ANEXO I – TERMO DE REFERÊNCIA E SEU ANEXO

TERMO DE REFERÊNCIA

INTRODUÇÃO

O presente Termo de Referência tem por objetivo descrever os elementos necessários e suficientes, com nível de precisão adequado, para subsidiar o processo licitatório, demonstrando sua viabilidade e conveniência. Seu conteúdo dependerá da natureza da solução a ser licitada, sendo mais complexo e minucioso na medida em que a contratação assim exigir. Ele será elaborado com base nas informações constantes do Estudo Técnico preliminar.

1 - OBJETO DA CONTRATAÇÃO

1.1 Contratação de empresa especializada em fornecimento de Licenças Microsoft na modalidade Enterprise Agreement (EA), com suporte, implantação, consultoria e treinamento.

2 - JUSTIFICATIVA E FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1 JUSTIFICATIVA DA NECESSIDADE

1. O CREA-SP, órgão da administração pública indireta, cujo dever legal, além da sua obrigação, em razão de lei, de Órgão de Fiscalização, implica em cumprir e fazer cumprir as Leis e Resoluções baixadas pelo CONFEA, bem como a legislação geralvigente que rege as relações dos componentes da Administração Pública Direta e Indireta. Portanto, os serviços prestados peloConselho é fundamental para a salvaguarda da sociedade, necessitando assim, armazenar e trabalhar com dados de múltiplos entes, sejam eles profissionais do sistema, empresas, e da população em geral. Dentre esses dados, o CREA-SP emite Anotações de Responsabilidade Técnicas para cada obra executada pelos Engenheiros e Empresas cadastrados.

2. Para atender todas as necessidades de comunicação necessárias e inerentes à sua prestação de serviços à Sociedade, o CREA-SP atualmente utiliza os serviços de colaboração da Microsoft através do pacote Office 365, o qual fornece e-mail, drivevirtual na nuvem da Microsoft e colaboração através do aplicativo Teams.

3. O CREA-SP também possui diversos outros produtos da Microsoft, a saber, o Banco de Dados SQL Server, ServidoresWindows, Active Directory e Servidor de e-mail Exchange.

4. Há também que ser observada a questão da Lei Geral de Proteção de Dados (LGPD).

5. A LGPD foi criada em 2018 entrando em vigor através da Lei 13.709 no o intuito de proteger dados pessoais em semelhançaa RGPD (Regulamento Geral sobre a Proteção de Dados) em vigor na União Europeia desde 2016.

6. No contexto da necessidade de aderência por parte do CREA-SP à LGPD, recebemos **solicitações e recomendações doData Protection Officer (DPO)** do CREA-SP.

7. Baseados na necessidade de adequar o CREA-SP às recomendações necessárias para atender aos requisitos da LGPDelencados nas recomendações recebidas do DPO, o CREA-SP, através desta contratação irá realizar a implementação de políticas e ferramentas que garantam adequação do gerenciamento de informações ao tripé da segurança da informação: confidencialidade, integridade e disponibilidade.

8. A confidencialidade é a propriedade da informação que pretende garantir o acesso unicamente às pessoas autorizadas.

9. A integridade assegura que os dados mantenham suas características originais, tais como foram definidas no momento emque foram criados. A informação, assim, fica protegida contra a alteração não autorizada.

10. A disponibilidade garante que as informações estejam à disposição de gestores e colaboradores para consulta a qualquermomento, assegurando sua acessibilidade.

11. Com o advento da LGPD e também do trabalho remoto (tele trabalho) que cresceu com a pandemia do Covid-19, surgiu a necessidade do CREA-SP gerenciar os dispositivos que os funcionários usam para realizar seus trabalhos diários. Esses dispositivos, quer sejam computadores, aparelhos celulares, notebooks ou *tablets* estão agora distribuídos, nas residências dosfuncionários ou em qualquer lugar onde eles estejam trabalhando, ambientes no qual a equipe de T.I. não exerce controle.

12. Levando em conta esse novo cenário, há necessidade de implantar ferramentas e processos que possam permitir que otele trabalho seja utilizado dentro dos padrões dos três pilares da segurança definidos acima, com os seguintes recursosmínimos:

a) Gerenciamento de Dispositivos Remotos (Celulares e Notebooks)
b) Segurança de Login
c) Controle do acesso privilegiado
d) Segurança contra perda de Dados
e) Segurança de proteção de dados e Criptografia

13. Esta contratação justifica-se na necessidade de:

a) Renovar as licenças já de posse do CREA-SP para seus produtos da Microsoft que estão sem suporte como osservidores Windows, Banco de Dados SQL Server e acesso ao DevOps. Aquisição necessária para realizar a satuializações de segurança, receber as novas versões e o suporte necessário da Microsoft.
b) Contratar serviços online para colaboração de e-mail, drive virtual na Nuvem, Teams e Office.
c) Implantar de ferramentas de segurança elencadas no parágrafo anterior.
d) Adquirir os serviços necessários para implantar todos os recursos de segurança adquiridos .
e) Realizar o treinamento dos usuários e da equipe de sustentação na utilização correta e eficaz dos recursosadquiridos.

2.2 JUSTIFICATIVAS ESPECÍFICAS

1. Justificativa da necessidade de Licenças para os Conselheiros

1.1 Foi realizado levantamento junto à SUPCOL (Superintendência dos Colegiados) do CREA-SP.
Neste levantamento ficou determinado que os Conselheiros necessitam utilizar os aplicativos do Office (Word, Excel, etc.) e que os mesmos fazem uso dos computadores do CREA-SP, com esses aplicativos, para realizar trabalhos inerentes ao seu cargo.

2. Justificativa da necessidade de Reserva Técnica para licenças do Pacote Office 365

2.1 Licenças reservadas para contratações de novos colaboradores ou terceiros, que deve ocorrer por meio aquisição prévia, ao invés de aditivo contratual com acréscimo de quantitativo, pois as referidas contratações decorrem de necessidades dinâmicas, e não é possível mensurar com previsibilidade razoável que possa tempestivamente serem satisfeitas mediante procedimento de aditivo contratual sob pena de prejudicar o andamento das atividades institucionais e a satisfação do interessepúblico.

3. Justificativa da Necessidade de integrar o sistema de Telefonia VoIP

3.1. Com o Advento da Pandemia de Covid 19, o Teams passou a ser a ferramenta oficial de comunicação do CREA-SP,apesar da mesma não ter interligação com o sistema telefônico do CREA.
3.2. Em razão do ocorrido a ferramenta Teams passou a ser utilizada nas rotinas das atividades das Unidades do Conselho,portanto, se faz necessário a integração da ferramenta com o Sistema requerido, visando possibilitar que sejam as ligações entre o Teams e os ramais internos e também do Teams diretamente para celulares e telefones Fixos, e vice-versa, sejam realizadas, trazendo diversos benefícios relacionados a efetividade e eficiência das comunicações e consequentemente melhores resultados na prestação de serviços oferecidos pelo CREA-SP aos profissionais e empresas registrados.

4. Justificativa da Necessidade de Treinamento dos usuários

4.1. O CREA-SP tem que atender ao disposto na LGPD, conforme já mencionado anteriormente. Portanto, para atender aoDPO (**Data Protection Officer),** a Gerência do DOP do CREA-SP apresentou diversas solicitações e recomendações referentes a segurança da informação. Muitas dessas recomendações estão contempladas no treinamento dos usuários.
4.2. Além das recomendações, é consenso no meio da segurança de informação que o elo mais fraco na corrente da Segurança é o usuário. De nada adianta ter um sistema amplamente tecnológico, com centenas de recursos de segurança, seo usuário não estiver treinado para utilizá-los corretamente.
4.3. É preciso incutir na mentalidade do colaborador a necessidade de estar sempre atento às boas práticas e políticas desegurança.
Dito isso, se justifica a realização da capacitação dos usuários através de workshops relacionados aos aplicativos de segurançae melhores práticas relacionados ao pacote Microsoft 365 (objeto desta contratação)

3 - DESCRIÇÃO DA SOLUÇÃO

3.1 DESCRIÇÃO GERAL DA SOLUÇÃO

1. A Solução é composta pela aquisição de Licenças e Serviços conforme abaixo:

3.1.1 DESCRIÇÃO DAS LICENÇAS E DOS PRODUTOS

1. A aquisição de licenças visa suprir as seguintes necessidades:

a) Aquisição de Licenças para os produtos online do pacote Microsoft 365.
b) Aquisição de Licenças para os produtos da Microsoft que o CREA-SP utiliza em seu backoffice (Servidores, Bancode Dados, Desenvolvimento, etc.)

2. De acordo com a Tabela A, o CREA-SP irá adquirir licenças para utilização dos seguintes produtos:

Item	Descrição
1	Licenças de Microsoft 365 E3
2	Licenças de Microsoft 365 E5
3	Licenças Exchange online - Plano 1
4	Licenças Microsoft EMS + Security E3
5	Windows Server Standard Core
6	Windows Server DC Core
7	Windows Remote Desktop Services - Device CAL
8	SQL Server Enterprise Core

9	Visual Studio Pro
10	Visual Studio Enterprise
11	Azure DevOps Server. User CAL
12	Microsoft Visio Professional
13	Licença Microsoft Phone System - Add on

Tabela A - Lista dos produtos objeto de aquisição de Licenças

3. Segue abaixo a descrição detalhada de cada um deles:

3.1.1.1 Itens 1 e 2 da Tabela A - Microsoft 365 E3 e Microsoft 365 E5

1. Trata-se do ambiente colaboração dos usuários do CREA-SP, pacote de aplicativos de escritório (Word, Excel, PowerPoint), Videoconferência (Microsoft Teams), funcionalidades Mobile e pacote de segurança.

2. Itens do licenciamento E3 e E5

CATEGORIA	DESCRIÇÃO	E3	E5
Windows 10	Windows 10 Enterprise	✓	✓
	Microsoft Defender para Ponto de Extremidade		✓
Enterprise Mobility + Security	Azure Active Directory Premium Plano 1	✓	✓
	Azure Active Directory Premium Plano 2		✓
	Microsoft Defender para Identidade		✓
	Proteção de Informações do Azure Plano 1	✓	✓
	Proteção de Informações do Azure Plano 2		✓
	Azure Rights Management	✓	✓
	Cloud App Security Discovery	✓	✓
	Autenticação Multifator do Microsoft Azure	✓	✓
	Microsoft Intune	✓	✓
Microsoft 365 Apps	Microsoft 365 Apps para Grandes Empresas	✓	✓
Office 365*	Office para a Web	✓	✓
	Aplicativos Móveis para o Office 365	✓	✓
	Exchange Online Plano 2	✓	✓
	Exchange Kiosk		
	Proteção do Exchange Online	✓	✓
	Descoberta Eletrônica Avançada do Office 365		✓
	Conformidade Avançada do Office 365		✓
	Prevenção Contra Perda de Dados do Office 365	✓	✓
	Prevenção Contra Perda de Dados de Comunicação(Teams)		✓
	SharePoint Online Plano 2	✓	✓
	SharePoint Online Kiosk		
	Microsoft Teams	✓	✓

Skype for Business OnlinePlano 2	✓	✓
Skype for Business OnlinePlano 1	✓	✓
Audioconferência		✓
Sistemas de Telefonia		✓
Gerenciamento de Dispositivo Móvel do Office 365	✓	✓
Microsoft Defender para Office 365 Plano 1		✓
Microsoft Defender para Office 365 Plano 2		✓
Microsoft Cloud App Security		✓
Office 365 Privileged Access Management		✓
Microsoft Forms	✓	✓
Microsoft KaizalaPro	✓	✓
Microsoft MyAnalytics	✓	✓
Microsoft Planner	✓	✓
Microsoft StaffHub	✓	✓
Microsoft Stream para Office 365 para Trabalhadores deLinha de Frente	✓	✓
Microsoft Stream para Office 365 para E3	✓	✓
Microsoft Stream para Office 365 para E5		✓
Power BI Pro		✓
PowerApps para o Office 365	✓	✓

Power Automate para Office 365	✓	✓
Sway	✓	✓
To-Do	✓	✓
Yammer Enterprise	✓	✓

Tabela - Itens do licenciamento E3 e E5

3.1.1.2 Item 3 da Tabela A - Exchange online - plano 1

1. Trata-se de e-mail corporativo seguro e confiável com uma caixa de correio de 50 GB por usuário.

2. Cada usuário recebe 50 GB de armazenamento na caixa de correio e pode enviar mensagens de até 150 MB.
3. Os usuários podem conectar versões compatíveis do Outlook ao Exchange Online para continuar usando os aplicativoscliente avançados que já conhecem.
4. No caso do acesso para cliente Web, o Outlook na Web oferece uma experiência premium baseada em navegador, quecorresponde à aparência do cliente completo do Outlook.
5. A Caixa de Entrada Destaques facilita o rastreamento dos emails mais importantes. A Caixa de Entrada inclui duas guias:Destaques (para os emails nos quais você precisa atuar imediatamente) e Outros (para os emails restantes). Sempre que desejar, você pode alternar entre as guias e conferir o fluxo de emails na guia Outros.
6. Compara calendários para agendar reuniões e acessar recursos de colaboração, como calendários compartilhados,grupos, lista de endereços global, contatos externos, tarefas, salas de conferência e delegação
7. Todas as caixas de correio contam com proteção premier antimalware e antispam por meio da Proteção do ExchangeOnline.
8. Mantem a Caixa de Entrada limpa movendo automaticamente mensagens antigas para um Arquivo Morto no Local.

3.1.1.3 Item 4 da Tabela A - Enterprise Mobility + Security E3

1. O Microsoft Enterprise Mobility + Security fornece uma solução de segurança orientada por identidade que oferece umaabordagem holística aos desafios de segurança nessa era de foco em dispositivos móveis e na nuvem.

2. O **Enterprise Mobility + Security E3** inclui:

a) Azure Active Directory Premium P1
b) Microsoft Intune
c) Proteção de Informações do Azure P1
d) Microsoft Advanced Threat Analytics
e) Azure Rights Management (parte da Proteção de Informações do Azure)
f) Direitos de CAL do Windows Server

3.1.1.4 Item 5 da Tabela A - Windows Server Standard Core

1. O Windows Server é o sistema operacional para servidores da Microsoft.
2. A licença de Windows Server Standard é ideal para Servidores não virtualizados.

3.1.1.5 Item 6 da Tabela A - Windows Server Core DC (Datacenter)

1. O Windows Server é o sistema operacional para servidores da Microsoft.
2. A licença de Windows Datacenter Server Core DC é adequada para ambientes virtualizados, pois cada licença atende adois núcleos do processador que hospeda o sistema operacional virtualizado.

3. O licenciamento de Windows Datacenter é baseado em processadores físicos. Cada licença de software abrange 2processadores físicos.

3.1.1.6 Item 7 da Tabela A - Windows Remote Desktop Services

1. Os Serviços de Área de Trabalho Remota (RDS) são a plataforma de escolha para a construção de soluções de virtualização para cada necessidade do cliente final, incluindo o fornecimento de aplicativos virtualizados individuais, fornecendo acesso móvel e remoto à área de trabalho segura e fornecendo aos usuários finais a capacidade de executarseus aplicativos e desktops a partir da nuvem.

3.1.1.7 Item 8 da Tabela A - SQL Server Enterprise Core

1. Gerenciador de Banco de Dados para aplicações transacionais e Analíticas, possuindo componentes nativos para desenvolvimento de uma plataforma completa de Data Warehouse e Business Intelligence (ETL, Data Quality, OLAP eReporting).
2. A Edição Enterprise é ideal para aplicativos que exigem desempenho de missão crítica em memória, segurança e alta disponibilidade m ambiente de Datacenter (virtualizado).

3.1.1.8 Item 9 da Tabela A- Visual Studio Pro

1. O Visual Studio Professional é uma solução integrada e de ponta a ponta. Ambiente de desenvolvimento integrado avançado que dispõe de ferramentas de suporte, serviços e benefícios. Produtividade, DevOps, ferramentas de testesmanuais e automatizados, treinamento, créditos de Azure e benefícios da assinatura MSDN. Licença com extensões incluídas da Microsoft para Visual Studio Team Foundation Server e Visual Studio Team Services.

3.1.1.9 Item 10 da Tabela A - Visual Studio Enterprise

1. Ambiente de desenvolvimento de software profissional, como descrito no Visual Studio Pro, com colaboração em equipe.
2. O licenciamento Enterprise é uma solução de nível empresarial com recursos avançados para equipes que trabalham emprojetos de qualquer tamanho ou complexidade, incluindo testes avançados e DevOps.

3.1.1.10 Item 11 da TAbela A - Azure DevOps Server. User CAL

1. Anteriormente conhecido como Team Foundation Server (TFS), o Azure DevOps Server é um conjunto de ferramentas de desenvolvimento de software colaborativo, hospedado no local.
2. O Azure DevOps Server se integra ao seu IDE ou editor existente, permitindo que sua equipe multifuncional trabalhe demaneira eficaz em projetos de todos os tamanhos.

3.1.1.11 Item 12 da Tabela A - Microsoft Visio Professional

1. O Microsoft Office Visio Professional é um aplicativo de diagramação que ajuda a documentar, projetar, comunicar e automatizar ideias, processos e sistemas complexos para que você possa tomar medidas mais eficazes.
2. Possui Recursos projetados para facilitar a criação de diagramas, incluindo:

a) acesso mais rápido a ferramentas usadas com frequência, formas e estênceis novos e atualizados e temas eefeitos aprimorados e expandidos.
b) Ferramentas para tornar o trabalho em equipe mais simples, como a capacidade de trabalhar juntos no mesmodiagrama ao mesmo tempo e comentários aprimorados no Visio e nos Serviços do Visio.
c) Suporte de toque aprimorado, incluindo para Windows 8 e Visio Services no novo Microsoft SharePoint.
d) Opções para tornar seus diagramas mais dinâmicos vinculando formas a dados em tempo real, com um conjuntoexpandido de fontes suportadas.
e) A capacidade de compartilhar seus diagramas com outras pessoas por meio de um navegador (mesmo se elesnão tiverem o Visio instalado) por meio do Microsoft Office 365 ou do SharePoint.

f) Suporte para padrões de diagramação atualizados, incluindo Unified Modeling Language (UML) 2.4, BusinessProcess Model and Notation (BPMN) 2.0 e Windows Workflow Foundation 4.0.

3.1.1.12 Item 13 da Tabela A - Microsoft Phone System (add-on)

1. O Sistema de Telefonia (Phone System) habilita os recursos de controle de chamada e PBX na nuvem com MicrosoftTeams e Skype for Business Online.
2. Com Sistema de Telefonia, os usuários podem usar o Teams ou Skype for Business Online para fazer e receberchamadas, transferir chamadas e mudos ou chamadas não intermediados.
3. Com o Sistema de Telefonia os usuários podem clicar em um nome no seu livro de endereços e fazer chamadas Teamsou Skype for Business Online para essa pessoa.
4. Para fazer e receber chamadas, Sistema de Telefonia usuários podem usar seus dispositivos móveis, um fone de ouvidocom um laptop ou computador ou um dos muitos telefones IP que funcionam com Teams e Skype for Business Online.

3.1.2 DESCRIÇÃO DOS SERVIÇOS

1. Os serviços contratados serão os necessários para a implantação dos diversos itens de configuração para adequar oCREA aos parâmetros mínimos de segurança dos aplicativos da Microsoft Utilizados. A aquisição de serviços está divididaem três modalidades:

a) Aquisição de Serviços de Instalação, migração e Implantação dos features adquiridos através das Licenças doPacote Microsoft 365.
b) Aquisição de Serviços sob demanda para a configuração e implantação de Novos Features durante a vigência doContrato.
c) Aquisição de Serviços de capacitação da equipe de sustentação e dos usuários do CREA-SP na utilização e administração dos recursos adquiridos.

3.1.2.1 SERVIÇOS DE INSTALAÇÃO, MIGRAÇÃO E IMPLANTAÇÃO

1. Os serviços de Instalação e migração e implantação visam configurar e instalar no CREA os dispositivos contratados juntamente com as licenças de office 365, e também migrar o ambiente atual, construindo políticas processos adequadospara garantir a constante manutenção do novo ambiente.

2. O Serviços poderão ser realizados de forma remota (exceto os com indicação expressa no respectivo item), desde que não atrapalhe na sua execução dentro do prazo solicitado. A forma de realização dos serviços , remota ou presencial, deverá ser definida em comum acordo entre o CREA e a CONTRATADA no momento do planejamento.

3. Considerando-se a possibilidade dos serviços serem realizados de forma presencial, em São Paulo-SP, caso a CONTRATADA necessite deslocar profissionais até a sede do CREA, para realizar as atividades aqui previstas, deverá arcar com todas as despesas decorrentes de viagens, deslocamento, hospedagem, alimentação e outros, sem custos adicionais para a CONTRATANTE;

4. Os serviços deverão ser executados por técnicos com certificação Microsoft adequada para cada serviço.

Os serviços estão listados na Tabela B, abaixo:

ID	Descrição	Valor R$
1	Implantação do Intune	
2	Implantação do Multifator de Autenticação (MFA)	
3	Implantação de Políticas de acesso condicional	
4	Implantação do System Center/Intune para controle de atualização de softwares da Microsoft (Windows, office, etc)	
5	Implantação do SSPR (Self-Service Password Reset)	

6	Implantação de conformidade de políticas de administração deActive Directory	
7	Migração do Office 365 E1 para o Microsoft Office E3	
8	Implementação de políticas de DLP	
9	Implementação de criptografia e Distributed Key Manager(DKM)	
10	Implementação do PIM para a equipe de administração doOffice.	
11	Desenvolvimento de indicadores de BI para área de Suporte	
12	Desenvolvimento de indicadores de BI para saúde deServidores	
13	Atualização do Servidor Exchange	
14	Migração de Servidores Windows Server Antigos	
15	**Total**	

Tabela B - Sumarizadora dos serviços de instalação, implantação e migração

3.1.2.2 SERVIÇOS SOB DEMANDA

1. Nesse item prevê-se o levantamento de requisitos, a especificação, serviços de sustentação (Exchange, Active Directory,System Center, etc.) e customizações no ambiente Office 365, limitado à no máximo 600 horas anuais, (1800 horas em 3 anos) conforme limites mensais negociados com a CONTRATADA**.**

2. A prestação dos serviços técnicos especializados sob demanda se dá em virtude da necessidade de garantir a melhorutilização da solução e deverá ser executada preferencialmente dentro do horário que compreende entre 8h às 18 horas, desegunda-feira a sexta-feira, exceto feriados.

3. Os serviços sob demanda, visam proteger o CREA-SP durante a evolução natural dos produtos da Microsoft. Ao serincorporada qualquer nova funcionalidade aos softwares, caso seja de interesse do CREA-SP, poderá solicitar da CONTRATADA a sua implantação.

4. Havendo qualquer necessidade futura, não atendida pelos serviços de implantação e migração, relacionada aosaplicativos adquiridos, mediante negociação, a CONTRATADA poderá ser acionada.

5. A CONTRATADA poderá ser acionada para realizar qualquer serviço de consultoria na implantação de features dosprodutos Microsoft adquiridos nesta contratação.

6. A CONTRATADA poderá ser acionada para realizar consultoria na utilização dos produtos e serviços adquiridos nestacontratação.

7. A CONTRATADA poderá ser acionada para realizar "troubleshooting", na identificação e correção de problemas relacionados aos produtos e serviços adquiridos nesta contratação.

8. A prestação dos Serviços Técnicos Especializados nas Tecnologias será requisitada, sob demanda, por solicitação formalda CONTRATANTE, por meio de Ordem de Serviço (OS) mensuradas em horas e especificadas em RAT (Relatório de atendimentos técnicos);

9. A critério da CONTRATANTE os serviços poderão ser realizados de forma REMOTA ou ON-SITE, ou seja, no ambienteda CONTRATANTE, sendo detalhadas as atividades a serem executadas, prazos e produtos a serem entregues, responsáveis pela CONTRATANTE e CONTRATADA, recursos a serem usados, valores, condições de homologação e outras informações pertinentes;

10. Considerando-se a possibilidade dos serviços serem realizados de forma presencial, em São Paulo-SP, caso a

CONTRATADA necessite deslocar profissionais até a sede do CREA, para realizar as atividades aqui previstas, deverá arcar com todas as despesas decorrentes de viagens, deslocamento, hospedagem, alimentação e outros, sem custos adicionais para a CONTRATANTE;

11. O aceite e o posterior pagamento dos serviços, softwares e treinamentos executados e entregues pela CONTRATADA, não a exime das responsabilidades quanto às garantias específicas associadas a cada produto desenvolvido e estabelecidona OS, ficando a CONTRATADA responsável pela correção de todos os erros, defeitos, bugs, falhas e quaisquer outras irregularidades pelo período mínimo de 03 (três) meses, contado a partir de emissão do Termo de Aceite Definitivo;

12. O prazo para alocação dos profissionais da CONTRATADA, a partir da formalização da solicitação, é de 10 dias uteis.

13. A responsabilidade de dimensionar adequadamente o quantitativo de recursos necessários para a perfeita execuçãodos serviços sob demanda é compartilhada entre a CONTRATADA e CONTRATANTE, devendo ser negociada a cada solicitação;

14. A CONTRATANTE reserva-se o direito de alocar as horas conforme sua conveniência, não sendo devido o pagamento à CONTRATADA de quaisquer valores a título de franquia ou garantia de alocação mínima das horas.

15. Todos os Serviços prestados pela CONTRATADA devem contar com profissionais que tenham plenas condições de cumprir, de maneira não cumulativa os seguintes definidos no item Serviços e as tarefas definidas na descrição dos serviçossob demanda específicos.

16. O CREA-SP terá o direito de propriedade sobre todos os produtos desenvolvidos sob demanda pela CONTRATADA,bem como toda documentação a eles associados.

3.1.2.3 SERVIÇOS DE CAPACITAÇÃO

1. Os serviços de capacitação visam instruir os usuários e colaboradores do CREA-SP, bem como os analistas de suporte esustentação nas novas políticas, processos e comportamentos esperados após a implementação dos diversos dispositivos de controle e segurança que serão instalados através dos serviços de instalação, migração e implantação adquiridos através deste processo.

2. Ao final da implantação de cada serviço definido na Tabela B, será realizado o serviço de capacitação correspondente naTabela C.

ID	Descrição	Valor R$
1	Implantação do Intune Implantação do Multifator de Autenticação (MFA)Implantação de Políticas de acesso condicional	
2	Implantação do System Center/Intune para controle de atualização de softwares da Microsoft (Windows, office, etc)	
3	Implantação do SSPR (Self-Service Password Reset)	
4	Implantação de conformidade de políticas de administração deActive Directory	
5	migração do Office 365 E1 para o Microsoft Office E3	
6	Implementação de políticas de DLP	
7	Implementação de criptografia e Distributed Key Manager(DKM)	
8	Implementação do PIM para a equipe de administração doOffice.	
9	Desenvolvimento de indicadores de BI para área de Suporte	
10	Desenvolvimento de indicadores de BI para saúde deServidores	

11	Atualização do Servidor Exchange	
12	Passagem de conhecimento - Asbuilt - Migração de ServidoresWindows ServerAntigos	
13	Worshops de implantação e utilização dos recursos do Microsoft365 (segurança, meeting, calling, configuração, utilização, etc)	
14	Total	

Tabela C - Sumarizadora de preços de Serviços de Capacitação

3.1.2.4 CORRELAÇÃO ENTRE OS SERVIÇOS DE SERVIÇOS DE INSTALAÇÃO, MIGRAÇÃO E IMPLANTAÇÃO e a CAPACITAÇÃO

1. Na tabela abaixo pode ser verificada a correlação entre os serviços.

ID	INSTALAÇÃO, MIGRAÇÃO E IMPLANTAÇÃO (Tabela B)	CAPACITAÇÃO (Tabela C)
1	Implantação do Intune	ITEM 1
2	Implantação do Multifator de Autenticação (MFA)	
3	Implantação de Políticas de acesso condicional	
4	Implantação do System Center/Intune para controle de atualização de softwares da Microsoft (Windows, office, etc)	ITEM 2
5	Implantação do SSPR (Self-Service Password Reset)	ITEM 3
6	Implantação de conformidade de políticas de administração deActive Directory	ITEM 4
7	Migração do Office 365 E1 para o Microsoft Office E3	ITEM 5
8	Implementação de políticas de DLP	ITEM 6
9	Implementação de criptografia e Distributed Key Manager(DKM)	ITEM 7
10	Implementação do PIM para a equipe de administração doOffice.	ITEM 8
11	Desenvolvimento de indicadores de BI para área de Suporte	ITEM 9
12	Desenvolvimento de indicadores de BI para saúde deServidores	ITEM 10
13	Atualização do Servidor Exchange	ITEM 11
14	Migração de Servidores Windows Server Antigos	ITEM 12
15	**Total**	

Tabela de Correlação entre Serviços de Implantação e capacitação

2. Quando for terminado e aceito o serviço na Tabela B, deverá ser dado início o serviço de capacitação correspondente naTabela C.
3. A dependência na execução dos serviços não implica na dependência de pagamento. Após executado, ao ser aceitoformalmente, pelo CREA-SP, o serviço de implantação da tabela B, ele será imediatamente pago a CONTRATADA, mediante os procedimentos administrativos adequados. O mesmo se aplica ao serviço de capacitação correspondente.

4 - ESPECIFICAÇÃO TÉCNICA

4.1 REQUISITOS DOS SERVIÇOS DE INSTALAÇÃO, MIGRAÇÃO E IMPLANTAÇÃO

1. A CONTRATADA deverá fornecer os serviços constantes na Tabela B - Sumarizadora dos serviços de instalação,implantação e migração deste Termo de Referência.
2. Estes serviços serão detalhados e especificados na sequência do documento

4.1.1 SERVIÇO DE IMPLANTAÇÃO DO INTUNE

1. A CONTRATADA deverá realizar a Implantação do sistema Intune para os dispositivos do CREA-SP.
2. Esse serviço deve ser realizado de forma presencial, na sede do CREA-SP, em Pinheiros.

3. Quantidade Máxima de dispositivos
    a) 500 Celulares Corporativos
    b) 200 Notebooks com 8GB de memória

4.1.1.1 ENTREGAS MÍNIMAS QUE A CONTRATADA DEVERÀ FORNECER

1) Plano de Projeto de implementação do Intune
    a) - Gerenciamento de Mobile (iOS e Android) e Devices com Windows 10;
    b) - Configuração do AD Hybrid para gerenciamento das estações.
2) Procedimento de uso passo a passo para usuários
3) Procedimento de uso passo a passo para usuários
4) Procedimento de configuração das política de administração para a equipe de sustentação
5) Prazo de entrega: 45 dias úteis

4.1.2 SERVIÇO DE IMPLANTAÇÃO DO MFA (Multifator de Autenticação)

1. A CONTRATADA deverá realizar a implantação de sistema de MFA para todas as contas contratadas através desteprocesso

4.1.2.1 ENTREGAS MÍNIMAS QUE A CONTRATADA DEVERÀ FORNECER

1. Plano de Projeto de implementação do MFA
    a) MFA para aplicativos do Office 365 para acesso externo.
2. Procedimento de uso passo a passo para usuários
3. Procedimentos de configuração de políticas de administração para a equipe de sustentação
4. Prazo de entrega: 15 dias úteis

4.1.3 SERVIÇO DE IMPLANTAÇÃO DAS POLÍTICAS DE ACESSO CONDICIONAL

1. A CONTRATADA deverá realizar a implantação de no máximo 20 políticas de acesso condicional para trabalharem emconjunto com o sistema de MFA a serem definidas posteriormente em projeto.

4.1.3.1 ENTREGAS MÍNIMAS QUE A CONTRATADA DEVERÁ FORNECER

1. Plano de Projeto de implementação de políticas de acesso condicional
    a) Até 20 políticas de acesso condicional
2. Procedimentos de configuração de políticas de administração para a equipe de sustentação
3. Prazo de entrega: 45 dias úteis

4.1.4 SERVIÇO DE IMPLANTAÇÃO DO SCCM (System Center)

1 A CONTRATADA deverá realizar a implantação do System Center/Intune para controle de atualização desoftwares da Microsoft (Windows, office, entre outros)

4.1.4.1 ATIVIDADES MÍNIMAS QUE A CONTRATADA DEVERÁ REALIZAR

1. Instalar ultima versão do SCCM
2. Instalar ultima versão do SQL Server para o SCCM
3. Configurar o SCCM reporting services
4. Criar os seguintes relatórios mínimos
    a) Relatório de Software
    b) Relatório de Hardware

4.1.4.2 CONSIDERAÇÕES:

1. 30 localidades irão necessitar de Distribution Point.
2. SCCM para gerenciamento de inventario, updates, distribuição de software, imagens, políticas
3. Intune configurar Co-Gerenciamento

4.1.4.3 ENTREGAS MÍNIMAS QUE A CONTRATADA DEVERÁ FORNECER

1. Plano de Projeto para implantação do System Center/Intune para controle de atualização de softwares da Microsoft
2. Criar os seguintes procedimentos passo a passo:
3. Instalação e configuração do System Center/Intune

    a) Como conectar no SCCM
    b) Como atualizar uma estação windows com os últimos patches de segurança
    c) Como retirar relatório de inventário de hardware
    d) Como retirar relatório de inventário de software
    e) Como descobrir se um software está instalado numa maquina

4. Prazo de Entrega: 90 dias úteis

4.1.5 SERVIÇO DE IMPLANTAÇÃO DO SSPR (SELF-SERVICE PASSWORD RESET)

1. A CONTRATADA deverá Implementar o recurso SSRP para todas as contas contratadas

4.1.5.1 ENTREGAS MÍNIMAS QUE A CONTRATADA DEVERÀ FORNECER

1. Plano de Projeto para implantação do SSPR
2. Procedimento de uso passo a passo para usuários
3. Procedimentos de configuração de políticas de administração para a equipe de sustentação
4. Prazo de entrega: 15 dias úteis

4.1.6 SERVIÇO DE IMPLANTAÇÃO DE CONFORMIDADE DA FLORESTA DE ACTIVE DIRECTORY

1. A CONTRATADA deverá elaborar um projeto de Conformidade de políticas de administração de Active Directory.
2. A CONTRATADA deverá realizar uma análise da arquitetura atual do Active Directory, Verificação de conformidade comas melhores práticas de administração e segurança e Implantação de modelo de administração.

4.1.6.1 CONSIDERAÇÕES:

1. O CREA-SP Possui os seguintes itens a serem considerados neste serviço

a) 1 Floresta

b) 3 Domínios
c) Nível funcional 2012 R2

4.1.6.2 ENTREGAS MÍNIMAS QUE A CONTRATADA DEVERÁ FORNECER

1. Plano de Projeto para implantação de conformidade da Floresta de Acitive Diretory
2. Procedimento de configuração de conformidade da Floresta de Active Diretory
3. Procedimento de configuração do modelo de administração do Active Diretory
4. Prazo de entrega: 90 dias úteis

4.1.7 SERVIÇO DE IMPLEMENTAÇÃO DO MICROSOFT E3

1. A CONTRATADA deverá realizar a implementação/Migração do plano atual de licenciamento e contas de e-mail (Office365 E1) para o plano contratado Microsoft 365 E3.
2. A CONTRATADA deverá realizar a migração das 300 contas de e-mail de sistemas corporativo e de unidades administrativas, (***Ex: atendimento@creasp.org.br***), para contas de grupo do Office 365, incluindo cópia das mensagens earquivos das contas antigas para as contas de grupo.

4.1.7.1 ENTREGAS MÍNIMAS QUE A CONTRATADA DEVERÁ FORNECER

1. Plano de Projeto para implementação/migração das contas E1 para E3 no Microsoft 365
2. Procedimento de uso passo a passo para usuários
3. Procedimentos de configuração de políticas de administração para a equipe de sustentação
4. Prazo de entrega: 60 dias úteis

4.1.8 SERVIÇO DE IMPLANTAÇÃO DE POLÍTICAS DE AIP/DLP

1. A CONTRATADA deverá realizar a configuração das políticas para classificação de documentos do Office 365 e políticasde DLP para prevenção de perda de dados.

2. Será responsabilidade da CONTRATADA, em conjunto com a CONTRATANTE levantar as políticas necessárias para o ambiente do CREA-SP.

4.1.8.1 ENTREGAS MÍNIMAS

1. Plano de Projeto para implementação das políticas AIP/DLP.
2. Procedimento de uso passo a passo para usuários
3. Procedimentos de configuração de políticas de administração para a equipe de sustentação
4. Prazo de entrega: 45 dias úteis

4.1.9 SERVIÇO DE IMPLANTAÇÃO DA CRIPTOGRAFIA, BITLOCKER E DKM

1. A CONTRATADA deverá realizar a implantação do Bitlocker para criptografia de discos em 800 estações de trabalho/notebooks com Windows 2010 do CREA-S e a Implantação do serviço de Gerenciamento de chaves do BitLocker

2. Esse serviço deve ser realizado de forma presencial, na sede do CREA-SP, em Pinheiros;

4.1.9.1 ENTREGAS MÍNIMAS

1. Plano de Projeto para implementação e gerenciamento do Bitlocker
2. Procedimento de uso passo a passo para usuários

3. Procedimentos de configuração de políticas de administração para a equipe de sustentação
4. Prazo de entrega: 60 dias úteis

4.1.10 SERVIÇO DE IMPLEMENTAÇÃO DO PIM

1. A CONTRATADA deverá Implementar o PIM para as 10 licenças de E5 que serão administradores do Microsoft 365

4.1.10.1 ENTREGAS MÍNIMAS

1. Plano de Projeto para implementação do PIM
2. Procedimento de uso passo a passo para usuários que dispõe de licença E5
3. Procedimentos de configuração de políticas de administração para a equipe de sustentação
4. Prazo de entrega: 30 dias úteis

4.1.11 SERVIÇO DE INDICADORES PARA ACOMPANHAMENTO DE EXECUÇÃO DE CHAMADOS TÉCNICOS

1. A CONTRATADA deverá realizar o Desenvolvimento de indicadores para o power BI para área de Suporte acompanhar aexecução dos chamados técnicos. (chamados em aberto, em espera, atendidos, etc) utilizando da integração com a ferramenta GLPI (https://glpi-project.org/).

2. O GLPI possui apenas uma base de dados mysql que deverá ser consultada para elaboração dos indicadores.

4.1.11.1 ENTREGAS MÍNIMAS

1. Plano de Projeto para implementação do PIM
2. Procedimento de uso passo a passo para usuários que dispõe de licença E5
3. Procedimentos de configuração de políticas de administração para a equipe de sustentação
4. Prazo de entrega: 30 dias úteis

4.1.12 SERVIÇO DE IMPLEMENTAÇÃO DE INDICADORES DE SAÚDE DE SERVIDORES

1. A CONTRATADA deverá realizar o Desenvolvimento de indicadores para Power BI para saúde de 1 Servidor (Utilizaçãode Memória, CPU, DISCO, REDE) integrando com Zabbix.

2. O CREA-SP possui um servidor Zabbix já instalado, com sua base de dados em MySQL que deverá ser consultada para elaboração do indicador.

3. Entende-se por saúde, o tempo que o servidor ficou acessível, ou disponível.

4.1.12.1 ENTREGAS MÍNIMAS

1. Plano de Projeto para Criação de dashboard para indicadores de monitoração da ferramenta Zabbix
2. Procedimento de uso passo a passo para usuários técnicos
3. Procedimentos de configuração para a equipe de sustentação
4. Prazo de entrega: 30 dias úteis

4.1.13 SERVIÇO DE ATUALIZAÇÃO DO EXCHANGE SERVER

1. A CONTRATADA deverá realizar a atualização de versão, instalação de patches de segurança do Exchange Serverinstalado "on premisses" no CREA-SP.

2. O CREA-SP tem apenas um servidor exchange interno que é utilizado como relay para algumas aplicações, também internas. Este servidor precisa ser atualizado.

3. Toda a configuração atual do servidor deve ser levantada pela CONTRATADA.
4. A CONTRATADA deverá deixar o Servidor em Conformidade com praticas de segurança da Microsoft.

4.1.13.1 ENTREGAS MÍNIMAS

1. Plano de Projeto para atualização do Exchange Server
2. Procedimento de uso passo a passo para usuários técnicos
3. Procedimentos de configuração de administração para a equipe de sustentação
4. Prazo de entrega: 20 dias úteis

4.1.14 SERVIÇO DE MIGRAÇÃO DO WINDOWS SERVER ANTIGOS

1. A CONTRATADA deverá realizar a migração de Servidores Windows Server ANTIGOS para a versão mais atual.
2. Será responsabilidade da CONTRATADA, em conjunto com a CONTRATANTE, a identificação dos problemas decorrentes da migração, ajudando a identificar as falhas e encontrar possíveis soluções, no que tange aos produtos da Microsoft..
3. Esse serviço deve ser realizado de forma presencial, na sede do CREA-SP, em Pinheiros.

4. Os seguintes servidores devem ser migrados.

Item	Nome	S.O.	Função
1	ARCAS	Microsoft Windows Server 2008 R2 (64-bit)	SHAREPOINT + TEAM FOUNDATION SERVER
2	CREAINFO1	Microsoft Windows Server 2003 Standard (32-bit)	BELISE - SERV. LICENÇAS BORLAND - DELPHI 2007
3	EGEO-1-DC	Microsoft Windows Server 2008 R2 (64-bit)	SERVICO IIS - CREANET (FUNCIONÁRIOS) (NODE 01)
4	EGEO-2-DC	Microsoft Windows Server 2008 R2 (64-bit)	SERVICO IIS - CREANET (FUNCIONÁRIOS) (NODE 02)
5	EGEO-4-DC	Microsoft Windows Server 2008 R2 (64-bit)	SERVICO IIS - CREANET (FUNCIONÁRIOS) (NODE 03)
6	HERMES	Microsoft Windows Server 2008 (64-bit)	SERVIDOR TOMCAT/APACHECREADOC
7	HERMIONE	Microsoft Windows Server 2008 R2 (64-bit)	DESENV - SQL
8	MOROS	Microsoft Windows Server 2008 R2 (64-bit)	SERVICO IIS - [DESENV] CREANET (IIS:80), [DESENV] NOVA INTRANET (IIS:1945), [HOMOLOG] CREANET (IIS:88)
9	MOROS02	Microsoft Windows Server 2008 R2 (64-bit)	SERVICO IIS - DESENV. CREANET (UDE)
10	ONIRO-2-DC	Microsoft Windows Server 2008 R2 (64-bit)	SERVICO IIS - CREANET (USO INTERNO PRODUÇÃO) (NODE 2)
11	ONIRO-3-DC	Microsoft Windows Server 2008 R2 (64-bit)	SERVICO IIS - CREANET (PROFISSIONAIS) (NODE 3)
12	ONIRO-6-DC	Microsoft Windows Server 2008 R2 (64-bit)	SERVICO IIS - CREANET (PROFISSIONAIS) (NODE 6)
13	ONIRO-8-DC	Microsoft Windows Server 2008 R2 (64-bit)	SERVICO IIS - CREANET (PROFISSIONAIS) (NODE 8)
14	SEI-WIN-DB1	Microsoft Windows Server 2012 (64-bit)	SISTEMA SEI e LOG APP CREANET - DB

15	SELENE	Microsoft Windows Server 2008 (64-bit)	SERVICO IIS - REEMBOLSO, CONSULTA PÚBLICA TRANSPARÊNCIA, SAT, FALE CONOSCO, DENUNCIA ON LINE. [PROD]IIS - [PROD] Reembolso (IIS:1030), - [PROD] Consulta Pública de Transparência (IIS:1050), - [PROD] SAT (IIS:1025), - [PROD] Fale Conosco (IIS:1369), - [PROD] Denúncia On-Line (IIS:1369), - [PROD] IMPLANTA-ANTIGO -[DESENV] SAT (IIS:1026),
16	SEMELE	Microsoft Windows Server 2008 R2 (64-bit)	DESENV. IMPLANTA
17	TOAD	Microsoft Windows Server 2008 R2 (64-bit)	APLICAÇÃO TOAD
18	TRITON	Microsoft Windows Server 2008 (64-bit)	[PROD] Banco de dados DB2 - SAT

4.1.14.1 ENTREGAS MÍNIMAS

1. Plano de Projeto para Migração de Servidores para versão mais atual
2. Documentação técnica final de atualização dos servidores Windows Servers
3. Passagem de conhecimento para o time técnico por meio de workshop.
4. Prazo de entrega: 30 dias úteis

4.2 REQUISITOS DO SERVIÇOS SOB DEMANDA

1. A CONTRATADA deverá fornecer os serviços solicitados, utilizando os seguintes profissionais:

1.1. Profissional Gerente de Projeto - Profissional com experiência igual em gestão de projetos

a) Considerando a complexidade / inviabilidade técnica de se utilizar a técnica de pontos de função paraprojetos de infraestrutura, é
responsabilidade dos técnicos do CREA-SP, validar previamente a alocação de horas a ser apresentada pelaCONTRATADA para cada serviço sob demanda que for solicitado pelo CREA-SP.

1.2 - Profissional Consultor Microsoft 365 - Profissional com experiência em:

a) Customização e Parametrização dos aplicativos Online.
b) Criação de fluxos automatizados com o Microsoft Flow.
c) Criação, customização e parametrização de aplicativos com o Microsoft PowerApps.
d) Criação, customização e parametrização de formulários com o Microsoft Forms.
e) Criação, customização e parametrização de aplicativos do Microsoft 365, incluindo, mas não se limitando a,Intune, MFA, Regras de acesso confidencial, Criptografia Bitlocker, Gerenciamento centralizado de chaves criptográficas, Segurança, Teams, Sharepoint e outros;

1.3 - Profissional Consultor em Sustentação de T.I. - Profissional com experiência em:

a) Customização e Parametrização dos aplicativos On premisses.
b) Segurança dos produtos Microsoft, incluindo, mas não se limitando a: Servidores, Exchange, Active Directory,etc
c) Criação, customização e parametrização e configurações , incluindo, mas não se limitando a: ServidoresWindows, Active Directory, Exchange Server, System Center.

1.4 - Arquiteto de Infraestrutura de Segurança

a) Profissional com Experiencia em desenhar arquitetura de serviços para os produtos Microsoft 365, Sustentação de T.I (Servidores Windows, Active Directory, Exchange, System Center)

4.3 REQUISITOS DO SERVIÇO DE CAPACITAÇÃO

1. A CONTRATADA devera fornecer a capacitação, que compreende a realização das atividades especificadas na Tabela D,abaixo (também listadas na Tabela C):

TABELA D: Atividades de Treinamento por tópico

ID	Projeto	Atividades de Treinamento Necessárias
1	Implantação do Intune Implantação do Multifatorde Autenticação (MFA) Implantação de Políticas de acesso condicional	- 4 Workshops técnico para equipe de T.I. - 4 Workshops para usuários Disponibilização, para a equipe de sustentação deTI, do seguinte treinamento oficial da Microsoft: - Curso **Managing Modern Desktops** - Curso **Microsoft 365 Security Administration** - Curso **Microsoft Identity and Access Administrator**
2	Implantação do System Center/Intune para controle de atualização de softwaresda Microsoft (Windows, office, etc)	- 2 Workshops técnico para equipe de T.I. Disponibilização, para a equipe de sustentação deTI, do treinamento oficial da Microsoft: - **Administering System Center Configuration Manager**
3	Implantação do SSPR (Self-Service Password Reset)	- 2 Workshops técnicos para equipe de T.I. - 2 Workshops para usuários
4	Implantação de conformidade de políticas de administração de ActiveDirectory	- 2 Workshops técnicos para equipe de T.I. Disponibilização, para a equipe de sustentação deTI, dos seguinte treinamento oficial da Microsoft: - Curso **Identity with Windows Server**
5	migração do Office 365 E1 para o Microsoft Office E3	- 2 Workshops técnicos para equipe de T.I.
6	Implementação de políticasde DLP	- 2 Workshops técnicos para equipe de T.I. - 2 Workshops para usuários

7	Implementação de criptografia nos dispositivosde acesso e Distributed KeyManager (DKM)	- 2 Workshops técnicos para equipe de T.I. - 2 Workshops para usuários
8	Implementação do PIMpara a equipe de administração do Office.	- 2 Workshops técnicos para equipe de T.I.
9	Desenvolvimento de indicadores de BI para áreade Suporte	- 2 Workshops técnicos para equipe de T.I.
10	Desenvolvimento de indicadores de BI para saúde de Servidores	- 2 Workshops técnicos para equipe de T.I.
11	Atualização do Servidor Exchange	- 2 Workshops técnicos para equipe de T.I. Disponibilização, para a equipe de sustentação deTI, do seguinte treinamento oficial da Microsoft: - Curso **Administering Microsoft Exchange Server 20XX/20XX** (última versão disponível)
12	Migração de Servidores Windows Server 2012 R2	- 2 Workshops técnicos para equipe de T.I. Disponibilização, para a equipe de sustentação deTI, do treinamento oficial da Microsoft: - Curso **Securing Windows Server 20XX** (última versão disponível)
13	Worshops de implantação e utilização dos recursos do Microsoft 365 (segurança, meeting, calling, configuração, utilização, e outros)	- 24 Workshops para usuários Disponibilização, para a equipe de sustentação deTI, dos seguintes treinamentos oficiais da Microsoft: - Curso **Microsoft 365 Messaging** - Curso **Microsoft Information Protection Administrator** - Microsoft 365 Certified: **Managing Microsoft Teams**

4.3.1 REQUISITOS DA REALIZAÇÃO DE WORKSHOPS

1. Os workshops devem ser preferencialmente oferecidos por plataforma online Teams.
2. Cada workshop deve ter duração mínima de 3 horas e máxima de 4.

4.3.2 REQUISITOS DOS TREINAMENTOS OFICIAIS MICROSOFT

1. Cada treinamento deve ser oferecido para 5 (cinco) profissionais do CREA-SP.
2. Os Cursos oferecidos poderão ser entregues ao CREA-SP em formas de voucher.

3. Os treinamentos devem ser preferencialmente em plataforma OnLine com a possibilidade de escolha do aluno paratreinamentos presenciais quando disponíveis em São Paulo.

4. Quando possível os treinamentos devem ser oferecidos em língua Portuguesa.

5. Cada treinamento deverá fornecer ao termino um certificado reconhecido pela Microsoft.

6. Os requisitos programáticos mínimos estão descritos no ANEXO A - Conteúdo Programático.

7. Se algum treinamento for descontinuado, deverá ser negociado com o CREA-SP e fornecido o treinamento equivalente,que forneça o objetivo e o conteúdo programático similar ao requisitado.

8. Caberá à CONTRATANTE todos os custos de deslocamentos, alimentação e diárias do(s) participantes(s).

9. A disponibilidade dos cursos e agenda para execução irão depender do cronograma de cursos do Centro deTreinamento.

10. Caberá a CONTRATANTE todos os trâmites para matrícula/inscrição do participante para o curso no Centro de Treinamento.

11. No caso de utilização de Voucher(s), o aceite por parte do CREA-SP está atrelado ao recebimento do(s) voucher(s), após a certificação junto à entidade fornecedora do treinamento, de que o mesmo é válido e corresponde ao treinamentoespecificado neste Termo de Referência.

12. Abaixo segue os requisitos de cada treinamento, que devem ser fornecidos em conjunto com a capacitação de cadaprojeto a ser implementado, conforme os módulos e itens da Tabela D:

4.3.2.1

Curso SC-400T00-A: Microsoft Information Protection Administrator

1. **Duração mínima:**2 Dias
2. **Objetivo:**

a) Ensinar como proteger informações em sua implantação do Microsoft 365. Este curso se concentra nagovernança de dados e proteção de informações dentro de sua organização.

b) O curso abrange a implementação de políticas de prevenção de perda de dados, tipos de informações confidenciais, rótulos de sensibilidade, políticas de retenção de dados e criptografia de mensagens do Office365, entre outros tópicos relacionados.

4.3.2.2 Curso MS-500T00-A: Microsoft 365 Security Administration

1. **Duração mínima:** 4 dias
2. **Objetivo:**

a) O aluno deverá sr ensinado como assegurar o acesso dos usuários aos recursos da sua organização.

b) O curso deve cobrir a proteção da palavra-passe do utilizador, autenticação multi-factor, como permitir a Azure Identity Protection, como configurar e utilizar o Azure AD Connect, e introduzi-lo ao acesso condicionalno Microsoft 365.

c) Ensinar sobre tecnologias de proteção contra ameaças que ajudam a proteger o seu ambiente Microsoft 365. Especificamente, aprender sobre os vectores de ameaças e as soluções de segurança da Microsoftpara mitigar as ameaças.

d) Ensinar sobre a pontuação segura, proteção Exchange Online, Azure Advanced Threat Protection,Windows Defender Advanced Threat Protection, e gestão de ameaças.
e) No curso aprender sobre tecnologias de proteção de informação que ajudam a proteger o seu ambienteMicrosoft 365.
f) O curso deve discutir conteúdos geridos por direitos de informação, encriptação de mensagens, assim como rótulos, políticas e regras que apoiam a prevenção da perda de dados e a proteção de informação.
g) Aprender sobre arquivamento e retenção no Microsoft 365, bem como sobre gestão de dados e comoconduzir pesquisas e investigações de conteúdo.
h) Este curso deve abranger políticas e etiquetas de retenção de dados, gestão de registos no local paraSharePoint, retenção de correio eletrônico, e como conduzir pesquisas de conteúdo que suportam investigações de eDiscovery.

4.3.2.3 Curso MS-203T00-A: Microsoft 365 Messaging

1. Duração mínima: 5 dias
2. Objetivo: Examinar os principais elementos da administração de mensagens do Microsoft 365, incluindo fluxo e transporte de mensagens, segurança, proteção ativa e conformidade de mensagens, infraestrutura de mensagense mensagens híbridas.

4.3.2.4 Curso SC-300T00-A: Microsoft Identity and Access Administrator

1. Duração mínima: 4 dias
2. Objetivo:

a) Oferecer ao Profissional de Identidade e Acesso de IT, juntamente com o IT Security Professional, os conhecimentos e habilidades necessários para implementar soluções de gerenciamento de identidade baseadas no Microsoft Azure AD, e tecnologias de identidade conectadas.
b) Este curso deve incluir conteúdo de identidade para Azure AD, registro de aplicativos corporativos, acesso condicional, governança de identidade e outras ferramentas de identidade.

4.3.2.5 MS-700T00-A: Managing Microsoft Teams

1. Duração Mínima: 5 Dias
2. Objetivo:

a) configurar, implementa e gerencia cargas de trabalho do Office 365 para o Microsoft Teams visando a colaboração e comunicação eficiente e efetiva em um ambiente empresarial.
b) Este curso deve abranger seis elementos centrais -

- Visão geral do Microsoft Teams,
- Implementação de governança,
- Segurança e conformidade para o Microsoft Teams,
- Preparando para uma implantação do Microsoft Teams,
- Implantando e gerenciando equipes,
- Gerenciando colaboração e gerenciando comunicação no Microsoft Teams.

c) Deverá oferecer uma visão geral do Microsoft Teams incluindo arquitetura do Teams e cargas horárias do Office365 relacionadas.
d) Deverá oferecer uma visão geral de segurança e conformidade no Microsoft Teams e finalmente mostrar umavisão geral de como gerenciar o Microsoft Teams.

e) Ao implementar a governança, segurança e conformidade para o Microsoft Teams, deverá ensinar a planejar econfigurar a governança para grupos do Office 365 incluindo expiração e políticas de nomeação.
f) Em seguida, deverá implementar segurança e ensinar o aluno configurando acesso condicional, MFA ou Gestãode Ameaça para o Microsoft Teams.
g) Finalmente, deverá implementar conformidade para Teams usando políticas de DLP, casos de eDiscovery oupolíticas de supervisão.
h) Deverá preparar o ambiente para uma implantação do Microsoft Teams, planejar um upgrade do Skype for Business para o Microsoft Teams ao avaliar caminhos de upgrade com modos de coexistência e upgrade, gerenciamigrações de reunião e configura definições de coexistência e upgrade. i) Em seguida, planejar e configurar definições de rede para o Microsoft Teams, e finalmente implantar e gerenciar os terminais do Microsoft Teams.
Ao implantar e gerenciar equipes, deverá ensinar como criar e gerenciar equipes, gerenciar afiliação e acesso tantopara usuários internos quanto externos.
j) Ao gerenciar a colaboração no Microsoft Teams, gerenciar experiências de chat e colaboração tais comodefinições de equipe ou políticas de criação de canal privado.
k) Finalmente, gerenciar definições para aplicações do Teams como políticas de configuração de aplicação, Apps,robôs e conectores no Microsoft Teams ou publicar uma aplicação personalizada no Microsoft Teams.
l) Este curso deverá ser concluído com o gerenciamento de comunicação no Microsoft Teams. O alune deverá aprender como gerenciar experiências de evento e reuniões ao vivo, gerenciar números de telefone ou Sistema deTelefone para o Microsoft Teams e finalmente como solucionar problema de áudio, vídeo e problemas de cliente.

4.3.2.6 Curso MD-101T00-A: Managing Modern Desktops

1. **Duração mínima:** 5 dias
2. **Objetivo:**

a) Neste curso, os alunos deverão aprender como planejar e implementar uma estratégia de implantação desistema de operação usando métodos de implantação modernos, assim como implementar uma estratégia de atualização.
b) Os alunos deverão serão introduzidos a componentes principais de gestão moderna e estratégias de cogerenciamento. Este curso também deve abranger o que é necessário para incorporar o Microsoft Intunepara a empresa.
c) Os alunos deverão aprender sobre métodos para implantação e gerenciamento de aplicações e aplicações baseadas em navegador. Os alunos deverão ser introduzidos aos conceitos principais de segurança em gestão moderna incluindo autenticação, identidades, acesso e políticas de conformidade.
d) Os alunos deverão ser introduzidos a tecnologias como Azure Active Directory, Azure Information Protection e Windows Defender Advanced Threat Protection, assim como alavancá-las para proteger dispositivos e dados.

4.3.2.7 Curso 20742-B: Identity with Windows Server

1. **Duração Mínima:** 5 dias
2. **Objetivo:**

a) Deverá ensinar aos profissionais de TI como implementar e configurar o Active Directory Domain Services(AD DS) em um ambiente distribuído, como implementar a Política de Grupo, como executar o backup e arestauração e como monitorar e solucionar problemas relacionados ao Active Directory, além de problemas relacionados ao Windows Server 20xx.
b) Além disso, o curso deverá ensinar aos estudantes como implementar outras funções de servidor do Active Directory, como Active Directory Federation Services (AD FS) e Active Directory Certificate Services(AD CS).

4.3.2.8 Curso 20744-C: Securing Windows Server 20XX (A verão disponível à época)

1. **Duração mínima:** 5 dias
2. **Objetivo:**

a) Deverá ensinar aos profissionais de TI como otimizar a segurança da infraestrutura de TI queadministram.

b) Este curso deverá começar enfatizando a importância de assumir que as violações de rede já ocorrerame, em seguida, ensinar como proteger credenciais administrativas e direitos para ajudar a garantir que os administradores possam executar apenas as tarefas que precisam, quando precisam.

4.3.2.9 Curso 20703-1-B: Administering System Center Configuration Manager

1. **Duração mínima:** 5 dias
2. **Objetivo:**

a) Deverá descrever como usar o Gerenciador de Configuração e seus sistemas de site associados paragerenciar eficientemente os recursos de rede.

b) Deverá ensinar tarefas diárias de gerenciamento, incluindo como gerenciar aplicativos, saúde do cliente, inventário de hardware e software, implantação do sistema operacional e atualizações de software usando oGerenciador de Configuração.

c) Deverá ensinar como otimizar a System Center Endpoint Protection, gerenciar a conformidade e criarconsultas e relatórios de gerenciamento.

4.3.2.10 Curso 20345-1-B: Administering Microsoft Exchange Server 20XX/20XX (Última Versão disponível)

1. **Duração Mínima:** 5 dias.
2. **Objetivo:**

a) Este curso deverá ensinar os profissionais de TI a administrar e dar suporte ao Exchange Server. O cursodeverá abordar como instalar e configurar o Exchange Server.

b) Ele também deverá abordar como gerenciar destinatários de e-mail e pastas públicas, incluindo comoexecutar operações em massa usando o shell de gerenciamento do Exchange.

c) Além disso, o curso deverá abordar como gerenciar a conectividade do cliente, transporte e limpeza demensagens e implementações do Exchange Server de alta disponibilidade.

d) Ele também deverá abordar como implementar soluções de recuperação de desastres. Por último, o cursodeverá abordar como manter e monitorar uma implementação do Exchange Server e como administrar o Exchange Online em uma implementação do Office 365.

4.4 OUTROS REQUISITOS LEGAIS

1. A CONTRATADA deve executar o objeto do certame em estreita observância dos ditames estabelecido pela Leinº13.709/2018 (Lei Geral de Proteção de Dados Pessoais (LGPD)).

4.5 REQUISITOS GERAIS PARA A EXECUÇÃO DOS SERVIÇOS

1. Serem realizados com base nas boas práticas preconizadas por modelos como ITIL (IT lnfrastructure Library),COBIT e PMBOK (Project Management Body of Knowledge);

2. Serem executados dentro dos parâmetros estabelecidos neste processo de contratação, com observância às recomendações aceitas pela boa técnica, normas e legislação, bem como observar conduta adequada na utilizaçãodos materiais, equipamentos, ferramentas e utensílios, observando sempre os critérios de qualidade;

3. Adequar-se aos padrões normativos orientados pela Política de Segurança do CREA-SP;

4. Elaborar documentos, relatórios gerenciais e outros, referentes ao acompanhamento da execução das Ordens deServiços;

5. Realizar os serviços de modo que não prejudiquem o andamento normal das atividades do Órgão em horário de seuexpediente;

6. Implantar o planejamento, a execução e a supervisão permanente dos serviços demandados;

7. Responsabilizar-se pela definição da forma, metodologia, processos, local e modelo e execução dos serviços.

5 - DEVERES E RESPONSABILIDADES DA CONTRATANTE

5.1 OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATANTE

1. Observar e fazer cumprir fielmente o que estabelece este Termo de Referência;

2. Receber o objeto no prazo e condições estabelecidas no Termo de Referência;

3. Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA;

4. Comunicar a CONTRATADA toda e qualquer ocorrência relacionada com a execução do Contrato;

5. Acompanhar e fiscalizar o cumprimento das obrigações da CONTRATADA por meio de um fiscal;

6. Colocar à disposição da CONTRATADA os elementos e informações necessárias à consecução do objeto do Contrato;

7. Atestar a entrega do objeto, receber e promover o pagamento das faturas correspondentes, quando apresentadas na formaestabelecida no contrato;

8. Aplicar à CONTRATADA as penalidades contratuais e regulamentares cabíveis, garantidos o contraditório e a ampla defesa;

9. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais e ostermos de sua proposta.

6 - DEVERES E RESPONSABILIDADES DA CONTRATADA

6.1 1. Executar os serviços conforme especificações deste Termo de Referência e de sua proposta;

2. Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, osserviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

3. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com os artigos 14 e 17 a 27, doCódigo de Defesa do Consumidor (Lei nº 8.078, de 1990);

4. Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas emlegislação específica, cuja inadimplência não transfere responsabilidade à CONTRATANTE;

5. Relatar à CONTRATANTE toda e qualquer irregularidade verificada no decorrer da prestação dos serviços;

6. Executar o objeto do certame em estrita observância dos ditames estabelecido pela Lei 13.709/2018 (Lei Geral de Proteçãode Dados Pessoais (LGPD)).

7. Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATANTE (por intermédio de prepostodesignado para acompanhamento do contrato), principalmente no tocante à eficiência e agilidade da execução dos serviços objeto deste Termo de Referência, e que deverá responder pela fiel execução do contrato;

8. Reconhecer o Gestor do Contrato, bem como outros servidores que forem indicados pela CONTRATANTE, para realizar assolicitações relativas ao contrato firmado, tais como manutenção, configuração, entre outras;

9. Apresentar Nota Fiscal/Fatura com a descrição dos serviços prestados, nas condições deste Termo de Referência, comoforma de dar início ao processo de pagamento pela CONTRATANTE;

10. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução doobjeto contratual;

11. Assumir as responsabilidades pelos encargos fiscais e comerciais resultantes da contratação.

12. Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado em contrato, os serviçosefetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução;

13. Propiciar todos os meios necessários à fiscalização do contrato pela CONTRATANTE, cujo representante terá poderes parasustar o fornecimento, total ou parcial, em qualquer tempo, sempre que considerar a medida necessária;

14. Acatar as orientações da CONTRATANTE, sujeitando-se à mais ampla e irrestrita fiscalização, prestando os esclarecimentos solicitados e atendendo as reclamações formuladas;

15. Prestar esclarecimentos à CONTRATANTE sobre eventuais atos ou fatos noticiados que se refiram à CONTRATADA, independente de solicitação;

16. Comunicar à CONTRATANTE, por escrito, qualquer anormalidade nos serviços e prestar os esclarecimentos julgadosnecessários;

17. Não veicular publicidade ou qualquer outra informação acerca da prestação dos serviços do Contrato, sem préviaautorização da CONTRATANTE;

18. Não fazer uso das informações prestadas pela CONTRATANTE para fins diversos do estrito e absoluto cumprimento docontrato em questão;

7 - MODELO DE EXECUÇÃO DO CONTRATO

7.1 - Rotinas de Execução

7.1.1 DO ACOMPANHAMENTO E FISCALIZAÇÃO

1. O acompanhamento e a fiscalização da execução do Contrato consistem na verificação da conformidade da prestação dos serviços, dos materiais, técnicas e equipamentos empregados, de forma a assegurar o perfeito cumprimento do ajuste, queserão exercidos por um ou mais representantes da Administração, especialmente designados, na forma dos artigos 67 e 73 daLei Federal no 8.666, de 21 de junho de 1993.

2. A verificação da adequação da prestação do serviço deverá ser realizada com base nos critérios previstos neste Termo deReferência;

3. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de materialinadequado ou de qualidade inferior e, na ocorrência desta, não implica em corresponsabilidade da Contratante ou de seus agentes e prepostos, de conformidade com o artigo 70 da Lei Federal no 8.666, de 21 de junho de 1993.

7.1.2 DA VIGÊNCIA

1. O Contrato terá vigência de 36 (trinta e seis) meses a partir da data de sua assinatura, podendo ser prorrogado até o limitede 48 (quarenta e oito) meses, na forma da Lei nº 8.666/93.

2. O Contratado deverá sujeitar-se aos acréscimos e supressões contratuais estabelecidos na forma do Art. 65 da Lei n.8.666/93.

7.1.3 DA TRANSIÇÃO CONTRATUAL

1. Em casos de interrupção contratual e ocorrendo mudança de fornecedor da solução, todo conhecimento adquirido ou desenvolvido, bem como toda informação produzida pelos atendimentos de chamados de suporte deverão ser disponibilizadosà CONTRATANTE ou empresa por ela designada em até 30 (trinta) dias corridos após o encerramento do contrato. As informações disponibilizadas devem ser em formato digital, inteligível para humanos, e na língua portuguesa.

2. A CONTRATADA deverá elaborar o Plano de Transição, no prazo de 60 (sessenta) dias corridos antes do encerramento docontrato, para a transferência integral e irrestrita dos conhecimentos e das competências necessárias e suficientes para promover a continuidade dos serviços.

3. A CONTRATANTE poderá estabelecer prazo inferior caso haja rescisão contratual.

4. Nenhum pagamento será devido à CONTRATADA pela elaboração ou pela execução do Plano de Transição. O fato da empresa CONTRATADA ou seus representantes não cooperarem ou reterem qualquer informação ou dado solicitado pela CONTRATANTE, que venha a prejudicar, de alguma forma, o andamento da transição das tarefas e serviços para um novo prestador, constituirá quebra de contrato, sujeitando-a as obrigações em relação a todos os danos causados à CONTRATANTE.

7.1.4 DA SOLICITAÇÃO E PLANEJAMENTO DAS ATIVIDADES

1. Todas as configurações e serviços devem ser planejados e acordados entre a CONTRATADA e a equipe de infraestrutura de T.I.C. do CREA-SP (EINFRA)

2. Todo e qualquer serviço será solicitado pelo CREA-SP através de uma Ordem de Serviço.

3. Após receber a Ordem de Serviço, a CONTRATADA terá no máximo 10 dias uteis para apresentar o plano de trabalho.

4. Antes de realizar qualquer serviço a CONTRATADA deve apresentar um plano de trabalho contendo no mínimo, e não selimitando, as seguintes informações:

a) Analistas responsáveis da empresa CONTRATADA, incluíndo informações de contato (celular, etc)
b) Analistas responsáveis do CREA-SP, incluíndo informações de contato (celular, etc)
c) Descrição da Atividade

d) Descrição do equipamento/produto/serviço que será configurado
e) Descrição dos impactos/riscos
f) Ações que serão realizadas durante o serviço
g) Ações preventivas para minimizar o impacto dos riscos e ameaças detectados
h) Cronograma
i) Plano de RoolBack em caso de falha
j) Plano de Day After (acompanhamento pós mudança)
k) Plano de Escalonamento
l) Caso seja uma atividade de Serviço sob demanda, deverá contar a quantidade de horas estimadas para a execuçãodo serviço.

3. Qualquer atividade será realizada somente depois da aprovação do plano pela EINFRA.

7.1.5 DA EXECUÇÃO DAS ATIVIDADES - RAT (Relatórios de atendimentos técnicos)

1. Após a execução de qualquer serviço solicitado, tenha ele sido bem ou mal sucedido, a CONTRATADA deverá apresentarum relatório de execução, contendo no mínimo, e não se limitando, as seguintes informações:

a) As Built contendo todas as informações pertinentes ao serviço executado,
b) Desenhos topológicos (caso pertinente).
c) Endereçamento IP utilizados.
d) Senhas e usuários utilizados para as configurações.
e) Pendências, caso houver.
f) Plano de ação para solucionar as pendências, com responsabilidades, responsáveis e cronograma.
g) Servidores e serviços afetados.
h) Efeitos colaterais (caso pertinente), ações de contingência.
i) Conclusão
j) Contatos dos responsáveis pela execução dos serviços

7.1.6 DA RESCISÃO

1 - Contrato poderá ser rescindido:

1.1 - Por ato unilateral e escrito da Administração, nas situações previstas nos incisos I a XII e XVII do art. 78 da Lei nº8.666, de 1993, e com as consequências indicadas no art. 80 da mesma Lei, sem prejuízo da aplicação das sanções previstas neste Termo;

1.2 - Amigavelmente, nos termos do art. 79, inciso II, da Lei nº 8.666, de 1993.

2 - Os casos de rescisão contratual serão formalmente motivados, assegurando-se à Contratada o direito à prévia e ampladefesa.

3 - A Contratada reconhece os direitos do CREA-SP em caso de rescisão administrativa prevista no art. 77 da Lei nº 8.666, de1993.

4 - O termo de rescisão, sempre que possível, será precedido:

4.1 - Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

4.2 - Relação dos pagamentos já efetuados e ainda devidos;

4.3 - Indenizações e multas."

7.2 - Quantidade Mínima de Bens ou Serviços para Comparação e Controle

7.2.1 AUFERIMENTO DOS SERVIÇOS E PRODUTOS

1. Os produtos serão auferidos mediante recebimento dos itens contratados, nas datas previamente acordadas entre o CREA-SP e a Contratada devidamente atestados pelo gestor/fiscal do contrato.
2. Os serviços serão auferidos após a execução dos mesmos, mediante recebimento do relatório de execução, e da comprovação, por parte da EINFRA, de que foram executados de acordo com a ordem de serviço emitida. mediante atesto doGestor do Contrato.

7.3 - Mecanismos Formais de Comunicação entre a Contratada e a Administração

7.3.1 São mecanismos formais de comunicação entre a CONTRATADA e a CONTRATANTE:

a) E-mails: forma rápida de comunicação para tratar de informações pouco críticas;
b) Ofícios: Comunicação para tratar de assuntos gerais.

7.3.2 Toda a comunicação entre a CONTRATANTE e a CONTRATADA deverá ser sempre formal como regra, exceto em casos excepcionais que justifiquem outro canal de comunicação.

7.4 - Forma de Pagamento em Função dos Resultados

7.4.1 FORMAS DE PAGAMENTO

7.4.1.1 O pagamento dos serviços e produtos serão realizados mediante a entrega dos mesmos, após aceitação e atesto do gestor do contrato e emissão da devida nota fiscal.

7.4.2 DA NOTA FISCAL

1. O CREA-SP efetuará o pagamento no 15o (décimo quinto) dia após a apresentação da nota fiscal/fatura, a qual deverá ser entregue na Unidade de Infraestrutura do CREA-SP, na Sede Faria Lima, localizada na Av. Brigadeiro Faria Lima, 1059 – Pinheiros – CEP 01452-920 – São Paulo/SP, ficando a CONTRATADA obrigada a entregar juntamente com a Nota Fiscal, bemcomo manter durante execução dos serviços os documentos abaixo relacionados acompanhados da nota fiscal/fatura:

2. Comprovante de Regularidade com o Fundo de Garantia do Tempo de Serviço– Certificado de Regularidade do FGTS CRF.

3. Comprovante de regularidade para com a Fazenda Federal- Certidão de débitos relativos a créditos tributários Federais e àDivida ativa da União.

4. Comprovante de inexistência de débitos inadimplidos perante a Justiçado Trabalho, mediante a apresentação de Certidão

5. A nota fiscal/fatura será analisada, minimamente, quanto aos itens a seguir descritos:
   a. Correlação entre os valores indicados na nota fiscal/fatura o da proposta da empresa.
   b. Ausência de emendas ou rasuras na nota fiscal/fatura.
   c. O correto preenchimento dos dados do CREA-SP (nome, CNPJ, dados contratuais) e da discriminação dos serviços;
   d. Pertinência dos cálculos aritméticos da nota fiscal/fatura – o valor total deverá corresponder ao somatório dos valoresindividuais lançados na mesma,
   e. Correlação entre o valor da nota fiscal e os valores empenhados;
   f. Correlação entre o CNPJ da CONTRATADA e o constante na proposta e na nota de empenho;

6. O Crea-SP efetuará retenção de impostos eventualmente incidentes sobre o valor do bem/serviço, conforme previsto na LeiFederal no 9.430, de 27 de dezembro de 1996 e Instrução Normativa RFB no 1.234,de 11 de janeiro de 2012 e anexo;

7. A CONTRATADA é responsável pelos encargos fiscais, trabalhistas e previdenciários incidentes sobre os serviçoscontratados;

8. Se a CONTRATADA descumprir qualquer termo ou condição a que se obrigar no presente certame, por sua exclusiva culpa,poderá a Administração reter o pagamento, até que seja sanado o respectivo inadimplemento, não sobrevindo, portanto, qualquer ônus ao Conselho resultante desta situação;

9. Na hipótese do CREA-SP, por sua exclusiva culpa, efetuar com atraso qualquer pagamento previsto no Contrato, ficarásujeito multa de 2% (dois por cento) ao mês sobre o valor devido, calculada proporcionalmente aos dias de atraso.

7.4.3 CRONOGRAMA FÍSICO FINANCEIRO PARA O PERÍODO DE 36 MESES

1. A Tabela a seguir lista os principais marcos e eventos que ocorrerão durante a execução do Contrato:

Item	Descrição	Ano 1	Ano 2	Ano 3
1	Assinatura do contrato	N.A	N.A	N.A
2	Licenças de Software Microsoft (Itens 1-13 da TabelaA - Precificação Total deste Termo de Referência)	Parcela 1/3	Parcela 2/3	Parcela 3/3
3	Serviços sobDemanda	600 Horas	600 Horas	600 Horas
4	Serviço de implantação e migração Conforme tabela Tabela B - Sumarizadora de preços de Serviços deInstalação e migração	Pagamento Total mediante recebimento	N.A	N.A
5	Serviços de capacitação. Conforme tabela Tabela C - Sumarizadora de preços de Serviços de Capacitação	- Pagamento total mediante recebimento	N.A	N.A

7.4.4 DO REAJUSTE

1. Os preços são fixos e irreajustáveis no prazo de um ano contado da data limite para a apresentação das propostas.
2. Dentro do prazo de vigência do contrato e mediante solicitação da contratada, os preços contratados poderão sofrer reajusteapós o interregno de um ano, aplicando-se o índice ICTI (Índice de Custo da Tecnologia da Informação), previsto no art. 24 da Instrução Normativa nº 1, de 4 de Abril de 2019, do Ministério da Economia/Secretaria Especial de Desburocratização, Gestão e Governo Digital/Secretaria do Governo Digital:

> *"...Art. 24. Nas contratações de serviços de Tecnologia da Informação em que haja previsão de reajuste de preços por aplicação de índice de correção monetária, é obrigatória a adoção do Índice de Custos de Tecnologia da Informação - ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada – IPEA".*

3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros doúltimo reajuste.

8 - PROCEDIMENTOS DE FISCALIZAÇÃO DA EXECUÇÃO CONTRATUAL

8.1 PAPEIS E RESPONSABILIDADES

8.1.1 PAPEIS E RESPONSABILIDADES DO CREA NA FISCALIZAÇÃO DO CONTRATO

8.1.1.1 GESTOR DO CONTRATO

1. Servidor com atribuições gerenciais, designado para coordenar e comandar o processo de gestão e fiscalização daexecução contratual, indicado por autoridade competente.

8.1.1.2 FISCAL TÉCNICO

1. Servidor representante da Área de Tecnologia da Informação, indicado pela autoridade competente dessa áreapara fiscalizar tecnicamente o contrato.

8.1.1.3 FISCAL ADMINISTRATIVO

1. Servidor representante da Área Administrativa, indicado pela autoridade competente dessa área para fiscalizar ocontrato quanto aos aspectos administrativos.

8.1.2 PAPEIS E RESPONSABILIDADES DA CONTRATADA NA FISCALIZAÇÃO CONTRATUAL

8.1.2.1 PREPOSTO

1. Representante da CONTRATADA, responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto ao Órgão, incumbido de receber, diligenciar, encaminhar e responder às principais questões técnicas, legais e administrativas referentes ao andamento contratual:

2. Fazer a gestão geral do contrato, com o objetivo de garantir a execução dos serviços dentro dos prazosestabelecidos, atendendo a todos os requisitos de qualidade;

3. Realizar a gestão, por parte da CONTRATADA, quanto aos aspectos de caráter administrativo e legal do contrato;

4. Informar ao CREA-SP sobre problemas de qualquer natureza que possam impedir o andamento normal dosserviços;

5. Garantir a elaboração e entrega dos documentos e relatórios necessários;

6. Garantir a execução dos procedimentos administrativos referentes aos recursos envolvidos na execução dosserviços contratados;

7. Estar apto a prestar tempestivamente todas as informações (por meio de documentos impressos ou digitais) sobreas regularidades fiscais e financeiras da empresa, bem como a manutenção de todos os requisitos contratuais. Irregularidades administrativas ou contratuais poderão ensejar rescisão contratual;

8. Supervisionar todos os processos do trabalho, garantindo a qualidade dos serviços prestados;

9. Propor novas rotinas, processos e fluxos de trabalho, visando maior eficácia no serviço prestado;

10. Gerenciar o cumprimento de prazos e prioridades estabelecidos;

11. Gerenciar e acompanhar o desempenho da prestação de serviço.

8.2 CONTROLE E FISCALIZAÇÃO DA EXECUÇÃO

1. O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade da prestação dos serviços e da alocação dos recursos necessários, de forma a assegurar o perfeito cumprimento do ajuste, devendo ser exercidos por um ou mais representantes da CONTRATANTE, especialmente designados, na forma dos arts. 67 e 73 da Lei nº8.666, de 1993, e do art. 10 do Decreto nº 9.507, de 2018.

2. O representante da CONTRATANTE deverá ter a experiência necessária para o acompanhamento e controle da execuçãodos serviços e do contrato.

3. A verificação da adequação da prestação do serviço deverá ser realizada com base nos critérios previstos neste Termo deReferência e Anexos.

4. A execução do contrato será acompanhada e fiscalizada por meio de instrumentos de controle, que compreendam amensuração dos aspectos mencionados no art. 47 e no ANEXO V, item 2.6, i, ambos da IN nº 05/2017.

8.3 ENTREGA E CRITÉRIOS DE ACEITAÇÃO DO OBJETO

1. Prazo de entrega das licenças: no máximo 10 (dez) dias corridos a partir da assinatura do contrato. O descumprimento aoprazo citado sujeitará a EMPRESA CONTRATADA a penalidade de multa.

2. A entrega deve ser realizada no horário das 11:00 às 18:00 horas, de segunda a sexta- feira, considerando o calendário de feriados da cidade de São Paulo. A EMPRESA CONTRATADA deverá obter autorização para entrega, junto ao CREA-SP, comantecedência mínima de 24 horas, sob o risco dos produtos não serem recebidos.

3. Os instaladores dos softwares contratados, assim como suas atualizações, deverão estar disponíveis para download emconta registrada em nome do CREA-SP ou de representante indicado pelo CREA-SP em site oficial designado pelo fabricante.

4. A entrega (realização) dos serviços será acordada entre o CREA-SP e a CONTRATADA no momento da negociação doplano de trabalho para cada serviço.

8.3.1 CONDIÇÕES DE RECEBIMENTO

8.3.1.1 RECEBIMENTO DAS LICENÇAS DE SOFTWARE

1. Quando da entrega, a EMPRESA CONTRATADA deverá apresentar documento ou comprovação através de site web,fornecido pelo fabricante dos mesmos, que comprove a contratação das licenças compatível ao requerido no edital.

2. As produtos serão aceitos, mediante elaboração de relatório, da seguinte forma:

- Provisoriamente, quando da entrega.
- Definitivamente, após a verificação de todos os itens do termo de referência.

3. O aceite pelo CREA-SP não exclui a responsabilidade civil da empresa vencedora por vícios qualitativos, quantitativos outécnicos dos materiais ou por desacordo com as especificações estabelecidas neste termo de referência, verificadas posteriormente.

8.3.1.2 RECEBIMENTO DOS SERVIÇOS

1. Quando da entrega, a EMPRESA CONTRATADA deverá apresentar relatório de execução.

2. As serviços serão aceitos, mediante elaboração de relatório, da seguinte forma:

- Provisoriamente, quando da entrega do relatório.
- Definitivamente, após a verificação de conformidade do serviço prestado com o solicitado na Ordem de serviço correspondente.

3. O aceite pelo CREA-SP não exclui a responsabilidade civil da empresa vencedora por vícios qualitativos, quantitativos outécnicos dos materiais ou por desacordo com as especificações estabelecidas neste termo de referência, verificadas posteriormente.

9 - Bens e Serviços

	Bem/Serviço	Qtd.	Unidade	Valor Unitário (R$)	Valor Total (R$)
1	Microsoft 365 E3 - COD. AAA-10756	1.026	Licenças	10.196,70	10.461.814,20
2	Microsoft 365 E5 - COD. AAD-33168	10	Licenças	18.213,93	182.139,33
3	Licenças Exchange online, Plano 1 - COD.TRA-00047	40	Licenças	1.154,93	46.197,33
4	Microsoft EMS E3 + Security - COD. AAA-10732	40	Licenças	3.607,19	144.287,47
5	Windows Server Standard Core - COD. 9EM-00562	32	Licenças	2.243,76	71.800,32
6	Windows Server DC Core - COD. 9EA-00039	36	Licenças	10.760,17	387.366,00
7	Remote Desktop Services - COD. 6VC-01251	100	Licenças	2.036,95	203.694,67
8	SQL Server Enterprise Core - COD. 7JQ-00341	16	Licenças	225.963,21	3.611.091,31
9	Visual Studio Pro - COD. 77D-00110	12	Licenças	14.874,87	178.498,40
10	Visual Studio Enterprise - MX3-00115	2	Licenças	99.962,57	199.925,15
11	Azure DevOps Server. User CAL - COD. 126-00169	14	Licenças	7.390,44	103.433,16
12	Microsoft Visio Professional - COD. D87-01057	10	Licenças	10.275,12	102.751,20
13	Microsoft Phone System (add-on) - COD. LK6-00004	84	Licenças	2.328,81	195.620,32
14	Serviços sob Demanda (600 horas ano x 3anos). Conforme especificados	1.800	Horas	283,79	510.828,00
15	Serviço de implantação e migração Conforme tabela Tabela B - Sumarizadorade preços de Serviços de Instalação e migração	1	Serviço	552.560,44	552.560,44
16	Serviços de capacitação. Conforme tabela Tabela C - Sumarizadora de preços de Serviços de Capacitação	1	Serviço	192.125,94	192.125,94
				Valor Total (R$)	**17.144.166,24**

10 - ESTIMATIVA DAS QUANTIDADES

1. PREMISSAS

Todos os cálculos e estimativas de quantitativos estão contextualizados e justificados nos Estudos Técnicos Preliminares destacontratação.

1.1. A tabela a seguir lista os recursos necessários e os planos da Microsoft que permitem sua utilização.

Item	Funcionalidade	Exchange Online	EMS E3	Microsoft 365 E3	Microsoft 365 E5
1	Intune	N.A	x	x	x
2	Autenticação multifator (MFA)	N.A	x	x	x
3	Políticas de Acesso Condicional	N.A	x	x	x
4	SSPR (redefinição de senha de autoatendimento)	N.A	N.A	x	x
5	Privileged Identity Management (PIM)	N.A	N.A	N.A	x
6	e-mail	x	N.A	x	x
7	Gerenciamento de Chaves de Criptografia BitLocker	N.A.	x	x	x
8	DPL (Data Loss Prevention)	N.A.	x	x	x
9	Gerenciamento de chaves do BitLocker (DKM)	N.A.	x	x	x

Tabela de Funcionalidades por plano Microsoft

2. ESTIMATIVAS DAS QUANTIDADES

2.1. As justificativas abaixo estão listadas de acordo com os item da planilha de cotação de preços

2.2. Itens 1 ao 4 - Licenças do pacote Microsoft office 365

2.2.1 O calculo dos quantitativos de licenças do pacote Microsoft Office 365 levou em consideração os seguintes estudospreliminares realizados pela equipe de planejamento:

2.2.2. Estudo 1 - Estudo da Utilização atual de e-mails, por tipo.

a) Este estudo visou levantar a utilização de e-mails pelo CREA-SP, tanto o quantitativo, quanto o qualitativo, separandoas contas por tipo.

2.2.3. Estudo 2 - Estudo de volumetria de novas contas de terceiros solicitadas

a) Este estudo visou levantar a quantidade de contas de usuários terceirizados e a volumetria de solicitações desse tipode contas.

b) Neste estudo temos um total de 20 contas de terceiros (13 em 2020) e (7 em 2021 - jan a maio. Se projetarmos atédezembro, podemos utilizar a mesma média de 13 contas em 2021).

c) Desta forma, a equipe de planejamento irá utilizar uma média de 14 novas contas por ano.

2.2.4. Estudo 3 - Estudo do quantitativo de colaboradores

a) Este estudo visou levantar o quantitativo de colaboradores registrados no CREA-SP

2.2.5. Estudo 4 - Estudo das necessidades de Conselheiros

a) Este estudo visou levantar junto ao departamento de colegiados, quais as necessidades dos conselheiros referentes autilização dos aplicativos do pacote Office.

2.2.6. Estudo 5 - Estudo da Necessidade de Core Call Bridges

a) Este estudo visou levantar, junto à microsoft, a necessidade da aquisição de licenças de Core Call Bridge

2.3. Item 1 - Licenças para colaboradores - Microsoft Office 365 - E3

2.3.1. Os colaboradores que receberão licenças do Tipo E3 são os necessitam das funcionalidades descritas na tabela abaixo:

Item	Funcionalidade	Necessidade
1	Aplicativos do Pacote Office	Sim
2	MFA - Autenticação Multifator	Sim
3	SSRP (Self-Service Password Reset)	Sim
4	PIM (PIM (Privileged Identity Management)	Não
5	Gerenciamento de Dispositivos - Intune	Sim
6	Políticas de Acesso Condicional	Sim
7	Gerenciamento de Chaves de Criptografia	Sim

A = Total de colaboradores: 717 (Estudo 3)B =
Total de conselheiros: 260
C = Total de Colaboradores terceiros = 20 (Estudo 2)
D = Total de Licenças de Reserva Técnica para Terceiros: (anos do contrato) * (volumetria média anual de contas novas para terceiros/Estudo 2) = 3 * 13 = 39
E = Total de Funcionários da EINFRA que não receberão as licenças E3 = 10 (Valor a ser subtraído do valor total de licenças E3necessárias, pois esses usuários receberão licenças E5)

Total = (A + B + C + D) - E = (717 + 260 + 20 + 39) - 10 = 1036 - 10 = 1026

2.4. Item 2 - Licenças para Administradores do Microsoft Office 365 - E5

2.4.1. Como pode ser visto no quadro abaixo, os administradores do Office 365 necessitam do recurso PIM. Por isso serãocontemplados com licenças do tipo E5, as únicas que fornecem esse recurso.

Item	Funcionalidade	Necessidade
1	Aplicativos do Pacote Office	Sim
2	MFA - Autenticação Multifator	Sim
3	SSRP (Self-Service Password Reset)	Sim
4	PIM (PIM (Privileged Identity Management)	Sim
5	Gerenciamento de Dispositivos - Intune	Sim
6	Políticas de Acesso Condicional	Sim
7	Gerenciamento de Chaves de Criptografia	Sim

TOTAL = Funcionários da Equipe de Infraestrutura de TI (EINFRA) = 10

2.5. Item 3 e Item 4 - Licenças para sistemas corporativos - Exchange Online (Plano 1) + EMS/E3

2.5.1. Os sistemas corporativos do CREA que utilizam e-mail para enviar informações serão contemplados com licenças do tipo Exchange Online, as quais não possuem aplicativos do Office associadas, servindo apenas para enviar e receber e-mails, sendoportanto, mais baratas.

Item	Funcionalidade	Necessidade
1	Aplicativos do Pacote Office	Não
2	MFA - Autenticação Multifator	Não
3	SSRP (Self-Service Password Reset)	Não
4	PIM (PIM (Privileged Identity Management)	Não
5	Gerenciamento de Dispositivos - Intune	Não
6	Políticas de Acesso Condicional	Sim
7	Gerenciamento de Chaves de Criptografia	Sim

A = Quantidade de contas de sistemas: 30 (Estudo 1)
B = Quantidade de Reserva técnica para novos sistemas (cálculo abaixo): 7

2.5.2. Quantitativo de licenças para reserva técnica, para novos sistemas em fase de implantação e/ou projeto:
a) Sistema e atendimento do CallCenter (em fase de implantação): 2 emails (homologação e produção).
b) Sistema Barramento (em fase de implantação): 2 emails (homologação e produção)
c) Sistema de atendimento - substituto do Atendimento Web (em fase de implantação): 2 emails (homologação eprodução)
d) Sistema SCCM (System Center): 1 email

Total = 30 + 7 = 37 + 3 (arredondamento) = 40

2.6. Item 5 - Windows Server Standard

2.6.1. O CREA-SP possui dois servidores com 12 cores cada, totalizando 24 processadores, para sistemas quenecessitam de uma máquina com hardware e sistema operacional exclusivos.
2.6.2. Para esta quantidade de processadores é necessário um quantitativo de 32 licenças de Windows server standard,pois o licenciamento mínimo é de 16 cores para cada servidor,

2.7. Item 6 - Licenças Windows Server Core DataCenter

2.7.1. A licença de Windows Datacenter Server é adequada para ambientes virtualizados, pois cada licença atende a doisnúcleos do processador que hospeda o sistema operacional virtualizado.
2.7.2. O licenciamento de Windows Datacenter é baseado em processadores físicos. Cada licença de software abrange 2processadores físicos, para licenciar os 72 cores, atualmente instalados.
2.7.3. Para esta quantidade de processadores/cores é necessário um total de 36 licenças.

2.8. Item 7 - Windows Remote Desktop Services - Device CAL

2.8.1. Atualmente é uma Licença necessária para acessos simultâneos de RDP, porém válido apenas para Windows 2012R2 ou inferior.
2.8.2. Levando em consideração que o Conselho possui 717 funcionários /colaboradores que estão habilitados a utilizareste serviço sob demanda, e que o justifica o quantitativo atual de 600 licenças que foi adquirido anteriormente pelo Conselho.
2.8.3. O serviço é atualmente utilizado para acesso da ferramenta SIPRO.

2.8.4. Com a evolução da rede MPLS, a maioria dos funcionários passou a utilizar os serviços do SIPRO sem anecessidade de conexão via RDP. Desta forma a equipe de planejamento verificou que não há necessidade de renovação, ou aquisição de 600 licenças.

2.8.5. Verificou -se portanto, que um quantitativo de 100 licenças seria o suficiente para atender as necessidades do CREA. Visto que são licenças baseadas em dispositivo e não em pessoas, vários usuários poderão utilizar a mesma licença, desde que não

simultaneamente. Portanto a conexão simultânea de 100 dispositivos é o suficiente para atendera demanda.

2.9. Item 8 - SQL Server Enterprise DataCenter

2.9.1. Gerenciador de Banco de Dados para aplicações transacionais e Analíticas, possuindo componentes nativos paradesenvolvimento de uma plataforma completa de Data Warehouse e Business Intelligence (ETL, Data Quality, OLAP eReporting).
2.9.2. A Edição Enterprise é ideal para aplicativos que exigem desempenho de missão crítica em memória, segurança ealta disponibilidade m ambiente de Datacenter (virtualizado).
2.9.3. O ambiente produtivo de banco de dados SQL Server do CREA-SP é composto de diversos servidores. Todos hospedados em máquinas virtualizadas na infraestrutura física do CREA-SP.
2.9.4. Para o licenciamento de SQL, cada licença adquirida possibilita licenciar 2 Cores.
2.9.5. Para a quantidade de processadores é necessário 16 licenças de SQL Server Enterprise.

1.10. Item 9 e 10 Visual Studio

2.10.1. O Visual Studio é uma solução integrada e de ponta a ponta. Ambiente de desenvolvimento integrado avançadoque dispõe de ferramentas de suporte, serviços e benefícios. Produtividade, DevOps, ferramentas de testes manuais eautomatizados, treinamento, créditos de Azure e benefícios da assinatura MSDN. Licença com extensões incluídas da Microsoft para Visual Studio Team Foundation Server e Visual Studio Team Services.

2.10.2. Ambiente de desenvolvimento de software profissional, como descrito no Visual Studio Pro, com colaboração emequipe.
2.10.3. O licenciamento Enterprise é uma solução de nível empresarial com recursos avançados para equipes que trabalham em projetos de qualquer tamanho ou complexidade, incluindo testes avançados e DevOps.

2.10.4. Em levantamento com a área de desenvolvimento do CREA-SP foi levantada a quantidade de 12 Licenças de Visual Studio Professional e 2 Licenças de Visual Studio Enterprise.

2.11. Item 11 - Licenças Azure DevOps Server User CAL

2.11.1. A quantidade de licenças de Azure DevOps deve se a mesma das Licenças de Visual Studio. 14 Unidades

2.12. Item 12 - Microsoft Visio Professional para Office 365

2.12.1. O software Microsoft Visio visa ao atendimento das demandas de Tecnologia da Informação do CREA-SP para odesign de plataformas e ambientes de hardware e software.
2.12.2. A Equipe da EINFRA é formada por 10 pessoas. Portanto sendo necessárias 10 Licenças.

2.13. Item 13 - Licenças Microsoft Phone System (add-on)

2.13.1. Essas licenças serão utilizadas pelos Gestores do CREA-SP para interligar os sistemas de Telefonia Voip aoTeams.
2.13.2. Funcionários que ocupam cargos de gestão (funções de confiança e comissionados) é de 84.

2.14. Item 14 - Serviços sob Demanda

2.14.1. São serviços que serão utilizados na Consultoria técnica na implantação de soluções relativas ao Pacote Microsoft Office365 e integração com as demais soluções tecnológicas implementadas no CREA-SP.
2.14.2. Os Serviços de implantação listados acima deverão ser contratados na forma de pagamento único, após execução.
2.14.3. Para realizar manutenções esporádicas nas implementações executadas, e na implementação de novos serviços necessários ao CREA-SP e relacionados as licenças de software adquiridas e aos planos de serviços em nuvem do MicrosoftOffice 365, a equipe de planejamento utilizará o modelo de contratação híbrida.
2.14.4. Como não há meio de estimar o quantitativo do horas utilizadas para serviços ainda não planejados, e não há históricoanterior por se tratarem de serviços novos, a equipe de planejamento utilizou como parâmetro um quantitativo mensal de 50 horas, que parece se rum valor razoável tendo em vista a multiplicidade de perfis técnicos que deverão atuar nas soluções. Ouseja, para atendimento de uma demanda, a CONTRATADA deverá disponibilizar profissional gerente de projeto, além de profissionais tecnicamente capacitados em cada um dos produtos afetados.
2.14.5. Apesar de ser subjetiva esta estimativa, não trará nenhum prejuízo financeiro ao CREA-SP, pois não há obrigatoriedadeda contratação, e o CREA-SP só pagará pelas horas efetivamente utilizadas, as quais deverão previamente planejadas em conjunto com o fiscal do contrato para garantir que estão sendo calculadas de forma adequada.

2.15. Item 15 - Serviço de Implantação e Migração

2.15.1. Para realizar a implantação dos serviços e dispositivos adquiridos através das licenças do Microsoft Office 365, a equipede planejamento identificou as seguintes necessidades:

a) Implantação do Intune
b) Implantação do Multifator de Autenticação (MFA)
c) Implantação de Políticas de acesso condicional
d) Implantação do System Center/Intune para controle de atualização de softwares da Microsoft (Windows, office, etc)
e) Implantação do SSPR (Self-Service Password Reset)
f) Implantação de conformidade de políticas de administração de Active Directory- Análise da Arquitetura atual do Active Directory, Verificação de conformidade com as melhores práticas de administração e g) segurança. Implantação de modelo deadministração
h) Implementação pacote Microsoft Office E3. (migração do Office 365 E1 para o Microsoft Office E3)
i) Implementação do DLP (Data Loss Prevention)
j) Implantação de criptografia do BitLocker e Distributed Key Manager (DKM)
k) Implementação do PIM para a equipe de administração do Office.
l) Desenvolvimento de indicadores de BI para área de Suporte acompanhar a execução dos chamados técnicos. (chamados emaberto, em espera, atendidos, etc) utilizando da integração com a ferramenta GLPI e ISM da ServiceAIDE
m) Desenvolvimento de indicadores de BI para saúde de 1 Servidor (Utilização de Memória, CPU, DISCO, REDE) integrandocom Zabbix

2.15.2. Além desses serviços listados, há também a necessidade de realizar as seguintes migrações:

a) Atualização do Servidor Exchange – Relay Utilizamos um servidor de Exchange para realizar relay de smpt das aplicações do CREA que enviam e-mail. Necessidade: Atualizar o Servidor e escrever melhores políticas de utilização

b) Migração de Servidores Windows Server 2012 R2 para a versão mais atual. Temos 20 servidores virtuais nessasituação que precisam ser migrados.

2.16. Item 16 - Serviços de Capacitação

2.16.1. Os quantitativos dos treinamentos e workshops está baseado nos projetos de implementação elencados anteriormente,conforme discriminados na tabela abaixo.
2.16.2. O item 15 da tabela refere-se a workshops que serão definidos durante o processo de migração, baseados nasnecessidades dos usuários do CREA-SP.
2.16.3. Esta estimativa, é inerentemente subjetiva, pois não há como verificar essa necessidade através de dados de problemaspassados, visto que o ambiente do Microsoft 365 é algo totalmente novo para os colaboradores do CREA-SP. O que eles utilizam hoje, é o office 365, com licenças do tipo E1, que não possuem os mesmos recursos de segurança avançados que os do Microsoft 365 E3.

2.16.4. Dito isso, a equipe de planejamento estima que a realização de um workshop por mês, durante um ano seja suficiente para treinar todos os funcionários e colaboradores do CREA-SP nas melhores práticas de utilização da ferramenta Teams e doambiente de colaboração do Microsoft 365. Um workshop por mês (dividido em duas turmas para melhor adequação no calendário dos funcionários) está dentro do princípio de razoabilidade, e caso não se julgue um número suficiente, ou esteja super dimensionado poderá ser incrementado/diminuído em 25% através de aditivo contratual.

2.16.5. A equipe da EINFRA é composta de 10 profissionais, sendo que cada treinamento oficial da Microsoft deve ser fornecidopara 5 pessoas, de forma a termos equipes multidisciplinares, treinadas em todas as áreas de conhecimento necessárias para administrar a solução como um todo e poder determinar políticas, procedimentos e necessidade de novos serviços que serãoimplementados através da utilização do banco de horas. Também melhorando a capacidade da equipe de fiscalizar a execução dos projetos e banco de horas, garantindo que sejam bem dimensionados e não consumam mais horas do que o efetivamente necessário para conclusão dos seus resultados com eficiência, eficácia, efetividade e economicidade.

ID	Projeto	Treinamento Necessário
1	Implantação do Intune	- 2 Workshops técnico para equipe de T.I. - 2 Workshops para usuários - Elaboração de procedimento passo a passo para usuários - Elaboração de procedimentos de política de administração para a equipe de sustentação Disponibilização, para a equipe de sustentação deTI, do seguinte treinamento oficial da Microsoft: - Curso Managing Modern Desktops
2	Implantação do Multifatorde Autenticação (MFA)	- 2 Workshops técnico para equipe de T.I. - Elaboração de procedimento passo a passo para usuários - Elaboração de procedimentos de política de administração para a equipe de sustentação Disponibilização, para a equipe de sustentação deTI, dos seguintes treinamentos oficiais da Microsoft: - Curso Microsoft 365 Security Administration - Curso Microsoft Identity and Access Administrator

3	Implantação de Políticas de acesso condicional	- 2 Workshops técnico para equipe de T.I. - Elaboração de procedimentos de política de administração para a equipe de sustentação
4	Implantação do System Center/Intune para controle de atualização de softwaresda Microsoft (Windows, office, etc)	- 2 Workshops técnico para equipe de T.I. - Elaboração de procedimentos de política de administração para a equipe de sustentação Disponibilização, para a equipe de sustentação deTI, do treinamento oficial da Microsoft: - Curso 20703-1-B: Administering System Center Configuration Manager
5	Implantação do SSPR (Self-Service Password Reset)	- 2 Workshops técnicos para equipe de T.I. - 2 Workshops para usuários - Elaboração de procedimento passo a passo para usuários - Elaboração de procedimentos de política de administração para a equipe de sustentação
6	Implantação de conformidade de políticas de administração de ActiveDirectory	- 2 Workshops técnicos para equipe de T.I. - Elaboração de procedimentos de política de administração para a equipe de sustentação Disponibilização, para a equipe de sustentação deTI, dos seguinte treinamento oficial da Microsoft: - Curso Identity with Windows Server
7	migração do Office 365 E1 para o Microsoft Office E3	- 2 Workshops técnicos para equipe de T.I. - Elaboração de procedimentos de política de administração para a equipe de sustentação
8	Implementação de políticasde DLP	- 2 Workshops técnicos para equipe de T.I. - 2 Workshops para usuários - Elaboração de procedimento passo a passo para usuários - Elaboração de procedimentos de política de administração para a equipe de sustentação
9	Implementação de criptografia nos dispositivosde acesso e Distributed KeyManager (DKM)	- 2 Workshops técnicos para equipe de T.I. - 2 Workshops para usuários
10	Implementação do PIMpara a equipe de administração do Office.	- 2 Workshops técnicos para equipe de T.I.
11	Desenvolvimento de indicadores de BI para áreade Suporte	- 2 Workshops técnicos para equipe de T.I.
12	Desenvolvimento de indicadores de BI para saúde de Servidores	- 2 Workshops técnicos para equipe de T.I.

13	Atualização do Servidor Exchange	- 2 Workshops técnicos para equipe de T.I. Disponibilização, para a equipe de sustentação deTI, do seguinte treinamento oficial da Microsoft: - Curso Administering Microsoft Exchange Server 2016/2019
14	Migração de Servidores Windows Server 2012 R2	- 2 Workshops técnicos para equipe de T.I. Disponibilização, para a equipe de sustentação deTI, do treinamento oficial da Microsoft: - Curso Securing Windows Server 2016
15	Worshops de implantação e utilização dos recursos do Microsoft 365 (segurança, meeting, calling, configuração, utilização, etc)	- 24 Workshops para usuários Disponibilização, para a equipe de sustentação deTI, dos seguintes treinamentos oficiais da Microsoft: - Curso Microsoft 365 Messaging - Curso Microsoft Information Protection Administrator - Microsoft 365 Certified: Teams Administrator Associate

11 - PLANILHA PARA COTAÇÃO DE PREÇO

Tabela A - Precificação Total

Item	Descrição	COD MICROSOFT	Qtde	Unidade	Preço Unitário R$	Preço Total R$
1	Microsoft 365 - M365 E3	AAA-10756	1026	Licenças		
2	Microsoft 365 E5	AAD-33168	10	Licenças		
3	Exchange online - Plano 1	TRA-00047	40	Licenças		
4	Microsoft EMS E3 + Security	AAA-10732	40	Licenças		
5	Windows Server Standard Core	9EM-00562	32	Licenças		
6	Windows Server DC Core	9EA-00039	36	Licenças		
7	Windows Remote Desktop Services -Device CAL	6VC-01251	100	Licenças		
8	SQL Server Enterprise Core	7JQ-00341	16	Licenças		
9	Visual Studio Pro	77D-00110	12	Licenças		
10	Visual Studio Enterprise	MX3-00115	2	Licenças		
11	Azure DevOps Server. User CAL	126-00169	14	Licenças		
12	Microsoft Visio Professional	D87-01057	10	Licenças		
13	Licenças Microsoft Phone System (add-on)	LK6-00004	84	Licenças		

14	Serviços sob Demanda (600 horas anox 3 anos) - deve fornecer as planilhas de formação de Custo	N.A	1800	Horas		
15	Serviço de implantação e migração Conforme tabela **Tabela B** - Sumarizadora de preços de Serviços deInstalação e migração	N.A	1	Serviço		
16	Serviços de capacitação. Conforme tabela **Tabela C** - Sumarizadora de preços de Serviços de Capacitação	N.A	1	Serviço		

Obs: Para o item 14 a empresa deve fornecer as planilhas de Formação de CustoTabela B -

Sumarizadora dos serviços de implantação e migração

ID	Descrição	Valor R$
1	Implantação do Intune	
2	Implantação do Multifator de Autenticação (MFA)	
3	Implantação de Políticas de acesso condicional	
4	Implantação do System Center/Intune para controle de atualização de softwares da Microsoft (Windows, office, etc)	
5	Implantação do SSPR (Self-Service Password Reset)	
6	Implantação de conformidade de políticas de administração deActive Directory	
7	Migração do Office 365 E1 para o Microsoft Office E3	
8	Implementação de políticas de DLP	
9	Implementação de criptografia e Distributed Key Manager(DKM)	
10	Implementação do PIM para a equipe de administração doOffice.	
11	Desenvolvimento de indicadores de BI para área de Suporte	
12	Desenvolvimento de indicadores de BI para saúde deServidores	
13	Atualização do Servidor Exchange	
14	Migração de Servidores Windows Server Antigos	
15	**(item 15 da Tabela A - Precificação Total) Total**	

Tabela C - Sumarizadora de preços de Serviços de Capacitação

ID	Descrição	Valor R$
1	Implantação do Intune Implantação do Multifator de Autenticação (MFA)Implantação de Políticas de acesso condicional	
2	Implantação do System Center/Intune para controle de atualização de softwares da Microsoft (Windows, office, etc)	
3	Implantação do SSPR (Self-Service Password Reset)	
4	Implantação de conformidade de políticas de administração deActive Directory	
5	migração do Office 365 E1 para o Microsoft Office E3	
6	Implementação de políticas de DLP	
7	Implementação de criptografia e Distributed Key Manager(DKM)	
8	Implementação do PIM para a equipe de administração doOffice.	
9	Desenvolvimento de indicadores de BI para área de Suporte	
10	Desenvolvimento de indicadores de BI para saúde deServidores	
11	Atualização do Servidor Exchange	
12	Passagem de conhecimento - Asbuilt - Migração de ServidoresWindows ServerAntigos	
13	Worshops de implantação e utilização dos recursos do Microsoft365 (segurança, meeting, calling, configuração, utilização, etc)	
14	**(item 16 da Tabela A - Precificação Total) Total**	

12 - FONTE DE RECURSOS ORÇAMENTÁRIOS

12.1 DOTAÇÃO ORÇAMENTÁRIA

Os recursos orçamentários para a presente contratação são oriundos:

- **Conta Contábil:** 6.2.2.1.1.01.04.09.005
- **Centro de Custo:** 01.03.17.09.01.01

13 - LOCAIS DE ENTREGA

13.1 Endereço: Av. Brigadeiro Faria Lima, 1059 - Pinheiros - São Paulo - SP

- Telefone para informações: (11) 3095 - 6484

14 - CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

REGIME DE EXECUÇÃO	( ) Empreitada	( ) Preço Global	(X) Preço Unitário

ADJUDICAÇÃO DO OBJETO	(X) Global	( ) Por Lote	( ) Por Item

14.1 - Qualificação Técnica

14.1.1 JUSTIFICATIVA QUALIFICAÇÃO TÉCNICA

1 Em face da criticidade dos equipamentos que suportam toda a infraestrutura de redes corporativa do CREA-SP, atenderem a todas as áreas de negócio da empresa e necessitarem de atendimento técnico especializado, com a possibilidade de troca de equipamentos, faz-se necessário que a empresa CONTRATADA demonstre a comprovação deaptidão aos serviços contratados através de atestado(s) de serviços similares de complexidade tecnológica.

14.1.2 1 É necessária comprovação de aptidão para a para o fornecimento de licenças, produtos, manutenção, atualização esuporte dos mesmos. serviços de implantação e migração com a devida transferência de conhecimento em características, quantidades e prazos compatíveis com o objeto desta licitação, por meio de apresentação de Atestado fornecido por pessoas jurídicas de direito público ou privado.

2 O(s) atestado(s) deverão ser apresentados em papel timbrado do emitente, conter identificação do signatário, nome,endereço, telefone e se for o caso, correio eletronico para contato, a fim de possibilitar possíveis diligências.

14.1.3 A Licitante Vencedora deverá apresentar obrigatoriamente, **na assinatura do Contrato** comprovação de que é revendedora ou distribuidora autorizada do Microsoft, no mínimo, na categoria Microsoft licensing solution provider (LSP). Estacomprovação pode ser feita através de qualquer das alternativas abaixo:

1. Indicação da página Internet (URL do website) do fabricante que contenha esta informação;
2. Cópia do contrato entre a Empresa Licitante e o fabricante;
3. Declaração do próprio fabricante informando se a Empresa Licitante é a própria fabricante, revendedora ou distribuidoraautorizada Select Partner (e/ou superior). Essa declaração deverá ser feita em papel timbrado do fabricante.

14.2 - Critérios de Seleção

14.2.1 - Critérios Gerais

14.2.1.1 DO TRATAMENTO DIFERENCIADO ÀS MICROEMPRESAS, EMPRESAS DE PEQUENO PORTE E COOPERATIVA

1. As microempresas e empresas de pequeno porte, que se beneficiarem do regime diferenciado e favorecido concedido pelaLei Complementar n. 123 de 2006, por ocasião da participação neste certame licitatório, deverão apresentar toda adocumentação exigida para habilitação, inclusive para efeito de comprovação de regularidade fiscal, mesmo que apresente alguma restrição.

2. Está vedada a participação de cooperativas nos termos da seção da vedação à participação de Cooperativas.

14.2.1.2 REGIME DE EXECUÇÃO

1. O regime da execução dos contratos é de EMPREITADA POR PREÇO UNITÁRIO.

14.2.2 - Subcontratação

14.2.2.1 Será permitida a subcontratação apenas e tão somente para os serviços de treinamento oficial da Microsoft.

14.2.3 - Formação de Consórcios

14.2.3.1 Não será permitida formação de Consórcio.

14.2.4 - Alteração Subjetiva

14.2.4.1 É admissível a fusão, cisão ou incorporação da CONTRATADA com/por outra pessoa jurídica, desde que sejam

observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas asdemais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa daAdministração à continuidade do contrato.

14.2.5 - Garantia Contratual

14.2.5.1 Não será exigida a prestação de garantia de execução para celebrar a contratação decorrente deste certame licitatório.

15 - PROCEDIMENTOS PARA APLICAÇÃO DAS SANÇÕES

15.1 - Sanções Administrativas

15.1.1 1 - Comete infração administrativa nos termos da Lei nº 8.666, de 1993 e da Lei nº 10.520, de 2002, a Contratada que:

1.1 - inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

1.2 - ensejar o retardamento da execução do objeto;

1.3 -fraudar na execução do contrato;1.4-

comportar-se de modo inidôneo;

1.5 - cometer fraude fiscal;

1.6 - não mantiver a proposta.

2 - A Contratada que cometer qualquer das infrações discriminadas no subitem acima ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

2.1 - Advertência por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para aContratante;

2.2 - Multa compensatória de 20% (vinte por cento) sobre o valor total do contrato, no caso de inexecução total doobjeto;

2.3 - Multa moratória de 1% (um por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até olimite de 10 (dez) dias;

2.3.1 - Em caso de inexecução parcial, a multa compensatória, no mesmo percentual do subitem acima, seráaplicada de forma proporcional à obrigação inadimplida;

2.4 - Suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual aAdministração Pública opera e atua concretamente, pelo prazo de até 02 (dois) anos;

2.5 - Impedimento de licitar e contratar com a União com o consequente descredenciamento no SICAF pelo prazo de até05 (cinco) anos;

3 - A Sanção de impedimento de licitar e contratar prevista neste subitem também é aplicável em quaisquer das hipótesesprevistas como infração administrativa no subitem "10.1" deste instrumento.

4. - As sanções previstas nos subitens 2.1, 2.3 e 2.4 poderão ser aplicadas à Contratada juntamente com as de multa,descontando-a dos pagamentos a serem efetuados.

5.- Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:

5.1. - Tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquertributos;

5.2.- Tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

5.3. - Demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

6.- A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditórioe a ampla defesa à Contratada, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.

7.- A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

8. - As penalidades serão obrigatoriamente registradas no SICA

16 - ANEXO DO TERMO DE REFERÊNCIA

ANEXO A - Conteúdo Programático.pdf

ANEXO A – CONTEÚDO PROGRAMÁTICO

CONTEÚDOS PROGRAMÁTICOS MÍNIMOS PARA OS TREINAMENTOS OFICIAIS MICROSOFT

CURSO: MICROSOFT INFORMATION PROTECTION ADMINISTRATOR

Duração mínima:2 Dias

Objetivo: aprender como proteger informações em sua implantação do Microsoft 365. Este curso se concentra na governança de dados e proteção de informações dentro de sua organização. O curso abrange a implementação de políticas de prevenção de perda de dados, tipos de informações confidenciais, rótulos de sensibilidade, políticas de retenção de dados e criptografia de mensagens do Office 365, entre outros tópicos relacionados.

O curso ajuda os alunos a se prepararem para o Microsoft Information Protection Administrator exam (SC-400).

Estrutura de tópicos do curso

Módulo 1: Implementar proteção de informações no Microsoft 365

As organizações exigem soluções de proteção de informações para proteger seus dados contra roubo e perda acidental. Aprenda como proteger suas informações confidenciais. Saiba como as soluções de governança e proteção de informações do Microsoft 365 ajudam você a proteger e controlar seus dados, em todo o seu ciclo de vida - onde quer que vivam ou onde quer que viajem. Saiba mais sobre as informações disponíveis para ajudá-lo a entender seu panorama de dados e conhecer seus dados. Aprenda a usar tipos de informações confidenciais para dar suporte à sua estratégia de proteção de informações. Aprenda como os rótulos de sensibilidade são usados para classificar e proteger os dados de negócios, garantindo que a produtividade do usuário e sua capacidade de colaboração não sejam prejudicadas.

Aulas

- Introdução à proteção e governança de informações no Microsoft 365
- Classificar dados para proteção e governança
- Criar e gerenciar tipos de informações confidenciais
- Descrever a criptografia do Microsoft 365
- Implantar criptografia de mensagem no Office 365
- Configurar rótulos de sensibilidade
- Aplicar e gerenciar rótulos de sensibilidade

Laboratório : Implementação de proteção de informações

- Atribuir permissões para conformidade
- Gerenciar a criptografia de mensagens do Office 365
- Gerenciar tipos de informações confidenciais
- Gerenciar classificadores treináveis
- Gerenciar rótulos de sensibilidade

Depois de concluir este módulo, os alunos serão capazes de :

- Descrever a abordagem da Microsoft para proteção e governança de informações.
- Listar os componentes da solução de Classificação de Dados.
- Descrever como usar tipos de informações confidenciais e classificadores treináveis.
- Implementar impressão digital de documentos
- Criar dicionários de palavras-chave personalizados
- Implantar criptografia de mensagem no Office 365

Módulo 2: Implementar a Prevenção contra Perda de Dados no Microsoft 365

Neste módulo, discutimos como implementar técnicas de prevenção de perda de dados para proteger seus dados do Microsoft 365. Aprenda como descobrir, classificar e proteger conteúdo sensível e crítico para os negócios em todo o seu ciclo de vida em sua organização. Aprenda a configurar e implementar políticas de prevenção de perda de dados e integrá-las ao Microsoft Cloud App Security. Aprenda como responder e mitigar as violações da política de perda de dados.

Aulas

- Prevenção de perda de dados no Microsoft 365
- Implementar prevenção contra perda de dados do Endpoint
- Configurar políticas de DLP para Microsoft Cloud App Security e Power Platform
- Gerenciar políticas e relatórios de DLP no Microsoft 365

Laboratório : Implementar prevenção contra perda de dados

- Gerenciar políticas DLP
- Gerenciar Endpoint DLP
- Testar políticas DLP
- Relatórios de gerenciamento de DLP

Depois de concluir este módulo, os alunos serão capazes de:

- Descrever o processo de configuração da proteção de informações.

- Articular as melhores práticas de implantação e adoção.
- Descrever a integração do DLP com o Microsoft Cloud App Security (MCAS).
- Configurar políticas no Microsoft Cloud App Security.
- Revisar e analisar relatórios DLP.
- Identificar e mitigar violações da política DLP.
- Mitigar violações DLP no MCAS.

Módulo 3: Implementar governança de informações no Microsoft 365

Neste Módulo, você aprenderá como planejar e implementar estratégias de governança da informação para uma organização. Aprenda como gerenciar seu ciclo de vida de conteúdo usando soluções para importar, armazenar e classificar dados críticos para os negócios de modo que você possa manter o que precisa e excluir o que não precisa. Aprenda como gerenciar a retenção para o Microsoft 365, e como as soluções de retenção são implementadas nos serviços individuais do Microsoft 365. Aprenda como usar a classificação inteligente para automatizar e simplificar o cronograma de retenção de registros regulamentares, legais e críticos para os negócios em sua organização.

Aulas

- Controle de informações no Microsoft 365
- Gerenciar a retenção de dados em cargas de trabalho do Microsoft 365
- Gerenciar registros no Microsoft 365

Laboratório : Implementar governança de informações

- Configurar etiquetas de retenção
- Implementar etiquetas de retenção
- Configurar retenção baseada em serviço
- Usar eDiscovery para recuperação
- Configurar gerenciamento de registros

Depois de concluir este módulo, os alunos serão capazes de:

- Descrever o processo de configuração da governança da informação.
- Articular as melhores práticas de implantação e adoção.
- Descrever os recursos de retenção em cargas de trabalho do Microsoft 365.
- Definir as configurações de retenção no Microsoft Teams e no SharePoint Online.
- Implementar retenção para itens da Exchange Mailbox.
- Recupere conteúdo protegido por configurações de retenção.
- Recupere itens protegidos de caixas de Exchange Mailboxes.
- Descrever o processo de configuração do gerenciamento de registros.

CURSO: MICROSOFT 365 SECURITY ADMINISTRATION

Duração mínima: 4 dias

Objetivo: Aprender como assegurar o acesso dos usuários aos recursos da sua organização. O curso deve cobrir a proteção da palavra-passe do utilizador, autenticação multi-factor, como permitir a Azure Identity Protection, como configurar e utilizar o Azure AD Connect, e introduzi-lo ao acesso condicional no Microsoft 365.

Aprender sobre tecnologias de proteção contra ameaças que ajudam a proteger o seu ambiente Microsoft 365. Especificamente, aprender sobre os vectores de ameaças e as soluções de segurança da Microsoft para mitigar as ameaças.

Aprender sobre a pontuação segura, proteção Exchange Online, Azure Advanced Threat Protection, Windows Defender Advanced Threat Protection, e gestão de ameaças.

No curso aprender sobre tecnologias de proteção de informação que ajudam a proteger o seu ambiente Microsoft 365.

O curso deve discutir conteúdos geridos por direitos de informação, encriptação de mensagens, assim como rótulos, políticas e regras que apoiam a prevenção da perda de dados e a proteção de informação.

Aprender sobre arquivamento e retenção no Microsoft 365, bem como sobre gestão de dados e como conduzir pesquisas e investigações de conteúdo.

Este curso deve abranger políticas e etiquetas de retenção de dados, gestão de registos no local para SharePoint, retenção de correio eletrônico, e como conduzir pesquisas de conteúdo que suportam investigações de eDiscovery.

Estrutura de tópicos do curso

Módulo 1: Gestão de utilizadores e grupos

Este módulo explica como gerenciar contas e grupos de usuários no Microsoft 365. Ele introduz a você o conceito de confiança zero, bem como a autenticação. O módulo estabelece a base para o restante do curso.

Lições

Conceitos de Gerenciamento de Identidade e Acesso

O modelo Trust Zero

Planeje sua solução de identidade e autenticação

Contas de usuário e funções

Laboratório : Inicialize seu inquilino - usuários e grupos

Configurar o locatório do Microsoft 365

Gerenciar usuários e grupos

Laboratório : Gerenciamento de senhas

Configurar Self-service password reset (SSPR) para contas de usuário no Azure AD

Usar Azure AD Smart Lockout

Depois de completar este módulo, os estudantes estarão aptos a:

Criar e gerenciar contas de usuário.

Descrever e usar funções de administrador do Microsoft 365

Planejar políticas de senha e autenticação

Descrever os conceitos de segurança Zero Trust.

Explicar o modelo do Trust Zero.

Módulo 2: Sincronização e Proteção de Identidade

Este módulo explica os conceitos relacionados à sincronização de identidades para o Microsoft 365. Especificamente, ele se concentra no Azure AD Connect e no gerenciamento da sincronização de diretórios para garantir que as pessoas certas estejam se conectando ao seu sistema Microsoft 365.

Lições

Sincronização do diretório do plano

Configurar e gerenciar identidades sincronizadas

Azure AD Identity Protection

Laboratório : Implementando a sincronização de identidades

Configure sua organização para sincronização de identidades

Depois de completar este módulo, os estudantes estarão aptos a:

Explicar a sincronização de diretórios

Planejar sincronização de diretório

Descrever e usar o Azure AD Connect.

Configurar pré-requisitos do Azure AD Connect

Gerenciar usuários e grupos com sincronização de diretórios.

Descrever a federação do Active Directory.

Habilitar a Azure Identity Protection

Módulo 3: Gerenciamento de Identidade e Acesso

Este módulo descreve o acesso condicional do Microsoft 365 e como pode ser usado para controlar o acesso aos recursos em sua organização. O módulo também explica o RBAC (Role Based Access Control) e as soluções para acesso externo. Discutimos a governança da identidade como um conceito e seus componentes.

Lições

Gestão de aplicações

Identidade Governança

Gerenciar o acesso ao dispositivo

Controlar de acesso baseado em função (RBAC)

Soluções para acesso externo

Gestão da Identidade Privilegiada

Laboratório: Uso do acesso condicional para ativar o MFA

Piloto de autenticação do MFA (requer MFA para aplicativos específicos)

Acesso condicional do MFA (concluir uma implantação do MFA)

Laboratório : Configurar Gestão de Identidade Privilegiada

Administrar os recursos do Azure

Atribuir funções de diretório

Ativar e desativar as funções do PIM

Cargos de diretório

Fluxos de trabalho de recursos do PIM

Ver histórico de auditoria das funções do Azure AD no PIM

Depois de completar este módulo, os estudantes estarão aptos a:

Descrever o conceito de acesso condicional

Descrever e usar políticas de acesso condicional.

Planejar a conformidade do dispositivo.

Configurar usuários e grupos condicionais.

Configurar o controle de acesso baseado em função

Descrever os conceitos de governança da identidade

Configurar e utilizar Gestão de Identidade Privilegiada

Módulo 4: Segurança no Microsoft 365

Este módulo explica as várias ameaças de ataque cibernético existentes. Em seguida, apresenta as soluções da Microsoft para mitigar essas ameaças. O módulo termina com uma explicação do Microsoft Secure Score e como ele pode ser usado para avaliar e relatar a postura de segurança da sua organização.

Lições

Vetores de ameaças e violações de dados

Estratégia e princípios de segurança

Soluções de segurança Microsoft

Secure Score

Laboratório: Uso do Microsoft Secure Score

Melhora da sua pontuação segura no Microsoft 365 Security Center

Depois de completar este módulo, os estudantes estarão aptos a:

Descrever várias técnicas que os hackers usam para comprometer as contas de usuário por e-mail.

Descrever as técnicas que os hackers usam para obter controle sobre os recursos.

Enumerar os tipos de ameaças que podem ser evitadas utilizando o EOP e o Microsoft Defender for Office 365.

Descrever os benefícios do Secure Score e que tipo de serviços podem ser analisados.

Descrever como usar o Secure Score para identificar falhas na sua postura de segurança atual do Microsoft 365.

Módulo 5: Proteção avançada contra ameaças

Este módulo descreve as várias tecnologias e serviços de proteção contra ameaças disponíveis no Microsoft 365. O módulo cobre a proteção de mensagens através do Exchange Online Protection, Microsoft Defender for Identity e Microsoft Defender for Endpoint.

Lições

Proteção em linha de troca (EOP)

Microsoft Defender for Office 365

Gerenciando anexos seguros

Gerenciando links seguros

Microsoft Defender for Identity

Microsoft Defender for Endpoint

Laboratório : Gerenciar Serviços de Segurança da Microsoft 365

Implementar políticas de defesa da Microsoft

Depois de completar este módulo, os estudantes estarão aptos a:

Descrever o pipeline anti-malware conforme o email é analisado pelo Exchange Online Protection.

Descrever como os Anexos seguros são usados para bloquear malware de dia zero em Anexos e documentos de email.

Descrever como os links seguros protegem os usuários de URLs mal-intencionados incorporados no e-mail e nos documentos que apontam para sites inseguros.

Configurar o Microsoft Defender para Identidade.

Configurar o Microsoft Defender para Endpoint.

Módulo 6: Gerenciamento de ameaças

Este módulo descreve o Microsoft Threat Management, que fornece as ferramentas para avaliar e identificar ameaças cibernéticas e formular respostas. Você aprenderá como usar o painel de Segurança e o Azure Sentinel para Microsoft 365.

Lições

painel de segurança

Investigação de ameaças e resposta

Azure Sentinel

Advanced Threat Analytics

Laboratório: Uso do simulador de ataques

Realizar um ataque simulado de spear phishing

Realizar ataques de senha simulados

Depois de completar este módulo, os estudantes estarão aptos a:

Descrever como o Threat Explorer pode ser usado para investigar ameaças e ajudar a proteger seu inquilino.

Descrever como o painel de segurança fornece aos executivos de nível C informações sobre os principais riscos e tendências.

Descrever o que é o Advanced Thread Analytics (ATA) e quais requisitos são necessários para implantá-lo.

Configurar o Advanced Threat Analytics.

Uso do simulador de ataques no Microsoft 365.

Descrever como o Azure Sentinel pode ser usado para o Microsoft 365.

Módulo 7: Microsoft Cloud Application Security

Este módulo centra-se na segurança de aplicativos no cloud no Microsoft 365. O módulo explicará a descoberta de cloud, conectores de aplicativos, políticas e alertas. Aprenderá como estas características funcionam para proteger os seus aplicativos no cloud.

Lições

Implementar Segurança de Aplicativos no Cloud

Utilizar informação de segurança de aplicativos no cloud

Após completar este módulo, os estudantes poderão:

Descrever Cloud App Security.

Explicar como implementar a Cloud App Security.

Controlar as suas Aplicativos de Cloud com Políticas.

Utilizar o Cloud App Catalog.

Utilizar o painel de controlo da Cloud Discovery.

Gerir as permissões dos aplicativos no cloud.

Módulo 8: Mobilidade

Este módulo se concentra na proteção de dispositivos e aplicativos móveis. Você aprenderá sobre o gerenciamento de dispositivos móveis e como ele funciona com o Microsoft Intune. Você também saberá sobre como o Intune e o Azure AD podem ser usados para proteger aplicativos móveis.

Lições

Gestão de Aplicativos Móveis (MAM)

Gestão de Dispositivos Móveis (MDM)

Implementar serviços de dispositivos móveis

Inscrição de dispositivos para Gestão de Dispositivos Móveis

Laboratório : Gestão de Dispositivos

Habilitação de gestão de dispositivo

Configuração do Azure AD for Intune

Criar políticas de conformidade e de acesso condicional

Depois de completar este módulo, os estudantes estarão aptos a:

Descrever considerações de aplicativos móveis.

Gerenciar dispositivos com o MDM.

Configurar domínios para MDM.

Gerenciar políticas de segurança do dispositivo.

Registrar dispositivos no MDM.

Configurar uma função do Gerenciador de inscrição do dispositivo.

Módulo 9: Proteção e Governação da Informação

Este módulo concentra-se na prevenção da perda de dados no Microsoft 365. Aprenderá sobre como criar políticas, editar regras, e personalizar as notificações dos usuários para proteger os seus dados.

Conceitos de proteção de informação

Governação e Gestão de Registos

Etiquetas de sensibilidade

Arquivamento no Microsoft 365

Retenção no Microsoft 365

Políticas de retenção no Centro de Conformidade Microsoft 365

Arquivamento e retenção em Exchange

Gestão de registos in loco em SharePoint

Laboratório : Arquivamento e Retenção

Inicializar a conformidade

Configurar etiquetas e políticas de retenção

Depois de completar este módulo, os estudantes estarão aptos a:

Configurar etiquetas de sensibilidade.

Configurar arquivamento e retenção no Microsoft 365.

Planear e configurar a Gestão de Registos

Módulo 10: Gerenciamento de direitos e criptografia

Este módulo explica o gerenciamento de direitos de informação no Exchange e no SharePoint. O módulo também descreve as tecnologias de criptografia usadas para proteger as mensagens.

Lições

Gestão de Direitos de Informação (IRM)

Extensão Segura de Correio Multifuncional na Internet (S-MIME)

Criptografia de mensagens do Office 365

Laboratório: Configurar o Office 365 Message Encryption

Configurar o Office 365 Message Encryption

Validar o gerenciamento de direitos de informação

Depois de completar este módulo, os estudantes estarão aptos a:

Descrever as diferentes opções de criptografia do Microsoft 365.

Descrever o uso de S/MIME.

Descrever e habilitar a criptografia de mensagens do Office 365.

Módulo 11: Prevenção de perda de dados

Este módulo abrange a prevenção de perda de dados no Microsoft 365. Você aprenderá a criar políticas, editar regras e personalizar as notificações do usuário para proteger seus dados.

Lições

Fundamentos da prevenção da perda de dados

Criar uma política de DLP

Personalizar uma política de DLP

Criar uma política de DLP para proteger documentos

Dicas de política

Laboratório: Implementar políticas de prevenção de perda de dados

Gerenciar políticas de DLP

Teste de MRM e Políticas de DLP

Depois de completar este módulo, os estudantes estarão aptos a:

Descrever prevenção de perda de dados (DLP).

Usar modelos de política para implementar políticas de DLP para obter informações mais usadas.

Configurar as regras corretas para proteger o conteúdo.

Descrever como modificar as regras existentes das políticas de DLP.

Configurar a opção de substituição do usuário para uma regra DLP.

Explicar como o SharePoint Online cria propriedades rastreadas a partir de documentos.

Módulo 12: Gestão de Conformidade

Este módulo explica o centro de Conformidade no Microsoft 365. Discute os componentes da pontuação de conformidade.

Lições

Centro de Conformidade

Depois de completar este módulo, os estudantes estarão aptos a:

Descrever como utilizar a pontuação de conformidade para tomar decisões organizacionais.

Descrever como as avaliações são utilizadas para determinar a pontuação de conformidade.

Módulo 13: Gestão de Risco de Informação Privilegiada

Este módulo concentra-se na funcionalidade relacionada com o risco interno dentro do Microsoft 365. Cobre não só a Gestão de Risco Insider no centro de conformidade, como também as barreiras de informação e a gestão de acesso privilegiado.

Lições

Risco interno

Acesso Privilegiado

Barreiras de informação

Construir muros éticos em Exchange Online

Laboratório : Gestão de Acesso Privilegiado

Estabelecer uma gestão de acesso privilegiada e processar um pedido

Depois de completar este módulo, os estudantes estarão aptos a:

Explicar e configurar a Insider Risk Management no Microsoft 365.

Configurar e aprovar pedidos de acesso privilegiado para administradores globais.

Configurar e utilizar as barreiras de informação para cumprir os regulamentos organizacionais.

Construir barreiras éticas em Exchange Online

Configurar o Customer Lockbox

Módulo 14: Descobrir e Responder

Este módulo se concentra na pesquisa e investigação de conteúdo. O módulo aborda como usar a descoberta eletrônica para conduzir investigações avançadas dos dados do Microsoft 365. Também abrange registros de auditoria e discute solicitações de titulares de dados GDPR.

Lições

Pesquisa de conteúdo

Auditoria de investigações de log

Descoberta eletrônica avançada

Laboratório : Gerenciamento de Pesquisa e Investigações

Investigar seus dados do Microsoft 365

Realizar uma solicitação de titular de dados

Depois de completar este módulo, os estudantes estarão aptos a:

Realizar pesquisas de conteúdo no Microsoft 365

Realizar e auditar a investigação dos registos.

Configurar o Microsoft 365 para registo de auditoria.

Utilizar Advanced eDiscovery

CURSO: MICROSOFT MESSAGING

Duração mínima: 5 dias

Objetivo: Examinar os principais elementos da administração de mensagens do Microsoft 365, incluindo fluxo e transporte de mensagens, segurança, proteção ativa e conformidade de mensagens, infraestrutura de mensagens e mensagens híbridas.

Estrutura de tópicos do curso

Módulo 1: Gerenciando a linha de transporte

Neste módulo, você aprenderá sobre os diferentes componentes de envio do Exchange, como o roteamento de mensagens funciona e como configurar o fluxo de mensagens para sua organização. Você examinará as tarefas que os administradores de mensagens devem concluir para configurar o transporte de mensagens. Você analisará as opções de transporte de mensagens e aprenderá a configurar domínios e conectores e como implementar um fluxo de trabalho de aprovação para mensagens. Você também aprenderá a gerenciar regras de transporte, que são uma configuração muito poderosa para controlar o fluxo de mensagens em sua organização.

Lições

- Visão geral dos serviços de transporte
- Configurando o transporte de mensagens
- Gerenciando regras de transporte

Laboratório: Configurar transporte de mensagens

- Criar conectores

Depois de completar este módulo, os estudantes estarão aptos a:

- Descrever os componentes de transporte do Exchange
- Planejar o encaminhamento eficiente de mensagens para sua organização
- Modificar o fluxo de mensagens para sua organização
- Descrever os agentes de transporte existentes e suas funções
- Configurar as diversas opções de transporte
- Planejar e configurar domínios para suas organizações
- Compreender como os conectores de recebimento e envio funcionam
- Descrever o funcionamento da moderação da mensagem para diferentes destinatários
- Compreender o que são regras de transporte
- Descrever como as regras de transporte funcionam
- Configurar regras de transporte personalizadas
- Descrever como as regras de transporte podem ser usadas para prevenir a perda de dados

Módulo 2: Gerenciando e diagnosticando problemas de fluxo de mensagens

Neste módulo, você examinará os componentes do fluxo de mensagens e aprenderá a gerenciar seu fluxo de mensagens, uma tarefa crucial para todo administrador do Exchange. Você conhecerá as diferenças entre gerenciar o fluxo de mensagens nas implantações do Exchange Online, Exchange Server e Exchange Híbrido. Do gerenciamento do fluxo de mensagens, você passará para o diagnóstico de problemas do fluxo de mensagens, como os e-mails que não estão sendo encaminhados corretamente dentro ou fora da organização ou quando as conexões seguras não podem ser estabelecidas com sucesso. Você aprenderá sobre as ferramentas que a Microsoft fornece para ajudá-lo a encontrar a causa raiz dos problemas e a corrigir o fluxo de mensagens. Você passará do diagnóstico de problemas do fluxo de mensagens para o diagnóstico de problemas de transporte, como problemas baseados em rede, problemas de conectores e agentes e problemas de arquitetura, além de como solucionar problemas de coexistência. Por último, você aprenderá a verificar os logs de eventos, protocolos e rastreamento quando todos os diagnósticos de problemas de disponibilidade de serviços e transporte de mensagens forem concluídos e se um problema ainda persistir ou se precisar encontrar dados de histórico sobre problemas no passado.

Lições

- Gerenciando o fluxo de e-mail
- Diagnosticando problemas de fluxo de e-mail
- Solucionando problemas de transporte
- Solucionando problemas com logs

Laboratório: Roteamento condicional de e-mail

- Criar regras de fluxo de e-mail

Depois de completar este módulo, os estudantes estarão aptos a:

- Gerenciar o fluxo de e-mail nas organizações
- Compreender o fluxo de e-mail para servidores Exchange
- Gerenciar o fluxo de e-mail para servidores Exchange
- Descrever e gerenciar o fluxo de e-mail em ambientes híbridos
- Entender como solucionar problemas de fluxo de e-mails SMTP
- Descrever como diagnosticar problemas com namespace compartilhado
- Descrever como diagnosticar problemas de criptografia com TLS
- Executar diagnósticos para problemas baseados em rede
- Descrever os procedimentos de diagnóstico de problemas de conectores e agentes
- Planejar o diagnóstico para verificação de problemas de arquitetura
- Entender como executar o diagnóstico de problemas de coexistência
- Criar pesquisas para o log de rastreamento de mensagens
- Descrever o diagnóstico de problemas usando os logs de protocolo
- Entender como trabalhar com o log de eventos do Exchange

Módulo 3: Gerenciando a proteção ativa de mensagens

Neste módulo, você aprenderá sobre os recursos e funcionalidades do Microsoft Exchange Online Protection (EOP). Você também aprenderá a planejar o encaminhamento de mensagens para este serviço, que fornece políticas antimalware e antispam para proteger sua organização contra spam e malware e contra violações da política de mensagens. Você analisará a proteção antimalware e antispam fornecida pelo Exchange Server e Online Protection e aprenderá a configurar filtros, políticas e configurações de spam e malware para fornecer proteção aos seus usuários. Você concluirá o módulo examinando a proteção avançada contra ameaças (ATP) e como ela estende a proteção fornecida pelo EOP ao filtrar ataques direcionados que poderiam passar pela linha de defesas do EOP, incluindo ameaças avançadas, como ataques de dia zero em anexos de e-mail e documentos do Office e proteção de hora de clique contra URLs mal-intencionados. Você aprenderá como o Microsoft 365 ATP protege os usuários contra ameaças avançadas por meio de recursos como anexos seguros e links seguros e como gera relatórios que fornecem aos administradores informações sobre ataques direcionados a seus locatário por e-mail.

Lições

- Planejando a proteção ativa de mensagens
- Gerenciando políticas antimalware e antispam
- Gerenciando a proteção avançada contra ameaças

Laboratório: Gerenciando a proteção ativa de mensagens

- Criar filtros de proteção ativa

Depois de completar este módulo, os estudantes estarão aptos a:

- Explicar o uso e os recursos do Exchange Online Protection
- Planejar o roteamento de mensagens para o Exchange Online Protection
- Investigar os comunicados e logs de EOP disponíveis
- Compreender os diversos campos do cabeçalho da mensagem relevantes para a proteção contra spam e spoofing
- Configurar filtros antispam e antimalware no Exchange Server
- Usar recursos adicionais para filtragem de spam de saída e quarentena
- Implementar recursos de proteção contra phishing e spoofing
- Criar regras de transporte para requisitos personalizados
- Descrever os recursos de proteção avançada contra ameaças
- Descrever a proteção fornecida pelas políticas de segurança de anexos e de links
- Compreender os recursos Spoof Intelligence
- Compreender o funcionamento das políticas antiphishing de ATP

Módulo 4: Gerenciando a conformidade

Este módulo começa descrevendo os diferentes recursos de conformidade no Centro de Segurança e Conformidade (SCC) que os administradores de mensagens podem usar para

cumprimento dos requisitos legais e regulamentares. Este módulo aborda a conformidade no Exchange ao examinar os recursos de conformidade disponíveis no Centro de Administração do Exchange para e implementações do Exchange Server e híbridas. Devido aos requisitos de retenção complexos dos ambientes de mensagens atuais, este módulo se concentra em como o arquivamento é realizado com o Exchange, para que você possa fornecer um ambiente eficiente e compatível aos seus usuários. Você também examinará como o armazenamento adicional de arquivamento é fornecido aos usuários, como as mensagens são processadas e arquivadas automaticamente e como o log de auditoria no Exchange fornece informações sobre ações de administrador, delegadas e do usuário nas caixas de correio dos usuários e na organização do Exchange. Por último, uma vez que as organizações devem cumprir os requisitos legais de descoberta (relacionados à política organizacional, conformidade ou ações judiciais), você examinará como o eDiscovery para Microsoft Exchange pode ajudá-lo a realizar pesquisas de descoberta de conteúdo relevante nas caixas de correio.

Lições

- Conformidade de mensagens no SCC
- Conformidade de mensagens no Exchange
- Gerenciar arquivamento e auditoria do Exchange Online
- Gerenciando a pesquisa de conteúdo

Depois de completar este módulo, os estudantes estarão aptos a:

- Descrever os diversos recursos de política e conformidade para mensagens
- Avaliar as diversas funções no Centro de Segurança e Conformidade
- Planejar as políticas de retenção para caixas de correio do Exchange Online
- Configurar políticas de prevenção de perda de dados (DLP) para dados no Microsoft 365
- Criar rastreamentos de mensagens para compreensão do fluxo de mensagens na sua organização do Exchange Online
- Descrever retenções contenciosas e in loco do Exchange Server
- Planejar a retenção e exclusão com o Message Records Management (MRM)
- Proteger seu fluxo de mensagens com políticas de prevenção de perda de dados no Exchange Server
- Investigar o log de rastreamento de mensagens na sua organização do Exchange
- Descrever o que é o arquivamento in loco e como funciona
- Compreender as diferenças entre registro no diário e arquivamento
- Saber para que são usados os logs de auditoria da caixa de correio e do administrador
- Compreender as pesquisas de conteúdo para procurar mensagens em sua organização
- Descrever casos de descoberta eletrônica e descoberta eletrônica in loco para Exchange
- Gerenciar casos avançados de descoberta eletrônica no Centro de Segurança e Conformidade

Módulo 5: Gerenciando configurações organizacionais

Este módulo começa com um exame sobre como gerenciar a autenticação de mensagens. Este módulo se concentra em como garantir que as contas dos usuários estejam bem protegidas e seguras e em como implementar vários recursos de segurança que não apresentam complexidade desnecessária no trabalho diário dos usuários, o que pode resultar em menor produtividade nos negócios e novos riscos à segurança. Em seguida, o curso abordará a autenticação de mensagens para as configurações organizacionais, onde aprenderá como definir as configurações que se aplicam a toda a organização ou a vários usuários da organização. Por último, você examinará como configurar o compartilhamento organizacional.

Lições

- Gerenciando a autenticação para mensagens
- Definindo configurações organizacionais
- Configurando o compartilhamento organizacional

Depois de completar este módulo, os estudantes estarão aptos a:

- Configurar opções de política de senha
- Configurar gerenciamento de senha de autoatendimento
- Implementar autenticação multifator
- Planejar políticas de senha
- Configurar políticas e limitação de carga de trabalho
- Configurar definições de cotas
- Configurar a integração do Exchange Server e do Skype for Business
- Implementar suplementos do Office 365
- Fornecer uma visão geral dos recursos de compartilhamento de delegação federada do Exchange
- Descrever componentes de compartilhamento federado
- Explicar as considerações para criar e implementar relações e certificados de confiança de federação
- Implementar relações da organização
- Implementar políticas de compartilhamento

Módulo 6: Gerenciando dispositivos móveis

Neste módulo, você começará examinando o gerenciamento de dispositivos móveis no Microsoft 365 e como as políticas de caixa de correio do Exchange ActiveSync e de dispositivos móveis oferecem suporte a esse esforço. Em seguida, você aprenderá a gerenciar e diagnosticar problemas de acesso ao dispositivo móvel. Além disso, o módulo descreve como configurar o acesso e a infraestrutura para dispositivos móveis, como compreender as implicações da limpeza remota de dispositivos móveis e conhecerá os métodos alternativos para gerenciamento de dispositivos móveis.

Lições

- Políticas de caixa de correio de dispositivo móvel
- Gerenciando o acesso a dispositivos móveis

Laboratório: Implementar o ActiveSync

- Implementar a sincronização ativa para caixas de correio simples e múltiplas

Depois de completar este módulo, os estudantes estarão aptos a:

- Descrever o funcionamento do Exchange ActiveSync
- Configurar políticas de caixa de correio para dispositivos móveis
- Compreender o gerenciamento de dispositivos móveis no Microsoft 365
- Configurar o acesso aos dispositivos móveis
- Compreender os componentes da infraestrutura de dispositivos móveis
- Explicar o funcionamento da limpeza remota de um dispositivo móvel
- Descrever alternativas para gerenciamento de dispositivos móveis
- Diagnosticar problemas de acesso ao dispositivo móvel

Módulo 7: Gerenciando permissões baseadas em função

Este módulo examina como os administradores de mensagens gerenciam permissões baseadas em funções, que é uma tarefa essencial para qualquer administrador de mensagens. Uma vez que o Exchange Server e o Exchange Online usam o modelo de permissão de controle de acesso baseado em função (RBAC), este módulo examinará os conceitos básicos do gerenciamento de RBAC. O módulo conclui examinando como um administrador de mensagens deve planejar e configurar permissões com cautela para não colocar em risco seu ambiente ou todo o Active Directory.

Lições

- Gerenciando funções de administrador
- Gerenciando funções de usuário
- Configuração do Exchange e permissão de divisão de RBAC e AD

Laboratório: Gerenciar funções e políticas de permissão

- Gerenciar funções e políticas de permissão

Depois de completar este módulo, os estudantes estarão aptos a:

- Descrever como o RBAC é usado para atribuir funções aos usuários
- Compreender o que são grupos de funções de gerenciamento para tarefas administrativas
- Atribuir as funções de gerenciamento internas para administração
- Criar funções de gerenciamento personalizadas e atribuí-las por meio de políticas de atribuição de função aos usuários

- Diagnosticar problemas de funções de gerenciamento de RBAC
- Descrever as funções internas do usuário final
- Configurar políticas de atribuição de função
- Criar novas funções personalizadas e políticas de atribuição de função
- Entender as diferenças entre permissões compartilhadas e permissões divididas
- Descrever as permissões de várias florestas
- Identificar as diferenças entre os modelos de permissão

Módulo 8: Gerenciando objetos e recursos de destinatário

Este módulo examina algumas das tarefas mais comuns que os administradores de mensagens executam, como criação e configuração de destinatários, listas e recursos de e-mail. Este módulo descreve os diversos tipos de destinatários do Exchange Server, inclusive como eles diferem entre si. Em seguida, o módulo abordará as várias tarefas que exigem que você crie e gerencie destinatários do Exchange no Exchange, incluindo caixas de correio de usuário, caixas de recursos, caixas de correio compartilhadas e contatos e usuários de e-mail. Você também aprenderá a gerenciar permissões para os destinatários e a criar e gerenciar grupos.

Lições

- Destinatários do Exchange
- Criando e gerenciando destinatários do Exchange
- Gerenciando endereços de e-mail, listas e recursos

Laboratório: Criar objetos e recursos de destinatário

- Criar destinatários do Exchange
- Criar grupos

Depois de completar este módulo, os estudantes estarão aptos a:

- Descrever os diferentes objetos de destinatário no Exchange
- Descrever as caixas de correio de recursos
- Descrever as caixas de correio compartilhadas
- Descrever as caixas de correio vinculadas e caixas de correio locais
- Descrever os grupos
- Criar e gerenciar configurações de caixa de correio
- Criar e gerenciar caixas de correio compartilhadas e de recursos
- Criar e gerenciar contatos e usuários de e-mail
- Criar e gerenciar permissões de destinatário
- Criar e gerenciar grupos
- Descrever listas de endereços
- Explicar como configurar listas de endereços
- Descrever políticas de catálogo de endereços
- Explicar como configurar os catálogos de endereços offline

- Descrever políticas de endereço de e-mail

Módulo 9: Gerenciando pastas públicas

Neste módulo, você aprenderá sobre pastas públicas no Exchange, analisará as considerações de planejamento para implementação de pastas públicas e discutirá alternativas para pastas públicas. Você também aprenderá a implementar e gerenciar caixas de correio de pasta pública, pastas públicas e permissões de pasta pública, além de como criar e gerenciar pastas públicas habilitadas para e-mail. O módulo conclui examinando como monitorar e diagnosticar problemas relacionados à pasta pública.

Lições

- Planejando a hierarquia de pastas pública
- Implementando e gerenciando pastas públicas
- Diagnosticando problemas de pastas públicas

Laboratório: Implementar pastas públicas

- Criar pastas públicas
- Gerenciar pastas públicas

Depois de completar este módulo, os estudantes estarão aptos a:

- Descrever pastas públicas no Exchange
- Planejar a hierarquia de pastas públicas
- Planejar caixas de correio de pasta pública
- Explicar as cotas de pasta pública
- Avaliar alternativas para pastas públicas
- Descrever as considerações para implementação de pastas públicas
- Implementar caixas de correio de pasta pública
- Gerenciar permissões de pasta pública
- Criar e gerenciar pastas públicas habilitadas para e-mail
- Monitorar pastas públicas
- Diagnosticar problemas de pastas públicas
- Diagnosticar problemas de acesso a pastas públicas

Módulo 10: Planejando um ambiente híbrido

Neste módulo, você examinará os requisitos necessários para realizar uma implementação híbrida e aprenderá sobre os recursos e componentes necessários ao realizar uma implementação híbrida. Este módulo examina todos os aspectos de planejamento necessários antes de executar o Hybrid Configuration Wizard. Isso inclui as opções de configuração do HCW, bem como os detalhes de Transferência de Configuração da Organização (OCT) e de Hybrid Agent. O módulo conclui com uma revisão das opções de fluxo de mensagens para uma implementação híbrida.

Lições

- Requisitos de implementação híbrida do Exchange
- Planejar a execução do assistente de configuração híbrida

Laboratório: Preparar o Azure AD para sincronização híbrida

- Preparar o Azure AD para sincronização híbrida

Depois de completar este módulo, os estudantes estarão aptos a:

- Descrever as opções de conexão disponíveis para conectar o Exchange local ao Microsoft 365
- Listar e descrever os componentes de uma implementação híbrida
- Descrever o Azure Active Directory Connect (Azure AD Connect)
- Identificar as opções de identidade do Microsoft 365 para o Exchange Hybrid
- Comparar a federação delegada do Exchange e do OAuth
- Planejar a configuração Exchange Hybrid
- Descrever a transferência de configuração da organização
- Explicar o Exchange Modern Hybrid e Hybrid Agent
- Planejar as opções de fluxo de e-mail para uma implementação híbrida

Módulo 11: Realizando migrações de caixa de correio

Este módulo examina as opções disponíveis para a migração de e-mails para o Exchange Online, como executar uma migração ou usar o FastTrack para mover caixas de correio dos servidores de e-mail existentes ao Exchange Online. Este módulo resume as opções de migração e coexistência e recomenda quando usar uma ou outra opção. O módulo examina os requisitos para executar uma migração IMAP, as opções de migração disponíveis e as etapas executadas durante uma migração. O módulo examina como planejar e executar uma migração de transição e em etapas. Ele compara cada uma dessas duas abordagens de migração e você aprenderá sobre os requisitos, as atividades de planejamento e o processo de migração de cada opção. O módulo conclui examinando importantes tarefas de migração adicionais, como a migração de um arquivo PST e as considerações para uma migração de pasta pública.

Lições

- Planejando migrações de caixa de correio
- Executando migrações IMAP
- Executando migrações de transição e em etapas
- Executando migrações avançadas

Depois de completar este módulo, os estudantes estarão aptos a:

- Descrever as estratégias de migração e coexistência com o Exchange Online

- Usar o FastTrack para mover caixas de correio
- Descrever os requisitos para uma migração IMAP e como é realizada
- Mover dados da caixa de correio usando uma migração IMAP
- Descrever os requisitos para as migrações de transição e de etapas
- Realizar a migração e mover as caixas de correio com uma migração de transição ou em etapas
- Importar arquivos PST para caixas de correio do Exchange Online
- Migrar pastas públicas para o Exchange Online

Módulo 12: Implementando e diagnosticado problemas de um ambiente híbrido

Neste módulo você aprenderá as principais áreas a serem planejadas em relação aos servidores de transporte de borda. Você aprenderá sobre os requisitos e práticas recomendadas para configurar uma implementação híbrida, que é a primeira etapa para sua organização do Exchange, independentemente de conectar suas organizações locais do Exchange e do Exchange Online para coexistência a longo prazo ou como parte de uma estratégia de migração em nuvem. Neste módulo, você examinará como gerenciar uma implementação híbrida e implementar a funcionalidade híbrida avançada. Você abordará os recursos que exigem uma implementação híbrida bem-sucedida, como coexistência de pasta pública ou armazenamento de anexos do OneDrive for Business para caixas de correio locais. Este módulo finaliza com uma introdução às técnicas de solução de problemas para uma implementação híbrida. Você aprenderá a solucionar problemas de sincronização de diretórios, incluindo autenticação de passagem (PTA) e login único, transporte do Exchange e solução de problemas de acesso de clientes, bem como do serviço de replicação de caixa de correio.

Lições

- Implementando e gerenciando um servidor de transporte de borda
- Configurando uma implementação híbrida usando o HCW
- Implementando a funcionalidade híbrida avançada
- Diagnosticando problemas de implementações híbridas

Laboratório: Implementar ambiente híbrido

- Configurar sua implementação híbrida
- Testar sua implementação híbrida

Depois de completar este módulo, os estudantes estarão aptos a:

- Descrever a finalidade e a funcionalidade dos servidores de transporte de borda
- Explicar os requisitos de infraestrutura para servidores de transporte de borda
- Descrever o EdgeSync
- Planejar o fluxo de mensagens com um servidor de transporte de borda

- Descrever os pré-requisitos para execução do Assistente de Configuração Híbrida do Office 365
- Explicar as práticas recomendadas para realizar uma implementação híbrida
- Gerenciar uma implementação híbrida
- Descrever quando configurar a coexistência de pasta pública com o Office 365
- Explicar como configurar o Oauth para um ambiente misto do Exchange
- Descrever como configurar anexos do OneDrive for Business para caixas de correio locais
- Diagnosticar problemas de sincronização de diretórios
- Diagnosticar problemas de autenticação de passagem e de login único
- Diagnosticar problemas de transporte com o Exchange Online
- Diagnosticar problemas de acesso ao cliente na coexistência
- Diagnosticar problemas do serviço de replicação de caixa de correio

CURSO: MICROSOFT IDENTITY AND ACCESS ADMINISTRATOR

Duração mínima: 4dias

Objetivo: Oferecer ao Profissional de Identidade e Acesso de IT, juntamente com o IT Security Professional, os conhecimentos e habilidades necessários para implementar soluções de gerenciamento de identidade baseadas no Microsoft Azure AD, e tecnologias de identidade conectadas. Este curso deve incluir conteúdo de identidade para Azure AD, registro de aplicativos corporativos, acesso condicional, governança de identidade e outras ferramentas de identidade.

Estrutura de tópicos do curso

Módulo 1: Implementar uma solução de gerenciamento de identidade

Aprenda a criar e gerenciar sua implementação inicial do Azure Active Directory (Azure AD) e a configurar os usuários, grupos e identidades externas que você usará para executar sua solução.

Aulas

- Implementar a configuração inicial do Azure AD
- Criar, configurar e gerenciar identidades
- Implementar e gerenciar identidades externas
- Implementar e gerenciar identidade híbrida

Laboratório : Gerenciar funções de usuário

Laboratório : Definir propriedades para todo o inquilino

Laboratório : Atribuir licenças aos usuários

Laboratório : Restaurar ou remover usuários excluídos

Laboratório : Adicionar grupos no Azure AD

Laboratório : Alterar atribuições de licença de grupo

Laboratório : Alterar atribuições de licença de usuário

Laboratório : Configurar a colaboração externa

Laboratório : Adicionar usuários convidados ao diretório

Laboratório : Explorar grupos dinâmicos

Depois de concluir este Módulo, os alunos serão capazes de:

- Implantar um Azure AD inicial com configurações personalizadas
- Gerenciar identidades internas e externas
- Implementar uma solução de identidade híbrida

Módulo 2: Implementar uma solução de autenticação e gerenciamento de acesso

Implemente e administre seu gerenciamento de acesso usando o Azure AD. Use MFA, acesso condicional e proteção de identidade para gerenciar sua solução de identidade.

Aulas

- Proteger o usuário do Azure AD com MFA
- Gerenciar autenticação de usuário
- Planejar, implementar e administrar o acesso condicional
- Gerenciar a proteção de identidade do Azure AD

Laboratório : Habilitar Azure AD MFA

Laboratório : Configurar e implantar a redefinição de senha de autoatendimento (SSPR)

Laboratório : Trabalhar com padrões de segurança

Laboratório : Implementar políticas, funções e atribuições de acesso condicional

Laboratório : Configurar controles de sessão de autenticação

Laboratório : Gerenciar valores de bloqueio inteligente do Azure AD

Laboratório : Ativar política de risco de login

Laboratório : Configurar a política de registro de autenticação do Azure AD MFA

Depois de concluir este Módulo, os alunos serão capazes de :

- Configurar e gerenciar a autenticação do usuário, incluindo MFA
- Controlar o acesso a recursos usando acesso condicional
- Usar a Proteção de Identidade do Azure AD para proteger sua organização

Módulo 3: Implementar gerenciamento de acesso para aplicativos

Explore como os aplicativos podem e devem ser adicionados à sua solução de identidade e acesso com o registro do aplicativo no Azure AD.

Aulas

- Planejar e projetar a integração da empresa para SSO
- Implementar e monitorar a integração de aplicativos corporativos para SSO
- Implementar o registro do aplicativo

Laboratório : Implementar gerenciamento de acesso para aplicativos

Laboratório : Criar uma função personalizada para o registro do aplicativo de gerenciamento

Laboratório : Registrar um aplicativo

Laboratório : Conceder consentimento de administrador para todo o locatário para um aplicativo

Laboratório : Adicionar funções de aplicativo a aplicativos e receber tokens

Depois de concluir este Módulo, os alunos serão capazes de:

- Registrar um novo aplicativo em seu Azure AD
- Planejar e implementar SSO para aplicativos corporativos
- Monitorar e manter aplicativos corporativos

Módulo 4: Planejar e implementar uma estratégia de governança de identidade

Projete e implemente a governança de identidade para sua solução de identidade usando direitos, revisões de acesso, acesso privilegiado e monitoramento de seu Azure Active Directory (Azure AD).

Aulas

- Planejar e implementar o gerenciamento de direitos
- Planejar, implementar e gerenciar análises de acesso
- Planejar e implementar acesso privilegiado
- Monitorar e manter o Azure AD

Laboratório : Criar e gerenciar um catálogo de recursos com direito ao Azure AD

Laboratório : Adicionar relatório de aceitação dos termos de uso

Laboratório : Gerenciar o ciclo de vida de usuários externos com governança de identidade do Azure AD

Laboratório : Criar avaliações de acesso para grupos e aplicativos

Laboratório : Configurar o PIM para funções do Azure AD

Laboratório : Atribuir função do Azure AD no PIM

Laboratório : Atribuir funções de recurso do Azure no PIM

Laboratório : Conectar dados do Azure AD ao Azure Sentinel

Depois de concluir este Módulo, os alunos serão capazes de :

- Gerenciar e manter o Azure AD desde a criação até a solução
- Usar revisões de acesso para manter seu Azure AD
- Conceder acesso a usuários com gerenciamento de direitos

CURSO: MS-700T00-A: Managing Microsoft Teams

Duração Mínima: 5 Dias

Objetivo: configurar, implementa e gerencia cargas de trabalho do Office 365 para o Microsoft Teams visando a colaboração e comunicação eficiente e efetiva em um ambiente empresarial.

Este curso deve abranger seis elementos centrais -

- Visão geral do Microsoft Teams,
- Implementação de governança,

- Segurança e conformidade para o Microsoft Teams,

- Preparando para uma implantação do Microsoft Teams,
- Implantando e gerenciando equipes,
- Gerenciando colaboração e gerenciando comunicação no Microsoft Teams.

Na visão geral do Microsoft Teams, deerá oferecer uma visão geral do Microsoft Teams incluindo arquitetura do Teams e cargas horárias do Office 365 relacionadas. Deverá oferecer uma visão geral de segurança e conformidade no Microsoft Teams e finalmente mostrar uma visão geral de como gerenciar o Microsoft Teams.

Ao implementar a governança, segurança e conformidade para o Microsoft Teams, deverá ensinar a planejar e configurar a governança para grupos do Office 365 incluindo expiração e políticas de nomeação.

Em seguida, deverá implementar segurança e ensinar o aluno configurando acesso condicional, MFA ou Gestão de Ameaça para o Microsoft Teams.

Finalmente, deverá implementar conformidade para Teams usando políticas de DLP, casos de eDiscovery ou políticas de supervisão.

Deverá preparar o ambiente para uma implantação do Microsoft Teams, planejar um upgrade do Skype for Business para o Microsoft Teams ao avaliar caminhos de upgrade com modos de coexistência e upgrade, gerencia migrações de reunião e configura definições de coexistência e upgrade. Em seguida, planejar e configurar definições de rede para o Microsoft Teams, e finalmente implantar e gerenciar os terminais do Microsoft Teams.

Ao implantar e gerenciar equipes, deverá ensinar como criar e gerenciar equipes, gerenciar afiliação e acesso tanto para usuários internos quanto externos.

Ao gerenciar a colaboração no Microsoft Teams, gerenciar experiências de chat e colaboração tais como definições de equipe ou políticas de criação de canal privado.

Finalmente, gerenciar definições para aplicações do Teams como políticas de configuração de aplicação, Apps, robôs e conectores no Microsoft Teams ou publicar uma aplicação personalizada no Microsoft Teams.

Este curso deverá ser concluído com o gerenciamento de comunicação no Microsoft Teams. O alune deverá aprender como gerenciar experiências de evento e reuniões ao vivo, gerenciar números de telefone ou Sistema de Telefone para o Microsoft Teams e finalmente como solucionar problema de áudio, vídeo e problemas de cliente.

Estrutura de tópicos do curso

Módulo 1: Visão Geral do Microsoft Teams

Na visão geral do Microsoft Teams, você obterá uma visão geral do Microsoft Teams incluindo arquitetura do Teams e cargas horárias do Office 365 relacionadas. Você será fornecido com uma visão geral de segurança e conformidade no Microsoft Teams e finalmente obterá uma visão geral de como gerenciar o Microsoft Teams.

Lições

- Visão Geral do Microsoft Teams
- Visão geral de segurança e conformidade no Microsoft Teams
- Visão Geral de gerenciamento do Microsoft Teams

Laboratório : Gerenciamento de funções e criação de equipes

- Prepare funções de equipe e licenças
- Crie nova equipe

Módulo 2: Implementação de Governança, Segurança e Conformidade do Microsoft Teams

Ao implementar a governança, segurança e conformidade para o Microsoft Teams, você planejará e configurará governança para grupos do Office 365 incluindo expiração e políticas de nomeação. Em seguida, você irá implementar segurança configurando acesso condicional, MFA ou Gestão de Ameaça para o Microsoft Teams. Finalmente, você irá implementar conformidade para Teams usando políticas de DLP, casos de eDiscovery ou políticas de supervisão.

Lições

- Implementação de Governança e Gestão de Ciclo de Vida para o Microsoft Teams
- Implementando Segurança para o Microsoft Teams
- Implementando Conformidade para o Microsoft Teams

Laboratório : Configuração de Segurança e Conformidade para equipes e conteúdo

- Implementação de Governança e Gestão de Ciclo de Vida para o Microsoft Teams
- Implementando Segurança para o Microsoft Teams
- Implementando Conformidade para o Microsoft Teams

Módulo 3: Como preparar o ambiente para uma implantação do Microsoft Teams

Ao preparar o ambiente para uma implantação do Microsoft Teams, você planeja um upgrade do Skype for Business para o Microsoft Teams ao avaliar caminhos de upgrade com modos de coexistência e upgrade, gerencia migrações de reunião e configura definições de coexistência e upgrade. Em seguida, você planeja e configura definições de rede para o Microsoft Teams, e finalmente você implantará e gerenciará os terminais do Microsoft Teams.

Lições

- Upgrade do Skype for Business para o Microsoft Teams
- Planejamento e configuração de definições de rede para o Microsoft Teams
- Implantação e gerenciamento de terminais do Microsoft Teams

Laboratório : Preparação de ambiente para o Teams

- Cálculo de capacidades de rede
- Avaliação de perfis de configuração
- Fornecimento de recursos de equipe

Módulo 4: Implantação e gerenciamento de equipes

Ao implantar e gerenciar equipes, você aprenderá como criar e gerenciar equipes, gerenciar afiliação e acesso tanto para usuários internos quanto externos.

Lições

- Crie e gerencie equipes
- Gerencie afiliação
- Gerencie acesso para usuários externos

Laboratório : Gerencie equipes

- Gerencie recursos de equipe
- Gerencie compartilhamento e acesso

Módulo 5: Gerencie colaboração no Microsoft Teams

Ao gerenciar a colaboração no Microsoft Teams, você gerenciará experiências de chat e colaboração tais como definições de equipe ou políticas de criação de canal privado. Finalmente, você gerenciará definições para aplicações do Teams como políticas de configuração de aplicação, Apps, robôs e conectores no Microsoft Teams ou publicará uma aplicação personalizada no Microsoft Teams.

Lições

- Gerencie experiências de chat e colaboração
- Gerencie definições para as aplicações do Teams

Laboratório : Modifique as definições de colaboração para o Teams

- Configure políticas de canal e mensagem
- Gerencie definições de aplicação para a equipe

Módulo 6: Gerencie comunicação no Microsoft Teams

Este curso é concluído com o gerenciamento de comunicação no Microsoft Teams. Você aprenderá como gerenciar experiências de evento e reuniões ao vivo, gerenciar números de telefone ou Sistema de Telefone para o Microsoft Teams e finalmente como solucionar problema de áudio, vídeo e problemas de cliente.

Lições

- Gerencie experiências de evento e reuniões em tempo real
- Gerencie números de telefone
- Gerencie sistema de telefone para o Microsoft Teams
- Solução de problemas de áudio, vídeo e problemas de cliente

Laboratório : Modifique as definições de comunicações para o Teams

- Configurar políticas de reunião.
- Gerencie sistema de telefone para o Microsoft Teams
- Resolução de problemas de áudio, vídeo e problemas de cliente

CURSO: Curso MD-101T00-A: Managing Modern Desktops

Duração mínima: 5 dias

Objetivo: Neste curso, os alunos deverão aprender como planejar e implementar uma estratégia de implantação de sistema de operação usando métodos de implantação modernos, assim como implementar uma estratégia de atualização. Os alunos deverão serão introduzidos a componentes principais de gestão moderna e estratégias de cogerenciamento. Este curso também deve abranger o que é necessário para incorporar o Microsoft Intune para a empresa.

Os alunos deverão aprender sobre métodos para implantação e gerenciamento de aplicações e aplicações baseadas em navegador. Os alunos deverão ser introduzidos aos conceitos principais de segurança em gestão moderna incluindo autenticação, identidades, acesso e políticas de conformidade.

Os alunos deverão ser introduzidos a tecnologias como Azure Active Directory, Azure Information Protection e Windows Defender Advanced Threat Protection, assim como alavancá-las para proteger dispositivos e dados.

Estrutura de tópicos do curso

Módulo 1: Planejando uma estratégia de implantação de sistema operacional

Este módulo explica como planejar e implementar uma estratégia de implantação. Os alunos aprenderão sobre os conceitos de suportar o desktop através de todo seu ciclo de vida. Este módulo também abrange avaliar um ambiente existente e as ferramentas usadas para preparar uma estratégia de implantação. Finalmente, os alunos serão

introduzidos às ferramentas e estratégias usadas para a implantação da área de trabalho.

Lições

- O Enterprise Desktop
- Avaliando Prontidão de Implantação
- Ferramentas e Estratégias de Implantação

Laboratório : Laboratório prático - Planejando a implantação do Windows 10

Depois de completar este módulo, os estudantes estarão aptos a:

- Descreva o ciclo de vida da área de trabalho empresarial.
- Descreva como avaliar um ambiente existente.
- Descreva métodos para eliminar bloqueadores de implantação.
- Descreva as ferramentas e métodos diferentes para implantação.

Módulo 2: Implementando o Windows 10

Este módulo abrange os métodos modernos da implantação do Windows usados em cenários comuns como atualização e migração do Windows 10, assim como implantação de novos dispositivos e atualização de dispositivos existentes. Os alunos aprenderão também sobre métodos alternativos da implantação de OS assim como considerações quando escolhendo métodos de implantação.

Lições

- Atualizando dispositivos para o Windows 10
- Implantando Novos Dispositivos e Atualização
- Migrando Dispositivos para o Windows 10
- Métodos de implantação alternativos
- Considerações de imagem

Laboratório : Laboratório de Práticas - Implementando o Windows 10

- Criando e implantando pacote de provisionamento
- Migrar configurações do usuário
- Implantando o Windows 10 com o AutoPilot

Após concluir este cursos, os aprendizes poderão:

- Desenvolver uma estratégia de implantação e atualização do sistema operacional.
- Compreender os diferentes métodos de implantação
- Entender em quais cenários as soluções locais e baseadas na nuvem podem ser usadas para
- Implantar e migrar áreas de trabalho para o Windows 10.

Módulo 3: Gerenciando atualizações para Windows 10

Este módulo aborda o gerenciamento de atualizações no Windows. Este módulo apresenta as opções de manutenção para o Windows 10. Os alunos aprenderão os diferentes métodos para implantar atualizações e como configurar políticas de atualização do Windows. Finalmente, os alunos aprenderão como assegurar e monitorar conformidade de atualização usando o Windows Analytics.

Lições

- Atualizando o Windows 10
- Windows Update para empresas
- Introdução ao Windows Analytics

Laboratório : Laboratório de Práticas - Gerenciando atualizações para Windows 10

- Definindo manualmente as configurações de atualização do Windows
- Configurando a atualização do Windows usando GPOs

Depois de completar este módulo, os estudantes estarão aptos a:

- Descrever os canais de manutenção do Windows 10.
- Configurar uma política de atualização do Windows usando configurações de política de grupo.
- Configurar a atualização do Windows para empresas para implantar atualizações do sistema operacional.
- Usar o Windows Analytics para avaliar a disponibilidade e atualizar a conformidade.

Módulo 4: Registro do dispositivo

Neste módulo, os alunos examinarão os benefícios e pré-requisitos para cogerenciamento e aprender como planejar para isso. Este módulo também abrangerá o Azure AD join e será introduzido ao

Microsoft INtune, assim como aprender como configurar políticas para cadastramento de dispositivos. O módulo será concluído com uma visão geral do inventário de dispositivos no Intune e dos relatórios usando o console do Intune, o Power BI e o Microsoft Graph.

Lições

- Opções de gerenciamento de dispositivos
- Visão geral do Microsoft Intune
- Gerenciar o registro e o inventário de dispositivos do Intune
- Gerenciando dispositivos com o Intune

Laboratório : Laboratório Prático - Registro e Gerenciamento de Dispositivos

Depois de completar este módulo, os estudantes estarão aptos a:

- Descrever os benefícios e métodos para migrar para o co-gerenciamento.
- Implantar um MDM com o Microsoft Intune.
- Configurar registro de dispositivo.
- Registrar área de trabalho e dispositivos móveis no Windows Intune.
- Configurar e baixar relatórios de inventário.

Módulo 5: Configurando perfis

Este módulo mergulha mais profundamente nos perfis de dispositivos do Intune, incluindo os tipos de perfis de dispositivos e a diferença entre perfis internos e personalizados. O aluno aprenderá sobre a atribuição de perfis a grupos do Azure AD e o monitoramento de dispositivos e perfis no Intune. O módulo será concluído com uma visão geral do uso do Windows Analytics para relatórios de integridade e conformidade.

Lições

- Configurando perfis de dispositivo
- Gerenciamento de perfis de usuário
- Dispositivos de monitoramento

Laboratório : Laboratório prático - Gerenciamento de perfis

Depois de completar este módulo, os estudantes estarão aptos a:

- Descrever os tipos de perfis de dispositivo.
- Criar e atribuir perfis de dispositivo.
- Configurar perfil de usuário e redirecionamento de pasta.
- Monitorar e relatar dispositivos usando o Intune e o Windows Analytics.

Módulo 6: Gerenciamento de aplicativos

Neste módulo, os alunos aprendem sobre o gerenciamento de aplicativos no local e soluções baseadas na nuvem. Este módulo abordará como gerenciar implantações do Office 365 ProPlus no Intune, além de como gerenciar aplicativos em dispositivos não registrados. O módulo será concluído com uma visão geral do Modo Empresarial com Internet Explorer e Microsoft Edge e rastreando seus aplicativos instalados, licenças e aplicativos atribuídos usando o Intune.

Lições

- Implementar o gerenciamento de aplicativos móveis (MAM)
- Implantar e atualizando aplicativos
- Administrando aplicativos

Laboratório : Laboratório Prático - Gerenciando Aplicativos

Depois de completar este módulo, os estudantes estarão aptos a:

- Descrever os métodos para gerenciamento de aplicativos.
- Implantar aplicativos usando o Intune e a política de grupo.
- Configurar Microsoft Store para Empresas.
- Implantar o Office365 ProPlus usando o Intune.
- Gerenciar e reportar inventário e licenças de aplicativos.

Módulo 7: Gerenciando a autenticação no Azure AD

Neste módulo, os alunos serão introduzidos ao conceito de diretório na nuvem com o Azure AD. Os alunos aprenderão as semelhanças e diferenças entre o Azure AD e o Active Directory DS e como sincronizar entre os dois. Os alunos explorarão o gerenciamento de identidades no Azure AD e aprenderão sobre proteção de identidades usando o Windows Hello for Business, bem como Proteção de Identidade do Azure AD e autenticação multifator.

Lições

- Visão geral do Azure AD
- Gerenciando identidades no Azure AD
- Protegendo identidades no Azure AD
- Gerenciando a autenticação do dispositivo

Laboratório : Laboratório de Práticas - Gerenciando objetos e autenticação no Azure AD

Depois de completar este módulo, os estudantes estarão aptos a:

- Descrever os recursos do Azure AD.
- Gerenciar usuários usando o Azure AD com o Active Directory DS.
- Implementar o Windows Hello for Business.
- Associar dispositivos ao Azure AD.

Módulo 8: Gerenciamento de acesso e conformidade de dispositivo

Neste módulo, os alunos serão introduzidos para gerenciamento de segurança de dispositivo. O módulo abrangerá seguramente o acesso de recursos corporativos e introduzirá conceitos como VPN sempre ligada e conectividade remota no Windows 10. Os alunos aprenderão como criar e implantar políticas de conformidade e usar políticas de conformidade para acesso condicional. O módulo termina com os dispositivos de monitoramento registrados no Intune.

Lições

- Visão geral do Microsoft Intune
- Implementar políticas de conformidade de dispositivos

Laboratório : Laboratório prático - Gerenciamento de acesso e conformidade

Depois de completar este módulo, os estudantes estarão aptos a:

- Descrever os métodos de Habilitando o acesso de redes externas.
- Implantar políticas de conformidade e acesso condicional.
- Usar o Intune para monitorar a conformidade do dispositivo.

Módulo 9: Gerenciando a segurança

Neste módulo, os alunos aprenderão sobre proteção de dados. Os tópicos incluem o Windows & Azure Information Protection e várias tecnologias de criptografia suportadas no Windows 10. Este módulo também abrange capacidades principais do Windows Defender Advanced Threat Protection e como implementar essas capacidades em dispositivos na sua organização. O módulo termina usando o Windows Defender e funcionalidades como antivírus, firewall e Credential Guard.

Lições

- Implementar proteção de dados do dispositivo
- Gerenciar o Windows Defender ATP
- Gerenciando o Windows Defender no Windows 10

Laboratório : Laboratório de prática - Gerenciando a segurança no Windows 10

Depois de completar este módulo, os estudantes estarão aptos a:

- Descrever os métodos Protegendo os dados do dispositivo.
- Descreve as capacidades e benefícios do Windows ATP.
- Implantar e gerenciar configurações para clientes Windows Defender.

CURSO: Curso 20742-B: Identity with Windows Server

Duração Mínima: 5 dias

Objetivo: Deverá ensinar aos profissionais de TI como implementar e configurar o Active Directory Domain Services (AD DS) em um ambiente distribuído, como implementar a Política de Grupo, como executar o backup e a restauração e como monitorar e solucionar problemas relacionados ao Active Directory, além de problemas relacionados ao Windows Server 20xx. Além disso, o curso deverá ensinar aos estudantes como implementar outras funções de servidor do Active Directory, como Active Directory Federation Services (AD FS) e Active Directory Certificate Services (AD CS).

Estrutura de tópicos do curso

Módulo 1: Instalação e configuração de controladores de domínio

Este módulo descreve os recursos do AD DS e como instalar controladores de domínio (DCs). Além disso, abrange as considerações para a implementação de DCs.

Lições

- Visão geral do AD DS
- Visão geral dos controladores de domínio do AD DS
- Implementação de um controlador de domínio

Laboratório: Implementação e administração do AD DS

- Implementação do AD DS
- Implementação de controladores de domínio realizando clonagem de controlador de domínio
- Administração de AD DS

Depois de completar este módulo, os estudantes estarão aptos a:

- Descrever o AD DS e seus componentes principais.
- Descrever a finalidade e as funções dos controladores de domínio.
- Descrever as considerações para a implementação de controladores de domínio.

Módulo 2: Gerenciamento de objetos no AD DS

Este módulo descreve como usar várias técnicas para gerenciar objetos no AD DS. Isso inclui a criação e configuração de objetos de usuário, grupo e de computador.

Lições

- Gerenciamento de contas de usuários
- Gestão de grupos no AD DS
- Gerenciamento de objetos de computador no AD DS
- Uso do Windows PowerShell para administração de AD DS
- Implementação e gerenciamento de OUs

Laboratório: Gerenciamento de objetos AD DS

- Criação e gerenciamento de grupos no AD DS
- Criação e configuração de contas de usuário no AD DS
- Gerenciamento de objetos de computador no AD DS

Laboratório: Administração do AD DS

- Delegação de administração para OUs
- Criação e modificação de objetos AD DS com o Windows PowerShell

Depois de completar este módulo, os estudantes estarão aptos a:

- Gerenciar contas de usuário no AD DS.
- Gerenciar grupos no AD DS.
- Gerenciar objetos de computador no AD DS.
- Usar o Windows PowerShell para administração de AD DS.
- Implementar e gerenciar OUs.
- Administrar o AD DS.

Módulo 3: Gerenciamento de infraestrutura AD DS avançada

Este módulo descreve como planejar e implementar uma implantação de AD DS que inclui vários domínios e florestas. O módulo fornece uma visão geral dos componentes em uma implantação de AD DS avançada, o processo de implementação de um ambiente AD DS distribuído e o procedimento para configurar relações de confiança de AD DS.

Lições

- Visão geral das implementações de AD DS avançadas
- Implementação de um ambiente AD DS distribuído
- Configuração de confiança de AD DS

Laboratório: Gerenciamento de domínio e de relações de confiança no AD DS

- Implementação de relações de confiança para florestas
- Implementação de domínios secundários no AD DS

Depois de completar este módulo, os estudantes estarão aptos a:

- Descrever os componentes de uma implementação de AD DS avançada.
- Implementar um ambiente AD DS distribuído.

- Configurar relações de confiança de AD DS.

Módulo 4: Implementação e administração de locais e replicação de AD DS

Este módulo descreve como planejar e implementar uma implementação de AD DS que inclui vários locais. O módulo descreve como a replicação funciona em um ambiente AD DS do Windows Server 2016.

Lições

- Visão geral da replicação de AD DS
- Configuração de locais AD DS
- Configuração e monitoramento da replicação de AD DS

Laboratório: Implementação de locais e replicação de AD DS

- Modificação do local padrão
- Criação de locais e sub-redes adicionais
- Configuração da replicação de AD DS
- Monitoramento e diagnóstico de problemas da replicação de AD DS

Depois de completar este módulo, os estudantes estarão aptos a:

- Descrever como a replicação de AD DS funciona.
- Configurar locais AD DS para ajudar a otimizar o tráfego de autenticação e replicação.
- Configurar e monitorar a replicação de AD DS.

Módulo 5: Implementação de políticas de grupo

Este módulo descreve como implementar uma infraestrutura de GPO. O módulo fornece uma visão geral dos componentes e tecnologias que compõem a estrutura de Políticas de Grupo.

Lições

- Introdução à Política de Grupo
- Implementação e administração de GPO
- Escopo e processamento de políticas de grupo
- Diagnosticar problemas na aplicação de GPO

Laboratório: Implementação de uma infraestrutura de Política de Grupo

- Criação e configuração de GPO
- Gerenciamento do escopo de GPO

Laboratório: Diagnóstico de problemas de uma infraestrutura de Política de Grupo

- Verificar a aplicação de GPO
- Diagnosticar problemas de GPO

Depois de completar este módulo, os estudantes estarão aptos a:

- Explicar o que é a Política de Grupo.
- Implementar e administrar GPO.
- Descrever o escopo e o processamento da Política de Grupo.
- Diagnosticar problemas na aplicação de GPO.

Módulo 6: Gerenciamento de configurações de usuário com Política de Grupo

Este módulo descreve como configurar as definições e preferências de Política de Grupo. Isso inclui a implementação de modelos administrativos, a configuração de redirecionamento de pastas e scripts e a configuração de preferências de Política de Grupo.

Lições

- Implementação de modelos administrativos
- Configuração de redirecionamento de pastas, instalação de software e scripts
- Configuração das preferências de Política de Grupo

Laboratório: Gerenciamento de configurações do usuário com GPO

- Uso de modelos administrativos para gerenciar as configurações do usuário
- Implementar configurações com preferências de Política de Grupo
- Configuração do redirecionamento de pastas
- Planejamento da Política de Grupo (opcional)

Depois de completar este módulo, os estudantes estarão aptos a:

- Implementar modelos administrativos.

- Configurar o redirecionamento de pastas, instalação de software e scripts.
- Configurar as preferências de Política de Grupo.

Módulo 7: Segurança de Active Directory Domain Services

Este módulo descreve como configurar a segurança do controlador de domínio, segurança de contas, segurança de senhas e Contas de Serviço Gerenciado de Grupo (gMSAs).

Lições

- Segurança de controladores de domínio
- Implementação de segurança de contas
- Implementação da autenticação de auditoria
- Configuração de contas de serviço gerenciado

Laboratório: Segurança do AD DS

- Implementação de políticas de segurança para contas, senhas e grupos administrativos
- Implementação e configuração de um RODC
- Criação e associação de um MSA de grupo

Depois de completar este módulo, os estudantes estarão aptos a:

- Proteger controladores de domínio.
- Implementar a segurança de contas.
- Implementar a autenticação de auditoria.
- Configurar contas de serviço gerenciado (MSAs).

Módulo 8: Implementação e gerenciamento de AD CS

Este módulo descreve como implementar uma implantação de AD CS. Isso inclui a implementação, administração e diagnóstico de problemas.

Lições

- Implementação de CAs
- Administração de CAs
- Diagnóstico de problemas e manutenção de CAs

Laboratório: Implementação e configuração de hierarquia CA de duas camadas

- Implementação de uma CA raiz offline
- Implantação de uma CA subordinada à empresa

Depois de completar este módulo, os estudantes estarão aptos a:

- Implementar CAs.
- Administrar CAs.
- Diagnosticar problemas e a realizar a manutenção de CAs.

Módulo 9: Implementação e gerenciamento de certificados

Este módulo descreve como implantar e gerenciar certificados em um ambiente AD DS. Isso envolve a implementação e o gerenciamento de modelos de certificados, o gerenciamento da revogação e recuperação de certificados, o uso de certificados em um ambiente de negócios e a implementação de cartões inteligentes.

Lições

- Implementação e gerenciamento de modelos de certificados
- Gerenciamento da implementação, revogação e recuperação de certificados
- Uso de certificados em um ambiente empresarial
- Implementação e gerenciamento de cartões inteligentes

Laboratório: Implementação e uso de certificados

- Configuração de modelos de certificados
- Registro e uso de certificados
- Configuração e implementação de recuperação de chaves

Depois de completar este módulo, os estudantes estarão aptos a:

- Implementar e gerenciar modelos de certificados.
- Gerenciar a implementação, revogação e recuperação de certificados.
- Usar certificados em um ambiente empresarial.
- Implementar e gerenciar cartões inteligentes

Módulo 10: Implementação e administração de AD FS

Este módulo descreve o AD FS e como configurá-lo em um cenário de organização única e em um cenário de organização de parceiros.

Lições

- Visão geral do AD FS
- Requisitos e planejamento do AD FS
- Implementação e configuração do AD FS
- Visão geral do proxy de aplicativo web

Laboratório: Implementação do AD FS

- Configuração de pré-requisitos do AD FS
- Instalação e configuração do AD FS
- Configuração de um aplicativo interno para AD FS
- Configuração de AD FS para parceiros de negócios federados

Depois de completar este módulo, os estudantes estarão aptos a:

- Descrever o AD FS.
- Descrever como implementar o AD FS.
- Descrever como implementar o AD FS para uma única organização.
- Descrever como estender o AD FS a clientes externos.
- Implementar o logon único (SSO) para suporte a serviços online.

Módulo 11: Implementação e administração de AD RMS

Este módulo descreve como implementar uma implantação de AD RMS. O módulo fornece uma visão geral do AD RMS, descreve como implementar e gerenciar uma infraestrutura de AD RMS e fornece exemplos de como configurar a proteção de conteúdo AD RMS.

Lições

- Visão geral do AD RMS
- Implementação e gerenciamento de uma infraestrutura de AD RMS
- Configuração da proteção de conteúdo de AD RMS

Laboratório: Implementação da infraestrutura de AD RMS

- Instalação e configuração do AD RMS
- Configuração de modelos do AD RMS
- Uso do de AD RMS em clientes

Depois de completar este módulo, os estudantes estarão aptos a:

- Descrever o AD RMS.
- Implementar e gerenciar uma infraestrutura de AD RMS.

- Configurar a proteção de conteúdo de AD RMS.

Módulo 12: Implementação da sincronização do AD DS com o Microsoft Azure AD

Este módulo descreve como planejar e configurar a sincronização de diretórios entre o Microsoft Azure Active Directory (Azure AD) e o AD DS no local. Os módulos descrevem os vários cenários de sincronização, como sincronização Azure AD, AD FS e Azure AD, e Azure AD Connect.

Lições

- Planejamento e preparação para sincronização de diretórios
- Implementando a sincronização do diretório com o Azure AD Connect
- Gerenciamento de identidades com a sincronização de diretórios

Laboratório: Configuração da sincronização de diretórios

- Preparação para sincronização de diretórios
- Configuração da sincronização de diretórios
- Gerenciamento de usuários e grupos e gerenciamento da sincronização de diretórios do Active Directory

Depois de completar este módulo, os estudantes estarão aptos a:

- Planejar e preparar-se para sincronização de diretórios.
- Implementar a sincronização de diretórios com o Microsoft Azure Active Directory Connect (Azure AD Connect).
- Gerenciar identidades com a sincronização de diretórios.

Módulo 13: Monitoramento, gerenciamento e recuperação de AD DS

Este módulo descreve como monitorar, gerenciar e manter o AD DS para ajudar a alcançar alta disponibilidade de AD DS.

Lições

- Monitoramento de AD DS
- Gerenciamento do banco de dados do Active Directory
- Opções de backup e recuperação do Active Directory para AD DS e outras soluções de identidade e acesso

Laboratório: Recuperação de objetos no AD DS

- Backup e recuperação do AD DS
- Recuperação de objetos no AD DS

Depois de completar este módulo, os estudantes estarão aptos a:

- Monitorar o AD DS.
- Gerenciar o banco de dados do Active Directory.
- Descrever as opções de backup e recuperação do Active Directory para AD DS e outras soluções de identidade e acesso.

CURSO: Curso 20744-C: Securing Windows Server 2016

Duração mínima: 5 dias

Objetivo: Deverá ensinar aos profissionais de TI como otimizar a segurança da infraestrutura de TI que administram. Este curso deverá começar enfatizando a importância de assumir que as violações de rede já ocorreram e, em seguida, ensinar como proteger credenciais administrativas e direitos para ajudar a garantir que os administradores possam executar apenas as tarefas que precisam, quando precisam.

Este curso descreve como usar a auditoria e o recurso Advanced Threat Analysis no Windows Server 2016 para identificar problemas de segurança. Você também aprenderá a mitigar ameaças de malware, proteger sua plataforma de virtualização e usar opções de implementação, como servidor Nano, e contêineres para aumentar a segurança. O curso também discute como você pode ajudar a proteger o acesso aos arquivos por meio de criptografia e controle dinâmico de acesso e como é possível aprimorar a segurança da sua rede.

Estrutura de tópicos do curso

Módulo 1: Ataques, detecção de violações e ferramentas Sysinternals

Este módulo compõe o curso para que os alunos pensem em segurança em ambientes onde a base da infraestrutura é composta

predominantemente de produtos da Microsoft. O módulo começa com a apresentação aos estudantes sobre a filosofia de “simulação da violação” e fazê-los entender os diferentes tipos de ataques que podem ocorrer, incluindo cronogramas de ataque e vetores. Além disso, permite que os estudantes estabeleçam os recursos-chave, como devem agir ao detectar um incidente e como as necessidades diretas e os requisitos legislativos de uma organização determinam as políticas de segurança.

Lições

- Compreendendo os ataques
- Como detectar falhas de segurança
- Examinar as atividades com as ferramentas Sysinternals

Laboratório: Estratégias básicas de detecção de violação e resposta a incidentes

- Identificando tipos de ataque
- Explorando as ferramentas Sysinternals

Depois de completar este módulo, os estudantes estarão aptos a:

- Descrever os tipos de ataques que podem ocorrer.
- Explicar como detectar falhas de segurança.
- Explicar como examinar as atividades usando o conjunto de ferramentas Sysinternals.

Módulo 2: Proteção de credenciais e acesso privilegiado

Este módulo abrange contas e direitos de usuário, contas de computador e serviços, credenciais, estações de trabalho de acesso privilegiado e a solução de senha do administrador local. Neste módulo, os estudantes aprenderão a configurar direitos do usuário e opções de segurança, proteger credenciais com o Securityedential Guard, implementar estações de trabalho de acesso privilegiado e gerenciar e implementar a Solução de Senha de Administrador Local, que permite gerenciar senhas de conta de administrador local.

Lições

- Compreendendo os direitos de usuário
- Contas de computador e serviços
- Proteção de credenciais
- Estações de trabalho de acesso privilegiados e Jump Servers

- Solução de senha de administrador local

Laboratório: Implementando direitos de usuário, opções de segurança e contas de serviço gerenciado de grupo

- Configuração dos direitos de usuário e opções de segurança da conta
- Delegar privilégios
- Criação de contas de serviço gerenciado de grupo
- Localização de contas problemáticas

Laboratório: Configuração e implementação de LAPs

- Instalação e configuração de LAPs
- Implementação e teste de LAPs

Depois de completar este módulo, os estudantes estarão aptos a:

- Configurar os direitos de usuário.
- Implementar contas de computador e serviços.
- Proteger credenciais.
- Descrever como configurar estações de trabalho de acesso privilegiado e jump servers.
- Configurar a Solução de Senha de Administrador Local (LAPS).

Módulo 3: Limitando os direitos do administrador com Just Enough Administration

Este módulo discute como implementar e configurar a solução Just Enough Administration (JEA), que é uma tecnologia administrativa que permite que os alunos apliquem princípios de controle de acesso baseados em função (RBAC) por meio de sessões remotas do Windows PowerShell.

Lições

- Compreendendo o JEA
- Verificação e implementação do JEA

Laboratório: Limitando privilégios de administrador com JEA

- Criando um arquivo de recursos de função
- Criando um arquivo de configuração de sessão
- Criando um terminal JEA
- Conectar e testar um terminal JEA

- Implementação de uma configuração JEA para outro computador

Depois de completar este módulo, os estudantes estarão aptos a:
- Compreender o JEA.
- Verificar e implementar o JEA.

Módulo 4: Gerenciamento e florestas administrativas de acesso privilegiado

Este módulo descreve os conceitos de florestas de Ambiente Administrativo de Segurança Aprimorado (ESAE), Microsoft Identity Manager (MIM), Administração Just In Time (JIT) ou Gerenciamento de Acesso Privilegiado (PAM).

Lições
- Florestas ESAE
- Visão geral do Microsoft Identity Manager
- Visão geral da administração JIT e PAM

Laboratório: Limitando privilégios de administrador com PAM
- Abordagem em camadas para a segurança
- Configuração de relações de confiança e entidades sombra
- Solicitando acesso privilegiado
- Gerenciando funções PAM

Depois de completar este módulo, os estudantes estarão aptos a:
- Descrever as florestas ESAE.
- Descrever o MIM.
- Compreender a administração JIT e PAM.

Módulo 5: Mitigação de malware e ameaças

Este módulo descreve como usar ferramentas como Windows Defender, Windows AppLocker, Microsoft Device Guard, Windows Defender Application Guard e Windows Defender Exploit Guard.

Lições
- Configuração e gerenciamento do Windows Defender
- Restrição de software
- Configuração e uso do recurso Device Guard

Laboratório: Proteger aplicativos com regras do Windows Defender, AppLocker e Device Guard

- Configuração do Windows Defender
- Configuração do AppLocker
- Configuração do Device Guard

Depois de completar este módulo, os estudantes estarão aptos a:

- Configurar e gerenciar o Windows Defender.
- Usar as políticas de restrição de software e AppLocker.
- Configurar e usar o recurso Device Guard.

Módulo 6: Analisando as atividades com auditoria e análise de log avançadas

Este módulo fornece uma visão geral da auditoria e, em seguida, oferece informações detalhadas sobre como configurar a auditoria avançada e auditoria e login do Windows PowerShell.

Lições

- Visão geral da auditoria
- Auditoria avançada
- Auditoria e login do Windows PowerShell

Laboratório: Configuração de auditoria avançada

- Configurando a auditoria do acesso ao sistema de arquivos
- Auditoria de acesso de domínio
- Gerenciamento de configuração avançada de políticas de auditoria
- Login e auditoria do Windows PowerShell

Depois de completar este módulo, os estudantes estarão aptos a:

- Descrever a auditoria.
- Compreender a auditoria avançada.
- Configurar a auditoria e o login do Windows PowerShell.

Módulo 7: Implementar e configurar o Advanced Threat Analytics e o Microsoft Operations Management Suite

Este módulo descreve as ferramentas Microsoft Advanced Threat Analytics e Microsoft Operations Management suite (OMS). O módulo também explica como usá-las para monitorar e analisar a segurança de uma implementação do Windows Server. Você também aprenderá

sobre o Microsoft Azure Security Center, que permite gerenciar e monitorar a configuração de segurança de cargas de trabalho no local e na nuvem.

Lições

- Implementação e configuração do ATA
- Implementação e configuração do Microsoft Operations Management Suite
- Implementação e configuração do Azure Security Center

Laboratório: Implantação do ATA, Microsoft Operations Management Suite e Azure Security Center

- Preparação e implementação do ATA
- Implementação e implementação do Microsoft Operations Management Suite
- Implementação e configuração do Azure Security Center

Depois de completar este módulo, os estudantes estarão aptos a:

- Implementar e configurar do ATA.
- Implementar e configurar o Microsoft Operations Management Suite.
- Implementar e configurar o Azure Security Center.

Módulo 8: Infraestrutura de virtualização segura

Este módulo descreve como configurar VMs de malha protegida, incluindo os requisitos para VMs blindados e com suporte para criptografia.

Lições

- Malha protegida
- Máquinas virtuais blindadas e protegidas por criptografia

Laboratório: Malha protegida com atestado confiável do administrador e VMs blindados

- Implementação de malha protegida com atestado confiável do administrador
- Implementação de VM blindado

Depois de completar este módulo, os estudantes estarão aptos a:

- Configurar a malha protegida.
- Descrever os VMs blindados e protegidos por criptografia.

Módulo 9: Proteção do desenvolvimento de aplicativo e da infraestrutura de carga de trabalho de servidor

Este módulo descreve o SCT, um conjunto de ferramentas gratuitas que podem ser baixadas e usadas para criar e aplicar configurações de segurança. Você também aprenderá a aprimorar a segurança da plataforma, reduzindo o tamanho e o escopo dos recursos de aplicação e computação por meio de cargas de trabalho de contêiner.

Lições

- Uso do SCT
- Compreendendo os contêineres

Laboratório: Uso do SCT

- Configuração de uma linha de base de segurança para o Windows Server 2016
- Implementação de uma linha de base de segurança para o Windows Server 2016

Laboratório: Implementação e configuração de contêineres

- Implementação e gerenciamento de um contêiner do Windows

Depois de completar este módulo, os estudantes estarão aptos a:

- Instalar o SCT e criar e implementar linhas de base de segurança.
- Configurar os contêineres do Windows e do Hyper-V no Windows Server 2016.

Módulo 10: Planejamento e proteção de dados

Este módulo descreve como configurar o Sistema de Arquivos com Criptografia (EFS) e a criptografia de unidade de disco BitLocker para proteger os dados inativos. Você também aprenderá a estender a proteção para a nuvem com a Proteção de Informações do Azure.

Lições

- Planejamento e implementação de criptografia

- Planejamento e implementação do BitLocker
- Proteção de dados com a Proteção de Informações do Azure

Laboratório: Proteção de dados com criptografia e BitLocker

- Criptografar e recuperar o acesso a arquivos criptografados
- Usando o BitLocker para proteger dados

Depois de completar este módulo, os estudantes estarão aptos a:

- Planejar e implementar criptografia.
- Planejar e implementar o BitLocker.
- Planejar e implementar a Proteção de Informação do Azure.

Módulo 11: Otimização e proteção de serviços de arquivo

Este módulo descreve como otimizar os serviços de arquivos ao configurar o Gerenciador de Recurso de Servidor de Arquivos (FSRM) e o Sistema de Arquivos Distribuído (DFS). Os estudantes também aprenderão a gerenciar o acesso a arquivos compartilhados configurando o Controle de Acesso Dinâmico (DAC).

Lições

- Gerenciador de Recursos de Servidor de Arquivos
- Implementar tarefas de classificação e gerenciamento de arquivos
- Controle de Acesso Dinâmico

Laboratório: Cotas e triagem de arquivos

- Configurar cotas do Gerenciador de Recursos de Servidor de Arquivos
- Configuração de relatórios de triagem e armazenamento de arquivos

Laboratório: Implementação do controle de acesso dinâmico

- Preparação para a implementação do controle de acesso dinâmico
- Implementação do controle de acesso dinâmico
- Validação e correção do controle de acesso dinâmico

Depois de completar este módulo, os estudantes estarão aptos a:

- Descrever o Gerenciador de Recursos de Servidor de Arquivos.

- Implementar tarefas de classificação e gerenciamento de arquivos.
- Implementar o Controle de Acesso Dinâmico.

Módulo 12: Proteção do tráfego de rede com firewalls e criptografia

Este módulo descreve como usar o Windows Firewall como uma parte importante da estratégia de proteção de uma organização. Ele descreve também o uso do protocolo IPsec para criptografar o tráfego de rede e estabelecer zonas de segurança em sua rede. Você também aprenderá sobre o recurso Datacenter Firewall, que pode ser usado para ajudar a proteger seus ambientes virtuais no local.

Lições

- Compreendendo as ameaças de segurança relacionadas à rede
- Compreendendo o Windows Firewall com segurança avançada
- Configurando o IPsec
- Datacenter Firewall

Laboratório: Configuração do Windows Firewall com segurança avançada

- Criando e testando regras de entrada
- Criando e testando regras de saída
- Criando e testando regras de segurança de conexão

Depois de completar este módulo, os estudantes estarão aptos a:

- Descrever as ameaças de segurança relacionadas à rede e como atenuá-las.
- Configurar o Windows Firewall com segurança avançada.
- Configurar o IPsec.
- Descrever o Datacenter Firewall.

Módulo 13: Proteção do tráfego de rede

Este módulo explora algumas das tecnologias do Windows Server 2016 que podem ser usadas para ajudar a mitigar ameaças à segurança da rede. O módulo explica como configurar o DNSSEC para ajudar a proteger o tráfego da rede e usar o Microsoft Message Analyzer para monitorar o tráfego de rede. O módulo também descreve como proteger o tráfego Server Message Block (SMB).

Lições

- Configuração de opções avançadas de DNS
- Examinando o tráfego de rede com o Message Analyzer
- Proteger e analisar o tráfego SMB

Laboratório: Proteção do DNS

- Configuração e teste do DNSSEC
- Configuração de políticas de DNS e RRL

Laboratório: Microsoft Message Analyzer e criptografia de SMB

- Instalação e uso do Message Analyzer
- Configuração e verificação da criptografia de SMB em compartilhamentos SMB

Depois de completar este módulo, os estudantes estarão aptos a:

- Configurar opções avançadas de DNS.
- Usar o Message Analyzer.
- Proteger o tráfego de SMB.

CURSO : Curso 20703-1-B: Administering System Center Configuration Manager

Duração mínima: 5 dias

Objetivo: Deverá descrever como usar o Gerenciador de Configuração e seus sistemas de site associados para gerenciar eficientemente os recursos de rede. Deverá ensinar tarefas diárias de gerenciamento, incluindo como gerenciar aplicativos, saúde do cliente, inventário de hardware e software, implantação do sistema operacional e atualizações de software usando o Gerenciador de Configuração. Deverá ensinar como otimizar a System Center Endpoint Protection, gerenciar a conformidade e criar consultas e relatórios de gerenciamento.

Estrutura de tópicos do curso

Módulo 1: Gerenciamento de computadores e dispositivos móveis na empresa

Este módulo descreve os recursos do Gerenciador de Configuração que você pode usar para executar tarefas complexas de gerenciamento, incluindo as seguintes tarefas; Inventário de hardware e software, gerenciamento de aplicativos, implantação de sistema operacional, gerenciamento de configurações, gerenciamento de atualizações de software, solução remota de problemas do cliente e proteção contra malware.

Microsoft System Center Configuration Manager (Configuration Manager) fornece vários recursos que podem ajudá-lo a gerenciar dispositivos e usuários tanto no local quanto em cloud. As organizações que usam o Gerenciador de Configuração descobrem que podem fornecer serviços IT mais eficazes em relação à implantação de software, gerenciamento de configurações e gerenciamento de ativos.

Este módulo apresenta as principais ferramentas de recursos, arquitetura e gerenciamento usadas com o Gerenciador de Configuração. Este módulo também fornece uma base que se relaciona com todas as outras características e tarefas de gestão discutidas nos módulos que seguem a seguir a este.

Aulas

- Visão geral da gestão de sistemas utilizando soluções de gestão empresarial
- Visão geral da arquitetura do Gerenciador de Configuração
- Visão geral das ferramentas administrativas do Gerenciador de Configuração
- Ferramentas para monitorar e solucionar problemas num site do Configuration Manager

Laboratório : Explorar as ferramentas do Gerenciador de Configuração

- Pesquisar no console do Configuration Manager
- Usar Windows PowerShell com o Gerenciador de Configuração
- Usar o Gerenciador de Serviços do Gerenciador de Configuração para gerenciar componentes
- Monitorar o status do local e do componente

- Revisar arquivos de log usando a ferramenta Rastreamento do Gerenciador de Configuração

Após a conclusão deste módulo, os alunos serão capazes de:

- Explicar como o Gerenciador de Configuração aborda os desafios de gerenciar sistemas e usuários na empresa atual.
- Descrever a arquitetura do Gerenciador de Configuração.
- Descrever as ferramentas de gerenciamento que você usa para executar funções administrativas para o Gerenciador de Configuração.
- Descrever as ferramentas que você usa para monitorar e solucionar problemas num site do Configuration Manager.

Módulo 2: Análise de dados usando consultas, relatórios e CMPivot

O banco de dados da Microsoft System Center Configuration Manager armazena uma grande quantidade de dados sobre os recursos em seu ambiente. Você pode nem sempre querer executar todas as tarefas de gerenciamento em todos os recursos simultaneamente. Portanto, para ajudá-lo a localizar dispositivos ou objetos de usuário em seu ambiente que atendam a critérios específicos, você pode criar consultas. Em seguida, você pode usar essas consultas para criar coleções ou para encontrar informações adicionais sobre recursos específicos. Este módulo descreve consultas e métodos de criação e execução.

Além das consultas, você pode executar relatórios para visualizar vários tipos de informações relacionadas ao ambiente do Gerenciador de Configuração. Para executar relatórios do Gerenciador de Configuração, você deve instalar e configurar um ponto de serviços de emissão de relatórios, que este módulo detalha.

Este módulo também abrange CMPivot, que permite coletar e visualizar dados em tempo real em todos os dispositivos conectados em seu ambiente. Isso permitirá que você tome decisões em tempo real.

Aulas

- Introdução a consultas
- Configuração Serviços SQL de Relatórios de Servidores
- Analisar o estado em tempo real de um dispositivo usando CMPivot

Laboratório : Criar e Executar consultas

- Criação de consultas de dados
- Criação de consultas de subseleção

Laboratório : Configuração SSRS

- Configuração de um ponto de serviços de relatório

Laboratório : Analisando o estado em tempo real de um dispositivo usando CMPivot

- Usar CMPivot para analisar o estado atual dos dispositivos

Após a conclusão deste módulo, os alunos serão capazes de:

- Criar e configurar consultas de mensagens de status e dados.
- Configurar e gerenciar Microsoft SQL Server Reporting Services (SSRS) e o ponto de serviços de reportagem.
- Usar CMPivot para consultar e visualizar o estado em tempo real dos dispositivos conectados em seu ambiente.

Módulo 3: Elaboração da infraestrutura de gerenciamento do Gerenciador de Configuração

Você pode gerenciar os recursos do computador e do usuário dentro de um ambiente da Microsoft System Center Configuration Manager (Configuration Manager) somente quando o Gerenciador de Configuração descobre esses recursos e os atribui a um site.

Neste módulo, você aprenderá sobre limites e grupos de limites que ajudam a criar locais de rede lógicos contendo dispositivos de computador que você precisa gerenciar em sua infraestrutura de Gerenciador de Configuração. Você pode usar essas configurações de limite para atribuição automática do site e para ajudar os clientes a encontrar conteúdo e serviços a partir de sistemas de sites associados. Você também aprenderá sobre os processos de descoberta que você pode usar para identificar computadores, usuários e a infraestrutura de rede dentro do seu ambiente de rede.

Em seguida, você aprenderá sobre coleções que suportam agrupamentos lógicos de recursos. Você usa esses agrupamentos para tarefas de gerenciamento, como direcionar atualizações de software, gerenciar implantações de aplicativos ou implantar configurações de conformidade em recursos.

Aulas

- Configuração de limites do site e grupos de limites
- Configuração da detecção de recursos
- Organizar recursos utilizando coleções de dispositivos e usuários

Laboratório : Configuração de limites e detecção de recursos

- Configuração de limites, grupos de limites e relações de recuo
- Configuração de métodos de detecção do Active Directory

Laboratório : Configuração de coleções de usuários e dispositivos

- Criar uma coleção de dispositivos
- Criar uma coleção de usuários
- Configuração de uma janela de manutenção

Após a conclusão deste módulo, os alunos serão capazes de:

- Configurar limites e grupos de limites.
- Configurar a detecção de recursos.
- Organizar recursos utilizando coleções de dispositivos e usuários.

Módulo 4: Implantação e gerenciamento do cliente Gerenciador de Configuração

Você pode instalar o software da Microsoft System Center Configuration Manager (Configuration Manager) do cliente em dispositivos baseados em servidores Windows, estações de trabalho e laptops. Em seguida, você pode gerenciar esses dispositivos e executar operações como relatórios de informações de inventário de hardware e software, Instalar e atualizar software e configurar configurações necessárias para conformidade.

O Configuration Manager oferece várias opções para instalar o software do cliente. Este módulo explica os sistemas operacionais e dispositivos operacionais suportados, os requisitos de software e diferentes métodos para instalar o software do cliente. Este módulo também descreve algumas das configurações padrão e personalizadas do cliente que você pode configurar. Depois de instalar o software do cliente, você pode configurar as configurações do cliente e controlar como os vários componentes do cliente interagem entre o dispositivo gerenciado e o ambiente Gerenciador de Configuração.

Aulas

- Visão geral do cliente Configuration Manager
- Implantação do cliente Gerenciador de Configuração
- Configuração e monitoramento do status do cliente
- Gerenciar as configurações do cliente e realizar operações de gerenciamento

Laboratório : Implantar o software da Microsoft System Center Configuration Manager do cliente

- Preparar o site para instalação do cliente
- Implantar o software cliente do Gerenciador de Configuração usando a instalação de push do cliente

Laboratório : Configuração e monitoramento do status do cliente

- Configuração e monitoramento do estado de saúde do cliente

Laboratório : Gerenciamento de configurações de clientes

- Configuração das configurações do cliente
- Execução de operações de gestão

Após a conclusão deste módulo, os alunos serão capazes de:

- Descrever os requisitos e considerações para a instalação do software Gerenciador de Configuração do cliente.
- Implantar o software do cliente Do Gerenciador de Configuração.
- Gerenciar as configurações do cliente do Gerenciador de configuração.

Módulo 5: Gerenciamento de estoque para PCs e aplicativos

Este módulo fornece uma visão geral da coleta de estoque e explica como você pode gerenciar as informações coletadas. Você também aprenderá sobre o processo de coleta de hardware e inventário de software, iniciando ciclos de inventário e iniciando e garantindo a coleta de estoque. Este módulo também abrange o uso de medição de software para monitorar o uso do programa e a configuração e gerenciamento de Inteligência patrimonial.

Aulas

- Visão geral da coleta de estoque

- Configuração do inventário de hardware e software
- Gerenciamento da coleta de estoque
- Configuração da medição de software
- Configuração e gerenciamento de Inteligência patrimonial

Laboratório : Configuração e gerenciamento da coleta de estoque

- Configuração e gerenciamento de inventário de hardware

Laboratório : Configuração de medição de software

- Configuração da medição de software

Laboratório : Configuração e gerenciamento de Inteligência patrimonial

- Preparando o site para inteligência patrimonial
- Configuração de Inteligência patrimonial
- Monitoramento de contratos de licença usando Inteligência patrimonial
- Visualização de relatórios de inteligência de ativos

Após a conclusão deste módulo, os alunos serão capazes de:

- Descrever a coleta de inventário.
- Configurar e coletar hardware e inventário de software.
- Gerenciar a coleta de inventário.
- Configurar a medição do software.
- Configurar a inteligência patrimonial.

Módulo 6: Distribuição e gerenciamento de conteúdo usado para implantações

Clientes da Microsoft System Center Configuration Manager (Configuration Manager) obtêm conteúdo, como pacotes, aplicativos, atualizações de software e até imagens do sistema operacional, a partir de uma infraestrutura de conteúdo composta por pontos de distribuição e fontes de cache por pares. Neste módulo, você revisará os recursos de distribuição e gerenciamento de conteúdo, configurará pontos de distribuição e aprenderá a distribuir e monitorar conteúdo. Você também executará a validação de conteúdo e a prestação de conteúdo.

Aulas

- Elaboração da infraestrutura para gerenciamento de conteúdo
- Distribuição e gerenciamento de conteúdo em pontos de distribuição

Laboratório : Distribuição e gerenciamento de conteúdo para implantações

- Instalação de um novo ponto de distribuição
- Gerenciamento de distribuição de conteúdo

Após a conclusão deste módulo, os alunos serão capazes de:

- Preparar a infraestrutura para gerenciamento de conteúdo.
- Distribuir e gerenciar conteúdo em pontos de distribuição.

Módulo 7: Implantação e gerenciamento de aplicativos

Neste módulo, você aprenderá sobre os métodos de criação, implantação e gerenciamento de aplicativos com o Gerenciador de Configuração. Você também aprenderá a usar o Centro de Software e o Catálogo de Aplicativos para instalar aplicativos disponíveis. Você aprenderá sobre o gerenciamento de implantações em aplicativos não convencionais. Além disso, você aprenderá a instalar aplicativos do Windows 10 e aplicativos virtualizados.

Aulas

- Visão geral do gerenciamento de aplicativos
- Criação de aplicativos
- Implantação de aplicativos
- Gerenciamento de aplicativos
- Implantação de aplicativos virtuais usando o Gerenciador de Configuração do Centro do Sistema (Opcional)
- Implantação e gestão de Aplicativos do Windows Store

Laboratório : Criação e implantação de aplicativos

- Criação de aplicativos com requisitos
- Implantação de aplicativos

Laboratório : Gerenciamento da superação de aplicativos e remoção

- Gerenciamento da superação de aplicativos
- Desinstalar o Aplicativo visualizador de Excel

Laboratório : Implantação de aplicativos virtuais usando o Gerenciador de Configuração (Opcional)

- Implantação de aplicativos virtuais

Laboratório : Usando o Gerenciador de Configuração para implantar aplicativos do Windows Store

- Configuração de suporte para sideloading de aplicativos do Windows Store
- Configuração de um aplicativo do Windows Store
- Implantação de aplicativos de Windows 10 para usuários

Após a conclusão deste módulo, os alunos serão capazes de:

- Descrever os recursos de gerenciamento de aplicativos de Configuration Manager.
- Criar aplicativos.
- Implantar aplicativos.
- Gerenciar aplicações.
- Configurar e implantar aplicativos virtuais.
- Configurar e implantar aplicativos do Windows Store.

Módulo 8: Manutenção de atualizações de software para PCs gerenciados

Este módulo explica como usar o recurso de atualizações de software em Configuration Manager para implementar um processo de gestão de ponta a ponta para a complexa tarefa de identificar, implantar e monitorar Microsoft e atualizações de software de terceiros para seus Clientes da Configuration Manager.

Aulas

- O processo de atualizações de software
- Preparando um site Configuration Manager para atualizações de software
- Gerenciamento de atualizações de software
- Configuração de regras de implantação automática
- Monitoramento e resolução de problemas de atualizações de software
- Habilitação de atualizações de terceiros

Laboratório : Configuração do site para atualizações de software

- Configuração e sincronização do ponto de atualização de software

Laboratório : Implantação e gerenciamento de atualizações de software

- Determinar a conformidade com a atualização de software
- Implantação de atualizações de software para clientes
- Configuração de regras de implantação automática

Após a conclusão deste módulo, os alunos serão capazes de:

- Descrever como o recurso de atualizações de software se integra com Configuration Manager.
- Preparar o site Configuration Manager para atualizações de software.
- Gerenciar atualizações de software usando Configuration Manager.
- Configurar regras de implantação automáticas.
- Monitorar e solucionar atualizações de software.
- Descrever como ativar atualizações de terceiros.

Módulo 9: Implementação de Endpoint Protection para PCs gerenciados

Este módulo explica como usar os recursos relacionados à segurança fornecidos pelo Configuration Manager para ajudar a proteger os computadores clientes contra ameaças de malware e definir configurações específicas do Firewall do Windows Defender para clientes. Com base na funcionalidade do System Center Endpoint Protection (Endpoint Protection), o Endpoint Protection no Configuration Manager oferece suporte à implantação, gerenciamento e monitoramento de políticas antimalware, configurações do Firewall do Windows Defender, políticas do Windows Defender Application Guard, políticas do Windows Defender Exploit Guard e Windows Defender Application Políticas de controle em computadores clientes.

Aulas

- Visão geral de Endpoint Protection em Configuration Manager
- Configuração, implantação e monitoramento de políticas da Endpoint Protection
- Configuração e implantação de políticas avançadas de ameaça

Laboratório : Implementação da Endpoint Protection no Centro de Sistemas da Microsoft

- Configuração do Endpoint Protection no Centro de Sistemas e configurações do cliente
- Configuração e implantação de Políticas do Endpoint Protection
- Monitoramento Endpoint Protection

Laboratório : Implementando políticas avançadas de ameaças

- Criação e implantação de políticas avançadas de proteção contra ameaças

Após a conclusão deste módulo, os alunos serão capazes de:

- Configurar Endpoint Protection para detectar e remediar malware e vulnerabilidades de segurança.
- Configurar, implantar e gerenciar Políticas da Endpoint Protection.
- Configurar e implantar políticas avançadas de proteção contra ameaças.

Módulo 10: Gerenciamento de conformidade e acesso seguro a dados

Muitas organizações corporativas exigem sistemas, como servidores, laptops, computadores desktop e dispositivos móveis, para atender a requisitos específicos de configuração e conformidade. As configurações de conformidade no Gerenciador de Configuração podem desempenhar um papel fundamental na identificação de configurações existentes, na descoberta de sistemas que têm alterações de configuração adversas e na correção dessas configurações automaticamente quando necessário.

As configurações de conformidade também podem ajudar a controlar como os usuários gerenciam e acessam dados no ambiente de rede corporativa. Para computadores que são executados em Windows 8 e sistemas operacionais mais recentes, você pode gerenciar dados usando redirecionamento de pastas, arquivos offline e perfis de roaming. Você também pode controlar o acesso a dados usando perfis de conexão remota, perfis em rede virtual privada (VPN), perfis Wi-Fi e perfis de certificados.

Este módulo descreve as configurações de conformidade que você pode gerenciar usando Configuration Manager. Você aprenderá a usar

essas configurações para manter os requisitos de configuração e fornecer acesso seguro a dados aos recursos corporativos.

Aulas

- Visão geral das configurações de conformidade
- Configuração de configurações de conformidade
- Visualização dos resultados de conformidade
- Gerenciamento de acesso a recursos e dados

Laboratório : Gerenciamento de configurações de conformidade

- Gerenciamento de itens de configuração e linhas de base
- Visualização de configurações e relatórios de conformidade
- Configuração da remediação nas configurações de conformidade
- Usar informações de conformidade para criar coleções

Após a conclusão deste módulo, os alunos serão capazes de:

- Descrever as características das configurações de conformidade.
- Configurar as configurações de conformidade.
- Ver os resultados de conformidade.
- Gerenciar o acesso a recursos e dados.

Módulo 11: Gerenciamento da implantação do sistema operacional

Este módulo explica como usar o recurso de implantação do sistema operacional em Configuration Manager para criar imagens do sistema operacional que você pode implantar em computadores não gerenciados e aqueles gerenciados por Configuration Manager. Existem vários cenários em que você pode implantar sistemas operacionais usando Configuration Manager, inclusive quando você está trabalhando com novos sistemas ou quando você está atualizando os existentes. A implantação do sistema operacional usa ambos componentes da Configuration Manager e do Windows para gerenciar e fornecer imagens do sistema operacional. Você pode fazer configurações num computador de referência antes de capturar uma imagem de seu sistema operacional ou usando sequências de tarefas que Configuration Manager cria depois de implantar a imagem num sistema de destino.

Este módulo também explica como usar Configuration Manager para criar uma estratégia para implantações de sistema operacional. E também, ele explica como gerenciar Windows como um serviço.

Este módulo explica como gerenciar Windows como um serviço.

Aulas

- Uma visão geral da implantação do sistema operacional
- Preparação de um local para implantação do sistema operacional
- Implantação de um sistema operacional
- Gerir o Windows como um serviço

Laboratório : Preparação do site para implantação do sistema operacional

- Gerenciamento das funções do sistema de site usadas para suportar a implantação do sistema operacional
- Gerenciamento de pacotes para suportar a implantação do sistema operacional

Laboratório : Implantação de imagens de sistema operacional para instalações de metal

- Preparando a imagem do sistema operacional
- Criar uma sequência de tarefas para implantar uma imagem
- Implantando uma imagem

Após a conclusão deste módulo, os alunos serão capazes de:

- Descrever a terminologia, os componentes e os cenários utilizados para implantar sistemas operacionais usando o Gerenciador de Configuração.
- Preparar um local para implantação do sistema operacional.
- Implantar uma imagem do sistema operacional.
- Descrever como gerenciar Windows como um serviço.

Módulo 12: Gerenciamento e manutenção de um site Configuration Manager

Este módulo descreve a administração baseada em funções, ferramentas remotas e as tarefas de manutenção do site que você pode gerenciar usando Configuration Manager. Este módulo também descreve como fazer backup e recuperar um sistema de site do

Gerenciador de Configuração e usar as recomendações do Management Insights para simplificar a administração.

Aulas

- Configuração da administração baseada em funções
- Configuração de Ferramentas Remotas
- Visão geral da manutenção do site do Configuration Manager e Management Insights
- Fazer backup e recuperar um site do Configuration Manager
- Atualização da infraestrutura do Gerenciador de Configuração

Laboratório : Configuração de administração baseada em funções

- Configuração de um novo escopo para administradores de Toronto
- Configuração de um novo usuário administrativo

Laboratório : Configuração de ferramentas remotas

- Configuração das configurações e permissões do cliente de ferramentas remotas
- Gerenciamento de desktops usando controle remoto

Laboratório : Manter um site do Configuration Manager

- Configurar tarefas de manutenção no Configuration Manager
- Configurar a tarefa do servidor do site de backup
- Recuperar um site de um backup

Após a conclusão deste módulo, os alunos serão capazes de:

- Configurar a administração baseada em funções.
- Configurar ferramentas remotas para suportar a atividade do cliente.
- Identificar tarefas de manutenção do site do gerenciador de configuração.
- Fazer backup e recuperar um site do Configuration Manager.
- Usar Atualizações e Manutenção para instalar atualizações na infraestrutura do Gerenciador de Configuração.

Duração Mínima: 5 dias

Objetivo: Este curso deverá ensinar os profissionais de TI a administrar e dar suporte ao Exchange Server. O curso deverá abordar como instalar e configurar o Exchange Server. Ele também deverá abordar como gerenciar destinatários de e-mail e pastas públicas, incluindo como executar operações em massa usando o shell de gerenciamento do Exchange. Além disso, o curso deverá abordar como gerenciar a conectividade do cliente, transporte e limpeza de mensagens e implementações do Exchange Server de alta disponibilidade. Ele também deverá abordar como implementar soluções de recuperação de desastres. Por último, o curso deverá abordar como manter e monitorar uma implementação do Exchange Server e como administrar o Exchange Online em uma implementação do Office 365.