KA SOLUTION
WWW.KASOLUTION.COM.BR

Curso Oficial da Microsoft

Microsoft 365 Mobilidade e Segurança (MS-101)

Microsoft 365 Mobilidade e Segurança (MS-101)

O curso de Mobilidade e Segurança do Microsoft 365 foi desenvolvido para pessoas que aspiram à função de Administrador do Microsoft 365 Enterprise. Este curso abrange três elementos centrais da administração corporativa do Microsoft 365: gerenciamento de segurança do Microsoft 365, gerenciamento de conformidade do Microsoft 365 e gerenciamento de dispositivos do Microsoft 365.

No gerenciamento de segurança, você examinará todos os tipos comuns de vetores de ameaças e violações de dados, e como as soluções de segurança do Microsoft 365 lidam com essas ameaças de segurança. Essas soluções incluem: uso do modelo de segurança Zero Trust, Microsoft Secure Score, Azure Identity Protection, Exchange Online Protection, Microsoft Defender para Office 365, Privileged Identity Management, Safe Attachments, Safe Links e serviços de inteligência de ameaças, como treinamento de simulação de ataque, explorador de ameaças, rastreadores de ameaças, e proteção contra ameaças da Microsoft.

No gerenciamento de conformidade, você examinará os principais aspectos da governança de dados, incluindo gerenciamento de direitos de informação, criptografia de mensagens, prevenção de perda de dados (DLP), gerenciamento de registros in-loco, criação de políticas e dicas de política de DLP e proteção de informações do Azure e Windows. No gerenciamento de dispositivos do Microsoft 365, você aprenderá a cogerenciar seus dispositivos Windows 10, como fazer a transição do Configuration Manager para o Intune e como implementar o Windows Autopilot, o Windows Analytics e o Mobile Device Management.

Carga Horária: 5 dias / 10 noites.

Módulo 1: Explore as métricas de segurança no Microsoft 365

Neste caminho de aprendizado, você examinará todos os tipos comuns de vetores de ameaças e violações de dados enfrentados pelas organizações hoje e aprenderá como as soluções de segurança do Microsoft 365 abordam essas ameaças à segurança, incluindo a abordagem Zero Trust. Você será apresentado ao Microsoft Secure Score, Privileged Identity Management, bem como ao Azure Identity Protection e ao Microsoft Defender para Office 365.

Lições

- Examine vetores de ameaças e violações de dados
- Explore o modelo de segurança Zero Trust
- Explore as soluções de segurança no Microsoft 365
- Examinar a pontuação de segurança da Microsoft (Microsoft Secure Score)
- Examinar o gerenciamento de identidades privilegiadas
- Examinar a Proteção de Identidade do Azure

Laboratório: Configuração de locatário e gerenciamento de identidade privilegiada

- Inicialize seu locatário do Microsoft 365
- Fluxos de trabalho de recursos PIM

Após concluir este módulo, os alunos serão capazes de:

- Descrever várias técnicas que os hackers usam para comprometer contas de usuários por e-mail
- Descrever as técnicas que os hackers usam para obter controle sobre os recursos
- Descrever as técnicas que os hackers usam para comprometer dados
- Descreva a abordagem Zero Trust para segurança no Microsoft 365
- Descrever os componentes da segurança Zero Trust
- Descreva as cinco etapas para implementar um modelo Zero Trust em sua organização
- Explicara rede Zero Trust
- Listar os tipos de ameaças que podem ser evitadas usando o EOP e o Microsoft Defender para Office 365
- Descrever como o Microsoft 365 Threat Intelligence pode beneficiar sua organização
- Monitorar sua organização por meio de auditorias e alertas
- Descrever como o ASM melhora a visibilidade e o controle sobre seu locatário por meio de três áreas principais
- Descreva os benefícios do Secure Score e que tipo de serviços podem ser analisados
- Descrever como coletar dados usando a API Secure Score
- Saber onde identificar ações que aumentarão sua segurança mitigando riscos
- Explicar como determinar as ameaças que cada ação irá mitigar e o impacto que tem no uso
- Explicar o Privileged Identity Management (PIM) na administração do Azure
- Configurar o PIM para uso em sua organização
- Funções de auditoria do PIM
- Explicar o Microsoft Identity Manager
- Explicar o gerenciamento de acesso privilegiado no Microsoft 365
- Descrever o Azure Identity Protection e que tipo de identidades podem ser protegidas
- Entender como habilitar a Proteção de Identidade do Azure
- Saber identificar vulnerabilidades e eventos de risco
- Planejar sua investigação na proteção de identidades baseadas em nuvem
- Planejar como proteger seu ambiente do Azure Active Directory contra violações de segurança

Módulo 2: Gerenciar seus serviços de segurança do Microsoft 365

Este caminho de aprendizado examina como gerenciar os serviços de segurança do Microsoft 365, incluindo proteção do Exchange Online, Microsoft Defender para Office 365, anexos seguros e links seguros. Você também será apresentado aos vários relatórios que ajudam uma organização a monitorar sua integridade de segurança.

Lições

- Examinar a proteção do Exchange Online
- Examinar o Microsoft Defender para Office 365
- Gerenciar anexos seguros
- Gerenciar links seguros
- Explore os relatórios nos serviços de segurança do Microsoft 365

Laboratório: Gerenciar os Serviços de Segurança do Microsoft 365

- Implementar uma política de anexos seguros
- Implemente uma política de links seguros

Após concluir este módulo, os alunos serão capazes de:

- Descrever o pipeline antimalware à medida que o email é analisado pelo Exchange Online Protection
- Liste vários mecanismos usados para filtrar spam e malware
- Descrever soluções adicionais para proteção contra phishing e spoofing
- Descrever os benefícios do recurso Spoof Intelligence
- Descrever como o Safe Attachments é usado para bloquear malware de dia zero em anexos de e-mail e documentos
- Descrever como os links seguros protegem os usuários de URLs maliciosos incorporados em e-mails e documentos
- Criar e modificar uma política de Anexos Seguros no Centro de Conformidade e Segurança
- Criar uma política de anexos seguros usando o Windows PowerShell
- Configurar uma política de anexos seguros para realizar determinadas ações
- Entender como uma regra de transporte pode ser usada para desabilitar a funcionalidade de anexos seguros
- Descrever a experiência do usuário final quando um anexo de email é verificado e considerado malicioso
- Criar e modificar uma política de links seguros no centro de conformidade e segurança
- Criar uma política de links seguros usando o Windows PowerShell
- Entender como uma regra de transporte pode ser usada para desabilitar a funcionalidade de links seguros
- Descrever a experiência do usuário final quando o Safe Links identifica um link para um site ou arquivo malicioso
- Descrever como os relatórios de segurança do Microsoft 365 mostram como sua organização está sendo protegida
- Entender onde acessar os relatórios gerados pelo EOP e pelo Microsoft Defender para Office 365
- Entender como acessar informações detalhadas dos relatórios gerados

Módulo 3: Implementar inteligência de ameaças no Microsoft 365

Neste caminho de aprendizado, você fará a transição dos serviços de segurança para a inteligência de ameaças, especificamente, usando o Painel de Segurança, o Microsoft Defender for Identity e o Microsoft Cloud Application Security para ficar à frente de possíveis violações de segurança.

Lições

- Explore a inteligência de ameaças no Microsoft 365
- Explore o painel de segurança
- Implementar o Microsoft Defender for Identity
- Implementar a segurança de aplicativos em nuvem da Microsoft

Laboratório: Implementar inteligência de ameaças

- Conduza um ataque Spear Phishing usando o Attack Simulator
- Conduza ataques de senha usando o Attack Simulator
- Prepare-se para políticas de alerta
- Implementar um alerta de permissão de caixa de correio
- Implementar um alerta de permissão do SharePoint
- Testar o alerta de descoberta eletrônica padrão (Default eDiscovery Alert)

Após concluir este módulo, os alunos serão capazes de:

- Entender como a inteligência de ameaças é alimentada pelo Microsoft Intelligent Security Graph
- Descrever como o painel de ameaças pode beneficiar os agentes de segurança de nível C
- Entenda como o Threat Explorer pode ser usado para investigar ameaças e ajudar a proteger seu locatário
- Descrever como o Painel de Segurança exibe os principais riscos, tendências globais e qualidade da proteção
- Descrever o que é o Microsoft Defender for Identity e quais requisitos são necessários para implantá-lo
- Configurar o Microsoft Defender for Identity
- Gerenciar os serviços do Microsoft Defender for Identity
- Descrever a segurança do aplicativo em nuvem
- Explicar como implantar o Cloud App Security
- Controle seus aplicativos de nuvem com políticas
- Solucionar problemas de segurança de aplicativos em nuvem

Módulo 4: Introdução à governança de dados no Microsoft 365

Este caminho de aprendizado examina os principais componentes do gerenciamento de conformidade do Microsoft 365. Isso começa com uma visão geral de todos os principais aspectos da governança de dados, incluindo arquivamento e retenção de dados, gerenciamento de direitos de informação, criptografia de mensagens do Office 365, gerenciamento de registros in-loco no SharePoint e prevenção de perda de dados (DLP).

Lições

- Explore o arquivamento no Microsoft 365
- Explore a retenção no Microsoft 365
- Explore o gerenciamento de direitos de informação
- Explore a criptografia de mensagens do Office 365
- Explore o gerenciamento de registros in-loco no SharePoint
- Explore a prevenção contra perda de dados no Microsoft 365
- Laboratório: Implementar Governança de Dados
- Configurar a criptografia de mensagens do Microsoft 365
- Validar o Gerenciamento de Direitos de Informação
- Inicializar a conformidade
- Configurar tags e políticas de retenção

Após concluir este módulo, os alunos serão capazes de:

- Entender a governança de dados no Microsoft 365
- Descrever a diferença entre o arquivamento in-loco e o gerenciamento de registros
- Explicar como os dados são arquivados no Exchange
- Reconhecer os benefícios do Gerenciamento de Registros In-loco no SharePoint
- Entender como o Gerenciamento de Registros de Mensagens funciona no Exchange
- Listar os tipos de marcas de retenção que podem ser aplicadas a caixas de correio
- Conhecer as diferentes opções de criptografia do Microsoft 365
- Entender como o Gerenciamento de Direitos de Informação (IRM) pode ser usado no Exchange
- Configurar a proteção de IRM para e-mails do Exchange
- Explicar como o IRM pode ser usado no SharePoint
- Aplique a proteção IRM a documentos do SharePoint
- Explicar as diferenças entre a proteção IRM e a classificação AIP
- Entender como funciona a criptografia de mensagens
- Executar criptografia em uma mensagem
- Realizar a descriptografia de uma mensagem
- Entender a cooperação de assinatura e criptografia simultaneamente
- Explicar o que são mensagens triplas
- Descrever quando você pode usar a criptografia de mensagens do Office 365
- Explicar como funciona a criptografia de mensagens do Office 365
- Descrever a prevenção contra perda de dados (DLP)
- Entender quais são as informações confidenciais e os padrões de pesquisa que o DLP está usando
- Saber o que é uma política de DLP e o que ela contém
- Reconhecer como as ações e condições funcionam juntas para DLP
- Expressar como as ações contêm funções para enviar e-mails nas partidas
- Mostrar dicas de política para os usuários se uma regra de DLP se aplicar
- Use modelos de política para implementar políticas de DLP para informações comumente usadas
- Explicar o dedo do documento
- Entender como usar o DLP para proteger documentos no Windows Server FCI

Módulo 5: Implementar a governança de dados no Microsoft 365

Este caminho de aprendizado examina como implementar os principais aspectos da governança de dados, incluindo a construção de barreiras de informações no Microsoft 365 e paredes éticas no Exchange Online, criando políticas DLP de modelos internos, políticas DLP personalizadas, políticas DLP para proteger documentos e dicas de política.

Lições

- Avalie sua prontidão de conformidade
- Implemente soluções de conformidade
- Criar barreiras de informação no Microsoft 365
- Criar uma política de DLP a partir de um modelo integrado
- Criar uma política de DLP personalizada
- Crie uma política de DLP para proteger documentos
- Implementar dicas de política para políticas de DLP

Laboratório: Implementar políticas de DLP

- Gerenciar políticas de DLP
- Teste as políticas de MRM e DLP

Após concluir este módulo, os alunos serão capazes de:

- Descrever o Centro de Conformidade do Microsoft 365 e como acessá-lo
- Descrever a finalidade e a função da pontuação de Conformidade
- Explicar os componentes de como a pontuação de conformidade de uma organização é determinada
- Explicar como as avaliações são usadas para formular pontuações de conformidade
- Explicar como o Microsoft 365 ajuda a abordar o Regulamento Global de Proteção de Dados
- Descrever a funcionalidade de gerenciamento de risco do insider no Microsoft 365
- Configurar políticas de gerenciamento de risco interno
- Configurar políticas de gerenciamento de risco interno
- Explicar os recursos de conformidade de comunicação no Microsoft 365
- Descrever o que é um muro ético no Exchange e como ele funciona
- Explicar como criar barreiras de informação no Microsoft 365
- Identificar as melhores práticas para construir e trabalhar com muros éticos
- Entender os diferentes modelos integrados para políticas de DLP
- Determinar como escolher os locais corretos para uma política de DLP
- Configure as regras corretas para proteger o conteúdo
- Habilitar e revisar a política de DLP corretamente
- Descrever como modificar as regras existentes das políticas de DLP
- Explicar como adicionar e modificar condições e ações personalizadas a uma regra DLP
- Descrever como alterar as notificações do usuário e dicas de política
- Configurar a opção de substituição do usuário para uma regra DLP
- Explicar como os relatórios de incidentes são enviados por uma violação de regra DLP
- Descrever como trabalhar com propriedades gerenciadas para políticas de DLP
- Explicar como o SharePoint Online cria propriedades rastreadas de documentos
- Descrever como criar uma propriedade gerenciada de uma propriedade rastreada no SharePoint Online
- Explicar como criar uma política DLP com regras que se aplicam a propriedades gerenciadas por meio do PowerShell
- Descrever a experiência do usuário quando um usuário cria um e-mail ou site contendo informações confidenciais

- Explicar o comportamento nos aplicativos do Office quando um usuário insere informações confidenciais

Módulo 6: Gerenciar a governança de dados no Microsoft 365

Este caminho de aprendizado se concentra no gerenciamento de governança de dados no Microsoft 365, incluindo gerenciamento de retenção em e-mail, solução de problemas de políticas de retenção e dicas de política que falham, bem como solução de problemas de dados confidenciais. Em seguida, você aprenderá a implementar rótulos de confidencialidade e a Proteção de Informações do Windows.

Lições

- Gerenciar a retenção no e-mail
- Solucionar problemas de governança de dados
- Explorar rótulos de sensibilidade
- Implementar rótulos de sensibilidade
- Implementar a governança de dados

Laboratório: Implementar Governança de Dados

- Implementar rótulos de sensibilidade
- Implementar a proteção de informações do Windows

Após concluir este módulo, os alunos serão capazes de:

- Determinar quando e como usar marcas de retenção em caixas de correio
- Atribuir política de retenção a uma pasta de e-mail
- Adicione políticas de retenção opcionais a mensagens de e-mail e pastas
- Remover uma política de retenção de uma mensagem de e-mail
- Explicar como a idade de retenção dos elementos é calculada
- Reparar as políticas de retenção que não são executadas conforme o esperado
- Entender como solucionar problemas sistematicamente quando uma política de retenção parece falhar
- Executar testes de política no modo de teste com dicas de política
- Descrever como monitorar as políticas de DLP por meio do rastreamento de mensagens
- Gerenciar a proteção de dados usando rótulos de confidencialidade
- Descrever os requisitos para criar um rótulo de confidencialidade
- Desenvolver uma estrutura de classificação de dados para seus rótulos de confidencialidade
- Criar, publicar e remover rótulos de confidencialidade
- Descrever o WIP e para que ele é usado
- Planejar uma implantação de políticas WIP
- Implementar políticas de WIP com o Intune e o SCCM
- Implementar políticas de WIP em aplicativos de área de trabalho do Windows

Módulo 7: Gerenciar pesquisas e investigações de conteúdo no Microsoft 365

Este caminho de aprendizado conclui esta seção sobre governança de dados examinando como gerenciar pesquisa e investigação, incluindo pesquisa de conteúdo no Centro de Conformidade e Segurança, auditoria de investigações de log e gerenciamento de descoberta eletrônica avançada.

Lições

- Pesquise conteúdo no centro de conformidade do Microsoft 365
- Conduzir investigações de log de auditoria
- Gerenciar descoberta eletrônica avançada

Laboratório: Gerenciar pesquisa e investigações

- Faça uma pesquisa de dados
- Investigue seus dados do Microsoft 365

Após concluir este módulo, os alunos serão capazes de:

- Descrever como usar a pesquisa de conteúdo
- Projetar sua pesquisa de conteúdo
- Configurar filtragem de permissão de pesquisa
- Explicar como pesquisar dados de terceiros
- Descrever quando usar scripts para pesquisas avançadas
- Descrever o que é o log de auditoria e as permissões necessárias para pesquisar uma auditoria do Microsoft 365
- Configurar políticas de auditoria
- Inserir critérios para pesquisar o log de auditoria
- Visualizar, classificar e filtrar resultados de pesquisa
- Exportar resultados de pesquisa para um arquivo CSV
- Pesquisar o log de auditoria unificado usando o Windows PowerShell
- Descrever a descoberta eletrônica avançada
- Configurar permissões para usuários na descoberta eletrônica avançada
- Criar casos na descoberta eletrônica avançada
- Pesquisar e prepare dados para descoberta eletrônica avançada

Módulo 8: Prepare-se para o gerenciamento de dispositivos no Microsoft 365

Este caminho de aprendizado fornece um exame aprofundado do gerenciamento de dispositivos do Microsoft 365. Você começará planejando vários aspectos do gerenciamento de dispositivos, incluindo a preparação de seus dispositivos Windows 10 para cogerenciamento. Você aprenderá como fazer a transição do Configuration Manager para o Microsoft Intune e será apresentado à Microsoft Store for Business e ao Mobile Application Management.

Lições

- Explore o cogerenciamento do dispositivo Windows 10
- Prepare seus dispositivos Windows 10 para cogerenciamento
- Transição do Configuration Manager para o Intune
- Examine a Microsoft Store for Business
- Planeje o gerenciamento de aplicativos

Laboratório: Implementar a Microsoft Store for Business

- Configurar a Microsoft Store for Business
- Gerenciar a Microsoft Store for Business

Após concluir este módulo, os alunos serão capazes de:

- Descreva os benefícios da cogestão
- Planeje a estratégia de cogestão da sua organização
- Descrever os principais recursos do Configuration Manager
- Descrever como o Azure Active Directory permite o cogerenciamento
- Identifique os pré-requisitos para usar o cogerenciamento
- Configurar o Configuration Manager para cogerenciamento
- Registrar dispositivos Windows 10 no Intune
- Transferir cargas de trabalho para o Intune
- Monitore sua solução de cogestão
- Verifique a conformidade para dispositivos cogerenciados
- Descrever o recurso e os benefícios da Microsoft Store for Business
- Configurar a Microsoft Store for Business
- Gerenciar configurações da Microsoft Store for Business

Módulo 9: Planeje sua estratégia de implantação do Windows 10

Este caminho de aprendizado se concentra no planejamento de sua estratégia de implantação do Windows 10, incluindo como implementar o Windows Autopilot e o Desktop Analytics e o planejamento do serviço de ativação de assinatura do Windows 10.

Lições

- Examine os cenários de implantação do Windows 10
- Explore os modelos de implantação do Windows Autopilot
- Planeje sua estratégia de ativação de assinatura do Windows 10
- Resolver erros de atualização do Windows 10
- Analisar dados de diagnóstico do Windows 10 usando o Desktop Analytics

Após concluir este módulo, os alunos serão capazes de:

- Planejar o Windows como um serviço
- Planeje uma implantação moderna
- Planejar uma implantação dinâmica
- Planeje uma implantação tradicional
- Descrever os requisitos do piloto automático do Windows
- Configurar piloto automático
- Descrever as implantações automáticas do piloto automático, implantações pré-provisionadas e implantações orientadas pelo usuário
- Implantar a criptografia BitLocker para dispositivos com piloto automático
- Entender o Windows 10 Enterprise E3 no CSP
- Configurar VDA para ativação de assinatura
- Implantar licenças do Windows 10 Enterprise
- Descrever correções comuns para erros de atualização do Windows 10
- Usar SetupDiag
- Solucionar erros de atualização
- Descrever o relatório de erros do Windows
- Compreender os códigos de erro de atualização e o procedimento de resolução
- Descrever a análise da área de trabalho
- Descrever a integridade do dispositivo
- Descrever a conformidade da atualização

Módulo 10: Implementar o Gerenciamento de Dispositivos Móveis no Microsoft 365

Este caminho de aprendizado se concentra no gerenciamento de dispositivos móveis (MDM). Você aprenderá como implantá-lo, como registrar dispositivos no MDM e como gerenciar a conformidade do dispositivo.

Lições

- Explorar o gerenciamento de dispositivos móveis
- Implantar o gerenciamento de dispositivos móveis
- Inscrever dispositivos no Gerenciamento de dispositivos móveis
- Gerenciar a conformidade do dispositivo

Laboratório: Gerenciar dispositivos com o Intune

- Ative o gerenciamento de dispositivos
- Configurar o Azure AD para Intune
- Criar políticas do Intune
- Registrar um dispositivo Windows 10
- Gerenciar e monitorar um dispositivo no Intune

Após concluir este módulo, os alunos serão capazes de:

- Gerenciar dispositivos com MDM
- Comparar MDM para Microsoft 365 e Intune
- Compreender as configurações de política para dispositivos móveis
- Controlar e-mail e acesso a documentos
- Ativar serviços de gerenciamento de dispositivos móveis
- Implantar o gerenciamento de dispositivos móveis
- Configurar domínios para MDM
- Configurar um certificado APNs para dispositivos iOS
- Gerenciar políticas de segurança do dispositivo
- Definir uma política de registro de dispositivo corporativo
- Registrar dispositivos no MDM
- Entender o Programa de registro de dispositivos Apple
- Entender as regras de inscrição
- Configurar uma função de gerenciador de registro de dispositivo
- Descrever as considerações de autenticação multifator
- Planejar a conformidade do dispositivo
- Configurar usuários e grupos condicionais
- Criar políticas de acesso condicional
- Monitorar dispositivos registrados