## Perguntas

Pergunta nº 7

Qual pontuação mede o progresso de uma organização na conclusão de ações que ajudam a reduzir riscos associados à proteção de dados e aos padrões regulatórios?

1. Pontuação segura da Microsoft
2. Pontuação de produtividade
3. Pontuação segura no Azure Security Center
4. Pontuação de conformidade

Referência:  
https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager?view=o365-worldwide https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score-calculation?view=o365-worldwide

Pergunta nº 8

O que você usa para fornecer integração em tempo real entre o Azure Sentinel e outra fonte de segurança?

1. Conexão do Azure AD
2. um espaço de trabalho do Log Analytics
3. Proteção de Informações do Azure
4. um conector

Para integrar o Azure Sentinel, primeiro você precisa se conectar às suas fontes de segurança. O Azure Sentinel vem com vários conectores para soluções da Microsoft, incluindo soluções do Microsoft 365 Defender e fontes do Microsoft 365, incluindo Office 365, Azure AD, Microsoft Defender for Identity e Microsoft Cloud App  
Security, etc.  
Referência: https://docs.microsoft.com/en-us/azure/sentinel/overview

Pergunta nº 9

Qual portal da Microsoft fornece informações sobre como os serviços de nuvem da Microsoft estão em conformidade com padrões regulatórios, como a Organização Internacional para  
Padronização (ISO)?

1. o centro de administração do Microsoft Endpoint Manager
2. Gerenciamento de custos do Azure + cobrança
3. Portal de confiança do serviço Microsoft
4. o centro de administração do Azure Active Directory

O Microsoft Service Trust Portal contém detalhes sobre a implementação de controles e processos da Microsoft que protegem nossos serviços de nuvem e os dados do cliente neles contidos.  
Referência:https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-service-trust-portal?view=o365-worldwide

Pergunta nº 10

No modelo de responsabilidade compartilhada para uma implantação do Azure, o que é de responsabilidade exclusiva da Microsoft para gerenciar?

1. a gestão de dispositivos móveis
2. as permissões para os dados do usuário armazenados no Azure
3. a criação e gestão de contas de usuários
4. a gestão do hardware físico

GPT-4o - Resposta

A escolha correta é D, gerenciamento do hardware físico. Sob o modelo de responsabilidade compartilhada do Azure, a Microsoft é responsável pela segurança física, disponibilidade e manutenção dos data centers, que incorporam aspectos como rede, servidores e hardware de armazenamento. Esse nível distinto de responsabilidade garante a robustez e a segurança da infraestrutura, o que permite que os clientes se concentrem mais no gerenciamento de seus aplicativos e dados.

Pergunta nº 18

No Microsoft Cloud Adoption Framework para Azure, quais duas fases são abordadas antes da fase Ready?

1. Plano
2. Gerenciar
3. Adotar
4. Governar
5. Definir estratégia

Referência:  
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/overview

Pergunta nº 22

Qual é um exemplo de criptografia em repouso?

1. criptografando comunicações usando uma VPN site a site
2. criptografando um disco de máquina virtual
3. acessando um site usando uma conexão HTTPS criptografada
4. enviando um e-mail criptografado

Referência:  
https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-atrest

Pergunta nº 23

Quais três afirmações descrevem com precisão os princípios orientadores do Zero Trust?

1. Defina o perímetro por localizações físicas.
2. Use a identidade como o principal limite de segurança.
3. Sempre verifique as permissões de um usuário explicitamente.
4. Sempre assuma que o sistema do usuário pode ser violado.
5. Use a rede como o principal limite de segurança.

Referência:https://docs.microsoft.com/en-us/security/zero-trust/

Pergunta nº 28

O que você pode usar para fornecer a um usuário uma janela de duas horas para concluir uma tarefa administrativa no Azure?

1. Azure Active Directory (Azure AD) Gerenciamento de Identidade Privilegiada (PIM)
2. Autenticação multifator do Azure (MFA)
3. Proteção de identidade do Azure Active Directory (Azure AD)
4. políticas de acesso condicional

Referência:  
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-policy-common

Pergunta nº 29

Em um modelo de identidade híbrida, o que você pode usar para sincronizar identidades entre o Active Directory Domain Services (AD DS) e o Azure Active Directory (Azure AD)?

1. Serviços de Federação do Active Directory (AD FS)
2. Microsoft Sentinel
3. Conexão do Azure AD
4. Gerenciamento de Identidade Privilegiada (PIM) do Azure AD

Referência:  
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-azure-ad-connect

Pergunta nº 33

Qual é o propósito da proteção por senha do Azure Active Directory (Azure AD)?

1. para controlar a frequência com que os usuários devem alterar suas senhas
2. para identificar dispositivos nos quais os usuários podem fazer login sem usar autenticação multifator (MFA)
3. para criptografar uma senha usando padrões de criptografia reconhecidos globalmente
4. para evitar que os usuários usem palavras específicas em suas senhas

O Azure AD Password Protection detecta e bloqueia senhas fracas conhecidas e suas variantes, e também pode bloquear termos fracos adicionais específicos da sua organização.  
Com o Azure AD Password Protection, listas de senhas banidas globais padrão são aplicadas automaticamente a todos os usuários em um locatário do Azure AD. Para dar suporte às suas próprias necessidades comerciais e de segurança, você pode definir entradas em uma lista de senhas banidas personalizada.  
Referência:  
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad-on-premises

Pergunta nº 34

Qual recurso do Azure Active Directory (Azure AD) você pode usar para avaliar a associação de grupo e remover automaticamente usuários que não precisam mais de associação a um grupo?

1. acessar avaliações
2. identidades gerenciadas
3. políticas de acesso condicional
4. Proteção de identidade do Azure AD

As  
revisões de acesso do Azure Active Directory (Azure AD) permitem que as organizações gerenciem com eficiência associações de grupo, acesso a aplicativos empresariais e atribuições de função.  
Referência:  
https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

Pergunta nº 40

Qual recurso do Azure Active Directory (Azure AD) você pode usar para fornecer acesso just-in-time (JIT) para gerenciar recursos do Azure?

1. políticas de acesso condicional
2. Proteção de identidade do Azure AD
3. Gerenciamento de Identidade Privilegiada (PIM) do Azure AD
4. políticas de método de autenticação

O Azure AD Privileged Identity Management (PIM) fornece acesso privilegiado just-in-time ao Azure AD e aos recursos do Azure.  
Referência:  
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

Pergunta nº 41

Quais três métodos de autenticação podem ser usados ​​pelo Azure Multi-Factor Authentication (MFA)?

1. mensagem de texto (SMS)
2. Aplicativo Microsoft Authenticator
3. verificação de e-mail
4. chamada telefônica
5. Pergunta de segurança

Referência:  
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods

Pergunta nº 42

Qual recurso do Microsoft 365 você pode usar para restringir a comunicação e o compartilhamento de informações entre membros de dois departamentos da sua organização?

1. políticas de rótulo de sensibilidade
2. Caixa de segurança do cliente
3. barreiras de informação
4. Gerenciamento de acesso privilegiado (PAM)

Referência:  
https://docs.microsoft.com/en-us/microsoft-365/compliance/information-barriers

Pergunta nº 46

Quais são os três métodos de autenticação suportados pelo Windows Hello for Business?

1. impressão digital
2. reconhecimento facial
3. ALFINETE
4. verificação de e-mail
5. Pergunta de segurança

Referência:  
https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-how-it-works-authentication

Pergunta nº 48

Você tem uma assinatura do Azure.  
Você precisa implementar ativação de função com limite de tempo e baseada em aprovação.  
O que você deve usar?

1. Windows Hello para empresas
2. Proteção de identidade do Azure Active Directory (Azure AD)
3. acessar avaliações no Azure Active Directory (Azure AD)
4. Azure Active Directory (Azure AD) Gerenciamento de Identidade Privilegiada (PIM)

Referência:  
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

Pergunta nº 50

Quando os padrões de segurança são habilitados para um locatário do Azure Active Directory (Azure AD), quais dois requisitos são impostos?

1. Todos os usuários devem se autenticar a partir de um dispositivo registrado.
2. Os administradores devem sempre usar a Autenticação Multifator (MFA) do Azure.
3. O registro do Azure Multi-Factor Authentication (MFA) é obrigatório para todos os usuários.
4. Todos os usuários devem se autenticar usando login sem senha.
5. Todos os usuários devem se autenticar usando o Windows Hello.

Os padrões de segurança facilitam a proteção da sua organização com as seguintes configurações de segurança pré-configuradas:  
✑ Exigir que todos os usuários se registrem na Autenticação Multifator do Azure AD.  
✑ Exigir que os administradores façam autenticação multifator.  
✑ Bloquear protocolos de autenticação legados.  
✑ Exigir que os usuários façam autenticação multifator quando necessário.  
✑ Proteger atividades privilegiadas, como acesso ao portal do Azure.  
Referência:  
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults

Pergunta nº 51

Que tipo de identidade é criada quando você registra um aplicativo no Active Directory (Azure AD)?

1. uma conta de usuário
2. uma identidade gerenciada atribuída pelo usuário
3. uma identidade gerenciada atribuída pelo sistema
4. um diretor de serviço

Quando você registra um aplicativo por meio do portal do Azure, um objeto de aplicativo e um principal de serviço são criados automaticamente em seu diretório inicial ou locatário.  
Referência:  
https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

Pergunta nº 52

Quais três tarefas podem ser executadas usando o Azure Active Directory (Azure AD) Identity Protection?

1. Configure o acesso externo para organizações parceiras.
2. Detecção de risco de exportação para serviços públicos de terceiros.
3. Automatize a detecção e a correção de riscos baseados em identidade.
4. Investigue os riscos relacionados à autenticação do usuário.
5. Crie e atribua automaticamente rótulos de sensibilidade aos dados.

GPT-4o - Resposta

O Azure Active Directory Identity Protection foi projetado especificamente para operações de segurança relacionadas a identidades. Ele permite que você automatize a detecção e a correção de riscos baseados em identidade, investigue completamente os riscos associados à autenticação do usuário e até mesmo exporte esses dados de detecção de risco para utilitários de terceiros para uma análise mais ampla. Lembre-se, embora o Azure AD seja robusto no gerenciamento de riscos de identidade, ele não lida com tarefas como criar rótulos de sensibilidade para dados; eles são gerenciados por meio de outras ferramentas de conformidade da Microsoft.

Pergunta nº 57

Quais são os dois recursos do Microsoft Defender for Endpoint?

1. investigação e remediação automatizadas
2. criptografia de transporte
3. detecção de TI sombra
4. redução da superfície de ataque

Referência:  
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide

Pergunta nº 65

Qual recurso do Microsoft Defender for Endpoint fornece a primeira linha de defesa contra ameaças cibernéticas reduzindo a superfície de ataque?

1. remediação automatizada
2. investigação automatizada
3. caça avançada
4. proteção de rede

A proteção de rede ajuda a proteger dispositivos de eventos baseados na Internet. A proteção de rede é um recurso de redução de superfície de ataque.  
Referência:  
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/network-protection?view=o365-worldwide

Pergunta nº 67

Quais dois tipos de recursos podem ser protegidos usando o Azure Firewall?

1. Máquinas virtuais do Azure
2. Usuários do Azure Active Directory (Azure AD)
3. Caixas de entrada do Microsoft Exchange Online
4. Redes virtuais do Azure
5. Sites do Microsoft SharePoint Online

GPT-4o - Resposta

O Azure Firewall serve para proteger limites de rede e gerencia o tráfego que flui em ambientes do Azure. Ele é especialmente projetado para proteger redes virtuais do Azure (D) controlando e inspecionando todo o tráfego de entrada e saída. Para aplicativos como sites do Microsoft SharePoint Online (E), o Azure Firewall pode impor estratégias e controlar o acesso, adicionando uma camada de segurança para interações com sites externos ou não confiáveis. Isso garante que o SharePoint Online permaneça seguro contra potenciais ameaças baseadas na Web, ajudando a gerenciar o acesso e o compartilhamento de dados de forma eficaz dentro das diretrizes organizacionais.

Pergunta nº 68

Você planeja implementar uma estratégia de segurança e colocar múltiplas camadas de defesa em toda uma infraestrutura de rede.  
Qual metodologia de segurança isso representa?

1. modelagem de ameaças
2. identidade como perímetro de segurança
3. defesa em profundidade
4. o modelo de responsabilidade compartilhada

Referência:  
https://docs.microsoft.com/en-us/learn/modules/secure-network-connectivity-azure/2-what-is-defense-in-depth

Pergunta nº 70

O que você pode usar para verificar anexos de e-mail e encaminhá-los aos destinatários somente se eles estiverem livres de malware?

1. Microsoft Defender para Office 365
2. Microsoft Defender Antivírus
3. Microsoft Defender para Identidade
4. Microsoft Defender para Endpoint

Referência:  
https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-advanced-threat-protection-service-description

Pergunta nº 71

Qual recurso fornece a capacidade de detecção e resposta estendida (XDR) do Azure Sentinel?

1. integração com o centro de conformidade do Microsoft 365
2. suporte para caça de ameaças
3. integração com o Microsoft 365 Defender
4. suporte para pastas de trabalho do Azure Monitor

Referência:  
https://docs.microsoft.com/en-us/microsoft-365/security/defender/eval-overview?view=o365-worldwide

Pergunta nº 72

O que você pode usar para fornecer detecção de ameaças para a Instância Gerenciada do Azure SQL?

1. Pontuação segura da Microsoft
2. grupos de segurança de aplicativos
3. Microsoft Defender para Nuvem
4. Bastião Azure

GPT-4o - Resposta

O Microsoft Defender for Cloud é a escolha apropriada para detecção de ameaças no Azure SQL Managed Instance. Ele inclui o plano Microsoft Defender for SQL, que monitora ativamente instâncias SQL para ameaças potenciais, como injeções de SQL, ataques de força bruta e atividades incomuns de banco de dados. Ele fornece alertas de segurança acionáveis ​​e recomendações para mitigar essas ameaças de forma eficaz, tudo convenientemente acessível a partir de uma única plataforma. O mergulho profundo em alertas e a orquestração de respostas a incidentes podem ser ainda mais simplificados pela integração com o Microsoft Sentinel.

Pergunta nº 74

Qual recurso do Azure Active Directory (Azure AD) você pode usar para restringir dispositivos gerenciados pelo Microsoft Intune de acessar recursos corporativos?

1. grupos de segurança de rede (NSGs)
2. Gerenciamento de Identidade Privilegiada (PIM) do Azure AD
3. políticas de acesso condicional
4. bloqueios de recursos

GPT-4o - Resposta

As políticas de acesso condicional no Azure AD são cruciais para gerenciar o acesso do dispositivo a recursos corporativos. Elas usam o status de conformidade do dispositivo, que é relatado pelo Intune após avaliar as políticas de conformidade definidas, para decidir se deve permitir ou bloquear o acesso. Esse mecanismo garante que apenas dispositivos que atendem aos padrões de segurança acessem dados confidenciais, mantendo um ambiente de TI seguro.

Pergunta nº 77

O que você deve usar no portal do Microsoft 365 Defender para visualizar tendências de segurança e rastrear o status de proteção de identidades?

1. Simulador de ataque
2. Relatórios
3. Caça
4. Incidentes

Referência:  
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/reports-and-insights-in-security-and-compliance?view=o365-worldwide

Pergunta nº 78

Você tem uma assinatura do Microsoft 365 E3.  
Você planeja auditar a atividade do usuário usando o log de auditoria unificado e a Auditoria Básica.  
Por quanto tempo os registros de auditoria serão retidos?

1. 15 dias
2. 30 dias
3. 90 dias
4. 180 dias

GPT-4o - Resposta

É essencial observar que o período de retenção para registros de auditoria no Microsoft 365 foi atualizado recentemente. Embora tradicionalmente a Auditoria Básica tivesse um período de retenção de 90 dias, as alterações instituídas a partir de 17 de outubro de 2023 estenderam o período de retenção padrão para 180 dias para Auditoria (Padrão). Esta atualização se aplica a logs gerados na data especificada ou após ela, garantindo um período mais estendido para auditoria e revisões de conformidade. Sempre verifique as diretrizes e atualizações mais recentes diretamente da Microsoft para se manter informado sobre quaisquer outras alterações nas políticas de auditoria.

Pergunta nº 79

A que tipo de recurso o Azure Bastion pode fornecer acesso seguro?

1. Arquivos do Azure
2. Instâncias gerenciadas do Azure SQL
3. Máquinas virtuais do Azure
4. Serviço de Aplicativo do Azure

O Azure Bastion fornece conectividade RDP/SSH segura e contínua para suas máquinas virtuais diretamente do portal do Azure por TLS.  
Referência:  
https://docs.microsoft.com/en-us/azure/bastion/bastion-overview

Pergunta nº 80

Quais são os três usos do Microsoft Cloud App Security?

1. para descobrir e controlar o uso da TI sombra
2. para fornecer conexões seguras às máquinas virtuais do Azure
3. para proteger informações confidenciais hospedadas em qualquer lugar na nuvem
4. para fornecer autenticação de passagem para aplicativos locais
5. para evitar vazamentos de dados para aplicativos não compatíveis e limitar o acesso a dados regulamentados

Referência:  
https://docs.microsoft.com/en-us/defender-cloud-apps/what-is-defender-for-cloud-apps

Pergunta nº 82

Você precisa se conectar a uma máquina virtual do Azure usando o Azure Bastion.  
O que você deve usar?

1. PowerShell remoto
2. o portal do Azure
3. o cliente de conexão de área de trabalho remota
4. um cliente SSH

Você pode criar uma conexão RDP com uma VM do Windows usando o Azure Bastion.  
Referência:  
https://docs.microsoft.com/en-us/azure/bastion/bastion-connect-vm-rdp-windows

Pergunta nº 83

Qual serviço inclui o recurso de treinamento de simulação de ataque?

1. Microsoft Defender para aplicativos em nuvem
2. Microsoft Defender para Identidade
3. Microsoft Defender para SQL
4. Microsoft Defender para Office 365

O treinamento de simulação de ataque no Microsoft Defender para Office 365 Plano 2 ou Microsoft 365 E5 permite que você execute simulações benignas de ataques cibernéticos em sua organização. Essas simulações testam suas políticas e práticas de segurança, bem como treinam seus funcionários para aumentar sua conscientização e diminuir sua suscetibilidade a ataques.  
Referência:  
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training

Pergunta nº 84

Que tipo de alerta você pode gerenciar no portal do Microsoft 365 Defender?

1. Microsoft Defender para Armazenamento
2. Microsoft Defender para SQL
3. Microsoft Defender para Endpoint
4. Microsoft Defender para IoT

A fila de alertas mostra o conjunto atual de alertas. Você acessa a fila de alertas em Incidentes e alertas > Alertas no início rápido do portal do Microsoft 365 Defender.  
Alertas de diferentes soluções de segurança da Microsoft, como Microsoft Defender for Endpoint, Microsoft Defender for Office 365 e Microsoft 365 Defender, aparecem aqui.  
Referência:  
https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-alerts

Pergunta nº 86

Com quais dois recursos do Azure um grupo de segurança de rede (NSG) pode ser associado?

1. uma sub-rede de rede virtual
2. uma interface de rede
3. um grupo de recursos
4. uma rede virtual
5. um aplicativo web do Azure App Service

Associação de grupos de segurança de rede  
Você pode associar um grupo de segurança de rede a máquinas virtuais, NICs e sub-redes, dependendo do modelo de implantação que você usa.  
Referência:  
https://aviatrix.com/learn-center/cloud-security/create-network-security-groups-in-azure/

Pergunta nº 87

Qual é um caso de uso para implementar políticas de barreira de informações no Microsoft 365?

1. para restringir o acesso não autenticado ao Microsoft 365
2. para restringir os bate-papos do Microsoft Teams entre determinados grupos dentro de uma organização
3. para restringir o e-mail do Microsoft Exchange Online entre determinados grupos dentro de uma organização
4. para restringir o compartilhamento de dados a destinatários de e-mail externos

Referência:  
https://docs.microsoft.com/en-us/microsoft-365/compliance/information-barriers-policies?view=o365-worldwide

Pergunta nº 88

O que você pode usar para implantar recursos do Azure em várias assinaturas de maneira consistente?

1. Microsoft Defender para Nuvem
2. Projetos do Azure
3. Microsoft Sentinel
4. Política do Azure

Referência:  
https://docs.microsoft.com/en-us/azure/governance/blueprints/overview

Pergunta nº 91

Qual recurso do centro de conformidade do Microsoft 365 você pode usar para identificar todos os documentos em um site do Microsoft SharePoint Online que contêm uma palavra-chave específica?

1. Auditoria
2. Gerente de conformidade
3. Pesquisa de conteúdo
4. Alertas

A ferramenta Content Search no Security & Compliance Center pode ser usada para encontrar rapidamente e-mails em caixas de correio do Exchange, documentos em sites do SharePoint e  
locais do OneDrive e conversas de mensagens instantâneas no Skype for Business.  
O primeiro passo é começar a usar a ferramenta Content Search para escolher locais de conteúdo para pesquisar e configurar uma consulta de palavra-chave para pesquisar itens específicos.  
Referência:  
https://docs.microsoft.com/en-us/microsoft-365/compliance/search-for-content?view=o365-worldwide

Pergunta nº 93

Qual recurso do Microsoft 365 você pode usar para restringir os usuários de enviar mensagens de e-mail que contenham listas de clientes e seus números de cartão de crédito associados?

1. políticas de retenção
2. políticas de prevenção de perda de dados (DLP)
3. políticas de acesso condicional
4. barreiras de informação

Referência:  
https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide

Pergunta nº 95

Em um fluxo de trabalho do Core eDiscovery, o que você deve fazer antes de pesquisar conteúdo?

1. Crie uma retenção de eDiscovery.
2. Execute a análise expressa.
3. Configurar detecção de privilégios entre advogado e cliente.
4. Exporte e baixe os resultados.

Referência:  
https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-core-ediscovery?view=o365-worldwide

Pergunta nº 96

Qual portal da Microsoft fornece informações sobre como a Microsoft gerencia privacidade, conformidade e segurança?

1. Portal de confiança do serviço Microsoft
2. Gerente de conformidade
3. Centro de conformidade do Microsoft 365
4. Suporte da Microsoft

Referência:  
https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-service-trust-portal?view=o365-worldwide

Pergunta nº 97

O que você pode proteger usando a solução de proteção de informações no centro de conformidade do Microsoft 365?

1. computadores de explorações de dia zero
2. usuários de tentativas de phishing
3. arquivos de malware e vírus
4. dados confidenciais sejam expostos a usuários não autorizados

Referência:  
https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection?view=o365-worldwide

Pergunta nº 98

O que você pode especificar nos rótulos de sensibilidade do Microsoft 365?

1. por quanto tempo os arquivos devem ser preservados
2. quando arquivar uma mensagem de e-mail
3. qual marca d'água adicionar aos arquivos
4. onde armazenar arquivos

Referência:  
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

Pergunta nº 102

Quais duas tarefas você pode implementar usando políticas de prevenção de perda de dados (DLP) no Microsoft 365?

1. Exiba dicas de políticas para usuários que estão prestes a violar as políticas da sua organização.
2. Habilitar criptografia de disco em endpoints.
3. Proteja documentos no Microsoft OneDrive que contenham informações confidenciais.
4. Aplique linhas de base de segurança aos dispositivos.

Referência:  
https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide

Pergunta nº 105

Qual recurso de conformidade do Microsoft 365 você pode usar para criptografar conteúdo automaticamente com base em condições específicas?

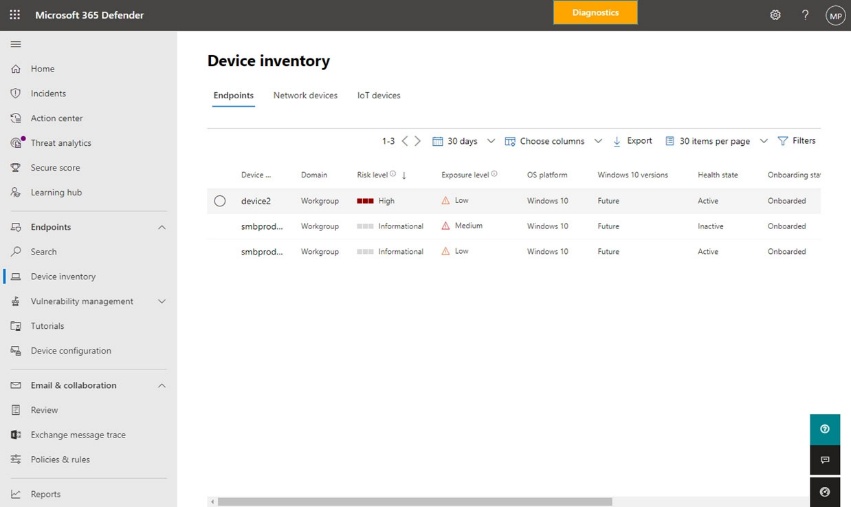
1. Pesquisa de conteúdo
2. rótulos de sensibilidade
3. políticas de retenção
4. eDescoberta

Referência:  
https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection?view=o365-worldwide

Pergunta nº 110

Quais são os dois cartões disponíveis no portal do Microsoft 365 Defender?

1. Dispositivos em risco
2. Pontuação de conformidade
3. Serviço de Saúde
4. Gerenciamento de usuários
5. Usuários em risco

A: O cartão Dispositivos em risco inclui um botão Exibir detalhes. Selecionar esse botão nos leva à página Inventário de dispositivos, conforme mostrado na imagem a seguir  
  
E: Os cartões do portal do Microsoft 365 Defender se enquadram nestas categorias:  
Identidades - Monitore as identidades em sua organização e acompanhe comportamentos suspeitos ou arriscados. Aqui você pode encontrar o cartão Usuários em risco.  
Dados - Ajude a rastrear a atividade do usuário que pode levar à divulgação não autorizada de dados.  
Dispositivos - Obtenha informações atualizadas sobre alertas, atividades de violação e outras ameaças em seus dispositivos.  
Aplicativos - Obtenha insights sobre como os aplicativos de nuvem estão sendo usados ​​em sua organização.  
Incorreto:  
Não C: O cartão Integridade do serviço pode ser acessado no centro de administração do Microsoft 365.  
Referência:  
https://docs.microsoft.com/en-us/microsoft-365/security/defender-business/mdb-respond-mitigate-threats

Pergunta nº 111

O que você deve usar para garantir que os membros de um grupo do Azure Active Directory usem autenticação multifator (MFA) ao entrarem?

1. Controle de acesso baseado em função do Azure (Azure RBAC)
2. Azure Active Directory (Azure AD) Gerenciamento de Identidade Privilegiada (PIM)
3. Proteção de identidade do Azure Active Directory (Azure AD)
4. uma política de acesso condicional

GPT-4o - Resposta

Para garantir que os membros de um grupo do Azure Active Directory utilizem autenticação multifator ao fazer login, implementar uma política de acesso condicional é altamente eficaz. Essas políticas permitem a aplicação de MFA sob condições específicas, fornecendo um mecanismo robusto para gerenciamento de segurança. Essa abordagem oferece uma postura de segurança personalizada que se adapta a vários cenários de login, reforçando a proteção geral de aplicativos e serviços conectados via Azure AD.

Pergunta nº 113

Você precisa manter uma cópia de todos os arquivos em um site do Microsoft SharePoint por um ano, mesmo que os usuários excluam os arquivos do site.  
O que você deve aplicar ao site?

1. uma política de retenção
2. uma política de risco interno
3. uma política de prevenção de perda de dados (DLP)
4. uma política de rótulo de sensibilidade

GPT-4o - Resposta

Absolutamente perfeito! Aplicar uma política de retenção é, de fato, o caminho a seguir para garantir que todos os arquivos em um site do Microsoft SharePoint sejam retidos por um ano, independentemente de serem excluídos pelos usuários. Essa estratégia ajuda a gerenciar dados de forma eficiente, permitindo que você decida proativamente se deseja reter o conteúdo, excluí-lo ou reter e excluir o conteúdo mais tarde. É uma ferramenta poderosa, especialmente no gerenciamento de requisitos operacionais e de conformidade. Portanto, ao pensar em manter cópias e supervisionar a exclusão de arquivos, a política de retenção é sua amiga.

Pergunta nº 114

Você precisa criar uma política de prevenção de perda de dados (DLP).  
O que você deve usar?

1. o centro de conformidade do Microsoft 365
2. o centro de administração do Microsoft Endpoint Manager
3. o centro de administração do Microsoft 365
4. o portal do Microsoft 365 Defender

GPT-4o - Resposta

Absolutamente, ao configurar uma política de Prevenção de Perda de Dados (DLP) no Microsoft 365, seu destino deve ser o Microsoft 365 Compliance Center, agora conhecido como Microsoft Purview Compliance Portal. Esta plataforma lida especificamente com governança de dados e tarefas de conformidade, incluindo claramente a capacidade de configurar e gerenciar políticas de DLP de forma eficaz. É aqui que você pode criar, testar e ajustar suas configurações de DLP para garantir que os dados da sua organização estejam adequadamente protegidos de acordo com seus padrões de conformidade exigidos.

Pergunta nº 115

O que é uma avaliação no Compliance Manager?

1. Uma iniciativa política que inclui múltiplas políticas.
2. Um dicionário de palavras que não são permitidas em documentos da empresa.
3. Um agrupamento de controles de um regulamento, padrão ou política específica.
4. Orientações recomendadas para ajudar as organizações a se alinharem aos seus padrões corporativos.

GPT-4o - Resposta

No Compliance Manager, uma avaliação não é apenas uma coleta aleatória, mas uma organização meticulosa de controles derivados de regulamentações, padrões ou políticas específicas. Essa configuração é fundamental para avaliar sua conformidade com regulamentações críticas do setor e regionais. É tudo sobre usar modelos de avaliação como uma espinha dorsal, que incluem todos os controles necessários e ações de melhoria necessárias para uma avaliação completa da conformidade. Essa abordagem estruturada é particularmente crucial para ajudar as organizações a adaptar seus procedimentos operacionais e de conformidade para gerenciar e mitigar riscos de conformidade de forma eficaz.

Pergunta nº 116

O que você pode usar para visualizar o Microsoft Secure Score para dispositivos?

1. Microsoft Defender para aplicativos em nuvem
2. Microsoft Defender para Endpoint
3. Microsoft Defender para Identidade
4. Microsoft Defender para Office 365

GPT-4o - Resposta

O Microsoft Defender for Endpoint é a ferramenta correta para verificar o Secure Score para dispositivos. Esta plataforma fornece insights aprofundados sobre a postura de segurança do seu dispositivo por meio do painel de gerenciamento de vulnerabilidades no portal do Microsoft 365 Defender. É essencial entender que as avaliações de segurança do dispositivo são especificamente relevantes para endpoints, distinguindo esta função de outros serviços do Microsoft Defender, como aqueles para o Office 365 ou Identity.

Pergunta nº 120

Quais são as responsabilidades dos clientes ao avaliar a segurança em um modelo de serviços de nuvem de software como serviço (SaaS)?

1. sistemas operacionais
2. controles de rede
3. aplicações
4. contas e identidades

GPT-4o - Resposta

A resposta correta deveria ser D, com foco em contas e identidades. No modelo SaaS, esses elementos continuam sendo responsabilidade do cliente, pois estão diretamente relacionados ao gerenciamento de quais indivíduos têm acesso ao serviço e à proteção de suas credenciais. A operação e a manutenção de aplicativos, redes e infraestrutura de sistemas são normalmente gerenciadas pelo provedor SaaS. Portanto, a ênfase deve ser em garantir práticas robustas de gerenciamento de identidade e acesso pelos clientes.

Pergunta nº 123

O que o Acesso Condicional avalia usando a Proteção de Identidade do Azure Active Directory (Azure AD)?

1. ações do usuário
2. associação ao grupo
3. conformidade do dispositivo
4. risco do usuário

GPT-4o - Resposta

As avaliações de risco do usuário, de fato, são um componente essencial que o Azure AD Identity Protection usa em políticas de acesso condicional. O acesso condicional aproveita isso para analisar vários fatores de risco, como propriedades de login desconhecidas, credenciais vazadas e outros que são indicativos de atividades potencialmente maliciosas. Ao configurar o acesso condicional, é crucial pesar as condições de risco do usuário para ajudar a mitigar o acesso não autorizado de forma eficaz.

Pergunta nº 124

Qual afirmação representa um princípio de privacidade da Microsoft?

1. A Microsoft gerencia as configurações de privacidade de seus clientes.
2. A Microsoft respeita as leis de privacidade locais aplicáveis ​​aos seus clientes.
3. A Microsoft usa dados de e-mail e bate-papo de clientes hospedados para publicidade direcionada.
4. A Microsoft não coleta nenhum dado do cliente.

GPT-4o - Resposta

Da análise, a opção B não apenas se alinha com o compromisso público da Microsoft, mas também se alinha melhor com o que é descrito como práticas de privacidade da Microsoft. Em vez de gerenciar as configurações de privacidade em nome dos clientes, a Microsoft fornece ferramentas que capacitam os usuários a configurar suas próprias configurações, alinhando-se mais com a opção B sobre o respeito às leis de privacidade locais. Este esclarecimento destaca a ênfase na conformidade local e no empoderamento do usuário sobre o gerenciamento direto pela Microsoft. Seja sempre cauteloso e revise como a Microsoft descreve seu tratamento de privacidade diretamente de seus recursos.

Pergunta nº 127

Qual recurso de conformidade você deve usar para identificar documentos que são currículos de funcionários?

1. classificadores pré-treinados
2. Explorador de atividades
3. eDescoberta
4. Explorador de conteúdo

Pergunta nº 130

Qual pilar da identidade está relacionado ao rastreamento dos recursos acessados ​​por um usuário?

1. autorização
2. auditoria
3. administração
4. autenticação

Pergunta nº 131

O que pode ser criado nos Serviços de Domínio do Active Directory (AD DS)?

1. aplicações de linha de negócios (LOB) que exigem autenticação moderna
2. contas de computador
3. aplicativos de software como serviço (SaaS) que exigem autenticação moderna
4. dispositivos móveis

Pergunta nº 134

Qual é uma função dos controles de sessão de acesso condicional?

1. aplicando a conformidade do dispositivo
2. aplicando a conformidade do aplicativo cliente
3. permitir experiências limitadas, como bloquear o download de informações confidenciais
4. solicitando autenticação multifator (MFA)

Pergunta nº 136

O que você pode usar para garantir que todos os usuários em um grupo específico usem autenticação multifator (MFA) para entrar no Azure Active Directory (Azure AD)?

1. Política do Azure
2. uma política de conformidade de comunicação
3. uma política de acesso condicional
4. uma política de risco do usuário

Pergunta nº 138

Quais são os três métodos de autenticação que os usuários do Azure AD podem usar para redefinir suas senhas?

1. notificação de aplicativo móvel
2. mensagem de texto para um telefone
3. perguntas de segurança
4. certificado
5. senha da imagem

Pergunta nº 141

Qual recurso de segurança está disponível no modo gratuito do Microsoft Defender for Cloud?

1. alertas de proteção contra ameaças
2. acesso de VM just-in-time (JIT) às máquinas virtuais do Azure
3. varredura de vulnerabilidades de máquinas virtuais
4. pontuação segura

Pergunta nº 142

A prevenção contra perda de dados do Microsoft 365 Endpoint (Endpoint DLP) pode ser usada em quais sistemas operacionais?

1. Somente Windows 10 e mais recentes
2. Somente Windows 10 e mais recentes e Android
3. Somente Windows 10 e mais recentes e iOS
4. Windows 10 e mais recentes, Android e iOS

Pergunta nº 146

Qual é o número máximo de recursos que o Azure DDoS Protection Standard pode proteger sem custos adicionais?

1. 50
2. 100
3. 500
4. 1000

Pergunta nº 147

Quais são os dois motivos para implantar várias redes virtuais em vez de usar apenas uma rede virtual?

1. para atender às políticas de governança
2. para conectar vários tipos de recursos
3. separar os recursos para o orçamento
4. para isolar os recursos

Pergunta nº 149

Você tem uma assinatura do Azure que contém vários recursos.  
  
Você precisa avaliar a conformidade e impor padrões para os recursos existentes.  
  
O que você deve usar?

1. Projetos do Azure
2. o serviço Detector de Anomalias
3. Microsoft Sentinel
4. Política do Azure

Pergunta nº 150

Qual métrica do Microsoft Defender for Cloud exibe a integridade geral de segurança de uma assinatura do Azure?

1. pontuação segura
2. saúde dos recursos
3. controles concluídos
4. o status das recomendações

Pergunta nº 153

Você precisa garantir a repetibilidade ao criar novos recursos em uma assinatura do Azure.  
  
O que você deve usar?

1. Microsoft Sentinel
2. Política do Azure
3. Lote do Azure
4. Projetos do Azure

Pergunta nº 154

Qual é uma característica de um rótulo de sensibilidade no Microsoft 365?

1. criptografado
2. restrito a categorias predefinidas
3. persistente

Pergunta nº 163

O que você deve usar para associar a mesma identidade a mais de uma máquina virtual do Azure?

1. uma conta de usuário do Azure AD
2. uma identidade gerenciada atribuída pelo usuário
3. uma identidade gerenciada atribuída pelo sistema
4. um grupo de segurança do Azure AD

Pergunta nº 165

Quais três formas de verificação podem ser usadas com o Azure AD Multi-Factor Authentication (MFA)?

1. perguntas de segurança
2. o aplicativo Microsoft Authenticator
3. Mensagens SMS
4. um cartão inteligente
5. Windows Hello para empresas

Pergunta nº 167

A prevenção contra perda de dados do Microsoft 365 Endpoint (Endpoint DLP) pode ser usada em quais sistemas operacionais?

1. Somente Windows 10 e mais recentes
2. Somente Windows 10 e mais recentes e Android
3. Somente Windows 10 e mais recentes e macOS
4. Windows 10 e mais recentes, Android e macOS

Pergunta nº 168

Você tem uma assinatura do Azure que contém um espaço de trabalho do Log Analytics.  
  
Você precisa integrar o Microsoft Sentinel.  
  
O que você deve fazer primeiro?

1. Crie uma consulta de busca.
2. Correlacione alertas com incidentes.
3. Conecte-se às suas fontes de segurança.
4. Crie uma regra de detecção personalizada.

Pergunta nº 173

Você planeja mover recursos para a nuvem.  
  
Você está avaliando o uso de modelos de nuvem de Infraestrutura como serviço (IaaS), Plataforma como serviço (PaaS) e Software como serviço (SaaS).  
  
Você planeja gerenciar apenas os dados, contas de usuário e dispositivos de usuário para um aplicativo baseado em nuvem.  
  
Qual modelo de nuvem você usará?

1. SaaS
2. PaaS
3. IaaS

Pergunta nº 176

Qual pontuação mede o progresso de uma organização na conclusão de ações que ajudam a reduzir riscos associados à proteção de dados e aos padrões regulatórios?

1. Pontuação de adoção
2. Pontuação segura da Microsoft
3. Pontuação segura no Microsoft Defender para Nuvem
4. Pontuação de conformidade

Pergunta nº 180

Você tem uma assinatura do Azure.  
  
Você precisa implementar ativação de função com limite de tempo e baseada em aprovação.  
  
O que você deve usar?

1. acessar avaliações no Azure AD
2. Gerenciamento de Identidade Privilegiada (PIM) do Azure AD
3. Proteção de identidade do Azure AD
4. Acesso condicional no Azure AD

Pergunta nº 181

O que você deve usar no portal do Microsoft 365 Defender para visualizar tendências de segurança e rastrear o status de proteção de identidades?

1. Relatórios
2. Incidentes
3. Caça
4. Pontuação segura

Pergunta nº 185

Qual portal contém o catálogo de soluções?

1. Portal de conformidade do Microsoft Purview
2. Portal do Microsoft 365 Defender
3. Centro de administração do Microsoft 365
4. Centro de administração de aplicativos do Microsoft 365

Pergunta nº 189

Quando você habilita a Autenticação Multifator (MFA) do Azure AD, quantos fatores são necessários para autenticação?

1. 1
2. 2
3. 3
4. 4

Pergunta nº 195

Qual solução Microsoft Purview pode ser usada para identificar vazamento de dados?

1. gestão de risco interno
2. Gerente de conformidade
3. conformidade de comunicação
4. eDescoberta

Pergunta nº 197

Qual solução realiza avaliações de segurança e gera alertas automaticamente quando uma vulnerabilidade é encontrada?

1. gerenciamento de postura de segurança em nuvem (CSPM)
2. DevSecOps
3. plataforma de proteção de carga de trabalho em nuvem (CWPP)
4. gerenciamento de informações e eventos de segurança (SIEM)

Pergunta nº 198

O que você pode usar para se proteger contra links maliciosos enviados em mensagens de e-mail, mensagens de bate-papo e canais?

1. Microsoft Defender para aplicativos em nuvem
2. Microsoft Defender para Office 365
3. Microsoft Defender para Endpoint
4. Microsoft Defender para Identidade

Pergunta nº 201

Qual serviço inclui o Microsoft Secure Score para dispositivos?

1. Microsoft Defender para IoT
2. Microsoft Defender para Endpoint
3. Microsoft Defender para Identidade
4. Microsoft Defender para Office 365

Pergunta #202

Qual portal da Microsoft fornece informações sobre como os serviços de nuvem da Microsoft estão em conformidade com padrões regulatórios, como a Organização Internacional para Padronização (ISO)?

1. o centro de administração do Microsoft 365
2. Gerenciamento de custos do Azure + cobrança
3. Portal de confiança do serviço Microsoft
4. o portal de conformidade do Microsoft Purview

Pergunta #204

Você tem uma assinatura do Azure que contém um espaço de trabalho do Log Analytics.  
  
Você precisa integrar o Microsoft Sentinel.  
  
O que você deve fazer primeiro?

1. Crie uma consulta de busca.
2. Correlacione alertas com incidentes.
3. Conecte-se às suas fontes de dados.
4. Crie uma regra de detecção personalizada.

Pergunta #205

Para que é usado o Azure Key Vault?

1. para implantar um serviço de segurança de rede baseado em nuvem que proteja os recursos de rede virtual do Azure
2. para proteger aplicativos baseados em nuvem contra ameaças cibernéticas e vulnerabilidades
3. para proteger chaves criptográficas e outros segredos usados ​​por aplicativos e serviços em nuvem
4. para fornecer conectividade RDP/SSH segura e contínua para máquinas virtuais do Azure via TLS do portal do Azure

Pergunta #206

Quando um usuário se autentica usando o login sem senha, o que ele deve selecionar no aplicativo Microsoft Authenticator?

1. uma resposta a uma pergunta de segurança
2. Um número
3. uma chave alfanumérica
4. uma frase-senha

Pergunta #209

Qual recurso oferece suporte ao e-mail como método de autenticação de usuários?

1. Proteção de ID do Microsoft Entra
2. Autenticação multifator (MFA) do Microsoft Entra
3. redefinição de senha de autoatendimento (SSPR)
4. Proteção de senha do Microsoft Entra

Pergunta nº 210

Qual recurso do Microsoft Purview pode usar algoritmos de aprendizado de máquina para detectar e proteger automaticamente itens confidenciais?

1. eDescoberta
2. Prevenção de perda de dados
3. Riscos de informação
4. Conformidade de comunicação

Pergunta nº 213

Quais são as duas ações que você pode executar usando o Azure Key Vault?

1. Guarde segredos.
2. Armazene modelos do Azure Resource Manager (ARM).
3. Implementar grupos de segurança de rede (NSGs).
4. Implemente a proteção DDoS do Azure.
5. Guarde as chaves.

Pergunta nº 214

Qual recurso está incluído no Microsoft Entra ID Governance?

1. Proteção de Identidade
2. Gerenciamento de identidade privilegiada
3. Gerenciamento de permissões
4. Credenciais verificáveis

Pergunta nº 215

O que você deve criar para pesquisar e exportar conteúdo preservado em uma retenção de eDiscovery?

1. um site do Microsoft SharePoint Online
2. um caso
3. uma pasta pública do Microsoft Exchange Online
4. Arquivos do Azure

Pergunta nº 216

Qual tipo de classificação de dados do Microsoft Purview oferece suporte ao uso de expressões regulares?

1. correspondência exata de dados (EDM)
2. classificador de impressão digital
3. tipos de informações sensíveis (SITs)
4. classificador treinável

Pergunta nº 219

Quais dois tipos de dispositivos podem ser gerenciados usando a prevenção de perda de dados de endpoint (Endpoint DLP)?

1. Windows 11
2. Linux
3. iOS
4. Mac OS
5. Andróide