

Microsoft 365
CERTIFIED

FUNDAMENTALS



TREINAMENTO OFICIAL MICROSOFT

CERTIFICAÇÃO MS-900

EP 4/5





 Subscribe

Aula 4 – MS-900

Descrever os princípios de conformidade e segurança da Microsoft

- Descrever os modelos de Confiança Zero e de responsabilidade compartilhada
- Descrever os conceitos de criptografia e hash

Gerenciamento de identidades e acessos

- Ter um bom entendimento de como os Princípios de Confiança Zero da Microsoft
- Gerenciar identidades e acessos no Microsoft 365 com o Azure Active Directory (Azure AD)
- Reduzir o risco de violações de segurança utilizando o Windows Hello e Autenticação Multifator (MFA)

Proteção contra ameaças

- Descobrir sua postura de segurança com o Centro de Segurança da Microsoft e o Secure Score.
- Descobrir o valor que o Gráfico de Segurança Inteligente da Microsoft e o Azure Sentinel oferecem na proteção das organizações.

Segurança na nuvem

- Explorar a estrutura do Cloud App Security.
- Descobrir os recursos do Microsoft Cloud Application Security (MCAS).
- Explorar como o Microsoft Cloud App Security se integra aos recursos de proteção contra ameaças e segurança da Microsoft.

Proteção de informações e governança

- Descobrir e identificar as informações em seu ambiente
- Entender como é possível proteger os dados de sua empresa.
- Entender como é possível administrar os dados de sua empresa.

Descrever os recursos de gerenciamento de segurança do Microsoft 365

- Descrever e explorar o Microsoft 365 Defender.
- Descrever como usar o Microsoft Secure Score.

Gerenciar riscos, descobrir e auditar

- Explorar os recursos do Microsoft 365 para gerenciamento de riscos internos.
- Descrever as ferramentas disponíveis para ajudar as organizações a encontrar dados relevantes de forma rápida e econômica.





Subscribe

Módulo 01

Descrever conceitos e metodologias de segurança e conformidade





Descrever a metodologia de confiança zero

Princípios de orientação da Confiança zero

- Verificação explícita
- Acesso com privilégio mínimo
- Pressuposição de violação

Seis pilares fundamentais

- Identidades
- Dispositivos
- Aplicativos
- Dados
- Infraestrutura
- Redes



Descrever o modelo de responsabilidade compartilhada

Responsabilidade	SaaS	PaaS	IaaS	No local
	Microsoft	Microsoft	Microsoft	Cliente
Informações e dados				
Dispositivos (Móveis e PCs)				
Contas e identidades				
Infraestrutura de identidade e diretório				
Aplicativos				
Controles de rede				
Sistema operacional				
Hosts físicos				
Rede física				
Datacenter físico				

RESPONSABILIDADE SEMPRE RETIDA PELO CLIENTE

A RESPONSABILIDADE VARIA CONFORME O TIPO DE SERVIÇO

TRANSFERÊNCIAS DE RESPONSABILIDADE PARA PROVEDORES DE NUVEM


 Microsoft 365
CERTIFIED
FUNDAMENTALS

Cliente

Descrever a defesa em profundidade

A defesa em profundidade usa uma abordagem de segurança em camadas, em vez de depender de um único perímetro.

Entre os exemplos de camadas de segurança estão:

- Segurança física
- Controles de segurança de identidade e acesso
- Perimeter security
- Segurança de rede
- Segurança da camada de computação
- Segurança da camada de aplicativo
- Segurança da camada de dados



Descrever ameaças comuns

101010
010101
101010

Violão de dados

Uma violação de dados é quando os dados são roubados, e isso inclui dados pessoais.



Ataque de dicionário

Um ataque de dicionário é um tipo de ataque de identidade em que um hacker tenta roubar uma identidade experimentando um grande número de senhas conhecidas.



Ransomware

Malware é o termo usado para descrever aplicativos mal-intencionados e códigos que podem causar danos e interromper o uso normal de dispositivos.



Ataques de interrupção

Um ataque de DDoS (negação de serviço distribuído) tenta esgotar os recursos de um aplicativo, fazendo com que o aplicativo fique indisponível para usuários legítimos.

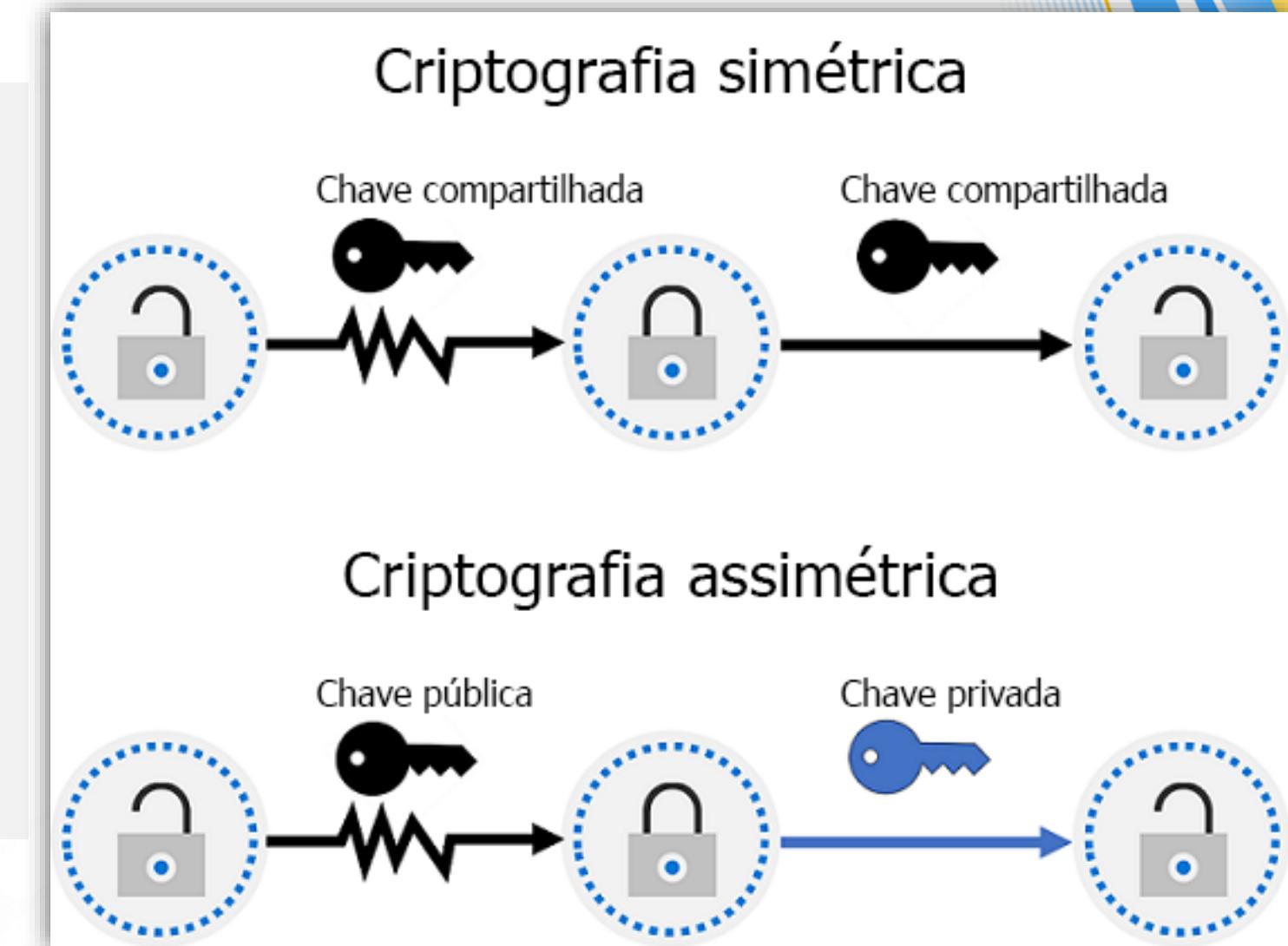
Descrever como a criptografia e o hashing podem proteger seus dados

Dois tipos de criptografia de nível superior:

- Criptografia simétrica
- Criptografia assimétrica

Criptografia e hash:

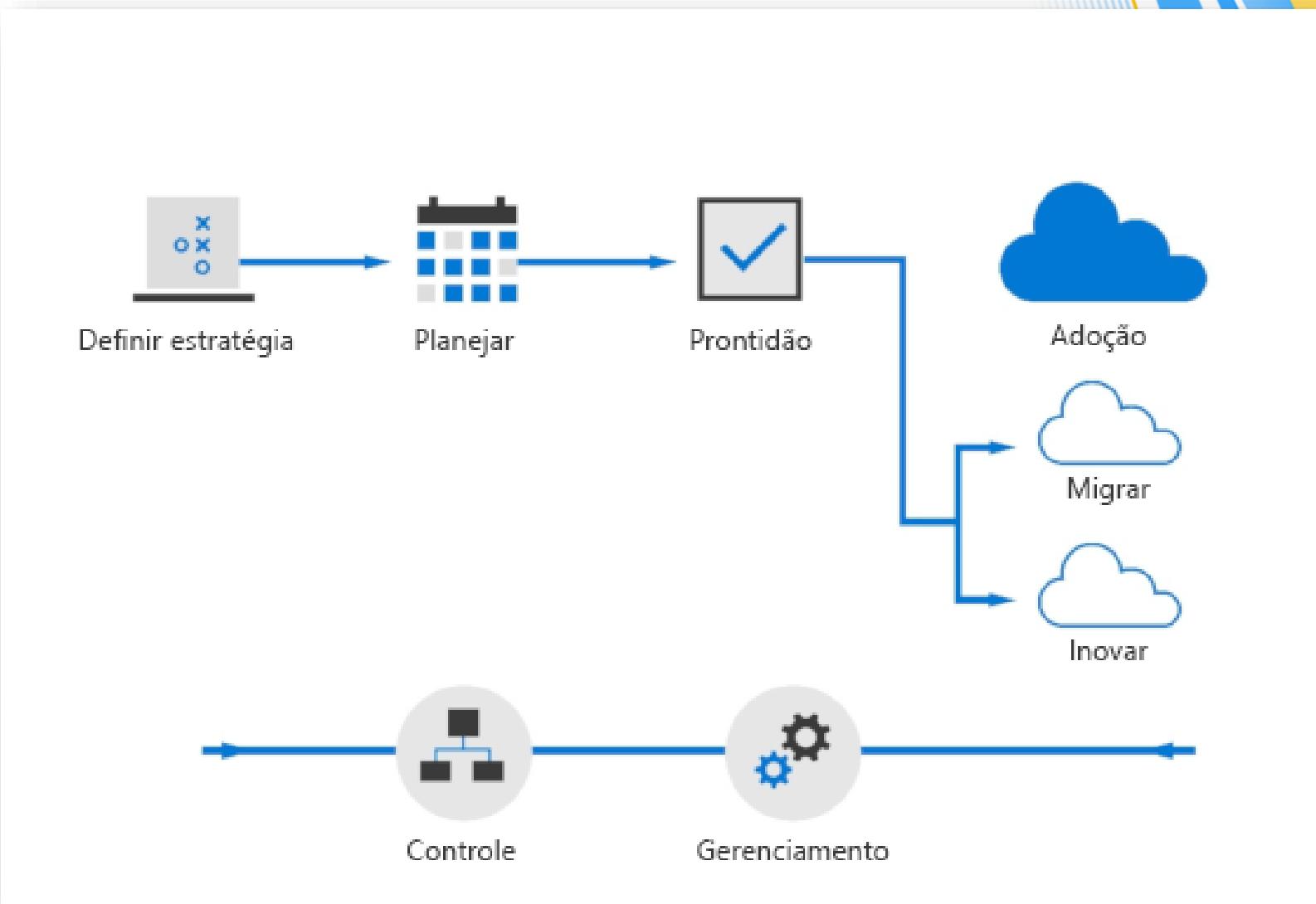
- Criptografia inativa
- Criptografia em trânsito
- Hash



Descrever o Cloud Adoption Framework

Cada uma das etapas a seguir faz parte do ciclo de vida de adoção da nuvem:

1. Estratégia
2. Plano
3. Prontidão
4. Adoção
 - Migração
 - Inovação:
5. Administração
6. Gerenciamento





Subscribe

Módulo 02

Descrever os recursos de gerenciamento de identidades e acessos do Microsoft 365





Subscribe

Agenda

Descrever o modelo de Confiança Zero da Microsoft e os conceitos de gerenciamento de identidades e acessos

Gerenciar identidades e acessos no Microsoft 365 com o Azure Active Directory

Reducir o risco de violações de segurança com autenticação segura





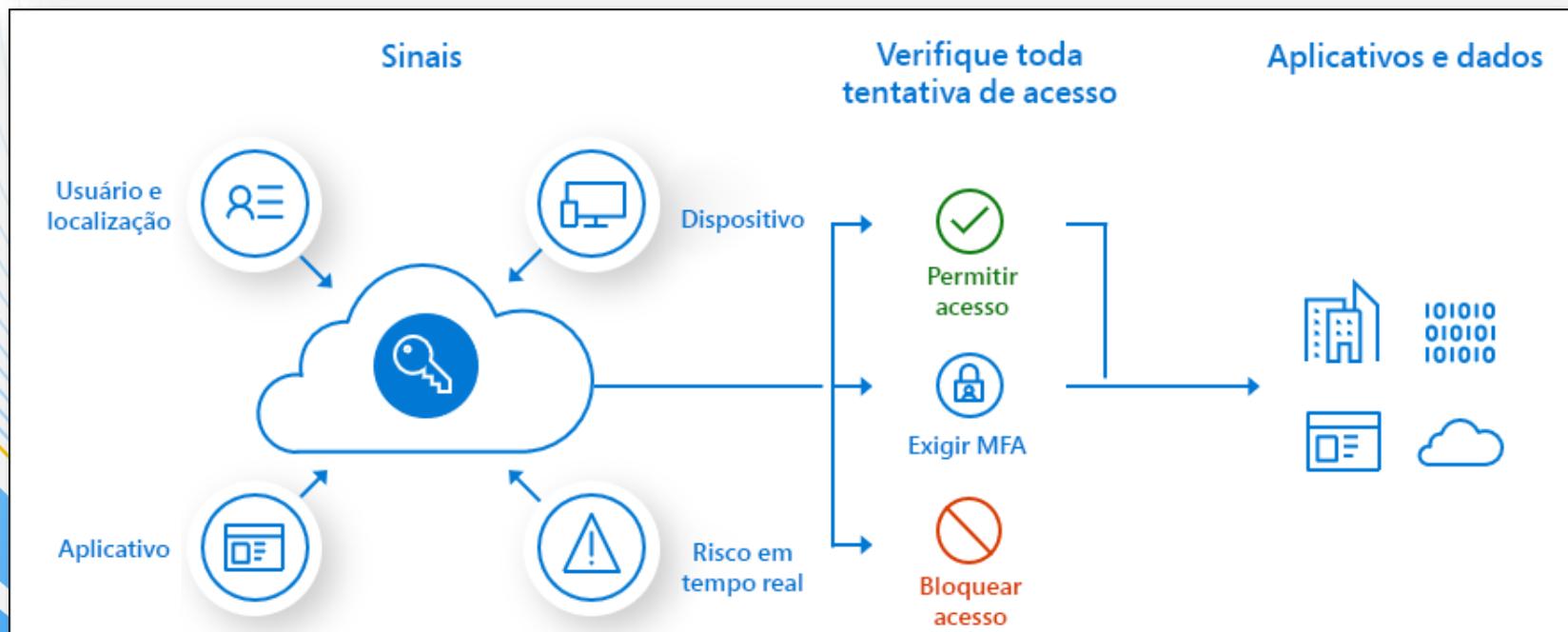
Descrever o modelo de Confiança Zero da Microsoft e os conceitos de gerenciamento de identidades e acessos

- **Gerenciamento de identidades e acessos**
 - Identidade híbrida
 - Identidade na nuvem
- **O modelo de segurança Confiança Zero**



Gerenciar identidades e acessos no Microsoft 365 com o Azure Active Directory

- Avaliação do sinal do Acesso Condicional
- Decisões de Acesso Condicional
- Aplicação por meio de políticas aplicadas
- Licenciamento de identidade e Acesso Condicional





Subscribe

Reducir o risco de violações de segurança com autenticação segura

- Autenticação segura
- Utilizar a autenticação multifator para melhorar a segurança da autenticação
- Por que usar autenticação sem senha
 - Implementar autenticação sem senha com o Azure AD
- Windows Hello
 - Acesso biométrico
- Microsoft Authenticator





Módulo 03

Descrever os recursos de proteção contra ameaças do Microsoft 365





Agenda

Identificar as ameaças de segurança comuns

Descobrir como a empresa pode prevenir, detectar e responder a ameaças

Definir sua postura de segurança com o Centro de Segurança da Microsoft e o Secure Score

Descrever o Gráfico de Segurança Inteligente da Microsoft e o Azure Sentinel



Identificar ameaças de segurança comuns

- Ameaças de segurança de rede comuns
- Ameaças de segurança de dados comuns



6



Descobrir como a empresa pode prevenir, detectar e responder a ameaças

- Microsoft 365 Defender
 - Microsoft Defender para Identidade
 - Microsoft Defender para Ponto de Extremidade
- Microsoft Cloud App Security
 - Microsoft Defender para Office 365

Experiência integrada do Microsoft 365



+



+



+



Identidade

Microsoft
Defender para
Identidade

Pontos de extremidade

Microsoft Defender
para Ponto de
Extremidade

Aplicativos

Microsoft Cloud
App Security

E-mail/Colaboração

Microsoft
Defender para
Office 365



Microsoft 365 Defender





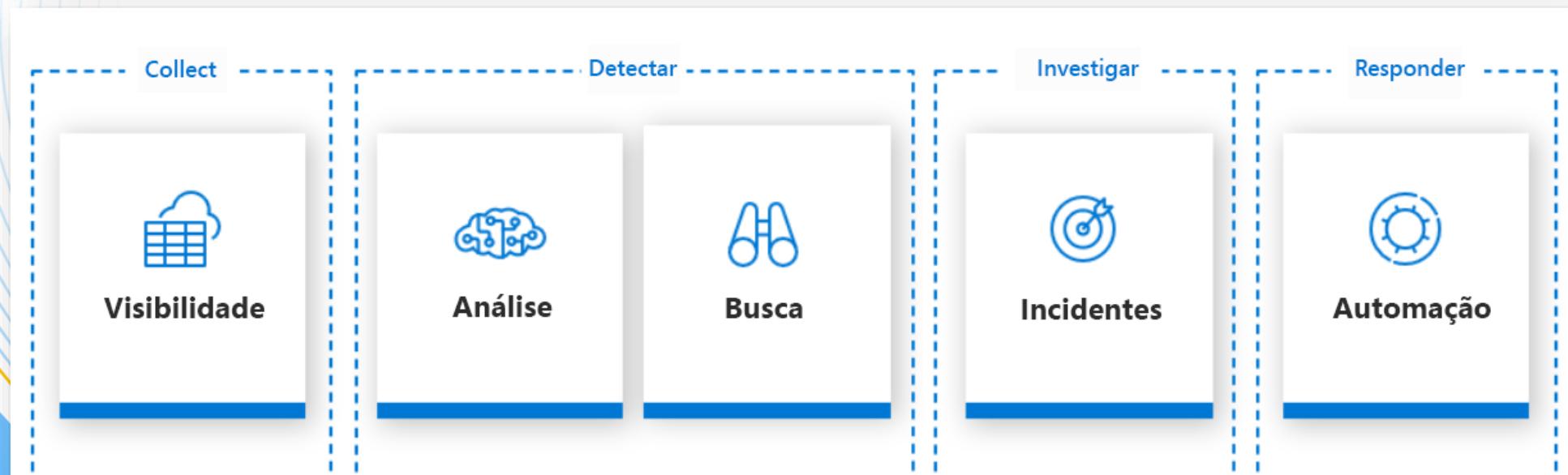
Definir sua postura de segurança com o Centro de Segurança da Microsoft e o Secure Score

- Microsoft 365 Defender
- Microsoft Security Score



Descrever o Gráfico de Segurança Inteligente da Microsoft e o Azure Sentinel

- API de Segurança do Microsoft Graph
- Azure Sentinel



Alimentado pela comunidade + apoiado pelos especialistas em segurança da Microsoft



Módulo 04

Descrever os recursos de segurança na nuvem do Microsoft 365





Subscribe

Agenda

Assumir o controle de seu ambiente de nuvem com o Microsoft Cloud App Security

Explorar os recursos de integração do Microsoft Cloud App Security





Assumir o controle de seu ambiente de nuvem com o Microsoft Cloud App Security

- Descobrir e controlar o uso de TI sombra
- Proteger suas informações confidenciais em qualquer lugar da nuvem
- Proteger contra ameaças cibernéticas e anomalias
- Avaliar a conformidade de seus aplicativos na nuvem





Explorar os recursos de integração do Microsoft Cloud App Security

- Integração com o Microsoft 365 Defender
- Integração com o Azure AD e a Proteção de Informações do Azure
- MCAS e Inteligência Contra Ameaças Avançada
- Integração do MCAS com o Power Automate





Módulo 05

Descrever os recursos de proteção de informações e de governança do Microsoft 365





Agenda

Descobrir e identificar informações importantes em seu ambiente

Proteger dados confidenciais em todo seu ciclo de vida

Administrar seus dados usando o Microsoft 365





Subscribe

Descobrir e identificar informações importantes em seu ambiente

- **Rótulos de confidencialidade** – permitem classificar e proteger os dados da sua organização, garantindo que a produtividade e a colaboração do usuário não sejam prejudicadas.
 - Criptografar
 - Comercializar o conteúdo
 - Aplicar o rótulo automaticamente
 - Proteger o conteúdo em contêineres, como sites e grupos





Descobrir e identificar informações importantes em seu ambiente

- **Proteção de Informações do Azure** – uma solução baseada em nuvem que ajuda as organizações a classificar e, opcionalmente, proteger documentos e emails aplicando rótulos.
- **Classificação de dados** – O portal de classificação de dados, acessado a partir do Centro de Conformidade do Microsoft 365, fornece instantâneos de como informações confidenciais e rótulos estão sendo usados nas localizações de sua organização.





Proteger dados confidenciais em todo seu ciclo de vida

- **Rótulos de confidencialidade** – classifique e proteja seus dados
 - Aplicar rótulos de confidencialidade automaticamente ao conteúdo
 - Usar rótulos de confidencialidade para aplicar criptografia
- **Criptografia de Mensagens do Office 365 (OME)** – Envie e receba mensagens de email criptografadas entre pessoas dentro e fora de sua organização.





Proteger dados confidenciais em todo seu ciclo de vida

- **Prevenção contra perda de dados (DLP)** – projetada para proteger informações confidenciais e impedir sua divulgação inadvertida, implementada por meio de políticas
- **Proteção de Informações do Windows** – Proteja sua organização contra vazamentos de dados acidentais ou maliciosos,
 - Ela fornece essa proteção para dispositivos de propriedade da empresa e dispositivos BYOD





Administrar seus dados usando o Microsoft 365

- Gerenciar dados
- Monitorar dados
- Gerenciar caixas de correio interativas
- Gerenciamento de registros





Subscribe

Módulo 06

Descrever os recursos do gerenciamento de conformidade do Microsoft 365



Necessidades comuns de conformidade

Diversas medidas para proteger dados:



Conceder aos indivíduos o direito de acessar seus dados a qualquer momento.



Conceder aos indivíduos o direito de corrigir ou excluir dados sobre eles, se necessário.



Apresentar períodos máximo ou mínimo de retenção dos dados.



Habilitar governos e órgãos regulatórios o direito de acessar e examinar os dados quando necessário.



Definir regras para quais dados podem ser processados e como isso deve ser feito.



Portal de Confiança do Serviço

O Portal de Confiança do Serviço fornece:

- Informações
- Ferramentas
- Outros recursos sobre as práticas de segurança, privacidade e conformidade da Microsoft.

Você pode acessar as soluções abaixo:

- Portal de Confiança do Serviço
- Gerenciador de Conformidade
- Documentos confiáveis
- Setores e regiões
- Central de Confiabilidade
- Recursos
- Minha biblioteca



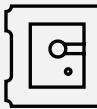
Princípios de privacidade da Microsoft



Controle: coloca você, o cliente, no controle de sua privacidade com ferramentas fáceis de usar e escolhas claras.



Transparência: ser transparente sobre a coleta e o uso de dados para que todos possam tomar decisões fundamentadas.



Segurança: proteger os dados confiados à Microsoft usando segurança e criptografia fortes.



Subscribe

Princípios de privacidade da Microsoft



Proteção legal robusta: respeitar as leis locais de privacidade local e lutar pela proteção legal da privacidade como um direito humano fundamental.



Sem direcionamento com base em conteúdo: sem uso de email, chat, arquivos ou outros conteúdos pessoais para direcionar publicidade.



Benefícios para você: quando a Microsoft coleta dados, eles são usados para beneficiar você, o cliente, e para melhorar suas experiências.





Centro de conformidade do Microsoft 365

Portal do centro de conformidade do Microsoft 365

- Uma visão de como a organização está atendendo às exigências de conformidade
- Soluções que podem ser usadas para ajudar na conformidade

The screenshot shows the Microsoft 365 Compliance Center homepage. The left sidebar contains navigation links such as Página Inicial, Gerenciador de Conformidade, Classificação de dados, Conectores de dados, Alertas, Relatórios, Políticas, Permissões, Soluções, Catálogo, Auditoria, Pesquisa de conteúdo, Conformidade com comunicações, Prevenção contra perda de dados, Solicitações do titular dos dados, Descoberta Eletrônica, Governança de informações, Proteção de informações, Gerenciamento de riscos internos, Gerenciamento de registros, and Conhecimento da privacidade. The main content area features a large "Bem-vindo ao Centro de conformidade do Microsoft 365" heading with a "Página Inicial" link. It includes a central graphic of a cloud with a scale and a checkmark, and three cards below: "Gerenciador de Conformidade" (Sua pontuação de conformidade: 57%), "Catálogo de soluções" (Descubra soluções para suas necessidades de conformidade), and "Uso de rótulo de retenção" (0 itens com rótulos de ...). A "Subscribe" button is visible in the top right corner of the browser window.

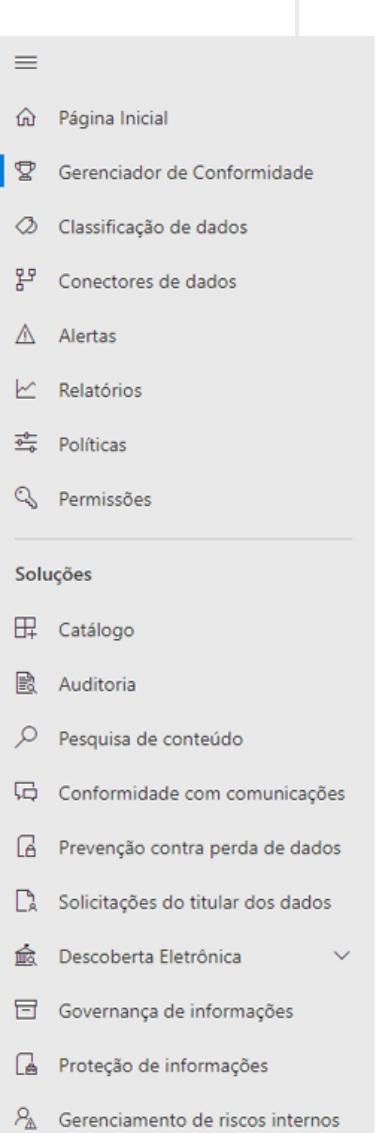
www.youtube.com/canaldacloud



Gerenciador de Conformidade

O Compliance Manager simplifica a conformidade e reduz os riscos, fornecendo:

- Avaliações pré-criadas baseadas em padrões
- Recursos de fluxo de trabalho para concluir avaliações de risco
- Ações de melhoria passo a passo
- Pontuação de conformidade, que mostra a postura geral de conformidade



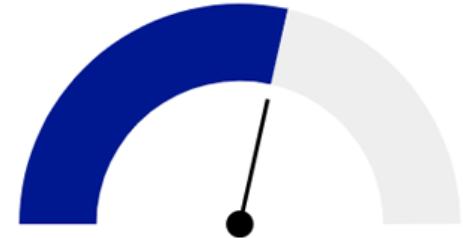
Gerenciador de Conformidade

[Visão geral](#) [Ações de melhoria](#) [Soluções](#) [Avaliações](#) [Modelos de avaliação](#)

O Gerenciador de Conformidade mede seu progresso em concluir ações que ajudam a reduzir os riscos em relação à proteção de dados normativos. [Encontrar ajuda e documentação](#)

Pontuação geral de conformidade

Sua pontuação de conformidade: 57%



10642/18590 pontos obtidos

Seus pontos alcançados

102/ 8050

Pontos gerenciados pela Microsoft obtidos

10540/ 10540

A Pontuação de Conformidade mede seu progresso no conteúdo de concluir as ações recomendadas que ajudam

Principais ações de melhoria

Não concluídas	Concluídas	Fora do escopo
608	4	0

Ação de melhoria	Impacto	Status do teste	Grupo
Habilitar redefinição de senha de autoat... +27 pontos	+27 pontos	● Parcialmente testado	Grupo padrão
Ocultar informações com tela de bloqueio +27 pontos	+27 pontos	● Nenhum	Grupo padrão
Use IRM to protect email messages and a... +27 pontos	+27 pontos	● Nenhum	Grupo padrão
Usar dispositivos de proteção de limite p... +27 pontos	+27 pontos	● Nenhum	Grupo padrão
Use IRM to protect online documents an... +27 pontos	+27 pontos	● Nenhum	Grupo padrão
Exigir dispositivos móveis para usar cript... +27 pontos	+27 pontos	● Nenhum	Grupo padrão
Usar S/MIME +27 pontos	+27 pontos	● Nenhum	Grupo padrão
Manage organizational users and groups +27 pontos	+27 pontos	● Nenhum	Grupo padrão
Assign roles to endpoint users +27 pontos	+27 pontos	● Nenhum	Grupo padrão

Pontuação de conformidade

Benefícios da pontuação de conformidade:

- Ajuda a organização a entender sua postura atual de conformidade.
- Ajuda a organização a priorizar ações com base em seu potencial para reduzir o risco.



A Pontuação de Conformidade mede seu progresso no sentido de concluir as ações recomendadas que ajudam

[Saiba como sua Pontuação de Conformidade é calculada](#)

Principais ações de melhoria

Não concluídas	Concluídas	Fora do escopo
608	4	0

Ação de melhoria Impacto

Habilitar redefinição de senha de autoat...	+27 pontos
Ocultar informações com tela de bloqueio	+27 pontos
Use IRM to protect email messages and a...	+27 pontos
Usar dispositivos de proteção de limite p...	+27 pontos
Use IRM to protect online documents an...	+27 pontos
Exigir dispositivos móveis para usar cript...	+27 pontos
Usar S/MIME	+27 pontos
Manage organizational users and groups	+27 pontos
Assign roles to endpoint users	+27 pontos

[Exibir todas as ações de melhoria](#)



Subscribe

Módulo 07

**Reducir o risco e simplificar o processo de descoberta
e auditoria**





 Subscribe

Agenda

Gerenciar o risco interno

Gerenciar a conformidade de comunicações

Restringir as comunicações com barreiras de informações

Controlar o acesso de administrador privilegiado

Aumentar o controle com o Sistema de Proteção de Dados do Cliente

Investigar com a Auditoria Avançada

Gerenciar investigações legais e de conformidade com a Descoberta Eletrônica Avançada





Gerenciar o risco interno

- O gerenciamento de risco interno ajuda a minimizar os riscos internos, permitindo que você detecte, investigue e execute ações em atividades de risco em sua organização.
 - Vazamentos de dados confidenciais
 - Violações de confidencialidade
 - Roubo de propriedade intelectual (IP)
 - Fraude
 - Treinamento interno
 - Violações de conformidade regulatória





Subscribe

Gerenciar a conformidade de comunicações

• Conformidade de comunicações

- Ajuda a minimizar os riscos de comunicação, ajudando a detectar, capturar e executar ações corretivas para mensagens inadequadas em sua organização.
- Políticas predefinidas e personalizadas permitem que você verifique as comunicações internas e externas em busca de correspondência de políticas
- Investigar emails examinados, Microsoft Teams, Yammer ou comunicações de terceiros
- Executa as ações corretivas apropriadas





Restringir as comunicações com barreiras de informações

- Barreiras de informações (IB) – são políticas que um administrador pode configurar para evitar a comunicação entre indivíduos ou grupos.
- Os cenários incluem:
 - Financeiro
 - Governamental
 - Jurídico
- As barreiras de informações se aplicam a chats e canais de equipes





Subscribe

Controlar o acesso de administrador privilegiado

- O **Privileged Access Management** permite o controle de acesso granular sobre tarefas de administrador privilegiadas no Microsoft 365.
- Habilitar o Privileged Access Management no Microsoft 365 permite que sua organização opere **sem acesso permanente**.
- Requer que os usuários solicitem acesso **just-in-time** para concluir tarefas elevadas e privilegiadas.



Aumentar o controle com o Sistema de Proteção de Dados do Cliente

- O **Sistema de Proteção de Dados do Cliente** garante que a Microsoft não poderá acessar seu conteúdo para realizar uma operação de serviço sem sua aprovação explícita.





Subscribe

Investigar com a Auditoria Avançada

A **Auditoria Avançada do Microsoft 365** fornece novas capacidades de auditoria que podem ajudar sua organização com investigações jurídicas e de conformidade.

- Retenção de longo prazo de logs de auditoria
- Políticas de retenção de log de auditoria
- Acesso a eventos fundamentais para investigações
- Acesso de alta largura de banda à API da Atividade de Gestão do Office 365





Gerenciar investigações legais e de conformidade com a Descoberta Eletrônica Avançada

- A solução **Descoberta Eletrônica Avançada** da Microsoft fornece um fluxo de trabalho de ponta a ponta para preservar, coletar, revisar, analisar e exportar conteúdo que atenda às investigações internas e externas da sua organização.
- Fluxo de trabalho da Descoberta Eletrônica Avançada
 - **Identificação**
 - **Preservação**
 - **Coleção**
 - **Processamento**
 - **Revisão**
 - **Análise**
 - **Produção e Apresentação**





Teste de conhecimento



www.youtube.com/canaldacloud



O que é o Windows como serviço?

1

A capacidade de executar o Windows como uma área de trabalho virtual

2

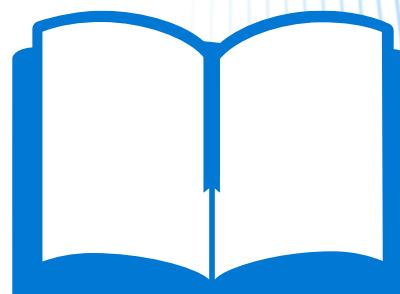
Windows 10 com atualizações regulares de recursos

3

Windows 10 Mobile

Explicação:

O Windows como serviço é um novo modelo para o Windows 10. Em vez de uma versão principal a cada três ou quatro anos, os recursos são lançados com mais frequência, como semestralmente.





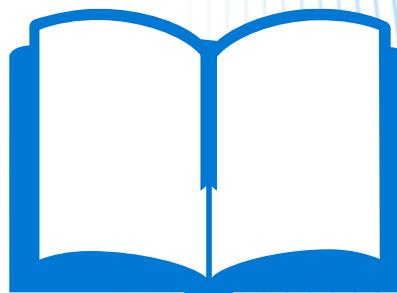
Como você controla a frequência das atualizações com o Windows-as-a-Service?

- 1 Atualizações do Windows
- 2 Anéis de implantação
- 3 Canal de Atendimento



Explicação:

O canal de serviço determina a frequência com que o Windows 10 é atualizado com novos recursos.





Qual grupo de usuários pode se beneficiar da Área de Trabalho Virtual do Azure?

1

Usuários que precisam executar um desktop Mac

2

Usuários que trabalham com dados confidenciais

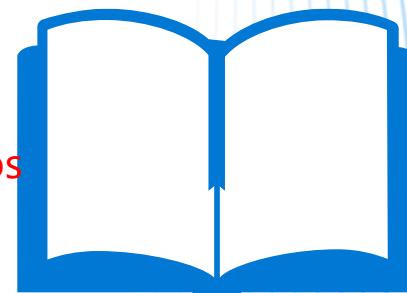
3

Usuários com baixa conectividade com a Internet



Explicação:

A Área de Trabalho Virtual do Azure pode ser configurada para garantir que os dados nunca sejam armazenados no dispositivo local.

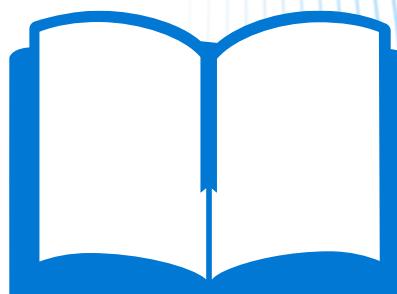




O que você usaria para gerenciar o Windows-as-a-Service?

- 1 Gerenciador de configuração
- 2 Atualizações do Windows
- 3 Área de trabalho virtual do Azure

Explicação:
O Configuration Manager permite configurar o Windows como serviço, incluindo Canais de serviço e anéis de implantação.



O que é MyAnalytics?

1

A capacidade de classificar automaticamente seu e-mail

2

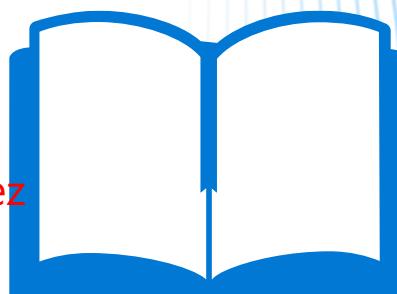
Análises sobre seus padrões de trabalho entregues como um e-mail

3

A capacidade de executar módulos de IA no Azure

Explicação:

O MyAnalytics é um resumo de seus padrões de trabalho gerados a partir de seu trabalho diário no Microsoft 365. Ele é entregue como um relatório por email uma vez por semana.





Subscribe

Obrigado!

▶ /canaldacloud

📷 @canaldacloud

↗️ /canaldacloud



www.youtube.com/canaldacloud

