mai. 2023
- **Preço:** 1510€
- **Horário:** Laboral - 09h00 - 17h00
- **Duração:** 28 horas

Learn how to protect information in your Microsoft 365 deployment.

This course focuses on data lifecycle management and information protection and compliance within your organization. The course covers implementation of data loss prevention policies, sensitive information types, sensitivity labels, data retention policies, Microsoft Purview Message Encryption, audit, eDiscovery, and insider risk among other related topics.

The course helps learners prepare for the Microsoft Information Protection Administrator exam (SC-400).

Destinatários

The information protection administrator translates an organization's risk and compliance requirements into technical implementation. They are responsible for implementing and managing solutions for content classification, data loss prevention (DLP), information protection, data lifecycle management, records management, privacy, risk, and compliance. They also work with other roles that are responsible for governance, data, and security to evaluate and develop policies to address an organization's risk reduction and compliance goals. This role assists workload administrators, business application owners, human resources departments, and legal stakeholders to implement technology solutions that support the necessary policies and controls.

Pré-requisitos

Before attending this course, students should have:

- Foundational knowledge of Microsoft security and compliance technologies.
- Basic knowledge of information protection concepts.
- Understanding of cloud computing concepts.
- Understanding of Microsoft 365 products and services.

Objectivos

- Learn how to protect your sensitive information
- Learn how to implement data loss prevention techniques to secure your Microsoft 365 data
- Learn how to plan and implement data lifecycle and records management strategies for an organization

Programa

Introduction to information protection and data lifecycle management in Microsoft Purview

- Introduction to information protection and data lifecycle management
- Know your data
- Protect your data
- Prevent data loss
- Govern your data

Classify data for protection and governance

- Data classification overview
- Classify data using sensitive information types
- Classify data using trainable classifiers
- Review sensitive information and label usage
- Explore labeled and sensitive content
- Understand activities related to your data

Create and manage sensitive information types

- Compare built-in versus custom sensitive information types
- Create and manage custom sensitive information types
- Describe custom sensitive information types with exact data match
- Implement document fingerprinting
- Create keyword dictionary

Understand Microsoft 365 encryption

- Introduction to Microsoft 365 encryption
- Learn how Microsoft 365 data is encrypted at rest
- Understand service encryption in Microsoft Purview
- Explore customer key management using Customer Key
- Learn how data is encrypted in-transit

Deploy Microsoft Purview Message Encryption

- Implement Microsoft Purview Message Encryption
- Implement Microsoft Purview Advanced Message Encryption

- Use Microsoft Purview Message Encryption templates in mail flow rules

Protect information in Microsoft Purview

- Information protection overview
- Configure sensitivity labels
- Configure sensitivity label policies
- Configure auto-labeling policies
- Manage, monitor, and remediate information protection

Apply and manage sensitivity labels

- Apply sensitivity labels to Microsoft Teams, Microsoft 365 groups, and SharePoint sites
- Plan on-premises labeling
- Configure on-premises labeling for the Unified Labeling Scanner
- Apply protections and restrictions to email and files
- Monitor label performance using label analytics

Prevent data loss in Microsoft Purview

- Data loss prevention overview
- Identify content to protect
- Define policy settings for your DLP policy
- Test and create your DLP policy
- Prepare Endpoint DLP
- Manage DLP alerts in the Microsoft Purview compliance portal
- View data loss prevention reports
- Implement the Microsoft Purview Extension

Configure DLP policies for Microsoft Defender for Cloud Apps and Power Platform

- Configure data loss prevention policies for Power Platform
- Integrate data loss prevention in Microsoft Defender for Cloud Apps
- Configure policies in Microsoft Defender for Cloud Apps
- Manage data loss prevention violations in Microsoft Defender for Cloud Apps

Manage data loss prevention policies and reports in Microsoft 365

- Configure data loss prevention for policy precedence
- Implement data loss prevention policies in test mode
- Explain data loss prevention reporting capabilities
- Review and analyze data loss prevention reports
- Manage permissions for data loss prevention reports
- Manage and respond to data loss prevention policy violations

Manage the data lifecycle in Microsoft Purview

- Data Lifecycle Management overview

- Configure retention policies
- Configure retention labels
- Configure manual retention label policies
- Configure auto-apply retention label policies
- Import data for Data Lifecycle Management
- Manage, monitor, and remediate Data Lifecycle Management

Manage data retention in Microsoft 365 workloads

- Explain retention in Exchange Online
- Explain retention in SharePoint Online and OneDrive
- Explain retention in Microsoft Teams 6 min Explain retention in Microsoft Yammer
- Recover content in Microsoft 365 workloads
- Activate archive mailboxes in Microsoft Exchange
- Apply mailbox holds in Microsoft Exchange
- Recover content in Microsoft Exchange

Manage records in Microsoft Purview

- Records management overview
- Import a file plan
- Configure retention labels
- Configure event driven retention
- Manage, monitor, and remediate records

Explore compliance in Microsoft 365

- Plan for security and compliance in Microsoft 365
- Plan your beginning compliance tasks in Microsoft Purview
- Manage your compliance requirements with Compliance Manager
- Examine the Compliance Manager dashboard
- Analyze the Microsoft Compliance score

Search for content in the Microsoft Purview compliance portal

- Explore Microsoft Purview eDiscovery solutions
- Create a content search
- View the search results and statistics
- Export the search results and search report
- Configure search permissions filtering
- Search for and delete email messages

Manage Microsoft Purview eDiscovery (Standard)

- Explore Microsoft Purview eDiscovery solutions
- Implement Microsoft Purview eDiscovery (Standard)
- Create eDiscovery holds
- Search for content in a case

- Export content from a case
- Close, reopen, and delete a case

Manage Microsoft Purview eDiscovery (Premium)

- Explore Microsoft Purview eDiscovery (Premium)
- Implement Microsoft Purview eDiscovery (Premium)
- Create and manage an eDiscovery (Premium) case
- Manage custodians and non-custodial data sources
- Analyze case content

Manage Microsoft Purview Audit (Standard)

- Explore Microsoft Purview Audit solutions
- Implement Microsoft Purview Audit (Standard)
- Search the audit log
- Export, configure, and view audit log records
- Use audit log searching to investigate common support issues

Prepare Microsoft Purview Communication Compliance

- Introduction to communication compliance
- Plan for communication compliance
- Identify and resolve communication compliance workflow
- Introduction to communication compliance policies
- Knowledge check
- Case study–Configure an offensive language policy
- Investigate and remediate communication compliance alerts

Manage insider risk in Microsoft Purview

- Insider risk management overview
- Introduction to managing insider risk policies
- Create and manage insider risk policies
- Knowledge check
- Investigate insider risk alerts
- Take action on insider risk alerts through cases
- Manage insider risk management forensic evidence
- Create insider risk management notice templates

Implement Microsoft Purview Information Barriers

- Explore Microsoft Purview Information Barriers
- Configure information barriers in Microsoft Purview
- Examine information barriers in Microsoft Teams
- Examine information barriers in OneDrive
- Examine information barriers in SharePoint

Manage regulatory and privacy requirements with Microsoft Priva

- Create and manage risk management policies
- Investigate and remediate risk management alerts
- Create rights requests
- Manage data estimate and retrieval for rights requests
- Review data from rights requests
- Get reports from rights requests

Implement privileged access management

- Introduction to privileged access management
- Case study–Implementing privileged access management

Manage Customer Lockbox

- Introduction to Customer Lockbox
- Manage Customer Lockbox requests

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.