

- Desative o software antivírus quando necessário (como durante instalações de software) e saiba quando reativar o software antivírus.
- Evite abrir anexos de remetentes desconhecidos.
- Use recursos anti-phishing em navegadores da Web e clientes de e-mail.

Treinamento anti-phishing

Phishing é um problema bem conhecido que continua a confundir os educadores de segurança de rede. O phishing requer usuários ingênuos ou vulneráveis que não estão familiarizados com a facilidade com que podem fornecer um lar para malware ou vírus. Isso geralmente é feito abrindo um e-mail que os usuários não olham cuidadosamente antes de abrir ou fornecendo informações que podem ajudar os hackers a acessar a rede.

O treinamento pode envolver relatórios semanais de exemplos de phishing. Alguns departamentos de TI até lançam internamente tentativas de phishing “falsas” para ver se alguém responde e precisa de mais treinamento.

Reinstalação do sistema operacional

A reinstalação do sistema operacional geralmente é uma boa solução para um computador infectado. É um processo complicado, mas muitos vírus estão tão bem escondidos que podem ser a melhor solução.

Antes de realizar a reinstalação:

- Isole o computador de todas as conexões de rede.
- Altere todas as senhas que foram usadas durante o período suspeito de infecção, principalmente senhas bancárias e de trabalho. (Não faz sentido alterar as senhas do computador porque elas precisarão ser redefinidas durante a instalação.)
- Faça backup dos arquivos de dados em um disco rígido externo. Não faça backup dos aplicativos; o vírus pode residir em um deles.

Durante e após a reinstalação:

- Mantenha o computador fora da rede durante o processo.

- Solicite todas as atualizações disponíveis.
- Habilite o firewall e instale qualquer outro software de segurança usado na rede.

- Verifique a unidade externa que contém os arquivos de backup para garantir que o vírus não seja reimpostado em um deles.
- Ative as atualizações automáticas para o sistema operacional e o software antivírus.

Ameaças e vulnerabilidades de engenharia social



Objetivo 2.4: Explicar ataques, ameaças e vulnerabilidades comuns de engenharia social.

Os botnets tornaram o hacking tão fácil que qualquer rede pode ser testada por hackers milhares de vezes por dia. O software antivírus/antimalware atualizado e outros softwares fazem o trabalho pesado na proteção de redes e dispositivos. Outra ameaça constante a uma rede de computadores são os usuários sendo manipulados ou induzidos a fazer o trabalho de hackers para eles. Essa técnica de hacking é conhecida como engenharia social. As seções a seguir descrevem a engenharia social e outras ameaças e vulnerabilidades às redes.

Engenharia social

Oito técnicas

comuns **de engenharia social** que todos os funcionários de uma organização devem conhecer são phishing, vishing, ombro surfando, baleação, uso não autorizado, personificação, mergulho no lixo e gêmeo do mal. As seções a seguir descrevem cada uma dessas técnicas.

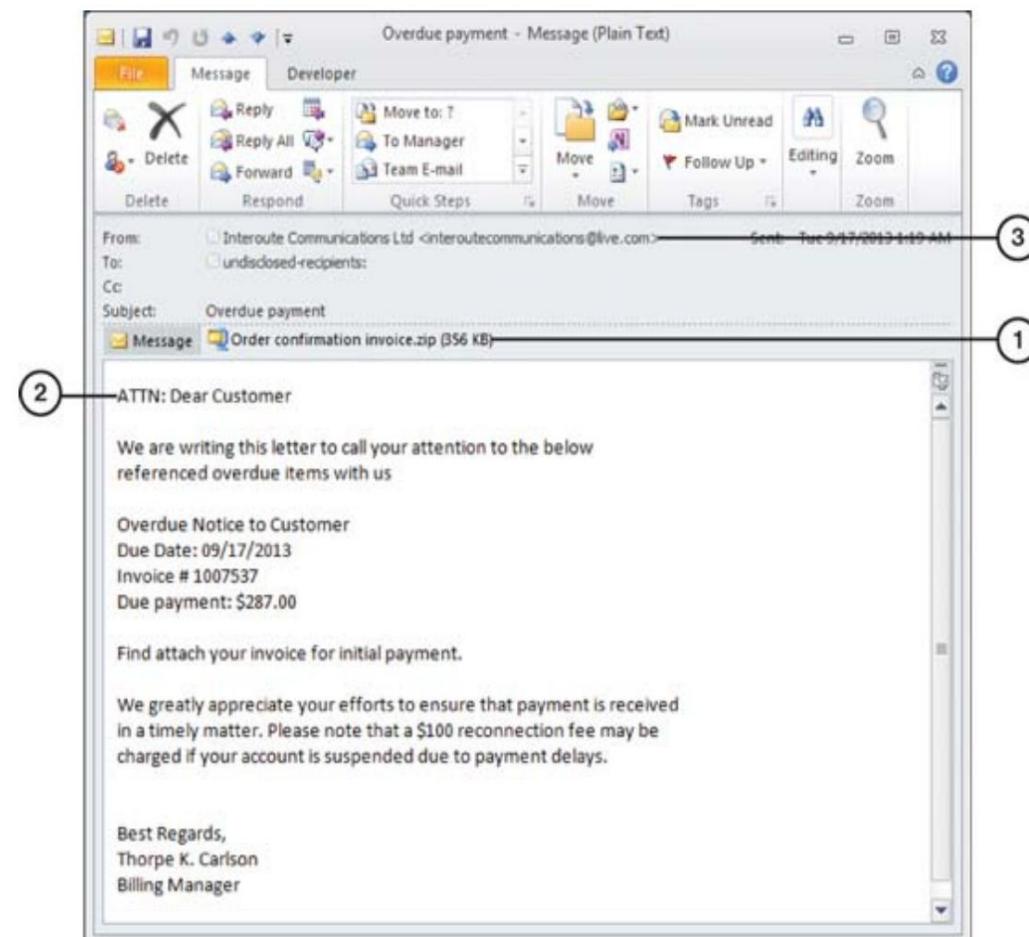
A chave para mitigar essas ameaças de engenharia social é uma combinação de garantir a conscientização dos funcionários, implementar políticas e protocolos para lidar com informações internas confidenciais e, sempre que possível, usar ferramentas de segurança cibernética.

Phishing

O **phishing** envolve a criação de sites falsos ou o envio de e-mails fraudulentos que induzem os usuários a fornecer informações pessoais, bancárias ou de cartão de crédito. Uma variação, o phishing por telefone, usa um sistema de resposta de voz interativa (IVR) que o usuário é induzido a ligar, para enganar o usuário a revelar informações.

O phishing é uma ameaça constante que os administradores podem enfrentar com avisos de conscientização que fornecem exemplos das ameaças mais recentes e educam os funcionários sobre a identificação de mensagens suspeitas.

A Figura 7-5 ilustra um típico e-mail de phishing.



1. Zip archive files are frequently used by malware; open the file and your system is infected
2. Genuine emails from a company you work with will be addressed to a person or account number
3. Live.com is typically used by personal email, not company email

Figura 7-5 Uma mensagem que pretende abordar um pagamento atrasado, mas mostra sinais clássicos de um ataque de phishing

vishing

Vishing envolve deixar mensagens de voz enganosas que parecem vir de uma fonte interna ou outra autoridade. Essas mensagens solicitam informações confidenciais, como folha de pagamento ou informações fiscais. Os ataques geralmente visam uma pessoa, organização ou empresa específica. A melhor proteção contra o vishing é implementar práticas de segurança que eduquem os usuários sobre como lidar com informações confidenciais dentro da organização.

caça à baleia

Whaling é um tipo específico de ataque de phishing que persegue funcionários de alto escalão (o peixe grande ou baleia) em uma organização, especialmente o CEO. Os ataques tendem a ser mais sofisticados e personalizados, parecendo partir de um executivo de alto escalão de outra empresa. Links dentro do correio ou site infectam o computador da liderança, permitindo acesso a informações mais sigilosas e possível autorização para transferências de fundos.

Representação

A representação é um tipo de engenharia social semelhante ao phishing, no qual um hacker envia um e-mail fingindo ser alguém de confiança da vítima. Pode levar tempo e pesquisa para o imitador descobrir como ganhar a confiança do alvo. A representação, também conhecida como comprometimento de e-mail comercial (BEC), não se restringe ao e-mail, mas pode ocorrer por telefone ou pessoalmente.

Bom senso e políticas rígidas sobre como comunicar informações confidenciais podem ajudar a evitar ataques de representação.

Surf de ombro

Shoulder surfing é a tentativa de visualizar documentos físicos na mesa de um usuário ou documentos eletrônicos exibidos em um monitor olhando por cima do ombro do usuário. Os surfistas de ombro às vezes observam o teclado para ver as senhas sendo inseridas. Eles agem secretamente, olhando pelos cantos e usando espelhos ou binóculos. Eles também podem se apresentar aos usuários e conversar, na esperança de que os usuários baixem a guarda.

Uma proteção comum contra surfar no ombro é usar uma tela de privacidade especial que limita o alcance de visualização de uma tela. Os funcionários devem ser treinados para estarem cientes de outras pessoas que possam ver suas telas e para deixar as telas bloqueadas quando estiverem longe de suas estações de trabalho.

Utilização não autorizada

A utilização não autorizada ocorre quando uma pessoa não autorizada tenta acompanhar uma pessoa autorizada em uma área segura seguindo essa pessoa de perto e agarrando a porta antes que ela se feche. Isso geralmente é feito sem o consentimento da pessoa autorizada; às vezes, a pessoa autorizada é levada a acreditar que o ladrão está autorizado. Se a pessoa autorizada estiver conscientemente envolvida, o ato é conhecido como piggybacking. As armadilhas, mencionadas anteriormente, são projetadas para impedir a utilização não autorizada.

Mergulhar na lixeira

Percorrer o lixo em busca de informações sobre uma rede - ou uma pessoa com acesso à rede - é chamado de **mergulho no lixo**. Esse tipo de atividade não precisa envolver uma lixeira de verdade, é claro — apenas alguém em busca de qualquer informação que o ajude a projetar socialmente uma maneira de entrar em uma rede. Para limitar as perspectivas de um mergulhador de lixo, trituradores de papel ou serviços de Trituração devem ser empregados para manter os dados fora de alcance.

Gêmeo mau

Um ataque de **gêmeos malignos** envolve a configuração de um ponto de acesso sem fio fraudulento em uma rede que imita o AP legítimo para usuários locais. O AP gêmeo maligno às vezes ataca o AP legítimo, então os usuários são enganados ao fazer login no gêmeo maligno. O gêmeo pode então farejar nomes de usuários e senhas e ouvir outras informações valiosas. Às vezes, um gêmeo do mal pode criar um portal falso que imita o site da empresa, para coletar ainda mais dados sobre qualquer pessoa que fizer logon.

Ameaças

Qualquer plano viável para proteger uma rede e dados deve ser baseado em uma compreensão clara das ameaças que todas as redes de TI enfrentam. Esta seção descreve ameaças e métodos comuns que pessoas de fora usam para comprometer as redes.

DDoS

Um **ataque distribuído de negação de serviço (DDoS)** ocorre quando vários (até milhares) de computadores foram comprometidos com malware especial que os transforma em bots. Os bots então recebem instruções de seu novo mestre para atacar um site da rede com milhares de solicitações. O tráfego é tão avassalador que o site fica inacessível pelo tráfego normal e é efetivamente desativado.

DoS

Um **ataque de negação de serviço (DoS)** envolve um computador atacando um alvo específico com um número esmagador de solicitações de serviço. Isso é muito semelhante a um ataque DDoS, mas sem os bots. As mensagens vindas de uma fonte ainda podem derrubar uma rede, com grande custo para uma empresa.

dia zero

Quando um software legítimo é vendido e distribuído, ele pode ter vulnerabilidades de segurança desconhecidas. Quando as falhas são descobertas, os usuários emitem alertas e a empresa de software cria um patch. Às vezes, os hackers observam esses alertas e exploram as vulnerabilidades antes que o patch seja instalado, daí o termo **ataque de dia zero**.

Falsificação

Spoofing é um termo geral para ataques de malware que pretendem vir de uma fonte confiável. Phishing, spear phishing e programas antivírus desonestos são três exemplos de falsificação.

Ataque no caminho

Um **ataque no caminho** (anteriormente conhecido como ataque man-in-the-middle [MiTM]) envolve um invasor interceptando uma conexão enquanto engana os endpoints fazendo-os pensar que estão se comunicando diretamente uns com os outros.

de outros. Essencialmente, o invasor se torna um proxy ou ponto de retransmissão não autorizado e não detectado; o invasor usa essa posição para capturar dados confidenciais ou transmitir informações alteradas para uma ou ambas as extremidades da conexão original.

força bruta

Um **ataque de força bruta** envolve quebrar senhas calculando e usando todas as combinações possíveis de caracteres até que a senha correta seja descoberta. Quanto mais longa for a senha usada e quanto maior for o número de caracteres possíveis em uma senha, mais demorado será o brute-forcing. Uma maneira de um administrador bloquear a força bruta é configurar os sistemas de autenticação para bloquear após um número especificado de senhas incorretas. Senhas mais longas também ajudam na luta contra ataques de força bruta.

Ataques de Dicionário

Os **ataques de dicionário** envolvem a tentativa de quebrar senhas tentando todas as palavras em uma lista, como um dicionário. Uma lista simples pode incluir senhas comumente usadas, como 12345678 e senha. Os ataques de dicionário podem ser bloqueados bloqueando os sistemas após um número especificado de senhas incorretas. Exigir senhas mais sofisticadas que não incluem informações identificáveis, como aniversários ou sobrenomes, também é uma estratégia.

Ameaça Interna

Muitos procedimentos de segurança são projetados para impedir que pessoas de fora de uma organização penetrem em uma rede e fujam com dados valiosos. No entanto, uma ameaça muito real vem de uma ameaça interna, na forma de funcionários desonestos ou infelizes ou de um fornecedor ou contratado confiável que tem acesso à rede ou à infraestrutura de rede. Muitos incidentes de espionagem corporativa ou governamental e roubo de propriedade intelectual foram executados por pessoas de dentro com altos níveis de acesso. Na verdade, um insider pode causar muito mais danos do que um outsider.

Prevenir ameaças internas é difícil, mas muitas das práticas de monitoramento e antiphishing também protegem contra fraudes internas.

É uma prática corporativa comum que, quando funcionários com acesso à rede são demitidos ou demitidos, suas credenciais sejam imediatamente rescindidas e eles não tenham mais acesso aos prédios ou à rede.

Injeção de Linguagem de Consulta Estruturada (SQL)

Structured Query Language (SQL) é uma linguagem padrão para comunicação entre bancos de dados. Essa linguagem pode ser usada para atacar um banco de dados para roubar informações importantes, como números de cartão de crédito, números de previdência social e outros dados privados. Também pode ser usado para simplesmente atacar uma empresa ou governo e destruir ou danificar fortemente os bancos de dados para que se tornem inúteis. Os administradores de banco de dados devem projetar cuidadosamente seus bancos de dados para reduzir a ameaça de consultas perigosas. Em um ataque de [**injeção de linguagem de consulta estruturada \(SQL\)**](#), o código malicioso é inserido em strings que são passadas posteriormente para um servidor de banco de dados.

Script entre sites (XSS)

[**Cross-site scripting \(XSS\)**](#) é uma técnica de injeção de código que usa scripts do lado do cliente. Envolve enganar um usuário, muitas vezes com um link em um e-mail ou por meio de algum outro ardil. Quando um usuário desavisado clica no link, o invasor pode injetar código malicioso em um aplicativo baseado na web. Esse código é então “confiável” no ambiente do usuário, mas pode roubar informações armazenadas em cookies ou outras informações valiosas.

A melhor defesa contra o XSS é ter configurações de firewall específicas para tipos de dados que entram nos sistemas e dados criptografados que saem do sistema. Dessa forma, se a informação for roubada, o ladrão não poderá lê-la.

Vulnerabilidades

Uma vulnerabilidade é uma fraqueza no plano de segurança de uma organização que pode permitir que as ameaças mencionadas anteriormente se tornem problemas reais. Muitas das vulnerabilidades listadas aqui devem parecer familiares agora, mas são brevemente revisadas nas seções a seguir.

Sistemas não compatíveis

Sistemas não compatíveis são sistemas marcados por um aplicativo gerenciador de configuração (por exemplo, Endpoint Configuration Manager da Microsoft) como não tendo os patches de segurança mais atualizados instalados.

Os sistemas que não possuem os patches de segurança mais atualizados são especialmente vulneráveis a ataques. Um exemplo disso é um usuário tentando fazer logon em uma rede corporativa com um computador pessoal que não foi atualizado para os padrões de rede que atendem às especificações da corporação.

Sistemas não corrigidos

Semelhante a sistemas não compatíveis, um sistema não corrigido não protegerá contra vulnerabilidades de dia zero recentemente descobertas e corrigidas. Quando os hackers sabem dessas vulnerabilidades, os ataques aumentam. Sistemas não corrigidos serão vulneráveis aos ataques. Os sistemas devem ser corrigidos dentro de uma semana após o lançamento de um patch.

Sistemas desprotegidos

Semelhante a um sistema sem patch, um sistema desprotegido que não possui firewalls e software antivírus (ou software de segurança desatualizado) é vulnerável às informações de vírus conhecidas mais recentes.

sistemas operacionais EOL

É perigoso manter sistemas operacionais (SO) em fim de vida útil (EOL) em uma rede. Quando o software ou hardware atinge o status EOL, atualizações e patches geralmente não estão mais disponíveis. Manter equipamentos e sistemas operacionais atualizados faz parte de um forte plano de segurança.

Traga seu próprio dispositivo (BYOD)

Traga seu próprio dispositivo (BYOD) O uso em uma rede restrita pode trazer grandes benefícios de produtividade e custo, mas com eles vêm sérios riscos. Qualquer malware ou vulnerabilidade em dispositivos pessoais pode se tornar uma vulnerabilidade séria quando o dispositivo recebe acesso à rede corporativa.

Os administradores de rede precisam ter certeza de que qualquer dispositivo permitido na rede esteja atualizado e em conformidade com as práticas de segurança. Muitas redes que permitem atividade BYOD exigem uma verificação de segurança online antes

eles têm acesso à rede. O uso de dispositivos pessoais deve ser restrito em uma rede segura.

Configurações de segurança do sistema operacional Microsoft Windows



Objetivo 2.5: Dado um cenário, gerenciar e definir as configurações básicas de segurança no sistema operacional Microsoft Windows.

A Microsoft disponibilizou várias configurações e ferramentas de segurança no sistema operacional Windows. Essas configurações e ferramentas permitem que usuários e administradores controlem o acesso ao computador, bem como a arquivos e pastas.

Defender Antivírus

O Windows vem com o Microsoft **Defender Antivirus**, que faz parte do pacote de segurança do Windows. Para acessar a Segurança do Windows, vá para **Iniciar > Segurança do Windows**. Na janela Security at a Glance, selecione Proteção contra vírus e ameaças. Na janela Proteção contra vírus e ameaças, você pode executar uma verificação rápida, selecionar opções de verificação, gerenciar configurações e verificar se há atualizações. Você pode até mesmo gerenciar a proteção contra ransomware.

Para aplicação no mundo real e o exame A+, certifique-se de saber como ativar e desativar a proteção em tempo real (em Gerenciar configurações) e entenda como manter suas definições atualizadas selecionando o link Verificar atualizações. O Windows Defender é abordado com mais detalhes posteriormente neste capítulo, na seção “Filtragem de conteúdo”.

A Microsoft oferece um ótimo recurso para configurar o Microsoft Defender Antivírus no Windows:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-antivirus-windows?view=o365-worldwide>

Firewall

Um **firewall** é um dispositivo físico ou programa de software que examina os pacotes de dados em uma rede para determinar se deve encaminhá-los ao seu destino ou bloqueá-los. Um firewall pode ser um firewall unidirecional, que protege apenas contra ameaças de entrada, ou um firewall bidirecional, que protege contra tráfego de entrada e saída não autorizado. A maioria dos programas de firewall de terceiros, como o ZoneAlarm, são firewalls bidirecionais. Um **firewall de software** pode ser configurado para permitir o tráfego entre endereços IP especificados e para bloquear o tráfego de e para a Internet, exceto quando permitido por programa.

Uma rede corporativa pode usar um servidor proxy com um firewall como a única conexão direta entre a Internet e a rede corporativa e, em seguida, usar um firewall no servidor proxy para proteger a rede corporativa contra ameaças.

Os firewalls físicos são computadores especializados cujo software é projetado para analisar rapidamente o tráfego de rede e tomar decisões de encaminhamento com base em regras definidas pelo administrador. Com o tempo, essa tarefa foi incorporada mais ao software dos computadores e ao design do sistema operacional. Um exemplo é o Windows Defender Firewall no Windows, discutido na seção “Configurações de segurança do sistema operacional Microsoft Windows”.

A maioria dos sistemas operacionais atuais possui algum tipo de firewall embutido:



- Conforme configurado inicialmente, o firewall padrão no Windows é um firewall unidirecional. No entanto, ele pode ser configurado para funcionar como um firewall bidirecional. Para obter mais informações sobre como funciona, consulte a seção “Configurações do firewall”, mais adiante neste capítulo.
- O macOS inclui um firewall de aplicativo. No OS X 10.6 e mais recente, o firewall do aplicativo oferece opções adicionais de personalização.
- O Linux, começando com distribuições baseadas no kernel 2.4.xe posterior, inclui o iptables para configurar o netfilter, sua estrutura de filtragem de pacotes. Para saber mais, consulte www.netfilter.org. Muitas distribuições e aplicativos Linux de terceiros estão disponíveis para ajudar a tornar o iptables e o netfilter mais fáceis de configurar.

Ativar/Desativar

O Firewall do Windows Defender foi abordado em detalhes no [Capítulo 6, “Sistemas operacionais”](#).

No entanto, não podemos deixar de enfatizar a importância de um conhecimento prático do Windows Defender Firewall para aplicativos do mundo real e para o exame A+. Você deve estar familiarizado com a ativação e desativação (ligar e desligar) do Firewall do Windows Defender e deve entender as configurações e os procedimentos relacionados à porta e aos aplicativos de segurança.

Para ativar ou desativar o Firewall do Windows Defender no Windows 10, faça o seguinte:

Etapa 1. Selecione **Iniciar > Configurações > Atualização e segurança > Windows Segurança > Firewall e proteção de rede**. Abra as configurações de segurança do Windows.

Etapa 2. Selecione um perfil de rede: **Rede de domínio, Rede privada ou Rede pública**.

Etapa 3. No Microsoft Defender Firewall, altere a configuração para **Ativado**.

Etapa 4. Para desativar o Firewall do Windows Defender, altere a configuração para **Desativado**. Desativar o Microsoft Defender Firewall pode tornar seu dispositivo (e sua rede, se houver) mais vulnerável a acesso não autorizado. Se você precisar usar um aplicativo que está sendo bloqueado, poderá permitir que ele seja usado pelo firewall em vez de desativá-lo.

Segurança Portuária

Gerenciar segurança de porta refere-se ao uso de um dispositivo de firewall ou um firewall de software para impedir que portas UDP ou TCP especificadas sejam usadas por um serviço, um aplicativo, um dispositivo específico ou todos os dispositivos. Desativar portas não utilizadas torna mais difícil para os hackers encontrar acesso furtivo a uma máquina.

Segurança de aplicativos

Muitos aplicativos são projetados para atualizar e se comunicar com outros computadores.

A autorização para comunicação externa pode ser gerenciada no Windows Defender Firewall.

Ao abrir o Windows Defender Firewall,

selecione Permitir um aplicativo ou recurso por meio do Windows Defender Firewall para abrir a janela mostrada na [Figura 7-6](#). Cada aplicativo e recurso pode ser ativado ou desativado neste menu.

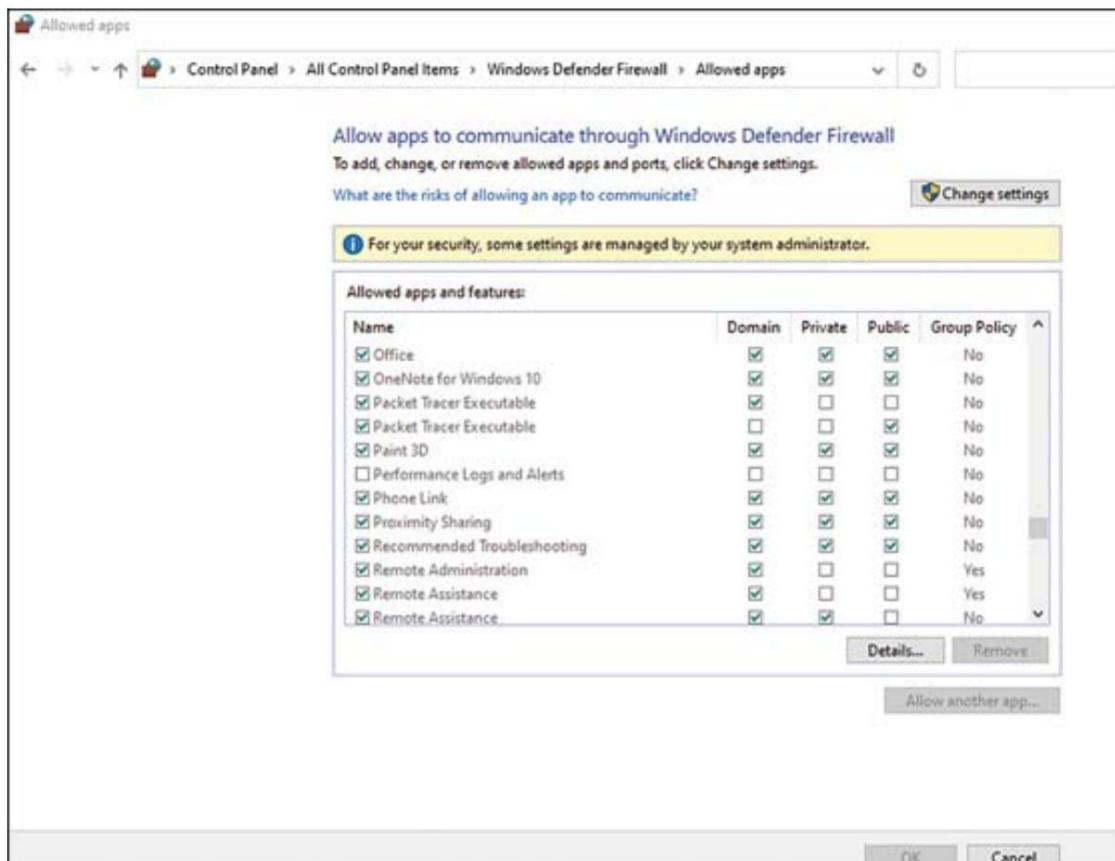


Figura 7-6 Gerenciando aplicativos no Windows Defender Firewall

A Microsoft também oferece excelentes instruções detalhadas para configurar Firewall do Windows com Segurança Avançada em

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/windows-firewall-with-advanced-security>

Controle de acesso

As próximas seções discutem os propósitos e princípios do controle de acesso através do seguinte:

- Usuários e grupos

- NTFS vs. [**permissões de compartilhamento**](#)
- Arquivos e pastas compartilhados
- Arquivos e pastas do sistema
- Autenticação de usuário
- Executar como administrador versus usuário padrão
- BitLocker
- BitLocker para ir
- Criptografia do sistema de arquivos (EFS)

Usuários e grupos

Os usuários no Windows podem ser atribuídos a diferentes grupos, cada um com diferentes permissões. As configurações de Diretiva Local (para PCs locais) e as configurações de Diretiva de Grupo (para PCs em rede conectados a um controlador de domínio executando o Active Directory) podem restringir os recursos do PC por grupo ou por PC. O exame 220-1102 cobre algumas das diferenças entre as contas.

Contas locais x contas da Microsoft

Ao configurar um computador no Windows 10, você pode escolher se deseja usar uma conta local ou uma conta da Microsoft. Cada um tem seu próprio propósito e você deve saber a diferença.

- **Conta local:** uma conta local é igual às contas sem rede que os usuários experimentaram nas edições anteriores do Windows. As configurações configuráveis incluem nome de usuário e senha locais, personalização da área de trabalho, acesso aos recursos do Windows, instalação de aplicativos e personalização da área de trabalho. Faltam os recursos adicionais do amplo ambiente online do Windows 10.
- **Conta da Microsoft:** usar uma conta da Microsoft estabelece um relacionamento online com a Microsoft e permite um acesso mais fácil a produtos comuns da Microsoft, como Skype, Outlook e até recursos de jogos no Xbox. O nome de usuário e a senha não são de preferência local, mas

em vez do e-mail da conta e da senha associada. Uma conta da Microsoft fornece configuração e sincronização simplificadas de dispositivos adicionais, bem como acesso fácil à Windows Store. Todas as contas da Microsoft podem ser combinadas e gerenciadas centralmente.

Contas padrão e de administrador

Existem três níveis de conta padrão no Windows:

- **Conta padrão:** as contas padrão têm permissão para executar tarefas de rotina. No entanto, essas contas são impedidas de executar tarefas que envolvam alterações em todo o sistema, como instalação de hardware ou software, a menos que possam fornecer uma senha de administrador quando solicitado pelo Controle de Conta de Usuário (UAC).
- **Conta de administrador:** os usuários com uma conta de administrador podem executar toda e qualquer tarefa.
- **Conta de convidado:** O nível de conta de convidado é o mais limitado. Uma conta de convidado não pode instalar software ou hardware ou executar aplicativos existentes; da mesma forma, uma conta de convidado não pode acessar arquivos em pastas de documentos compartilhadas ou no perfil de convidado. A conta de convidado é desativada por padrão. Se estiver habilitado para um usuário obter acesso ao computador, esse acesso deve ser temporário e a conta deve ser desativada novamente quando o usuário não precisar mais de acesso.

Observação

Quando um usuário é criado usando o miniaplicativo Users no Windows, o usuário deve receber uma conta padrão ou de administrador. Contas de convidados são usadas para visitantes.

Nas versões do Windows até 8.1, a conta de usuário avançado é um tipo de conta específico que tem mais permissões que os usuários padrão, mas menos que os administradores. Nessas versões, os usuários avançados têm os mesmos direitos e permissões que os usuários padrão; no entanto, um modelo de segurança personalizado pode ser

criado se o grupo Usuários Avançados precisar de permissões específicas, como para a operação de programas legados.

No Windows 10 e no Windows 11, o grupo Usuários avançados foi descontinuado; no entanto, está disponível para atribuição para compatibilidade com versões anteriores.

NTFS vs. Permissões de Compartilhamento

A Microsoft introduziu o **New Technology File System (NTFS)** como uma maneira aprimorada de armazenar arquivos em discos sobre o sistema FAT do Windows 95.

As mudanças nos sistemas de armazenamento facilitaram a implementação da segurança em nível de arquivo na forma de permissões. As permissões controlam o acesso local e de rede aos arquivos e podem ser definidas para usuários individuais ou grupos.

Permitir vs. Negar

Cada permissão tem duas configurações: Permitir e Negar. Geralmente, se você deseja que um usuário tenha acesso a uma pasta, adicione esse usuário à lista e selecione Permitir para obter a permissão apropriada. Se você não deseja permitir o acesso de um usuário, normalmente você simplesmente não adiciona o usuário a uma lista. Em alguns casos, um administrador deve emitir uma negação explícita se o usuário fizer parte de um grupo maior que já tem acesso a uma pasta pai, mas precisa ser mantido fora de uma subpasta específica.

Herança

Os atos de mover e copiar pastas e arquivos têm resultados diferentes, dependendo das permissões. Por exemplo, quando você copia uma pasta ou arquivo para um volume diferente, a pasta ou arquivo herda as permissões da pasta pai para a qual foi copiado (o diretório de destino). Quando você move uma pasta ou arquivo para um local diferente no mesmo volume, a pasta ou arquivo retém suas permissões originais.

Atributos de arquivo e pasta

Os atributos de arquivo são usados no Windows para indicar como os arquivos podem ser tratados. Eles podem ser usados para especificar quais arquivos devem ser copiados, quais arquivos

deve ser ocultado da GUI normal ou das listas de arquivos de linha de comando, se um arquivo é compactado ou criptografado e assim por diante, dependendo do sistema operacional.

Para exibir atributos de arquivo no Windows, clique com o botão direito do mouse em um arquivo no Explorador de Arquivos ou no Windows Explorer e selecione Propriedades. Para exibir atributos de arquivo na linha de comando do Windows, use o comando **Attrib**.



Arquivos e pastas compartilhados

Arquivos e pastas compartilhados têm suas permissões atribuídas na guia Segurança da folha de propriedades do objeto. As permissões de pastas e arquivos variam de acordo com o tipo de usuário ou grupo e podem incluir o seguinte:

- **Controle total:** conceda acesso completo ao conteúdo do arquivo ou pasta. Quando Controle total é selecionado, todos os itens a seguir são selecionados e ativados automaticamente.

- **Modificar:** altera o conteúdo do arquivo ou da pasta.
- **Read & Execute:** acesse o conteúdo de arquivos ou pastas e execute programas.
- **Listar conteúdo da pasta:** exibe o conteúdo da pasta.
- **Ler:** Acessar um arquivo ou pasta.
- **Escrever:** Adicionar um novo arquivo ou pasta.

Herança e propagação de permissão

Herança e propagação de permissão descrevem como arquivos e pastas recebem permissões.

Se você criar uma pasta, a ação padrão é que a pasta herde as permissões da pasta pai, ou seja, todas as permissões definidas na pasta pai são herdadas por qualquer subpasta da pasta pai. Para ver um exemplo disso, localize qualquer pasta em um volume NTFS (além da pasta raiz), clique com o botão direito do mouse e selecione Propriedades; em seguida, acesse a guia Segurança e clique em

o botão Avançado. No Windows 10 ou 11, a caixa de diálogo Configurações de segurança avançadas oferece estes botões: Adicionar, Remover, Exibir e Desabilitar herança.

Você também pode propagar alterações de permissão para subpastas que não são herdadas da pasta atual. Para fazer isso, selecione Substituir todas as permissões do objeto filho por permissões herdáveis deste objeto. Lembre-se de que as pastas herdam automaticamente do pai, a menos que você desative a herança, e você pode propagar entradas de permissão para subpastas a qualquer momento selecionando a opção Substituir.

Executar como administrador x usuário padrão

No Windows 10, pressione Windows+X e clique ou toque em Windows PowerShell para executar no modo padrão. Uma opção para executar como administrador também está disponível.

Controle de conta de usuário

O Controle de Conta de Usuário (UAC) permite que o usuário final selecione um nível de notificações sobre as alterações feitas no computador. O objetivo desta ferramenta é impedir alterações não autorizadas no computador; os vários níveis são projetados para permitir que os usuários finais adaptem as notificações ao seu nível de conforto. O UAC pode ser desativado, mas é melhor definir algum nível de notificação do que não ter nenhum.

Para acessar as configurações do UAC, basta digitar UAC na área de pesquisa da barra de tarefas. Selecione UAC para ver os controles UAC na [Figura 7-7](#).

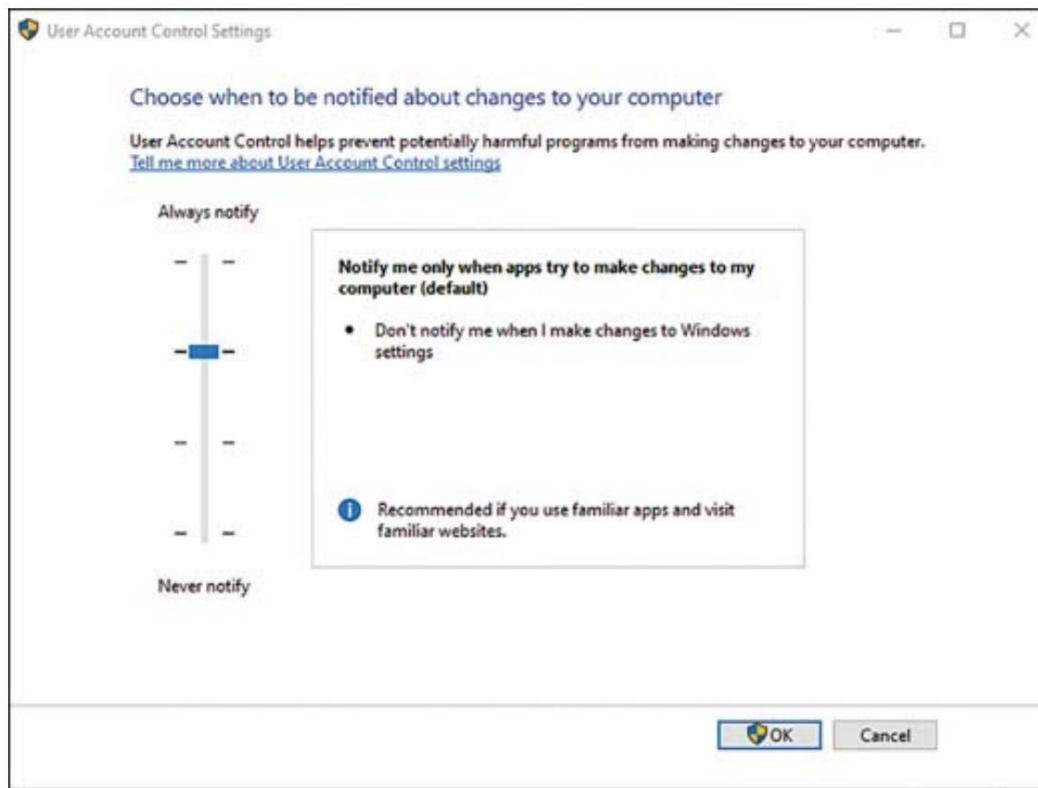


Figura 7-7 Controles UAC no Windows 10

Opções de sistema operacional de login

Autenticação é o processo de determinar com segurança que as pessoas autorizadas que acessam os computadores ou a rede são quem dizem ser. O Windows inclui uma variedade de protocolos de autenticação que podem ser usados em uma rede corporativa, incluindo Kerberos, TLS/SSL, PKU2U e NTLM.



Apple, Microsoft e Google usam autenticação mútua para vários serviços (também conhecido como **logon único [SSO]**) para habilitar um único login que fornece acesso a vários serviços. Por exemplo, um único login de conta da Microsoft fornece acesso ao email do Outlook, à Microsoft Store e ao OneDrive. Para possibilitar o SSO no Windows, os endereços IP do cliente são mapeados para nomes de usuário no Windows Active Directory. Da mesma forma, um único login da Apple fornece acesso ao iTunes, iCloud e outros serviços. Um único login do Google fornece acesso ao Gmail, Google Drive e outros serviços.

Outras opções do sistema operacional de login do Windows (além de nome de usuário e senha) incluem login com um PIN, uma impressão digital ou até mesmo reconhecimento facial. No Windows 10 e 11, você pode gerenciar como entrar em seu dispositivo acessando **Configurações > Contas > Opções de login**. Aqui você pode gerenciar opções como reconhecimento facial (Windows Hello), reconhecimento de impressão digital (Windows Hello) e PIN do Windows Hello, conforme mostrado na [Figura 7-8](#).

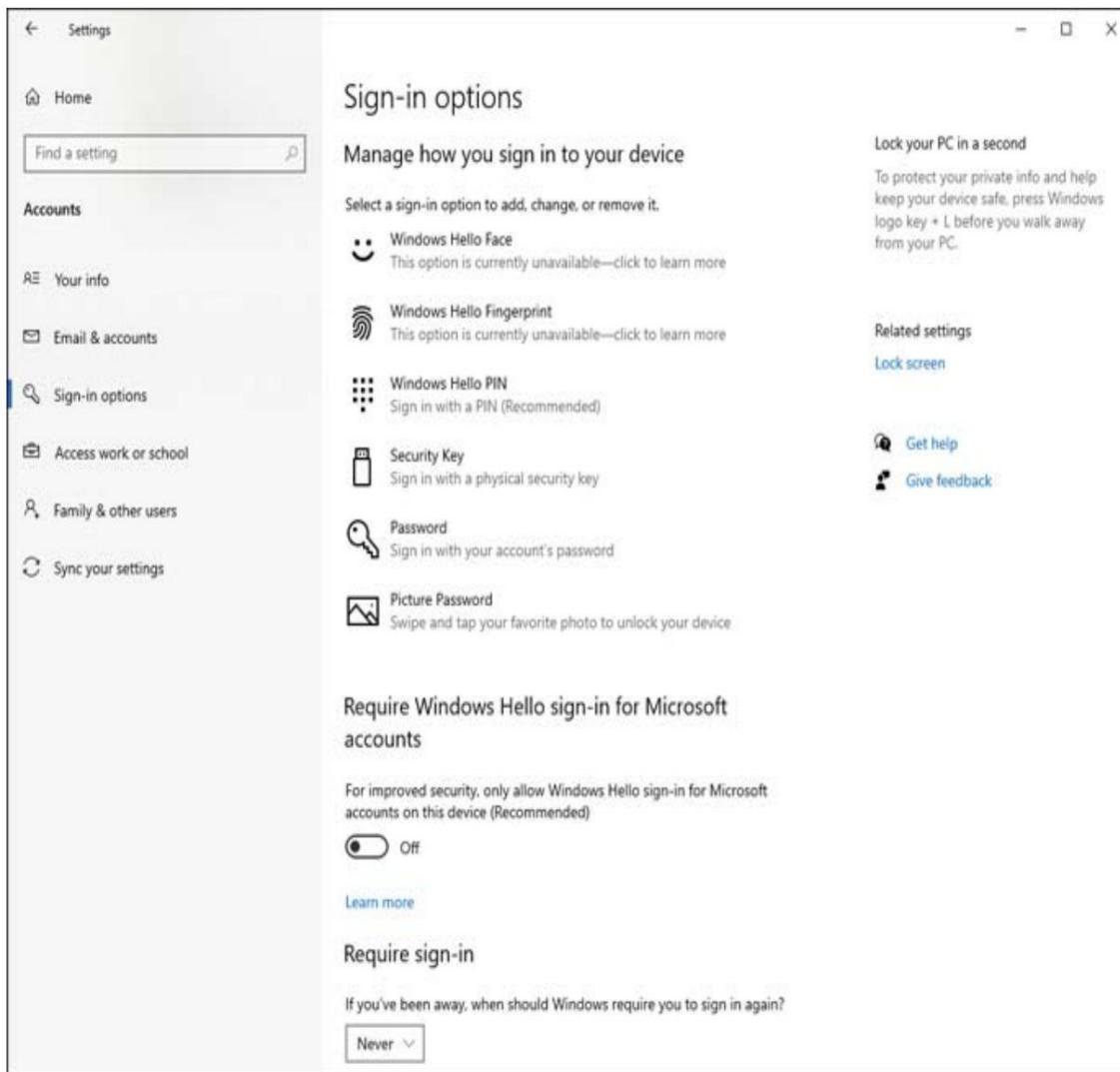


Figura 7-8 Opções de login do Windows

BitLocker

Para criptografar uma unidade inteira, você precisa de algum tipo de software de criptografia de disco completo. Várias opções estão atualmente disponíveis no mercado; uma opção desenvolvida para versões de negócios do Windows pela Microsoft é chamada

BitLocker. Este software pode criptografar todo o disco, que, depois de concluído, é transparente para o usuário. No entanto, o BitLocker tem alguns requisitos, incluindo os seguintes:

- Um chip Trusted Platform Module (TPM), que é um chip residente na placa-mãe que realmente armazena as chaves criptografadas.

ou

- Uma chave USB externa para armazenar as chaves criptografadas. O uso do BitLocker sem um chip TPM requer alterações nas configurações da Diretiva de Grupo.
- Um disco rígido com dois volumes, preferencialmente criado durante a instalação do Windows. Um volume é para o sistema operacional (provavelmente C :) e será criptografado; o outro é o volume ativo e permanece não criptografado para que o computador possa inicializar. Se um segundo volume precisar ser criado, a ferramenta de preparação de unidade BitLocker pode ajudá-lo; você pode baixá-lo no Centro de Download da Microsoft.

O software BitLocker é baseado no Advanced Encryption Standard (AES) e usa uma chave de criptografia de 128 bits.

Desde o Windows Vista SP1, é possível usar o BitLocker para criptografar volumes de disco rígido internos diferentes da unidade do sistema. Por exemplo, se um disco rígido for particionado como unidades C: e D:, o BitLocker poderá criptografar ambas as unidades.

O Windows 10 e 11 têm vários aprimoramentos que tornam o BitLocker mais fácil de usar, mas os fundamentos do BitLocker são os mesmos do Windows 7.

BitLocker para ir

Para habilitar o **BitLocker To Go** no Windows 10 ou 11, vá para **Painel de Controle > Sistema e Segurança > Criptografia de Unidade de Disco BitLocker**. Para unidades externas, basta clicar com o botão direito do mouse na unidade para criptografar e selecionar Ativar BitLocker para iniciar o processo de criptografia. Durante o processo, você será solicitado a especificar uma senha ou um cartão inteligente para obter credenciais para acessar a unidade conteúdo.

EFS

As edições do Windows voltadas para negócios incluem suporte para o **Encrypting File System (EFS)**. Como mostra a [Figura 7-9](#), o EFS pode ser usado para proteger arquivos de dados confidenciais e arquivos temporários e pode ser aplicado a arquivos ou pastas individuais. (Quando o EFS é aplicado a pastas, todos os arquivos em uma pasta criptografada também são criptografados.)

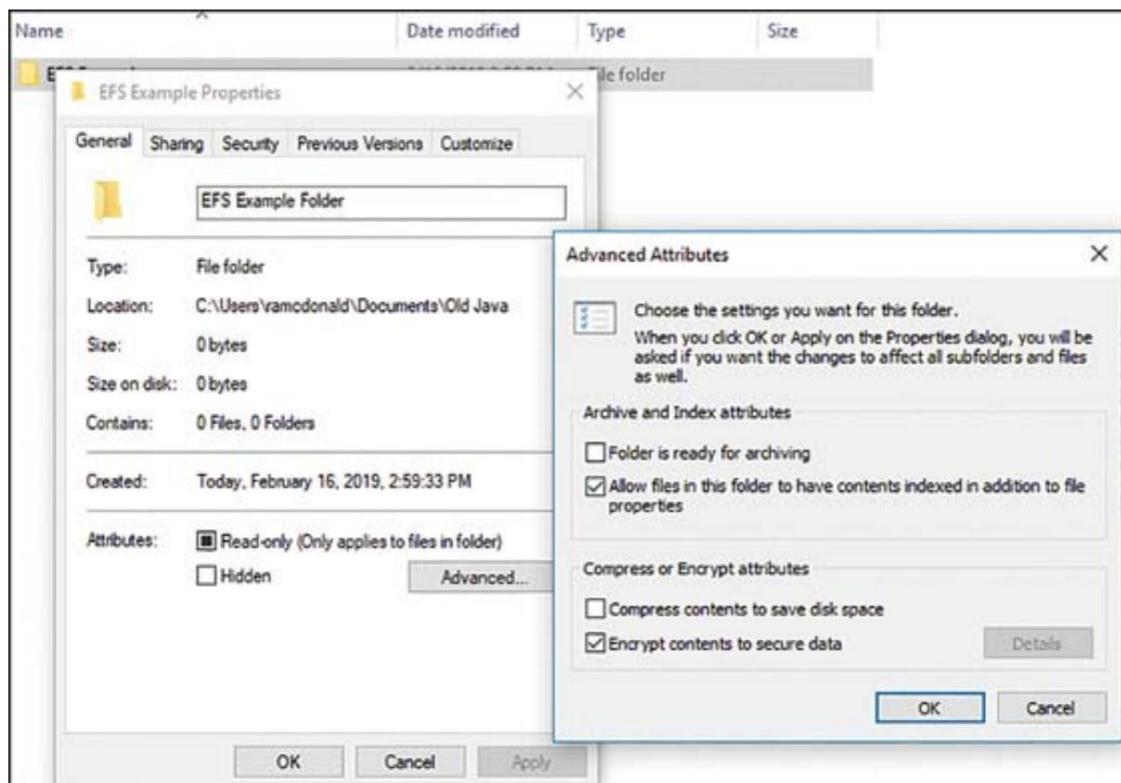


Figura 7-9 Etapas de criptografia EFS

Os arquivos EFS podem ser abertos apenas pelo usuário que os criptografou, por um administrador ou por detentores de chaves EFS (usuários que receberam a chave do certificado EFS para a conta de outro usuário). Assim, os arquivos ficam protegidos contra o acesso de hackers.

Os arquivos criptografados com EFS são listados com nomes de arquivo verdes quando exibidos no Windows Explorer ou no File Explorer. Somente os arquivos armazenados em uma unidade que usa NTFS podem ser criptografados.

Para criptografar um arquivo no Windows 10 ou 11, siga este processo:



Etapa 1. Clique com o botão direito do mouse no arquivo no Explorador de Arquivos e selecione **Propriedades**.

Etapa 2. Clique no botão **Avançado** na guia Geral.

Etapa 3. Clique na caixa de seleção **Criptografar conteúdo para proteger dados** vazia.

A [Figura 7-9](#) mostra as etapas para a criptografia EFS.

Etapa 4. Clique em **OK**.

Etapa 5. Clique em **Aplicar**. Quando solicitado, selecione a opção para criptografar o arquivo e a pasta principal ou apenas o arquivo, conforme desejado, e clique em **OK**.

Etapa 6. Clique em **OK** para fechar a folha de propriedades.

Para descriptografar o arquivo, siga o mesmo procedimento, mas desmarque a caixa de seleção **Criptografar conteúdo para proteger dados** na Etapa 3.

Observação

Para permitir a recuperação de arquivos criptografados EFS caso o Windows não possa iniciar, você deve exportar a chave do certificado EFS do usuário. Para obter detalhes, consulte o artigo da Microsoft TechNet “Create and Verify an Encrypting File System (EFS) Data Recovery Agent (DRA) Certificate”, em <https://docs.microsoft.com/en-us/windows/security/information-protection/certificado-windows-information-protection/create-and-verify-an-efs-dra>.

Práticas recomendadas de segurança para proteger uma estação de trabalho



Objetivo 2.6: Dado um cenário, configurar uma estação de trabalho para atender às melhores práticas de segurança.

Estações de trabalho seguras são a base de redes seguras. Se um hacker ou ladrão externo puder acessar uma estação de trabalho, toda a rede poderá ser

comprometido. As seções a seguir abordam o uso de senhas, gerenciamento de contas e outros métodos para tornar as estações de trabalho seguras.

Criptografia de dados em repouso

Como o ativo mais valioso de uma empresa geralmente são seus dados — seja na forma de informações de clientes, segredos comerciais ou informações de produção —, faz todo o sentido fazer o possível para protegê-los. Quando os dados ficam em uma estação de trabalho, eles podem ser comprometidos ao obter acesso à rede ou podem ser roubados fisicamente. Uma maneira de se proteger contra esses ataques é ter os dados totalmente criptografados enquanto estão “em repouso” no disco rígido da estação de trabalho, em um servidor ou na nuvem. Ter dados criptografados de forma robusta com métodos RSA ou AES garante que, se as unidades forem comprometidas, os dados ainda estarão inacessíveis.

Provedores de nuvem, como Amazon Web Services (AWS), IBM e Microsoft, fornecem opções e serviços de criptografia para dados armazenados nos servidores de nuvem. Considerando as perdas potenciais que os dados roubados podem trazer, práticas rigorosas de criptografia fazem sentido.

A criptografia de dados em repouso deve ser usada em laptops e outros sistemas que possam ser usados fora do ambiente de rede corporativa mais seguro. Laptops que contêm dados confidenciais não criptografados levaram a muitas violações de dados.



Melhores práticas de senha

Nem todas as senhas são igualmente seguras; alguns são muito fáceis de hackear. Os administradores devem usar configurações de política de segurança rigorosas e exigir que os usuários sigam diretrizes rígidas para as senhas que usam para acessar a rede. As diretrizes nas seções a seguir refletem as melhores práticas de senha.

Definindo Senhas Fortes

As diretrizes para definir senhas fortes devem incluir requisitos de comprimento mínimo e uma mistura de caracteres alfanuméricos e de símbolos.

Cada caractere extra em uma senha torna muito mais difícil de hackear. O uso de um gerador de senhas pode facilitar a criação de senhas fortes. Por exemplo, o gerador de senha do Norton Identity Safe (<https://identitysafe.norton.com/password-generator>) oferece senhas aleatórias altamente personalizáveis e pode gerar várias senhas ao mesmo tempo.

Expiração da Senha

Não importa o quão forte seja uma senha, ela se torna menos segura com o tempo. Quanto mais tempo uma senha estiver em uso, mais suscetível ela será a engenharia social, força bruta ou outros ataques. O risco de descoberta de senha por usuários não autorizados é minimizado por meio de uma política de expiração de senha, segundo a qual as senhas expiram após um determinado período de tempo e devem ser redefinidas.

Senha necessária do protetor de tela

Para ajudar a proteger os computadores contra uso não autorizado, pode ser solicitado que os usuários digitem suas senhas para retornar à área de trabalho após a exibição do protetor de tela.

Os usuários também devem ser obrigados a bloquear suas estações de trabalho para que um logon seja necessário para retornar à área de trabalho.

No Windows, a configuração de senha necessária do protetor de tela (caixa de seleção Ao retomar, exibir tela de logon) está localizada na janela Configurações do protetor de tela, que pode ser acessada em **Configurações > Personalização** no Windows 10. No macOS, use o menu Área de trabalho e protetor de tela para escolha um protetor de tela; use Segurança e Privacidade para exigir uma senha para desbloquear o sistema.

Senhas BIOS/UEFI

As senhas do BIOS/UEFI impedem que usuários não autorizados alterem as configurações.

Observe que eles podem ser removidos redefinindo o CMOS. Algumas placas-mãe apresentam um bloco de jumper ou um botão para redefinir o CMOS. Se esse recurso não estiver presente, o CMOS pode ser redefinido removendo a bateria do CMOS por vários minutos. O Capítulo 3, “Hardware”, aborda a configuração das configurações de segurança do BIOS/UEFI com mais detalhes.

Exigir Senhas

Os usuários de PC devem ser treinados para usar senhas para proteger suas contas de usuário.

Os administradores podem exigir isso por meio da Política de Segurança Local e da Política de Grupo no Windows. Os usuários devem ser informados com antecedência de que as senhas estão prestes a expirar, para que possam alterar as senhas com antecedência e evitar o bloqueio em um momento inconveniente.

As senhas podem ser configuradas para exigir que os usuários façam o seguinte:

- Altere as senhas periodicamente, para mantê-las atualizadas e seguras.
- Aplique um comprimento mínimo de senha, para manter as senhas fortes.
- Exija senhas complexas que incluam uma mistura de letras, números e caracteres especiais.

- Evite que senhas antigas sejam reutilizadas continuamente, rastreando senhas anteriores e não as permitindo.
- Aguarde um determinado número de minutos após um número especificado de logins malsucedidos antes de poder fazer login novamente.

Para criar uma senha ou ajustar as configurações de senha no Windows 10, vá para

Configurações > Contas > Opções de login. Para alterar ou aplicar configurações de política de senha, vá para o seguinte local usando o Console de gerenciamento de política de grupo:

Configuração do computador > Configurações do Windows > Configurações de segurança > Políticas de conta > Política de senha. A [Figura 7-10](#) mostra o caminho para essas configurações.

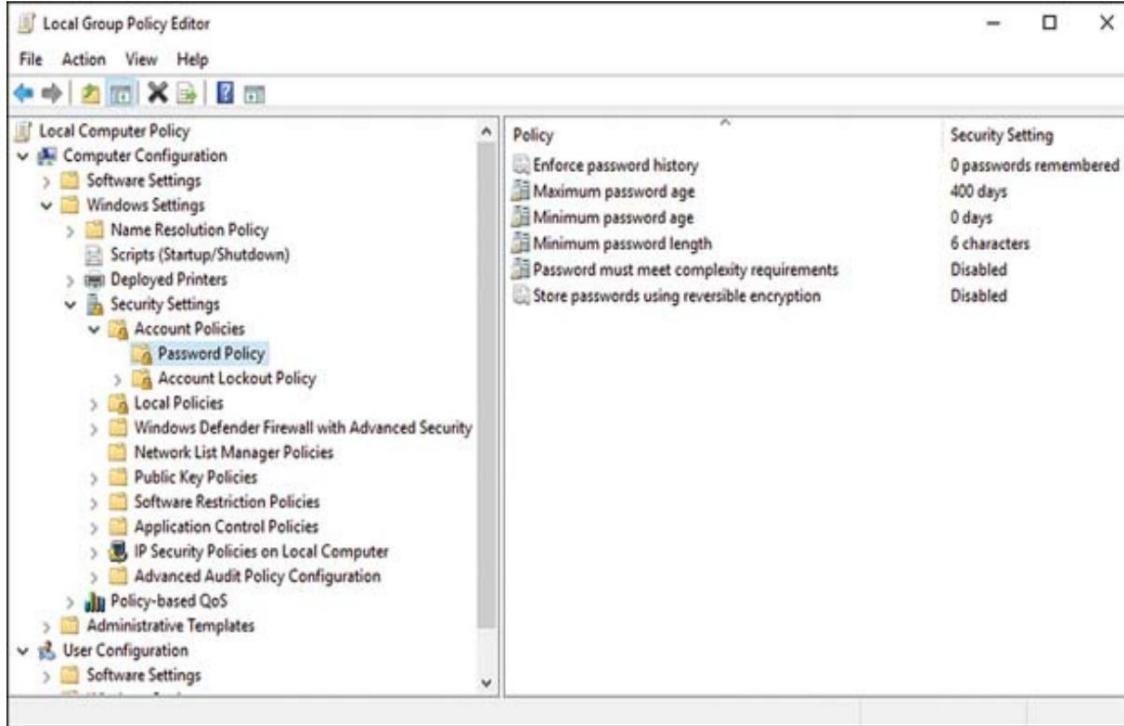


Figura 7-10 Configurações da Política de Senha

Práticas recomendadas para usuários finais

As práticas nesta seção podem parecer tão comuns que não merecem ser mencionadas, mas práticas preguiçosas se desenvolvem em um local de trabalho e se tornam um terreno fértil para ataques. Os usuários finais devem ter essas práticas incorporadas em suas práticas de trabalho.

Usar bloqueios de proteção de tela

O bloqueio automático de tela pode ser configurado para entrar em vigor após um determinado período de tempo ocioso, para ajudar a proteger um sistema caso um usuário se esqueça de bloquear o sistema manualmente. Antes que o bloqueio de tela possa ser usado, as contas devem ter o recurso de bloqueio de tela ativado. No Windows 10, vá para **Configurações > Personalização > Tela de bloqueio**.

No Windows, os usuários podem bloquear suas telas manualmente pressionando Windows+L no teclado ou pressionando Ctrl+Alt+Del e selecionando Bloquear computador.

No Linux, as chaves a serem usadas variam de acordo com o ambiente de desktop. No macOS, use Ctrl+Shift+Eject ou Ctrl+Shift+Power (para teclados sem a tecla Eject).

Faça logoff quando não estiver em uso

Deixar um computador conectado e desacompanhado é um convite aberto para problemas. Os usuários finais são responsáveis pela atividade em seus computadores quando estão ausentes, e o logoff é uma maneira simples de proteger o usuário e a empresa.

Proteger/Proteger Hardware Crítico

Todo mundo conhece alguém que perdeu um computador ou outro dispositivo móvel — ou, pior, teve ele roubado. As dores de cabeça que isso pode causar também são bem conhecidas, incluindo desastres financeiros e demissões. Os usuários finais nunca devem deixar seus dispositivos sem supervisão, nem por um minuto; esse tempo é tudo o que leva para o desastre acontecer. Se os usuários finais precisarem se desfazer de dispositivos, eles devem certificar-se de que os dispositivos estejam bloqueados com segurança em uma área confiável antes de sair.

Informações seguras de identificação pessoal (PII)

A perda de um código de acesso, um número de seguro social ou qualquer outra informação de identificação pessoal (PII) pode ser tão desastrosa quanto a perda de um dispositivo. O roubo de identidade pode arruinar uma pessoa financeiramente e ser quase impossível de se recuperar completamente. Armazenar PII em pastas criptografadas é uma jogada inteligente.



Gerenciamento de conta

Quando combinado com as configurações de segurança da estação de trabalho, as configurações de conta do usuário ajudam a impedir o acesso não autorizado à rede. As configurações de gerenciamento de conta descritas nas seções a seguir podem aumentar a segurança.

Restringindo Permissões de Usuário

As permissões de usuário para usuários padrão impedem alterações em todo o sistema, mas restrições adicionais podem ser definidas com a Diretiva de Grupo ou Diretiva de Segurança Local.

Restrições de tempo de login

Para evitar que uma conta de usuário seja usada após o expediente ou antes do início dos negócios, use as restrições de horário de login para especificar quando uma conta pode ser usada.

Desativando conta de convidado

A conta de convidado no Windows é um risco de segurança em potencial, portanto, deve ser desativada. Se os visitantes precisarem de acesso à Internet, uma rede sem fio para convidados que não se conecte à rede comercial é um bom substituto.

Bloqueio de Tentativas Falhadas

A política de senha deve especificar que um usuário será bloqueado após um número especificado de tentativas malsucedidas de fazer login em uma conta. Uma política de bloqueio também pode incorporar uma política de tempo limite que especifica quanto tempo o usuário deve esperar após um logon malsucedido antes de tentar fazer logon novamente.

Alteração de nomes de usuário e senhas padrão

Os nomes de usuário e senhas padrão do administrador para roteadores SOHO ou outros dispositivos ou serviços que tenham senhas padrão devem ser alterados. Nomes de usuário e senhas padrão estão disponíveis na documentação desses dispositivos, portanto, é fácil para um invasor encontrar os padrões e usá-los para controlar roteadores ou outros dispositivos que ainda estejam configurados com as senhas padrão.

Desativando Autorun/AutoPlay

Autorun é um recurso que permite que os programas sejam iniciados automaticamente quando um CD ou unidade USB ou flashcard é conectado a um computador. A Reprodução Automática é um recurso semelhante que oferece opções aprimoradas em um ambiente Windows. Tanto o Autorun quanto o AutoPlay permitem que o usuário selecione quais tipos de programas, atualizações e sincronizações podem ocorrer. Quando você desativa o Autorun, um disco óptico ou unidade USB não iniciará automaticamente seu aplicativo de execução automática (se houver um) e qualquer malware incorporado não terá chance de infectar o sistema antes de você verificar a mídia. A reprodução automática é um recurso semelhante que exibe um menu de aplicativos para usar na mídia em uma unidade óptica ou unidade flash USB.

A maneira mais fácil de desativar a Reprodução Automática no Windows é abrir o miniaplicativo Reprodução Automática em **Configurações > Dispositivos > Reprodução Automática** e desativar o botão. A Figura 7-11 mostra a janela Configurações de Reprodução Automática no Windows 10. A Figura 7-12 mostra como desativar a Reprodução Automática nas configurações de Diretiva de Grupo.

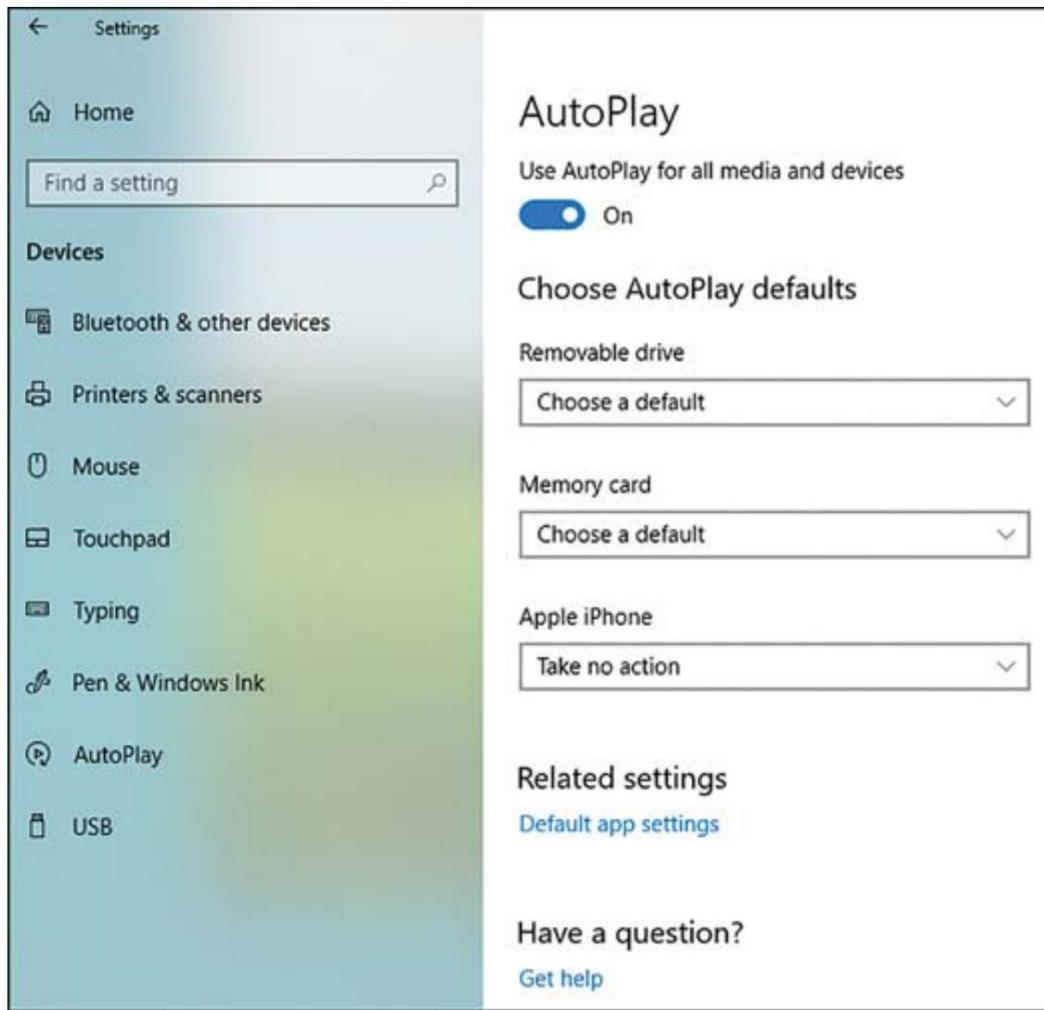


Figura 7-11 Configurações de reprodução automática no Windows

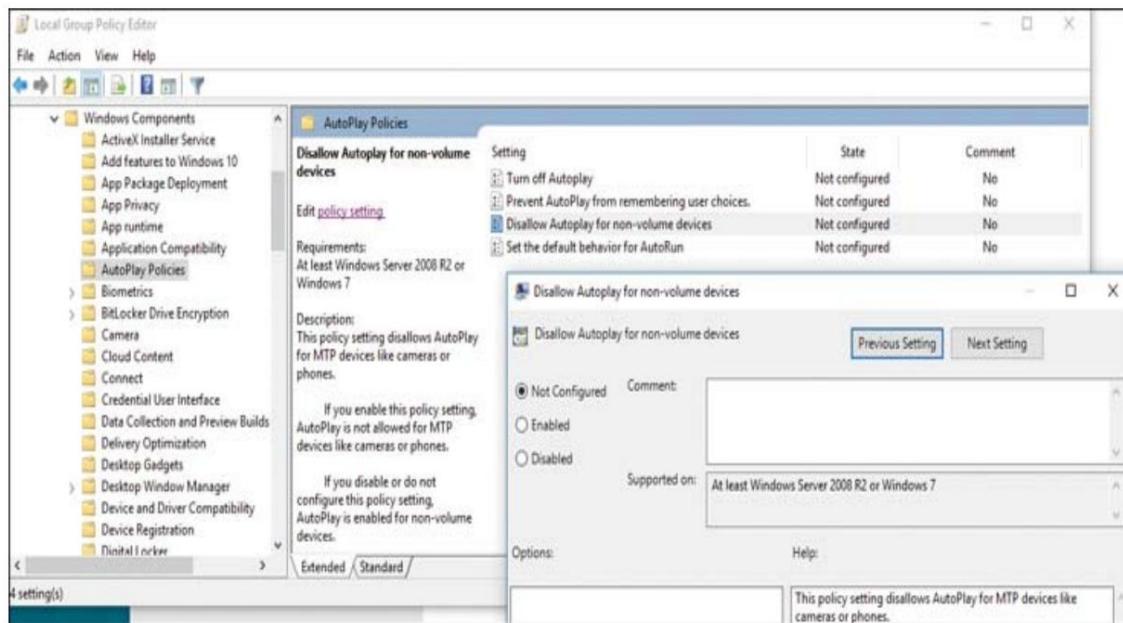


Figura 7-12 Desativando a reprodução automática nas configurações de política de grupo

Para desabilitar o Autorun no Windows usando a Diretiva de Grupo Local, conclua as seguintes etapas:

Etapa 1. Clique em **Iniciar** e, no campo de pesquisa, digite **gpedit.msc** para abrir o Editor de Diretiva de Grupo Local.

Etapa 2. Navegue até **Configuração do computador > Administrativo**

Modelos > Componentes do Windows > Políticas de Reprodução Automática.

Etapa 3. Clique duas vezes na configuração **Desativar reprodução automática** para exibir a janela de configuração Desativar reprodução automática.

Etapa 4. Clique no botão de opção **Ativado** e, em seguida, clique em **OK** para ativar a política denominada Desativar Reprodução Automática.

Observação

Laptops que fazem apresentações podem exigir o AutoPlay.

Por motivos de segurança, o macOS não oferece suporte a nenhum tipo de recurso de execução automática, mas é possível selecionar aplicativos que você deseja executar na inicialização. Para editar isso

lista, selecione **menu Apple > Preferências do Sistema > Usuários e Grupos > Itens de Login**.

No Linux, você pode desabilitar o Autorun em sistemas que usam o gerenciador de arquivos Nautilus alterando as propriedades na guia Mídia para habilitar Nunca avisar ou iniciar programas na inserção de mídia e desabilitar Procurar mídia quando inserido.

Protegendo dispositivos móveis



Objetivo 2.7: Explicar métodos comuns para proteger dispositivos móveis e incorporados.

Os dispositivos móveis evoluíram a ponto de poderem armazenar tantos dados valiosos quanto qualquer estação de trabalho. Adicione a isso o design compacto e fácil de esconder e o alto custo dos dispositivos, e fica claro por que os dispositivos móveis representam uma séria ameaça à segurança. As seções a seguir abordam métodos e práticas que podem atenuar ameaças a dispositivos móveis.



Observação

Para o exame 220-1102, familiarize-se com estes conceitos:

- Bloqueios de tela
- Limpezas remotas
- Aplicativos localizadores
- Aplicativos de backup remoto
- Restrições de tentativa de login com falha
- Antivírus/antimalware

- Patches/atualizações do sistema operacional
- Autenticação biométrica
- Criptografia completa do dispositivo
- autenticação multifator
- Aplicativos autenticadores
- Fontes confiáveis x fontes não confiáveis
- firewalls
- Políticas e procedimentos

Bloqueios de tela

A primeira etapa para proteger um dispositivo móvel é definir uma senha numérica ou outro tipo de bloqueio de tela. Essa senha bloqueia o dispositivo, tornando-o inacessível a todos, exceto aqueles que conhecem a senha e hackers experientes. Um bloqueio de tela pode ser um padrão desenhado na tela, um PIN (bloqueio por senha) ou uma senha. Uma senha muito forte geralmente é a forma mais forte de bloqueio de tela. A configuração de bloqueio de tela pode ser acessada em um dispositivo Android em **Configurações > Segurança**. No iPhone 12, vá para **Configurações > FaceID e senha > (digite a senha atual)**.

A navegação varia entre as versões do Android e do iPhone, mas as configurações aqui se aplicam a ambos os tipos de telefones, salvo indicação em contrário.

Você pode selecionar quanto tempo o telefone espera após a inatividade para bloquear; isso geralmente é definido como 3 ou 5 minutos, mas em um ambiente confidencial, pode ser apropriado definir isso como Imediato. Para habilitar o bloqueio automático, vá para **Configurações > Geral > Bloqueio automático** e selecione um número de minutos. Se for definido como Nunca, o dispositivo nunca entrará em modo de suspensão, anulando a segurança da senha e usando a valiosa energia da bateria. A configuração padrão é 2 minutos. Em um iPhone, o Bloqueio Automático está disponível na área Configurações de Exibição.

Além do tempo limite padrão, os dispositivos podem ser bloqueados pressionando rapidamente o botão liga/desliga. Se estiver configurado, a senha deve ser fornecida

sempre que um dispositivo móvel sai do estado de suspensão ou bloqueio e sempre que é inicializado pela primeira vez.

Alguns dispositivos oferecem suporte a outros tipos de bloqueio de tela, incluindo um bloqueio de impressão digital (no qual a impressão digital do usuário é comparada a uma lista de impressões digitais de usuários autorizados) e um bloqueio facial (no qual o rosto do usuário é comparado a uma lista de rostos de usuários autorizados). O Windows Hello, um recurso do Windows com suporte em alguns dispositivos, é um exemplo de bloqueio facial. O Face ID é a versão da Apple compatível com as versões mais recentes do iPhone e iPad Pro.

Um aplicativo de bloqueio de furto bloqueia imediatamente um dispositivo quando o usuário desliza a tela para um lado.

A próxima opção na tela de segurança é Senhas visíveis. Se esta opção estiver marcada, o dispositivo mostra a letra atual da senha que está sendo digitada pelo usuário. Esse tipo de configuração é vulnerável a surfistas de ombro (pessoas olhando por cima do ombro para descobrir sua senha) e deve ser desmarcado para que apenas asteriscos (*) sejam mostrados quando o usuário digitar uma senha.

Uma opção de armazenamento de credenciais também está disponível. Por padrão, as credenciais seguras são descartadas quando uma sessão é concluída. (Uma exceção a essa regra é um Gmail ou outro login semelhante.) No entanto, se Usar credenciais seguras estiver marcado e um usuário acessar um site ou aplicativo que exija um certificado seguro, as credenciais serão armazenadas no dispositivo. Um usuário pode definir uma senha aqui para que somente ele possa visualizar ou limpar credenciais ou instalar credenciais de um cartão de memória. O uso de credenciais seguras geralmente é configurado apenas se um usuário precisar acessar informações confidenciais da empresa na Internet.

O bloqueio por código pode ser acessado em dispositivos iPad e iPhone acessando **Ajustes > Código** e tocando em Bloqueio por código para exibir a tela Bloqueio por código. Toque em Ativar senha para definir uma senha.

Limpezas remotas

Um dispositivo móvel perdido ou ausente é uma séria ameaça à segurança. Um hacker pode passar por senhas e outros bloqueios de tela, o que significa que é apenas uma questão de tempo até que o hacker tenha acesso aos dados. Uma organização com informações confidenciais deve considerar permitir uma [**limpeza remota**](#) de um

dispositivo. Desde que o dispositivo móvel ainda tenha acesso à Internet, o programa de limpeza remota pode ser iniciado a partir de um computador desktop para excluir todo o conteúdo do dispositivo móvel remoto.

Alguns aparelhos (como o iPhone) possuem uma configuração que faz com que o aparelho seja apagado após um certo número de tentativas incorretas de senha (10, no caso do iPhone). Aplicativos de terceiros também estão disponíveis para download para a maioria dos dispositivos móveis e podem apagar os dados após um determinado número de tentativas. Alguns aplicativos configuram um dispositivo para tirar uma foto automaticamente após três tentativas malsucedidas e enviar a foto por e-mail ao proprietário do dispositivo. Exemplos de software que podem fazer isso incluem Google Sync, Google Apps Device Policy, Apple Data Protection e aplicativos de terceiros, como Mobile Defense. Em alguns casos, como com o Apple Data Protection, o comando que inicia a limpeza remota deve ser emitido de um servidor Exchange ou servidor de gerenciamento de dispositivo móvel (MDM). Obviamente, você também deve ter um plano de backup para que os dados no dispositivo móvel sejam copiados para um local seguro em intervalos regulares. Dessa forma, se os dados precisarem ser apagados, você sabe que pode recuperar a maioria ou todos os dados. O tipo de programa de limpeza remota, programa de backup e políticas sobre como eles são implementados podem variar entre as organizações.

Aplicativos localizadores

Ao instalar ou habilitar um aplicativo ou serviço localizador, como Android Device Manager, Lookout para iOS ou Android ou Find My iPhone (ou Find My App e AirTag), um usuário pode rastrear um dispositivo perdido. Esses aplicativos podem ser operados de qualquer outro telefone que tenha um aplicativo semelhante instalado, desde que a energia esteja ligada e a geolocalização esteja funcionando.

Aplicativos de backup remoto

backup de um dispositivo móvel é feito de duas maneiras: usando uma conexão USB a um computador desktop ou laptop ou à nuvem usando um aplicativo de backup remoto.

O Apple iCloud oferece um serviço gratuito de backup em nuvem para uma quantidade limitada de dados (atualmente, 5 GB), com mais espaço disponível por assinatura. itunes,

que pode ser usado para backup baseado em USB, faz backup de todo o dispositivo em um disco rígido sem custo adicional.

Os usuários do Android têm backup gratuito de e-mail, contatos e outras informações via Google Cloud. No entanto, o backup de fotos, músicas e outros conteúdos e documentos deve ser feito manualmente via USB ou com sincronização de arquivos na nuvem, usando um serviço como o Dropbox ou outro aplicativo de terceiros.

Os usuários de iOS e Android podem usar backups populares baseados em nuvem de terceiros que também são compatíveis com macOS e Windows, como Carbonite (carbonite.com) e iDrive (idrive.com).

Restrições de tentativas de login com falha A

maioria dos dispositivos móveis inclui restrições de tentativas de login com falha. Se uma pessoa não conseguir inserir a senha correta após um determinado número de tentativas, o dispositivo será bloqueado temporariamente e a pessoa deverá aguardar um determinado período de tempo antes de tentar a senha novamente. Se a pessoa não inserir a senha correta novamente, na maioria dos dispositivos, o tempo limite aumentará. Conforme mencionado anteriormente, vários logins com falha podem resultar em uma limpeza remota do disco rígido.

Antivírus/Antimalware

Assim como existe um software antivírus para PCs, existe um software *antivírus/antimalware* para dispositivos móveis. Esses são aplicativos de terceiros que precisam ser pagos, baixados e instalados no dispositivo móvel. Alguns exemplos comuns para Android incluem McAfee VirusScan Mobile, AVG, Lookout, Dr. Web e NetQin.

O iOS funciona um pouco diferente do Android. O iOS é um sistema operacional rigidamente controlado. Um benefício de ser um sistema operacional de código fechado é que escrever vírus para ele pode ser mais difícil, tornando-o um pouco mais difícil de comprometer. Mas nenhum sistema operacional está realmente a salvo de comprometimento. Por muito tempo, nenhum software antivírus existiu para iOS, mas a Apple agora permite o download de aplicativos anteriormente indisponíveis e software que a Apple não autorizou.

Patches e atualizações do sistema

operacional Patches e atualizações do sistema operacional ajudam a proteger os dispositivos móveis contra as vulnerabilidades e ameaças mais recentes. Por padrão, você é notificado automaticamente sobre atualizações disponíveis em dispositivos Android e iOS. No entanto, você também deve saber onde ir para atualizar manualmente esses dispositivos:

- No Android, vá para **Configurações > Geral > Sobre o dispositivo > Atualização de software** ou **Configurações > Sistema > Sobre o dispositivo > Atualização de software > Verificar atualizações.**
- Para iOS, vá para **Configurações > Geral > Atualização de Software.**

Grandes organizações que possuem muitos dispositivos móveis devem usar um conjunto de gerenciamento de dispositivo móvel (MDM). A McAfee e muitas outras empresas têm pacotes de software MDM que podem receber atualizações push e configurar muitos dispositivos móveis a partir de um local central. O software MDM de qualidade decente protege, monitora, gerencia e suporta vários dispositivos móveis diferentes em toda a empresa.

Autenticação biométrica

Os dispositivos Android e iOS atuais e mais antigos podem usar autenticação biométrica por meio do uso de leitores de impressão digital adicionais ou leitores de íris.

Dispositivos iOS recentes e atuais têm suporte integrado para leitura de impressão digital com todos os telefones com recurso Touch ID e versões de iPad.

Bloqueios faciais, como Microsoft Windows Hello e Apple Face ID, também são considerados um tipo de autenticação biométrica.

Criptografia de dispositivo

completo Com a criptografia de dispositivo completo, seus dados não são acessíveis a possíveis ladrões, a menos que conheçam a senha. Os dispositivos Apple iOS apresentam criptografia de dispositivo completo que é ativada quando uma senha é atribuída ao dispositivo. Para saber mais sobre esta e outrasseguranças do iOS, a Apple fornece um guia de segurança do iOS em <https://support.apple.com/guide/security/welcome/web>.

O Android 12 oferece suporte à criptografia de disco completo e à criptografia baseada em arquivo. A criptografia baseada em arquivo é a criptografia em arquivos individuais, o que significa que cada arquivo possui uma chave de criptografia separada para que todos os recursos do telefone não precisem ser vinculados ao processo de criptografia.

firewalls

O Android não inclui um firewall, portanto, aplicativos de terceiros devem ser usados para fornecer proteção contra tráfego indesejado da Internet. O Google Play oferece muitos aplicativos de firewall gratuitos para Android.

A Apple não inclui um firewall porque o design do iOS usa um recurso chamado sandboxing que executa aplicativos em um espaço protegido separado.

Políticas e procedimentos

Muitos dispositivos móveis de propriedade individual agora estão sendo usados em redes corporativas. Como esses dispositivos não foram configurados pela corporação, eles podem apresentar ameaças à segurança. Para evitar ameaças, as organizações precisam abordar essas questões em suas políticas e procedimentos.

BYOD x Dispositivos Corporativos

Veja a seguir os benefícios das políticas de trazer seu próprio dispositivo (BYOD):

- Nenhum custo de hardware para a organização
- Maior uso porque os funcionários estão satisfeitos com o dispositivo selecionado
- Maior produtividade

Possíveis desvantagens incluem o seguinte:

- Custos ocultos de gerenciamento e segurança
- Possibilidade de alguns funcionários não quererem comprar seus próprios dispositivos

Corporativo pessoalmente habilitado (COPE) é um modelo no qual a empresa é proprietária do dispositivo e às vezes permite que o funcionário o use para

uso pessoal. Este modelo é de grande benefício para a organização porque os dispositivos são pré-aprovados e são tipicamente similares em modelo. Eles são, portanto, mais fáceis de gerenciar e controlar com políticas de gerenciamento de dispositivos móveis (MDM) ou gerenciamento de aplicativos móveis (MAM).

Requisitos de segurança de perfil

Independentemente de uma organização usar dispositivos móveis corporativos, BYOD ou uma combinação deles, definir e seguir os requisitos de segurança de perfil é importante para obter maior produtividade sem incorrer em riscos significativos. Os problemas envolvidos incluem especificar dispositivos aprovados e versões do sistema operacional, exigir senhas e telas de bloqueio, exigir criptografia do dispositivo, abordar problemas de suporte e determinar quando e como remover informações da empresa quando um funcionário deixar a organização.

Internet das Coisas

Os dispositivos [da Internet das Coisas \(IoT\)](#), como dispositivos domésticos inteligentes, câmeras de segurança e assistentes de IA, como Alexa e Google Home, tornaram-se tão difundidos que podem ser encontrados em quase todos os lares e SOHO.

Esses dispositivos podem ser úteis ou divertidos, mas apresentam riscos à sua rede se não forem tomadas precauções.

Os dispositivos IoT não possuem padrões de segurança do setor, portanto, cada dispositivo abre uma porta diferente para um hacker. Como os dispositivos tendem a ser inseguros, a melhor solução é protegê-los quando eles se conectam à rede.

As etapas que podem tornar os dispositivos IoT mais seguros são semelhantes a outras práticas de segurança mencionadas em outras partes deste capítulo:

- Ativar a autenticação e/ou alterar as senhas padrão para torná-las mais seguras
- Manter os dispositivos atualizados com o software ou firmware mais recente
- Isolando-os em sua própria sub-rede ou rede, para controlar o acesso a servidores e outros dispositivos que os hackers possam procurar

Destrução e descarte de dados

**Objetivo 2.8:** Dado um cenário, use métodos comuns de destruição e descarte de dados.

Mesmo após computadores, dispositivos móveis e até mesmo alguns tipos de impressoras chegarem ao fim de suas vidas úteis, os discos rígidos internos contêm riscos potenciais à segurança. Os riscos também estão nas unidades flash, unidades externas e mídia óptica. Para evitar que informações confidenciais da empresa ou do cliente sejam acessadas de um computador ou outro dispositivo que esteja sendo descartado para revenda, reciclagem ou desmontagem de peças, siga os métodos descritos nas próximas seções.

Observação

Para o exame 220-1102, você deve entender a importância destes métodos:

- Métodos de destruição física
- Práticas recomendadas de reciclagem ou reaproveitamento
- Conceitos de terceirização

Métodos de destruição física A destruição física

transforma um dispositivo de armazenamento em massa em pequenos pedaços que não podem ser reconstruídos, tornando os dados internos irrecuperáveis. Os métodos incluem o seguinte:



- **Triturador:** Alguns trituradores de nível de escritório podem destruir a mídia óptica. Os recicladores eletrônicos usam trituradores pesados feitos para discos rígidos e dispositivos de armazenamento em massa, para reduzir os dispositivos de armazenamento, fita ou outros tipos de mídia em pequenos bits.

- **Broca/Martelo:** Remova os discos rígidos e destrua seus pratos com uma furadeira, martelo ou outro dispositivo; em seguida, recicle a sucata.
- **Eletromagnético (desmagnetização):** ferramentas como desmagnetizadores eletromagnéticos e desmagnetizadores de ímãs permanentes podem eliminar permanentemente as informações de um disco. A unidade está fisicamente intacta, mas faltam todos os dados, formatação e dados da trilha de controle. Use esse tipo de destruição física se quiser usar uma unidade para fins de exibição.
- **Incineração:** A incineração de fitas e outros tipos de mídia magnética e óptica é permitida em algumas áreas e está disponível em várias empresas.

As empresas de reciclagem de dados que destroem discos rígidos ou outros dispositivos de armazenamento podem fornecer um certificado de destruição para comprovar a conformidade com as leis locais ou políticas institucionais.

Práticas recomendadas de reciclagem ou reaproveitamento

Desde que os dados em um disco rígido ou outro dispositivo de armazenamento em massa possam se tornar irrecuperáveis, não é necessário destruir a mídia em si. A seguir estão algumas práticas recomendadas para reciclagem e reaproveitamento:



- **Formato de baixo nível versus formato padrão:** O formato padrão usado em sistemas operacionais é um formato rápido. Este tipo de formato limpa apenas a pasta raiz. O restante dos dados no disco pode ser recuperado até que seja substituído. Um formato longo reescreve a superfície do disco. No entanto, os programas de recuperação de dados disponíveis em muitas empresas terceirizadas podem recuperar dados de uma unidade formatada. Um formato de baixo nível que cria a infraestrutura física onde os dados serão armazenados em um disco é executado pelo fabricante da unidade antes que a unidade seja enviada e não pode ser executada em campo.
- **Sobrescrever:** Alguns programas de manutenção de disco de fornecedores de armazenamento em massa incluem opções para sobrescrever a área de dados de um disco rígido ou SSD com zeros. Os programas de recuperação de dados geralmente podem recuperar dados que foram substituídos dessa maneira.

- **Apagamento/limpeza de unidade:** Para garantir a destruição completa dos dados recuperáveis em um dispositivo de armazenamento, os dados devem ser substituídos por um programa que atenda ou exceda os padrões de destruição de dados reconhecidos, como o Departamento de Defesa dos EUA (DoD) 5220.22-M (que requer sete passagens) ou o método de segurança máxima de 35 passagens de Peter Gutman. Esses programas, conhecidos como limpezas de unidade, destroem dados existentes e informações de partição para impedir a recuperação de dados ou conduzir análises forenses. Use este método quando for importante manter o dispositivo de armazenamento como um dispositivo funcional para reaproveitamento (como doação ou revenda). Uma variedade de programas comerciais e freeware pode ser usada para essa tarefa, também conhecida como depuração de disco ou limpeza de disco.

Conceitos de Terceirização

Inúmeros exemplos de problemas e ações judiciais surgiram devido ao manuseio inadequado de dados e equipamentos. Equipamentos que são simplesmente jogados fora ou reciclados muitas vezes colocam recursos valiosos da empresa nas mãos de completos estranhos, que podem fazer o que quiserem com os dados.

As empresas devem ter políticas de destruição de dados em vigor, incluindo destruição de papel e discos rígidos. Geralmente, é economicamente vantajoso terceirizar essa tarefa de destruição para um fornecedor terceirizado que investiu no equipamento adequado e no treinamento da equipe. A terceirização para uma empresa qualificada garante que os métodos utilizados sejam seguros e seguros e que o descarte de dados seja legal.

A maioria das empresas não dispõe de equipamentos ou dados suficientes para justificar o investimento em equipamentos de destruição ou pessoal especializado.

Outra vantagem de terceirizar para uma empresa qualificada é que a empresa pode atestar que a destruição foi completa e correta e então emitir um ***certificado oficial de destruição/reciclagem*** para confirmar a destruição do material. Isso mostra aos parceiros de negócios e reguladores do governo que foi tomado cuidado para cumprir as práticas de segurança e as leis locais.

Configurando a segurança em redes SOHO



Objetivo 2.9: Dado um cenário, defina as configurações de segurança apropriadas em redes com e sem fio de pequeno escritório/escritório doméstico (SOHO).

As redes com e sem fio para pequenos escritórios/escritórios domésticos (SOHO) são importantes para empresas de todos os tamanhos, bem como para usuários individuais. No entanto, eles representam vulnerabilidades significativas se não forem devidamente protegidos. As seções a seguir explicam como os diferentes métodos de criptografia funcionam e detalham as etapas adicionais que devem ser seguidas para proteger completamente uma rede sem fio.

Configurações do roteador doméstico

Para estar seguro e navegar na Internet com segurança no mundo de hoje, configurações de segurança específicas devem ser consideradas ao instalar e configurar um roteador doméstico. A seguir estão algumas diretrizes importantes para redes com e sem fio SOHO.

Alterar senhas padrão

A documentação de quase todos os WAPs e roteadores sem fio lista a senha padrão do administrador. Esta documentação pode ser facilmente baixada em formato PDF ou HTML nos sites dos fornecedores. Como um invasor pode usar essas informações para controlar o dispositivo, é essencial alterar o padrão para uma senha privada. A maioria dos roteadores usa a caixa de diálogo Administração ou Gerenciamento para a senha e outras configurações de segurança.

GORJETA

Para proteger ainda mais um roteador ou WAP, configure o dispositivo para que ele possa ser gerenciado apenas com uma conexão Ethernet com fio.

Filtragem IP

As configurações que controlam o acesso à rede analisando o tráfego IP são conhecidas como listas de controle de acesso (ACLs). As configurações básicas em um SOHO são bastante fáceis de implementar simplesmente sabendo quais tipos de protocolos IP e tráfego serão permitidos. Por exemplo, muitas grandes redes negam o tráfego de ping filtrando o tráfego do protocolo ICMP nas redes. O tráfego pode ser filtrado por tipo de tráfego ou por endereço IP. Em termos gerais, **a filtragem de IP** permite controlar qual tráfego de protocolo de Internet (IP) é permitido para dentro e para fora da sua rede.

Atualizações de firmware

A maioria dos fornecedores de roteadores SOHO emite pelo menos uma **atualização de firmware** durante a vida útil de cada modelo de WAP e roteador sem fio. As atualizações podem resolver problemas operacionais e adicionar recursos que aprimoram a interoperabilidade, segurança e facilidade de uso do Wi-Fi. Para determinar se um WAP ou roteador sem fio tem uma atualização de firmware disponível, siga estas etapas:



Etapa 1. Visualize as caixas de diálogo de configuração do dispositivo para registrar a versão atual do firmware. Anote também o número do modelo do roteador e a revisão na parte traseira ou inferior do dispositivo.

Etapa 2. Visite o site do fornecedor do dispositivo para ver se uma nova versão do firmware está disponível.

Etapa 3. Baixe a atualização do firmware para um PC que possa ser conectado a o dispositivo com um cabo Ethernet.

Etapa 4. Conecte o PC ao dispositivo com um cabo Ethernet.

Etapa 5. Navegue até a caixa de diálogo de atualização de firmware do dispositivo.

Etapa 6. Siga as instruções para atualizar o firmware.

Filtragem de conteúdo

O departamento de TI é responsável pelo cumprimento da política de uso aceitável da infraestrutura de TI, bem como por garantir que o conteúdo inbound e outbound esteja de acordo com as expectativas. Protegendo a rede de

usuários errantes que explorariam conteúdo inapropriado na Web ou em e-mail é necessário.

Os filtros de conteúdo nos roteadores ajudam a controlar o acesso a sites impróprios e podem filtrar por endereço ou outras palavras-chave preocupantes. Esses filtros podem ser aplicados ao tráfego de entrada ou saída e, dependendo do roteador, permitem diferentes níveis de controle para usuários individuais.

Colocação Física/Locais Seguros

Em um ambiente de rede SOHO, a segurança física refere-se à prevenção do uso não autorizado da rede. Os mesmos princípios básicos de segurança física se aplicam a uma rede SOHO em um grande ambiente de escritório:



- Proteja o equipamento de rede em um armário ou sala de fiação trancada.
- Desative todas as tomadas Ethernet de parede não utilizadas, desativando suas portas de switch ou desconectando os patch panels no armário de fiação.
- Passe os cabos de rede fora de vista, nas paredes e acima do teto.
Tê-los fora de vista reduz as chances de alguém acessar a rede.
- Tranque as portas ao sair.
- Se possível, dedique uma sala com chave como espaço de trabalho em um escritório doméstico, para proteger os dispositivos da empresa e outros recursos dos perigos da vida familiar diária, como crianças e animais de estimação.

Reservas do protocolo de configuração de host dinâmico (DHCP)

O servidor DHCP embutido em quase todos os roteadores domésticos é responsável por fornecer endereços IP a todos os computadores na rede que solicitam um. Restringir o DHCP é uma maneira de controlar o acesso à rede.

A maioria dos servidores DHCP pode reservar endereços IP para computadores específicos e outros dispositivos, como impressoras, mapeando o endereço MAC físico do dispositivo e combinando-o com um endereço IP constante. **Host Dinâmico**

As reservas do protocolo de configuração (DHCP) permitem que o administrador da rede gerencie dispositivos e controle concessões de IP para usuários externos. Essas reservas também podem ser usadas em telefones IP e dispositivos IoT.

Os endereços IP estáticos, configurados pelo administrador da rede e não pelo DHCP, ainda são importantes para a estabilidade da rede. Dispositivos como switches, impressoras e servidores devem ter endereços estáticos para que estejam disponíveis quando um servidor DHCP estiver inativo.

IP WAN estático

A rede de longa distância em um SOHO é a conexão com o provedor de serviços de Internet (ISP). O **endereço IP WAN estático** é fornecido pelo ISP e é aplicado (geralmente automaticamente) à porta “Internet” no roteador. O endereço é “estático” porque não muda e não expira como um endereço dinâmico alugado. Este endereço está em uma rede diferente dos endereços SOHO locais porque pertence ao roteador do ISP.

Universal Plug and Play

Universal Plug and Play (UPnP) foi projetado para permitir que dispositivos em uma rede local (LAN) doméstica ou SOHO se conectem e cooperem facilmente com outros dispositivos na LAN. Como um exemplo semelhante de Plug and Play, considere uma impressora sendo conectada a um computador: O recurso Plug and Play do sistema operacional encontra um driver de dispositivo e permite que o dispositivo interaja. O UPnP ampliou essa ideia para uma LAN, para permitir que dispositivos de jogos, dispositivos IoT domésticos inteligentes e assistentes virtuais funcionem em uma LAN. O UPnP não se expande para redes corporativas.

Esse benefício de fácil configuração de dispositivos vem com falhas de segurança. Especialmente preocupante é o uso UPnP de encaminhamento de porta e sua falta de autenticação. Se for explorado de fora, o encaminhamento de porta concede acesso a dispositivos na LAN; isso não deve ser ativado universalmente, mas vem ativado por padrão em muitos roteadores. A melhor abordagem é proteger a SOHO LAN desabilitando o encaminhamento de porta e assumindo a tarefa de configurar manualmente os dispositivos na SOHO LAN.

Sub-rede filtrada

Uma **sub-rede filtrada**, anteriormente conhecida pela CompTIA como uma zona desmilitarizada (DMZ), permite o tráfego externo através de um endereço IP específico em uma LAN. Em um roteador SOHO, qualquer dispositivo atribuído à DMZ recebe tráfego que não é especificado para um determinado dispositivo. Usar um host DMZ faz sentido para jogos e outros tipos de tráfego quando você não pode especificar com antecedência as portas necessárias. No entanto, o host DMZ deve ter seu próprio firewall porque os hosts DMZ não são protegidos pelo firewall do roteador.



Segurança específica sem fio

As configurações padrão para uma rede sem fio devem ser alteradas para fornecer segurança. As seções a seguir discutem essas questões.

Alterando o Service Set Identifier (SSID)

O identificador de conjunto de serviço (SSID) pode fornecer uma grande quantidade de informações úteis para um possível hacker de uma rede sem fio. Toda rede sem fio deve ter um SSID; WAPs e roteadores sem fio geralmente usam o nome do fabricante ou o número do modelo do dispositivo como o SSID padrão. Se um SSID padrão for transmitido por uma rede sem fio, um hacker pode consultar a documentação de um roteador específico ou os modelos mais comuns de uma determinada marca e determinar o intervalo de endereços IP padrão, o nome de usuário e a senha padrão do administrador e outras informações que facilita o ataque à rede.

Para ajudar a “ocultar” os detalhes de sua rede e localização, uma substituição do SSID para uma rede sem fio segura não deve incluir nenhum dos itens a seguir:

- Seu nome
- O nome da sua empresa
- Sua localização
- Qualquer outra informação facilmente identificável

Um SSID que inclua informações obscuras (como o nome do seu primeiro animal de estimação) é um substituto adequado.

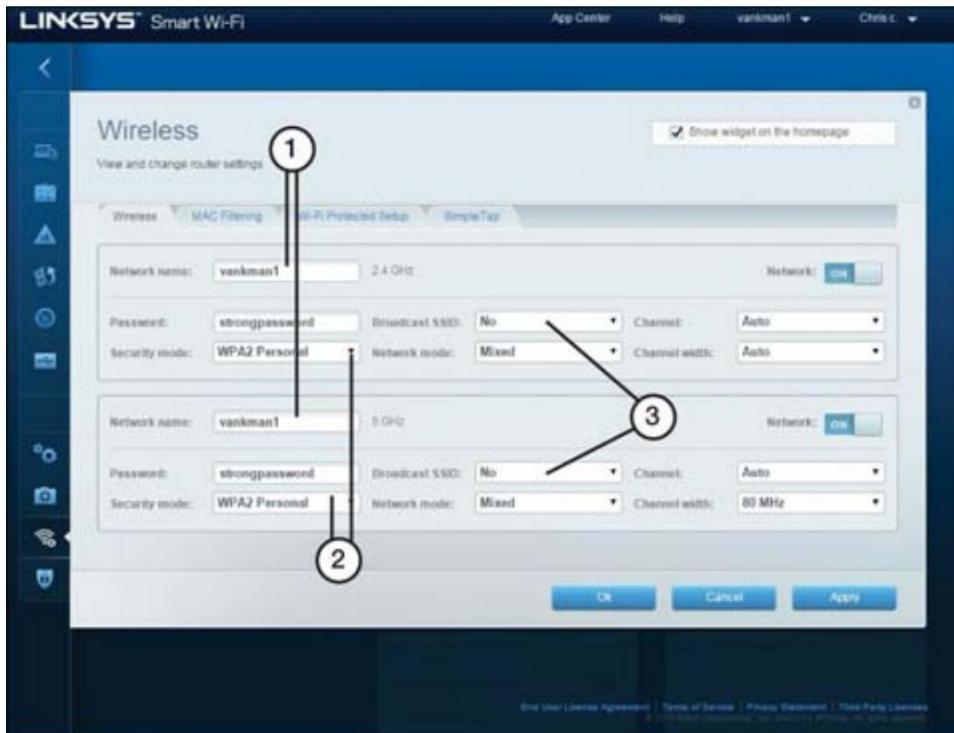
Configurações de criptografia

A importância de configurar a criptografia para os padrões mais recentes possíveis foi abordada anteriormente neste capítulo, na seção "Protocolos de segurança sem fio e autenticação". As informações ali contidas também se aplicam às redes SOHO porque uma SOHO pode ser configurada como uma extensão de um negócio. Nesse caso, todas as políticas de segurança da empresa também devem ser aplicadas na extensão SOHO.

Desativando transmissão SSID

Acredita-se que desabilitar a transmissão SSID seja uma maneira eficaz de impedir que uma rede sem fio seja detectada, e o exame de certificação A+ compartilha dessa opinião. Mas essa abordagem nem sempre é suficiente. Mesmo que desabilitar a transmissão SSID impeça que bisbilhoteiros casuais de largura de banda encontrem sua rede sem fio, a Microsoft não recomenda desabilitar a transmissão SSID como uma medida de segurança porque hackers sérios podem usar certos métodos para descobrir redes.

[A Figura 7-13](#) ilustra uma caixa de diálogo de configuração do roteador Linksys na qual várias dessas recomendações de segurança foram implementadas.



1. User-assigned SSID in place of factory default
2. WPA2 Personal security mode selected
3. SSID broadcast disabled

Figura 7-13 Configurando um roteador com SSIDs alternativos, WPA2 Criptografia habilitada e transmissão SSID desabilitada

Desativando o acesso de convidado

A conta de convidado em uma rede sem fio é um risco de segurança em potencial, portanto, deve ser desativada. Se os visitantes precisarem de acesso à Internet, uma rede sem fio separada para convidados que não se conecte à rede comercial é um bom substituto.

Mudando de Canais

Os canais de frequência sem fio podem se sobrepor aos canais vizinhos. Se isso acontecer, considere mudar o canal para um mais distante. Você também pode reduzir a potência de transmissão do canal sem fio que está sendo usado, para limitar o acesso a uma área menor. Isso pode ajudar a impedir que estranhos mal-intencionados ou funcionários desonestos se conectem a um roteador SOHO.

Configurações de

firewall Por padrão, a maioria dos WAPs e roteadores sem fio usam um recurso chamado Network Address Translation (NAT) para atuar como firewalls simples. O NAT impede que o tráfego da Internet determine os endereços IP privados usados pelos computadores na rede. No entanto, muitos WAPs e roteadores sem fio oferecem recursos de firewall adicionais que podem ser ativados, incluindo o seguinte:

- Registros de acesso
- Filtragem para tipos específicos de tráfego
- Suporte aprimorado para VPNs

Consulte a documentação do fabricante do roteador para obter mais informações sobre recursos avançados de segurança. A Figura 7-14 mostra um exemplo de configurações de firewall.

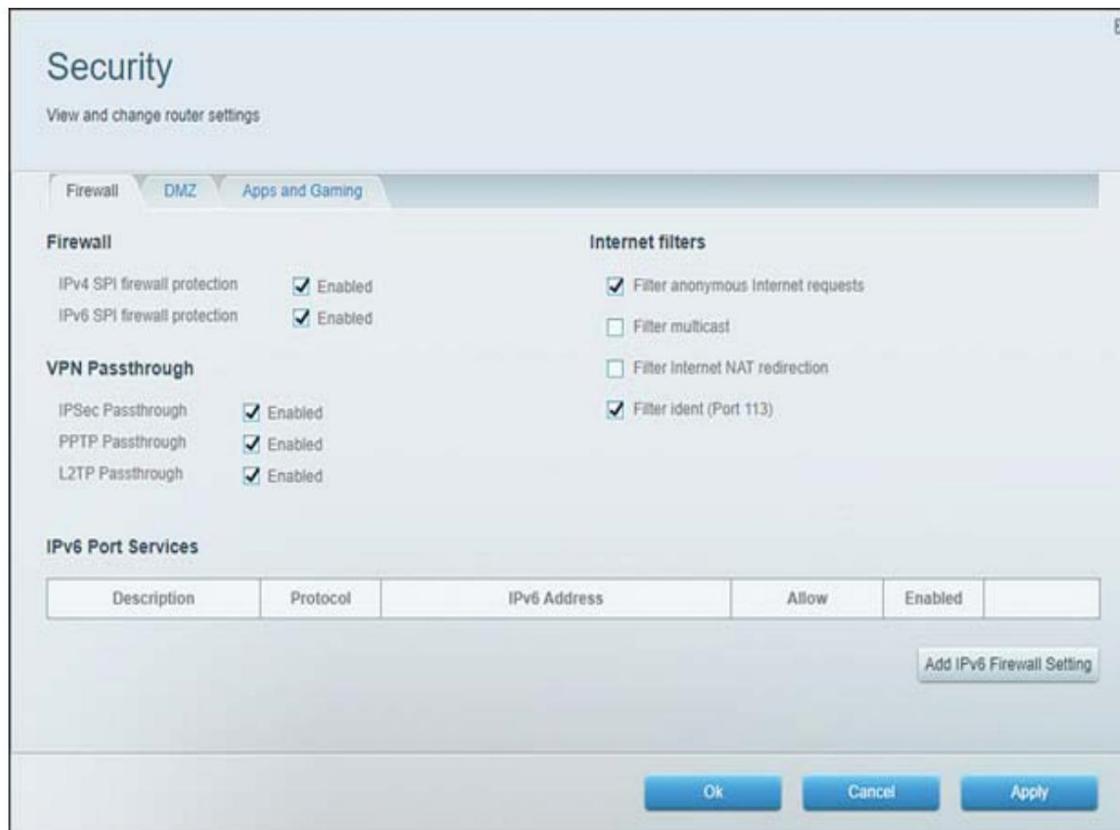


Figura 7-14 Configurações de firewall

Encaminhamento/mapeamento de porta

porta Use **o encaminhamento** de porta (também conhecido como **mapeamento de porta**) para permitir que o tráfego de entrada em uma determinada porta ou intervalo TCP ou UDP vá para um determinado endereço IP em vez de para todos os dispositivos em uma rede. Um exemplo básico é um servidor FTP interno a uma LAN. O servidor FTP pode ter o endereço IP 192.168.0.250 e pode ter a porta 21 aberta e pronta para aceitar transações de arquivo (ou uma porta de entrada diferente pode ser usada). Os clientes na Internet que desejam se conectar ao servidor FTP precisam saber o endereço IP do roteador, para que os clientes possam se conectar a um cliente FTP usando o endereço IP 68.54.127.95 e a porta 21. Se uma regra de encaminhamento de porta apropriada está em uso, o roteador vê esses pacotes e os encaminha para 192.168.0.250:21, ou qualquer porta escolhida. Muitos ISPs bloqueiam esse tipo de atividade, mas o encaminhamento de porta é um método comum e importante em redes maiores.

Desativação de portas

portas O bloqueio de portas TCP e UDP, também conhecido como **desativação de portas**, é executado com um aplicativo de firewall, como o Windows Defender Firewall com Segurança Avançada. Os hackers aproveitam as portas não utilizadas que ficam ociosas em uma rede, e desabilitar portas desnecessárias dificulta o acesso ao seu domínio.

Configurando o navegador e a segurança relevante

Configurações



Objetivo 2.10: Dado um cenário, instalar e configurar navegadores e configurações de segurança relevantes.

O navegador da web é indiscutivelmente o aplicativo mais usado no uso diário. Navegadores da Web como Google Chrome, Microsoft Edge, Apple Safari e Mozilla Firefox são usados bilhões de vezes por dia para tudo, desde o envio de e-mails; comunicar-se ao vivo com a família, amigos ou colegas de trabalho; e conduzir transações bancárias e outras transações altamente confidenciais. Saber como instalar, atualizar, configurar e proteger os navegadores mais usados é um

habilidade que todo técnico deve possuir. Livros inteiros foram escritos sobre configuração e segurança do navegador da web; esta seção enfoca os objetivos atuais do exame CompTIA A+.

Download e instalação do navegador

Ao baixar o software do navegador (ou qualquer aplicativo), você deve fazê-lo apenas de fontes confiáveis. A [Tabela 7-2](#) exibe links de referência da Internet de fontes confiáveis e confiáveis, onde você pode baixar com segurança os navegadores da Web mais populares em uso atualmente. Observe o *HTTPS* seguro no início de cada URL.



Tabela 7-2 Links de download de navegadores da Web confiáveis

Navegador	Ligaçāo
Microsoft	https://www.microsoft.com/en-us/edge
Beira	
cromada	https://www.google.com/chrome/
Raposa de fogo	https://www.mozilla.org/en-US/firefox/new/
Safári	https://support.apple.com/downloads/safari (somente macOS)

A instalação de um navegador da Web confiável geralmente é um processo direto. A seguir estão as etapas gerais para instalar o Google Chrome, que atualmente é o navegador mais popular, em um sistema baseado no Windows. A maioria das instalações do navegador da Web segue um processo semelhante:

Etapa 1. Baixe o arquivo de instalação.

Etapa 2. Se solicitado, clique em **Executar ou Salvar**.

Se você escolher Salvar, inicie a instalação com um destes métodos:

- Clique duas vezes no download.
- Clique em **Abrir arquivo**.

Etapa 3. Você pode ser perguntado: "Deseja permitir que este aplicativo faça alterações em seu dispositivo?" Clique em **Sim**. No Windows 10 ou 11, uma janela do Chrome é aberta quando tudo estiver concluído.

Se você usou um navegador diferente, como Microsoft Edge ou Safari, pode importar suas configurações para o Chrome.

Lembre-se dos seguintes pontos ao baixar navegadores da Web ou qualquer outro aplicativo pela Internet:

- Os sites que possuem um URL que começa com *HTTPS* são considerados seguros e confiáveis. Lembre-se de que o Hypertext Transfer Protocol Secure (*HTTPS*) é uma extensão segura do protocolo *HTTP*. O *HTTPS* usa a porta segura 443, enquanto o *HTTP* usa a porta não segura 80.
- Se você receber uma mensagem pop-up “Certificado não confiável” ao acessar um site, isso significa que seu navegador atual não sabe se o site é autêntico ou falso. Certificados SSL/TLS inválidos ou falsos geralmente indicam a presença de um site malicioso.

Observação

Certifique-se de baixar programas e arquivos de fontes confiáveis ou fontes que você sabe que são legítimas (por exemplo, Microsoft.com, Google.com, Mozilla.org, Apple.com e assim por diante, conforme observado na [Tabela 7-2](#)).

Hash

Hashing verifica se o conteúdo dos arquivos está inalterado. Um hash geralmente é criado em um arquivo antes de ser baixado; então outro hash é criado após o download. Os dois valores são comparados para garantir que o conteúdo seja o mesmo. Ao fazer download de arquivos, principalmente upgrades, patches e atualizações, certifique-se de verificar os valores de hash.

O hash também é importante se você armazenar um arquivo de instalação do navegador para uma instalação posterior porque deseja garantir que o arquivo de instalação não seja adulterado. Você pode fazer isso criando um hash Secure Hash Algorithm (SHA) do arquivo de instalação executável e armazenando-o para uso posterior. Quando chegar a hora de instalar a partir do arquivo de instalação executável, você pode executar o hash para

verifique a assinatura do arquivo. Os detalhes de hash estão além do escopo de A+. Para saber mais, visite <https://csrc.nist.gov/projects/Hash-Functions>.

Fontes não confiáveis

A seção anterior sobre hash forneceu um exemplo de uso de um hash SHA para verificar a integridade de um arquivo executável do navegador armazenado. Se a assinatura de hash corresponder, o arquivo de instalação é confiável. Se o hash não corresponder, diz-se que não é confiável. Este é um exemplo perfeito de uma fonte não confiável. Você deve sempre baixar as instalações de fontes confiáveis e, em seguida, protegê-las com hashing de arquivo, para detectar qualquer atividade maliciosa ou adulteração.

Extensões e Plug-ins

Extensões e plug-ins são usados para personalizar navegadores da web. Eles adicionam recursos e funcionalidades e permitem que você personalize seu navegador da web. As extensões geralmente representam o código-fonte, enquanto os plug-ins são executáveis. As extensões adicionam funcionalidade a um navegador da Web como um todo, enquanto os plug-ins adicionam recursos extras a páginas da Web específicas. Embora extensões e plug-ins bons (confiáveis) adicionem funcionalidade e recursos, os ruins (não confiáveis) podem causar grandes danos ao seu sistema. Eles podem usar recursos do sistema, inserir anúncios, redirecionar pesquisas na web e até mesmo coletar seus dados pessoais.

Você pode visualizar as extensões instaladas no Microsoft Edge inserindo **edge://extensions** na barra de endereço. Para ver as extensões instaladas no Google Chrome, digite **chrome://extensions** na barra de endereços. A partir desses locais, você também pode ativar ou desativar extensões ou procurar outras.

Observação

O Microsoft Edge e o Google Chrome agora usam principalmente extensões e quase eliminaram o uso de plug-ins. No entanto, o Mozilla Firefox ainda usa extensões e plug-ins.

Gerenciadores de senhas

Um gerenciador de senhas é um aplicativo que armazena senhas que você usa para vários sites ou serviços. Os gerenciadores de senhas geralmente são programas locais executados no sistema operacional. Eles também podem ser fornecidos por empresas terceirizadas de código aberto, como KeePass, ou provedores comerciais, como 1Pssword e Roboform. Os gerentes comerciais envolvem um custo nominal, mas geralmente são mais gerenciáveis para usuários menos experientes.

Credential Manager é o gerenciador de senhas para Windows e Microsoft Edge. O Google Chrome e o Mozilla Firefox usam gerenciadores de credenciais integrados. O macOS usa o Keychain como gerenciador de senhas. Essas ferramentas armazenam credenciais da Web e do sistema operacional.

Conexão/sites seguros — certificados válidos

Usar uma conexão segura com a Internet e conectar-se a sites que usam certificados válidos é fundamental para garantir a saúde e a segurança de seus dados e de seu sistema. Várias tecnologias ajudam você a ficar o mais seguro possível ao viajar pelo mundo por meio de um navegador da web. Para fins de certificação A+, as próximas seções se concentram em TLS e HTTPS.

Segurança da Camada de Transporte (TLS)

O TLS é o protocolo mais amplamente adotado usado para criptografar comunicações entre aplicativos da Web e servidores da Web e, por fim, proteger dados confidenciais em movimento (trânsito). O TLS 1.2 é amplamente usado; 1.3 é a versão mais recente, mas está listada como experimental no momento em que este livro foi escrito. Para ver as várias versões de TLS no Windows, acesse **Internet Options > Advanced**, conforme mostrado na [Figura 7-15](#). Essas configurações de TLS se aplicam ao Google Chrome e ao Microsoft Edge.

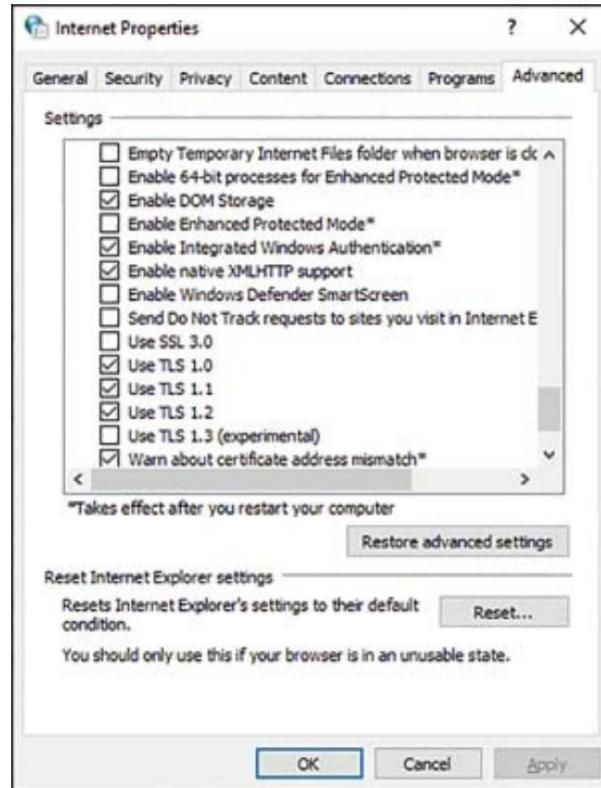


Figura 7-15 Opções da Internet Versões TLS

Protocolo de transferência de hipertexto seguro (HTTPS)

Conforme mencionado anteriormente, os sites que possuem um URL que começa com *HTTPS* são considerados seguros e confiáveis. Isso é importante aqui também. Lembre-se de que o Hypertext Transfer Protocol Secure (HTTPS) é uma extensão segura do protocolo HTTP, que não é confiável. Se você não vir um cadeado na barra de endereços URL do seu navegador, você não está usando HTTPS e a página da web não é segura. Você deve fechar imediatamente sua sessão.

Falando do cadeado em seu navegador, clicar com o botão direito do mouse no cadeado permite visualizar as informações do certificado sobre sua conexão. Você pode ver se o certificado é válido, determinar se a conexão é segura e visualizar detalhes sobre o protocolo de conexão em uso.

Configurações

Proteger os navegadores com as configurações apropriadas ajuda a evitar muitos problemas de segurança do sistema, incluindo spyware, ransomware e outros

atividades maliciosas. É importante configurar os navegadores da Web de seus clientes para facilitar o uso e garantir que seus clientes estejam cientes das ameaças de segurança que surgem na Internet.

Bloqueador de pop-up

Bloqueadores de pop-up impedem que pop-ups apareçam quando os usuários visitam um site. Os navegadores mais populares, como o Microsoft Edge e o Google Chrome, possuem recursos de bloqueador de pop-up integrados e bloqueiam pop-ups por padrão. No entanto, em alguns casos, você pode realmente querer permitir pop-ups.

Para definir pop-ups e configurações de redirecionamento no Microsoft Edge, execute as seguintes etapas:

Etapa 1. Toque em **Configurações**.

Etapa 2. Selecione **Permissões do site**.

Etapa 3. Selecione **Pop-ups e redirecionamentos**.

Etapa 4. Desative **pop-ups e redirecionamentos** para bloquear pop-ups ou ative-os para permitir pop-ups em seu dispositivo.

Para configurar pop-ups e configurações de redirecionamento no Google Chrome, execute as seguintes etapas:

Etapa 1. Abra o Chrome.

Etapa 2. No canto superior direito, clique em **Mais (três pontos verticais) > Configurações**.

Etapa 3. Clique em **Privacidade e segurança > Configurações do site**.

Etapa 4. Clique em **Pop-ups e redirecionamentos**.

Etapa 5. Escolha a opção desejada como configuração padrão.

Limpando Dados de Navegação

A limpeza dos dados do navegador envolve o uso de uma extensão do navegador que permite remover dados do navegador, como histórico, cache e cookies de uma barra de ferramentas do navegador. Na barra de ferramentas, você tem a opção de limpar todos os dados do navegador ou remover seletivamente várias informações ou tipos de dados para limpeza.

Limpar arquivos e imagens em cache (descrito a seguir) pode ajudar a corrigir problemas

você pode ter ao acessar páginas da web. A limpeza de cookies, por exemplo, pode ajudar com questões de privacidade. Lembre-se de que limpar os dados de navegação remove todos os arquivos temporários baseados em sites armazenados no sistema local, como histórico de navegação, cookies, senhas e cache.

Para limpar os dados do navegador no Microsoft Edge, selecione **Configurações** e clique em **Mais > Configurações > Privacidade, Pesquisa e Serviços**. Em Limpar dados de navegação, selecione **Escolher o que limpar**.

Para limpar os dados do navegador no Google Chrome, siga estas etapas:

Passo 1. No seu computador, abra o Chrome.

Etapa 2. No canto superior direito, clique em **Mais**.

Etapa 3. Clique em **Mais ferramentas**. Limpe os dados de navegação.

Etapa 4. Escolha um intervalo de tempo, como Última hora ou Todo o tempo.

Etapa 5. Selecione os tipos de informações que deseja remover.

Etapa 6. Clique em **Limpar dados**.

Limpando o Cache

Quando as páginas da web são acessadas, as informações são armazenadas no cache. Esse processo ocorre para que, se os dados forem necessários novamente, eles possam ser acessados rapidamente a partir do armazenamento local. Esse processo de cache significa menos viagens à Internet para acessar as mesmas informações. Limpar o cache às vezes é necessário se a cópia mais recente da página da web for necessária. Geralmente, esse é o caso durante o desenvolvimento da página da Web ou se você precisar acessar o mesmo site, mas usar credenciais ou informações de logon diferentes. A limpeza do cache do navegador remove imagens e formulários, o que impede o uso de formulários antigos e protege suas informações pessoais. Isso é semelhante à ação mencionada anteriormente de limpar os dados do navegador, mas tem a ver principalmente com imagens e formulários.

Modo de Navegação Privada

O modo de navegação privada é um recurso dos navegadores da web que não armazena dados ou informações de navegação na web. Na verdade, quando você fecha o modo de navegação privada, todos os dados e informações de navegação são removidos ou destruídos. No

Microsoft Edge, a navegação privada é chamada de navegação InPrivate; no Google Chrome, é chamado de modo de navegação anônima. Para entrar no modo InPrivate no Microsoft Edge, clique nos três pontos no canto superior direito da janela e selecione Nova janela InPrivate. A tela fica escura quando você entra na navegação InPrivate, conforme mostrado na [Figura 7-16](#). No aplicativo Safari em um computador Mac, você pode escolher **Arquivo > Nova janela privada** para usar a navegação privada. Para o exame A+, você deve saber como iniciar a navegação privada no Edge e no Chrome.

Key Topic

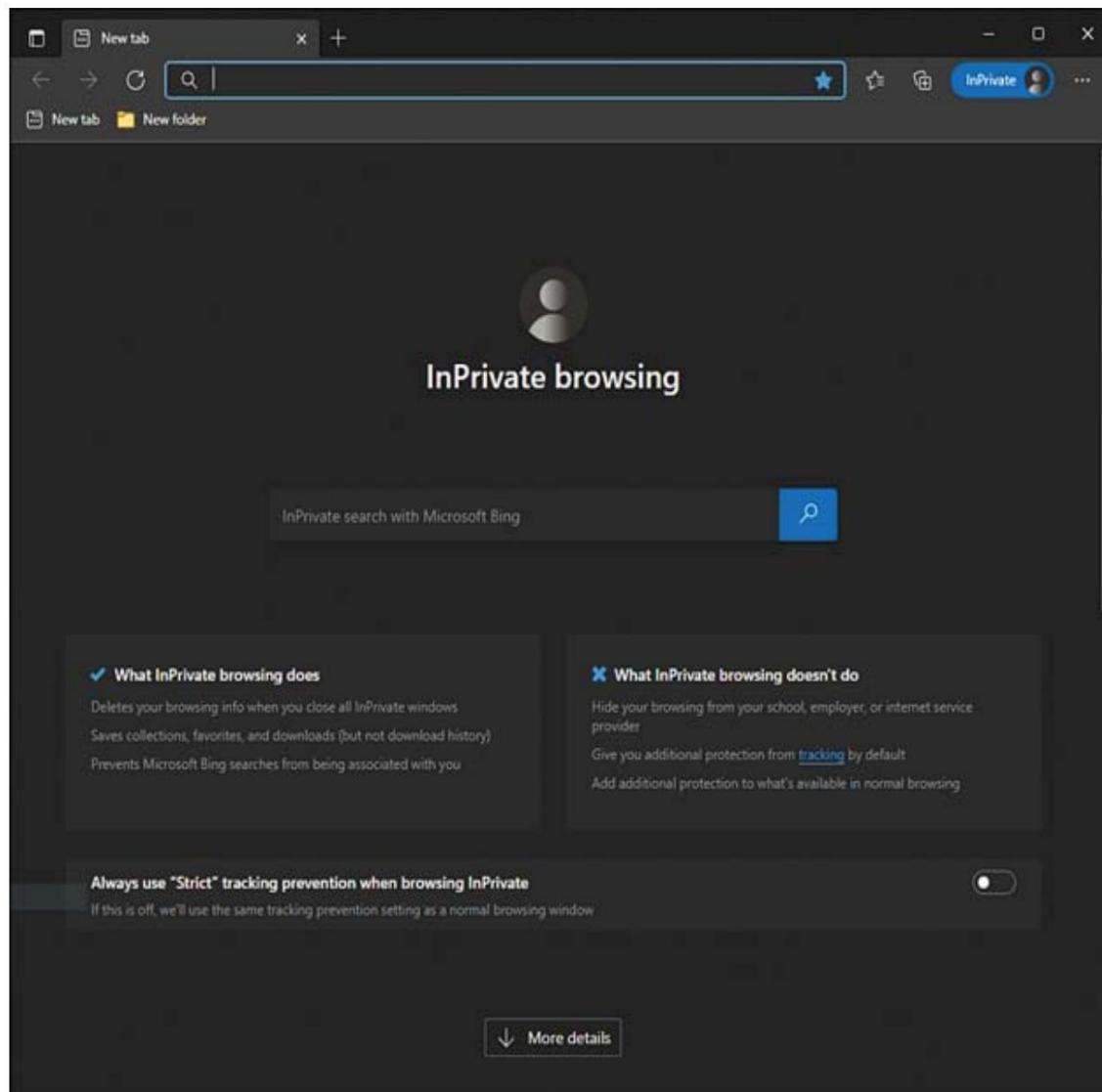


Figura 7-16 Navegação InPrivate no Microsoft Edge

Sincronização de dados de login/navegador

Como a maioria das pessoas acessa dados em vários dispositivos, incluindo desktops, laptops e dispositivos inteligentes, é extremamente importante que os dados sejam sincronizados em todos os dispositivos para que as mesmas informações estejam disponíveis. Nos velhos tempos da tecnologia, isso envolvia copiar um arquivo para a mídia e, em seguida, copiar esse arquivo para cada dispositivo para ter uma cópia atualizada. Atualmente, a *sincronização de dados do navegador* é um serviço em nuvem que quase todos os fornecedores de navegadores oferecem para compartilhar configurações e informações em todos os dispositivos. Contanto que você faça login com uma conta de usuário válida, seus dados serão sincronizados em todos os seus dispositivos.

Observação

Certifique-se de manter os dados de trabalho e os dados pessoais separados. Em alguns casos, uma sincronização de dados do navegador pode ser contra a política da empresa (por exemplo, se você sincronizar seu dispositivo pessoal com um sistema de trabalho). Sempre verifique a política de sua empresa antes de misturar configurações e dados pessoais com configurações e dados da empresa.

bloqueadores de anúncios

Um **bloqueador de anúncios** é uma ferramenta que se integra a um navegador da Web e usa filtragem para bloquear anúncios específicos. Os bloqueadores de anúncios auxiliam na privacidade online e ajudam a evitar anúncios infectados por spyware. A implementação de bloqueadores de anúncios é considerada uma boa prática de segurança. Na verdade, a NSA e a Agência de Segurança Cibernética e de Infraestrutura divulgaram recentemente importantes orientações recomendando o uso de bloqueadores de anúncios como uma importante medida de segurança.

Para ajustar as configurações do bloqueador de anúncios no Google Chrome, faça o seguinte depois de abrir o navegador Chrome:

Etapa 1. No canto superior direito, clique em **Mais (três pontos verticais) > Configurações**.

Etapa 2. Clique em **Privacidade e segurança > Configurações do site**.

Etapa 3. Clique em **Configurações de conteúdo adicionais > Anúncios**.

A Figura 7-17 exibe as configurações do bloqueador de anúncios no Google Chrome.

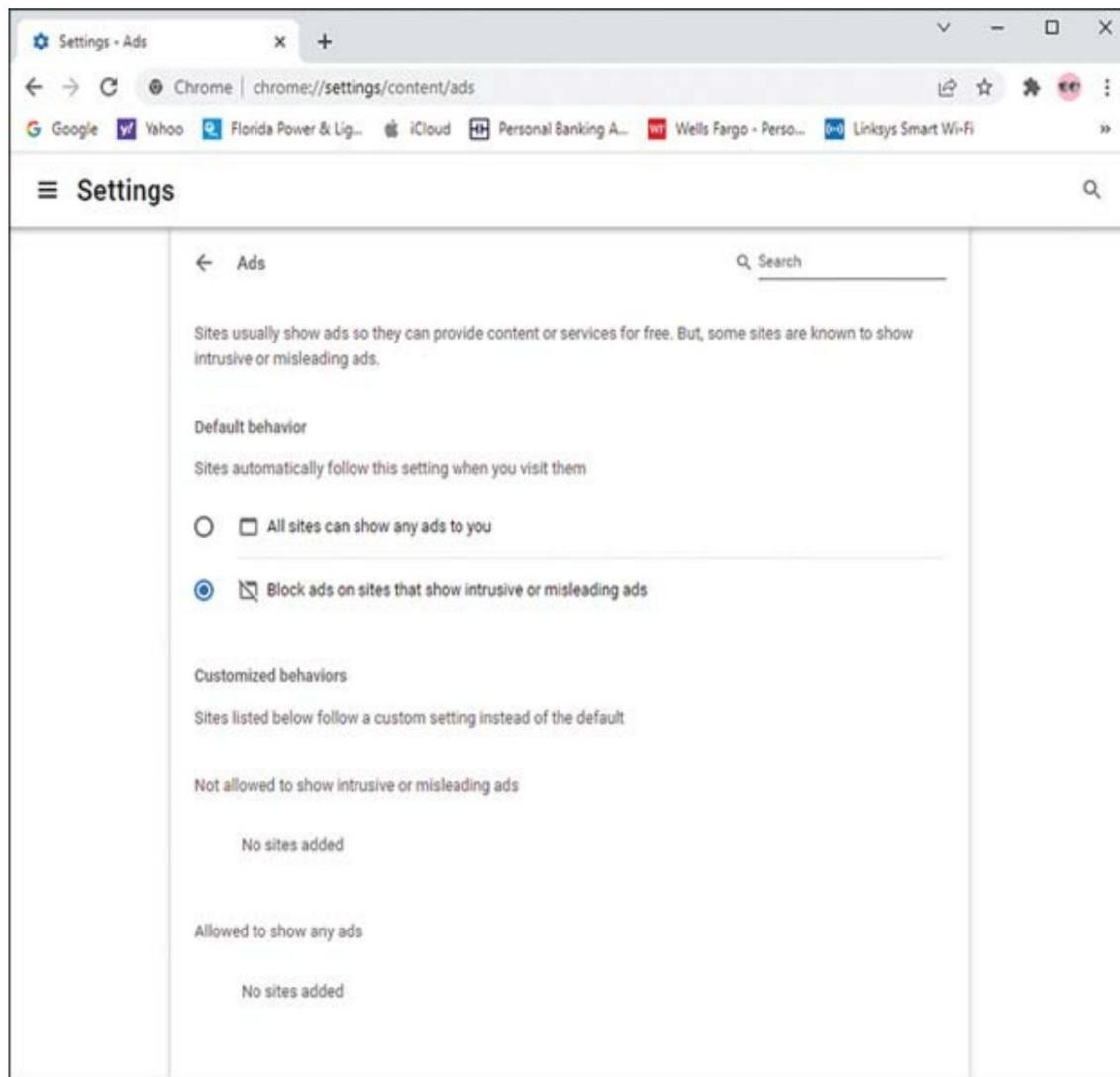


Figura 7-17 Configurações do bloqueador de anúncios no Google Chrome

Muitos (se não a maioria) programas de bloqueio de anúncios de terceiros são oferecidos gratuitamente. Por exemplo, o AdBlock é um complemento gratuito para o Microsoft Edge que bloqueia pop-ups, promoções de vídeo e outros anúncios que distraem.

Tarefas de preparação para exames

Conforme mencionado na Introdução, você tem várias opções para se preparar para o exame: os exercícios aqui; [Capítulo 10, “Preparação Final”](#); e as questões de simulação de exame no software de teste prático Pearson Test Prep.

Revise todos os tópicos principais

Revise os tópicos mais importantes do capítulo, indicados pelo ícone Tópico principal na margem externa da página. A [Tabela 7-3](#) lista esses tópicos-chave e os números das páginas em que cada um é encontrado.



Tabela 7-3 Tópicos-chave para o [Capítulo 7](#)

Tópico principal Elemento	Descrição	Página Número
Lista	Noções básicas do Active Directory	581
Lista	Protocolos sem fio e tipos de criptografia	582
Seção	Malware	584
Lista	Técnicas de proteção antivírus/antimalware	587
Seção	Ameaças de Engenharia Social e Vulnerabilidades	590
Lista	Firewalls do sistema operacional integrados	598
Seção	Arquivos e pastas compartilhados	603
Parágrafo	Logon único (SSO)	604
Degraus	Criptografando arquivos	607
Seção	Melhores práticas de senha	608
Seção	Gerenciamento de contas	612
Observação	Protegendo dispositivos móveis	615
Lista	Métodos de destruição física	621
Lista	Práticas recomendadas de reciclagem/reaproveitamento	622
Degraus	Atualizando o firmware do roteador SOHO	624

Tópico principal Elemento	Descrição	Página Número
Lista	Melhores práticas de segurança física em um ambiente de rede SOHO	625
Seção	Segurança específica sem fio	626
Tabela 7-2	Links de download de navegadores da Web confiáveis	630
Figura 7-16 Navegação InPrivate no Microsoft Edge		637

Definir termos-chave

Defina os seguintes termos-chave deste capítulo e verifique suas respostas no glossário:

[vestíbulo de controle de acesso](#)

postes de amarração

[cartões inteligentes](#)

[biometria](#)

[magnetômetros](#)

[princípio do privilégio mínimo lista](#)

[de controle de acesso \(ACL\)](#)

[autenticação multifator \(MFA\) hard token](#)

[token macio](#)

[gerenciamento de dispositivos móveis \(MDM\)](#)

[Active Directory](#)

[Protocolo de Integridade de Chave Temporal \(TKIP\)](#)

[Wi-Fi Protected Access 2 \(WPA2\)](#)

[Autenticação padrão de criptografia avançada \(AES\)](#)

[Wi-Fi Protected Access 2 \(WPA3\)](#)

[Serviço de usuário discado de autenticação remota \(RADIUS\)](#)

Sistema de controle de acesso do controlador de acesso ao terminal Plus (TACACS+)

Kerberos

malware

Trojan

rootkit

vírus

spyware

ransomware

vírus do setor

de inicialização do keylogger

criptomineradores

modo de

recuperação engenharia

social phishing vishing

caça às baleias

personificação do

ombro surfe não

autorizado lixeira

mergulho gêmeo do

mal

negação de serviço distribuído (DDoS) ataque

de negação de serviço (DoS) de dia zero

falsificação ataque no caminho ataque de

força bruta

ataque de dicionário

Injeção de Linguagem de Consulta Estruturada (SQL)

cross-site scripting (XSS)

Defender Antivírus

firewall

firewall de software
compartilhar permissões
Sistema de arquivos de nova tecnologia (NTFS)
Controle de conta de usuário (UAC)
logon único (SSO)
BitLocker
BitLocker para ir
Encrypting File System (EFS) criptografia
de dados em repouso antivírus de limpeza
remota

anti-malware
Certificação de desmagnetização
da Internet das Coisas (IoT) de
destruição/reciclagem
Filtros de
conteúdo de atualização
de firmware de filtragem de IP
Dynamic Host Configuration Protocol (DHCP) reserva endereço IP WAN estático

Sub-rede blindada Universal Plug and Play
(UPnP)
bloqueador de anúncio de hash de
mapeamento/encaminhamento de porta

Responder a perguntas de revisão

1. André estava atrasado para o trabalho e deixou seu crachá de segurança em seu carro.
Em vez de perder tempo voltando para o carro e correr o risco de se atrasar, ele esperou na porta externa e entrou atrás de outro funcionário. A outra funcionária não conhecia André e ficou irritada com ele por seguir tão de perto, então ela não permitiu que André a acompanhasse

a porta interna para trabalhar. Ele teve que voltar ao carro para pegar o distintivo. Quais conceitos de segurança estavam envolvidos nesse cenário? (Escolha duas.) **a.** Guarda de segurança **b.** Utilização não autorizada **c.** Vestíbulo de controle de acesso/mantrap **d.** surf de ombro

2. Alexa estava trabalhando em seu turno na sala do servidor quando um alarme disparou em um servidor que pertencia a um fornecedor de outra empresa. Ela não conseguiu acessar o botão de reinicialização no servidor. O que provavelmente a impediu de acessar o servidor cujo alarme estava disparando?

- a.** Falta de um chaveiro
- b.** Segurança em nível de rack
- c.** Falta de autenticação
- d.** Tela de privacidade

3. Associe o tipo de malware à sua descrição.

Descrição	Tipo de Malware
1. Infecta e regrava arquivos. Replica automaticamente, sem intervenção do usuário.	
2. Um método para ocultar malware de programas de detecção.	
3. Rastreia a navegação na web. Usa pop-ups para atrair a atenção do usuário.	
4. Criptografa os arquivos de destino e exige pagamento para descriptografar os arquivos.	
5. Infecta e regrava arquivos. Replica a si mesmo se um usuário executa o arquivo.	

Opções de resposta:

- a.** Spyware
- b.** Vírus

- c. Verme
 - d. Rootkit
 - e. ransomware
- 4.** Como profissional de TI, você deve certificar-se de empregar as melhores práticas de segurança. Qual das opções a seguir não é uma prática recomendada? **uma.**
Senhas fortes para contas de usuário **b.** Proteção antivírus/malware **c.** Alterar a senha padrão em um WAP **d.** criptografia WEP
- 5.** Qual das opções a seguir é geralmente a forma mais difícil de segurança para um hacker malicioso superar?
- uma.** Firewall
 - b.** Criptografia
 - c.** biometria
 - d.** Bloqueio físico e chave
- 6.** A biometria inclui o uso de qual dos seguintes? (Escolha tudo isso aplicar.)
- a.** Digitalização de impressão digital
 - b.** RFID
 - c.** Varredura de retina
 - d.** Símbolo
- 7.** Qual dos seguintes não é um tipo de token? **uma.**
Chaveiro **b.** Bloqueio de cabo
- c.** cartão RFID
 - d.** Cartão inteligente
- 8.** Qual dos seguintes é um programa que bloqueia ou permite que dados entrega de pacotes para endereços de rede?
- uma.** Servidor DHCP

- b.** Chaveiro
- c.** Firewall
- d.** servidor de rede

9. Qual das opções a seguir é uma característica de uma senha forte?

(Escolha todas as que se aplicam.)

- uma.** Não mais que seis caracteres
- b.** Somente letras
- minúsculas **c.** Uso de
- símbolos **d.** Uso de números

10. Mike foi chamado para uma estação de trabalho que estava funcionando lentamente. Depois de entrevistar o usuário e perguntar sobre a atividade recente, Mike determinou que o usuário abriu um e-mail falso e redefiniu sua senha. Em qual das opções a seguir o usuário provavelmente estava envolvido?

- uma.** Utilização
- não autorizada **b.**
- Mergulho no lixo **c.**
- Phishing **D.** surf de ombro

11. Fred determinou que a criptografia era a melhor solução para manter sua unidade flash USB segura enquanto viaja. Qual produto de segurança atende a essa necessidade?

- uma.** Consola de
- Recuperação **b.** Logon único (SSO)
- c.** BitLocker para ir
- d.** Bloqueio USB 3

12. Ellen trabalha em casa como contadora. Ela notou seu wireless rede lenta e se perguntou se seus vizinhos começaram a usar sua rede para streaming. Quais práticas de segurança ela pode empregar para garantir que seus vizinhos não tenham acesso à sua rede e que os arquivos de seus clientes sejam protegidos? (Escolha dois.)

uma. Alterar o endereço IP padrão no gateway padrão **b.** Mude o nome da rede e desabilite a transmissão SSID **c.** Usar filtragem de endereço MAC **d.** Alterar a senha do Netflix

13. Jen foi incumbida de reaproveitar laptops usados pelo departamento de recursos humanos. O que ela pode fazer para garantir que informações pessoais importantes não sejam comprometidas?

- uma.** Sobrescrever
- b.** Formato de baixo nível
- c.** Formato padrão
- d.** Limpeza de unidade

14. Hiro consegue fazer login em sua conta no trabalho, mas não consegue ver o trabalho que sua equipe está fazendo para um cliente de publicidade. Ele não teve nenhum problema antes de sair de férias. Qual é uma explicação razoável para esse problema? **uma.** As permissões de compartilhamento foram atualizadas enquanto ele estava fora. **b.** Hiro foi bloqueado devido a inatividade **c.** Hiro levou três tentativas para fazer login em seu computador e suas permissões foram suspensas após a segunda tentativa. **d.** O chefe pensou que Hiro estava saindo da empresa, então sua conta foi desativada.

15. Qual dos seguintes é usado para verificar se o conteúdo dos arquivos é inalterado?

- uma.** Fontes confiáveis
- b.** Hashing **c.** Bloqueadores de pop-up **d.** Modo de navegação privada

Capítulo 8

Solução de problemas de software

Este capítulo aborda os cinco objetivos do exame A+ 220-1102 relacionados à solução de problemas do sistema operacional Microsoft Windows, segurança do PC, remoção de malware, sistema operacional móvel e problemas operacionais e de segurança de aplicativos e tópicos relacionados. Esses objetivos podem abranger 22% das questões do exame:

- **Núcleo 2 (220-1102): Objetivo 3.1:** Dado um cenário, solucionar problemas comuns do sistema operacional Windows.
- **Núcleo 2 (220-1102): Objetivo 3.2:** Dado um cenário, solucionar problemas comuns de segurança de computadores pessoais (PC).
- **Núcleo 2 (220-1102): Objetivo 3.3:** Dado um cenário, use procedimentos de práticas recomendadas para remoção de malware.
- **Núcleo 2 (220-1102): Objetivo 3.4:** Dado um cenário, solucionar problemas comuns de sistemas operacionais móveis e aplicativos.
- **Núcleo 2 (220-1102): Objetivo 3.5:** Dado um cenário, solucionar problemas comuns de sistema operacional móvel e segurança de aplicativos.

Dado o uso generalizado de dispositivos móveis, a solução de problemas agora é mais do que apenas resolver problemas com computadores. No entanto, muitos dos mesmos princípios se aplicam, seja na solução de problemas com computadores, periféricos ou dispositivos móveis: conhecimento de produtos e funções do sistema operacional, compreensão das ferramentas necessárias para diagnosticar e reparar problemas e determinação para evitar a perda de dados, exceto quando inevitável . Este capítulo ajuda você a aplicar esses princípios.

“Eu já sei disso?” Questionário

O "Eu já sei disso?" questionário permite avaliar se você precisa ler o capítulo inteiro. A [Tabela 8-1](#) lista os principais títulos deste capítulo e a seção "Eu já sei disso?" perguntas do questionário que cobrem o material desses títulos para que você possa avaliar seu conhecimento nessas áreas específicas. As respostas para a pergunta "Eu já sei disso?" questionário aparecem no Apêndice A, "Respostas para a pergunta 'Eu já sei disso?' Questionários e perguntas de revisão.

Tabela 8-1 "Eu já sei disso?" Mapeamento de seção para pergunta

Seção de Tópicos Fundamentais	Perguntas
Solução de problemas comuns do sistema operacional Windows	1–3
Solução de problemas comuns de segurança do PC	4–6
Procedimentos de melhores práticas para remoção de malware	7
Solucionar problemas comuns de sistemas operacionais móveis e aplicativos	8–9
Solucionar problemas de aplicativos e sistemas operacionais móveis comuns	10
Problemas de segurança	

CUIDADO

O objetivo da autoavaliação é avaliar seu domínio dos tópicos deste capítulo. Se você não souber a resposta a uma pergunta ou tiver certeza apenas parcial da resposta, marque essa pergunta como errada para fins de autoavaliação. Dar a si mesmo crédito por uma resposta que você adivinhou corretamente distorce os resultados de sua autoavaliação e pode lhe dar uma falsa sensação de segurança.

- Kate está tendo acesso inconsistente à web; às vezes o acesso dela fica inativo por alguns minutos de cada vez. Ela não perde a conexão com sua rede local, mas não consegue navegar. Quais configurações do sistema ela pode verificar para ver sua rede local e status da Internet?

a. Conexões de rede

b. Atualização da Internet

- c. Status da rede
 - d. Ethernet
- 2. Qual mensagem pode indicar que um hardware incompatível está instalado ou que há problemas de registro durante a sequência de inicialização?
 - uma.** Um erro BSOD
 - b. Uma mensagem “Wirefault” durante a inicialização **c.** Um X vermelho na barra de tarefas
 - d. Uma mensagem “Rede não encontrada”
- 3. Qual das seguintes opções deve ser considerada quando um aviso mostra que o computador está com pouca memória? (Escolha todas as que se aplicam.)
 - a. A quantidade de RAM
 - b. Trocar configurações de arquivo/arquivo de página
 - c. Alterar as configurações de memória virtual
 - d. Verificando recursos no Gerenciador de Tarefas
- 4. Que tipo de malware pode alterar as configurações da página inicial? **uma.** Pop-ups
 - b. Redirecionamento do navegador
 - c. WannaCry **d.** Janelas abrindo rapidamente
- 5. Qual aviso destina-se a impedir o uso de aplicativos fraudulentos fonte?
 - uma.** Certificado
 - b. Atualização do sistema
 - c. Nem A nem B
 - d. Ambos a e B
- 6. Qual é o objetivo principal de um programa antivírus inicializável?
 - uma.** Ele permite a verificação contínua de malware.
 - b. Ele pode executar varreduras sem um sistema operacional.

- c.** Ele verifica o BIOS/UEFI em busca de vírus.
d. Ele verifica o sistema operacional enquanto ele carrega.
- 7.** Qual é a segunda etapa nos procedimentos de melhores práticas para remover malware?
- uma.** Identifique os sintomas.
b. Desative a Restauração do sistema no Windows.
c. Sistemas infectados em quarentena. **d.** Atualize o software antimalware.
- 8.** Ivan está tentando transmitir música em seu celular, mas seu aplicativo habitual não está trabalhando. Qual deve ser o *primeiro* passo dele?
- uma.** Mantenha o dedo no ícone do aplicativo até que ele mexa e, em seguida, exclua isto.
b. Reinicie o telefone. **c.** Desligue o telefone. **d.** Atualize o aplicativo.
- 9.** Lorna gosta de transmitir programas de TV em seu telefone enquanto está no ônibus. Um dia, seu serviço fica lento e ela não consegue assistir aos programas. Por que o telefone de Lorna pode ficar tão lento?
- uma.** Lorna mudou a rota do ônibus e agora segue um caminho diferente para trabalhos.
b. Lorna assistiu tanto à TV este mês que seu provedor reduziu sua taxa de dados.
c. Lorna esqueceu de pagar a conta. **d.** A operadora de telefonia de Lorna fundiu-se com uma empresa de TV a cabo, e essa empresa decidiu mudar seu serviço.
- 10.** Eric deseja personalizar a experiência do usuário de seu telefone além do que sua companhia telefônica oferece. O que ele deve fazer para fazer essas alterações no sistema operacional?
- uma.** Eric deve baixar um malware especial para seu telefone. **b.** Eric deve solicitar atualizações especiais do provedor de celular.

- c. Eric não pode fazer isso; é ilegal. d. Eric deve fazer o jailbreak de seu telefone.

Tópicos Fundamentais

Solução de problemas comuns do sistema operacional Windows



220-1102: Objetivo 3.1: Dado um cenário, solucionar problemas comuns do sistema operacional Windows.

A solução de problemas é uma habilidade essencial para um técnico de PC. A capacidade de reconhecer e corrigir problemas do sistema operacional começa com os conceitos abordados nesta seção.

Sintomas comuns O sistema

operacional Windows possui inúmeras linhas de código e vários processos funcionando simultaneamente. Ocasionalmente, alguns processos falham e causam problemas para todo o sistema. O desempenho é afetado de várias maneiras possíveis, desde desempenho lento até travamentos do sistema. Esta seção apresenta alguns dos problemas mais comuns do sistema operacional e informa como eles podem ser reconhecidos.

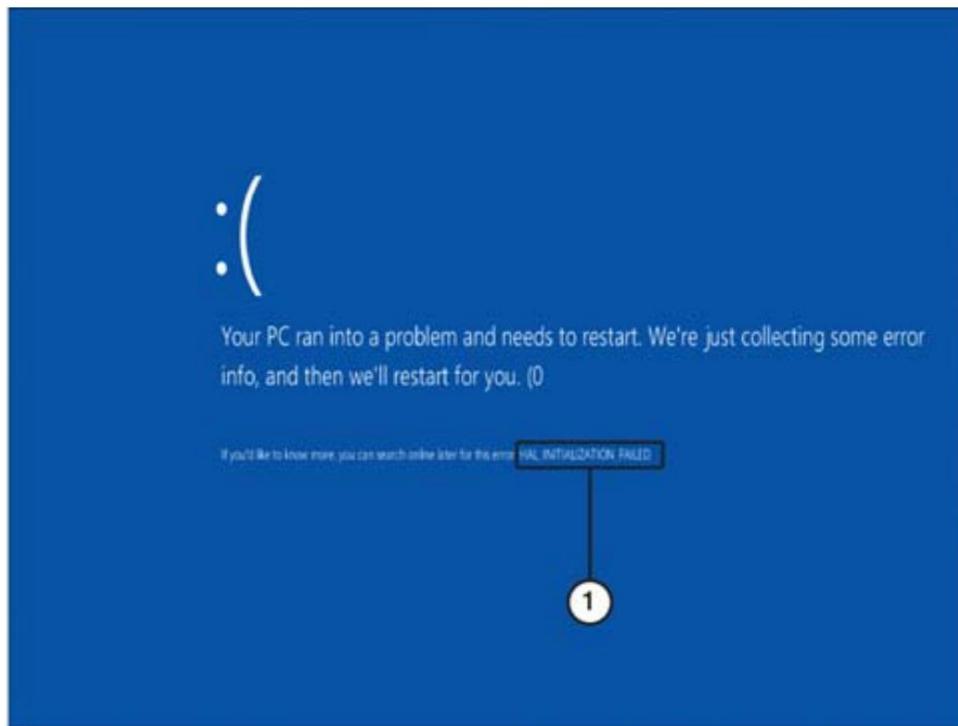
BSOD

Telas de falha proprietárias, como o erro STOP do Windows ([tela azul da morte \[BSOD\]](#)) podem ser causadas por erros de sistema operacional, aplicativo ou hardware.

Se o Windows estiver configurado para reiniciar quando ocorrer um erro STOP, o sistema reiniciará continuamente até que o erro seja resolvido. Para deixar uma mensagem de erro STOP na tela até que você decida reiniciar o sistema, desmarque a caixa de seleção Reiniciar automaticamente na configuração Falha do sistema no menu Iniciar.

e seção Recuperação das Propriedades Avançadas do Sistema. Isso é acessado através do Painel de controle > Sistema > Configurações avançadas do sistema. Em Inicialização e Recuperação, selecione Configurações. Mais detalhes e representações disso são destacados no Capítulo 5, “Solução de problemas de hardware e rede”.

No Windows 10, os erros STOP se parecem com o exemplo da Figura 8-1. O erro STOP é listado por nome.



1. STOP error message

Figura 8-1 Um erro STOP do Windows 10

Observação

Independentemente de quando ocorre um erro STOP/BSOD, seu sistema é interrompido por padrão. Se o computador não reiniciar sozinho, você deve desligar o sistema e ligá-lo novamente. Antes de fazer isso, no entanto, registre o texto da mensagem de erro e outras informações para que você possa pesquisar o problema se ele ocorrer novamente. Para obter mais informações, consulte a próxima seção, “Causas de erros BSOD”.

Causas de erros BSOD

Erros BSOD podem ser causados por qualquer um dos seguintes:



- **Hardware ou software incompatível ou com defeito:** Inicie o sistema no *modo* de segurança e desinstale o último hardware ou software instalado.
Adquira atualizações antes de reinstalar o hardware ou software.
Troque ou teste a memória. Execute SFC/scannow para verificar problemas com arquivos do sistema operacional.
- **Problemas de registro:** a *Restauração do sistema* também pode ser usada para reverter o sistema e o registro para um estado anterior.
- **Vírus:** Verifique se há vírus e remova qualquer um que seja descoberto.
- **Causas diversas:** verifique o Visualizador de eventos do Windows e também o log do sistema. Pesquise o BSOD no site de suporte da Microsoft.

Pesquisando causas e soluções de BSOD

Para determinar a causa exata de um erro STOP, anote o número ou o nome do erro (por exemplo, “STOP 0x0000007B, HAL INITIALIZATION FAILED”) e consulte o site de suporte da Microsoft: <https://support.microsoft.com>. Ao procurar o erro, certifique-se de especificar a versão do Windows em uso.

Observação

Os erros STOP geralmente são referidos com uma versão abreviada do código de erro ou pelo nome. Por exemplo, a versão abreviada de um erro 0x0000007B é 0x7B.

GORJETA

Infelizmente, você não pode fazer uma captura de tela de um BSOD para impressão porque um BSOD desliga completamente o Windows. Nessa situação, uma câmera digital ou smartphone pode ser usado para registrar a mensagem de erro exata.

A solução pode envolver uma ou mais das seguintes alterações em seu sistema:



- Alteração do registro do sistema. Às vezes, você pode baixar uma ferramenta automatizada de reparo do registro para executar essas alterações para você. Quer você faça as alterações manualmente ou automaticamente, faça backup do registro primeiro.
- Removendo um componente recém-adicionado.
- Substituir componentes como memória.
- Atualizando um aplicativo.

Desempenho Lento

Um sistema lento ou desempenho lento pode ser causado por muitos problemas no Windows. A [Tabela 8-2](#) lista algumas possíveis causas e soluções.



Tabela 8-2 Causas e soluções de desempenho lento/lento do sistema

Solução de problemas de desempenho do sistema Windows

Problema	Solução
O sistema não está configurado para desempenho máximo	Para resolver esse problema, defina a configuração de energia para alto desempenho usando o ícone de opções de energia na área de notificação ou as opções de energia no painel de controle. Esta opção não está disponível em tablets.

Solução de problemas de desempenho do sistema Windows

Problema	Solução
Unidade	Use a Limpeza de disco nas propriedades da unidade para remover arquivos indesejados, desfragmente a unidade e Se este não é rápido o suficiente para arquivos de paginação em uma unidade diferente, use a ferramenta de alocação de espaço que move páginas de paginação para temporários. para fragmentado
O sistema está superaquecendo e a CPU está funcionando em velocidade reduzida	Remova poeira e sujeira da CPU e dos ventiladores do sistema. Verifique se há fluxo de ar adequado através do sistema. Mude de volta para a configuração de energia balanceada.
A memória está baixa	Adicionar RAM; isso corrige muitos problemas de desempenho. Para melhor desempenho, exceda os mínimos recomendados para a versão do Windows em uso.
Ocorre queda repentina de desempenho	Verifique se há vírus e malware; isso é especialmente importante se o desempenho cair repentinamente.
Mensagens de erro do registro aparecem	O programa CCleaner é amplamente utilizado para esta tarefa.

Problemas de Inicialização

Problemas de inicialização, como falha na inicialização, podem ser causados por vários problemas, incluindo configuração incorreta da ordem de inicialização no BIOS/UEFI, arquivos de inicialização corrompidos ou ausentes, arquivos de driver ausentes ou até mesmo falha na bateria do CMOS.

O Windows usa os arquivos bootmgr e BCD durante o processo de inicialização. Se esses arquivos estiverem corrompidos ou ausentes, as mensagens de erro correspondentes serão exibidas:

- **bootmgr está faltando:** Esta mensagem aparece se o arquivo bootmgr estiver ausente ou corrompido. Essa tela preta provavelmente também incluirá a mensagem “Pressione Ctrl+Alt+Del para reiniciar”; no entanto, isso provavelmente não resolverá o problema.
- **Faltam informações necessárias no arquivo de dados de configuração de inicialização do Windows:** esta mensagem significa que a entrada do Gerenciador de inicialização do Windows (bootmgr) não está presente no armazenamento de dados de configuração de inicialização (BCD) ou que o arquivo Boot\BCD na partição ativa está danificado ou ausência de. As informações adicionais que você pode ver na tela incluem Arquivo: \Boot\BCD e Status: 0xc0000034.

Um arquivo bootmgr ausente pode ser reparado de duas maneiras:

- Inicialize com as opções de Recuperação do Sistema e selecione a opção Reparo de Inicialização. Isso deve reparar o sistema automaticamente e exigir a reinicialização. Para acessar as opções no Windows 10, localize o menu Configurações avançadas de inicialização.
- Inicialize nas opções de Recuperação do sistema e selecione a opção Prompt de comando. Digite o comando **bootrec /fixboot**, conforme mostrado na [Figura 8-2](#).

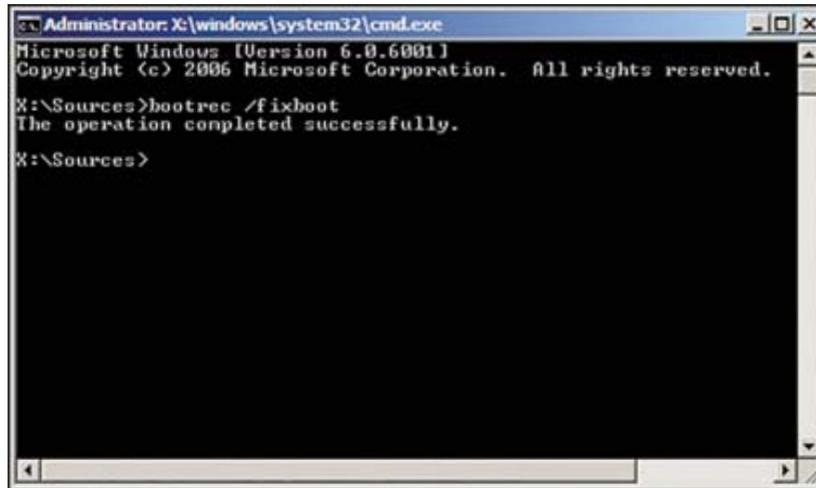


Figura 8-2 Reparando o BOOTMGR.exe no Prompt de Comando do Ambiente de Recuperação do Windows

Para saber mais sobre essas etapas, consulte <https://support.microsoft.com/en-us/kb/2622803>.

Para reparar o armazenamento BCD, use este processo curto:

Etapa 1. Inicialize nas opções de Recuperação do sistema e selecione a **opção Iniciar**

Opção de **reparo**. O Windows deve reparar automaticamente o sistema e exigir que você reinicie. Se não, vá para a segunda etapa.

Etapa 2. Inicialize nas opções de Recuperação do sistema e selecione a opção **Prompt de comando**. Digite **bootrec /rebuildbcd**. uma. Se a ferramenta Bootrec.exe for

executada com sucesso, o Windows apresentará

você com um caminho de instalação para um diretório do Windows. Para adicionar a entrada ao armazenamento BCD, digite **Sim**. Uma mensagem de confirmação é exibida, indicando que a entrada foi adicionada com sucesso.

Reinic peace o sistema.

- b.** Se a ferramenta Bootrec.exe não conseguir localizar nenhuma instalação ausente do Windows, você deverá remover o armazenamento BCD e criá-lo novamente. Para fazer isso, digite os seguintes comandos na ordem mostrada aqui e pressione Enter após cada comando:

[Clique aqui para ver a imagem do código](#)

```
Bcdedit /export C:\BCD_Backup ren c:  
\boot\bcd bcd.old  
Bootrec /rebuildbcd
```

Desligamentos frequentes

As reinicializações contínuas podem ser causadas por problemas com a fonte de alimentação ou por uma configuração do Windows ou de outro sistema operacional:

Quando a linha Power Good para a placa-mãe transporta uma tensão muito alta ou muito baixa, o processador é reinicializado, desligando o sistema e reiniciando-o. Teste os níveis de tensão da fonte de alimentação; substitua a fonte de alimentação se os testes de energia boa estiverem fora das especificações.

Falhas intermitentes de outros dispositivos externos USB ou de dispositivos internos podem ser causadas por cabos de dados, fontes de alimentação, conectores ou portas danificados.

Para solucionar esses problemas, siga estas etapas:

Etapa 1. Desligue o dispositivo (e o computador, se o dispositivo for interno) e substitua o cabo de dados por um substituto que esteja funcionando. Se um dispositivo USB estiver conectado a uma porta USB frontal ou a uma porta USB em um suporte de placa, verifique as conexões do cabo de cabeçalho USB na placa-mãe.

Etapa 2. Ligue o dispositivo ou computador.

Etapa 3. Teste o dispositivo ao longo do tempo. Se o dispositivo funcionar corretamente, o problema está resolvido.

Etapa 4. Se as etapas 1 a 3 não resolverem o problema, use os dados originais cabo e tente conectá-lo a uma porta interna ou externa diferente.
Repita as etapas 2–3.

Etapa 5. Tente as etapas de 1 a 4 novamente, mas desta vez use um conector de alimentação ou adaptador CA de substituição.

Passo 6. Quando você encontrar o componente defeituoso, o problema cessará. Se o problema não for resolvido com diferentes cabos de dados, conectores ou fontes de alimentação/adaptadores CA, o próprio dispositivo precisará ser substituído.

Desligamentos intermitentes ou frequentes geralmente são um problema de software. A atualização de drivers é uma solução confiável. Verifique também as configurações do modo de hibernação no Windows 10 para garantir que o computador não vá simplesmente hibernar.

Serviços não iniciando

Lembre-se de que os serviços são os vários aplicativos em segundo plano executados no Windows que executam as tarefas menores que mantêm o Windows 10 em execução.

Dezenas de serviços são executados no Windows 10, incluindo serviços ainda mais estendidos que oferecem suporte aos serviços do Windows. De vez em quando, um desses serviços pode falhar ao carregar durante a inicialização. Um motivo comum é que há tantos serviços em execução que um serviço que não seja do Windows interrompe um serviço do Windows durante o processo de inicialização. Para visualizar os serviços disponíveis, vá para a caixa de comando Executar (Windows+R) e digite **services.msc**.

No menu Serviços, selecione o serviço que está apresentando problemas e verifique seu status. Se estiver desativado, clique com o botão direito do mouse no serviço e clique em Iniciar para ativá-lo. A [Figura 8-3](#) mostra que o serviço de Compartilhamento de Dados nos Serviços

console está desabilitado. Clicar em Iniciar na guia Geral deve ativá-lo; caso contrário, a guia Recuperação (consulte a [Figura 8-3](#)) oferece mais opções para reiniciar o serviço. Essas opções estão disponíveis clicando com o botão direito do mouse no serviço e selecionando Propriedades.

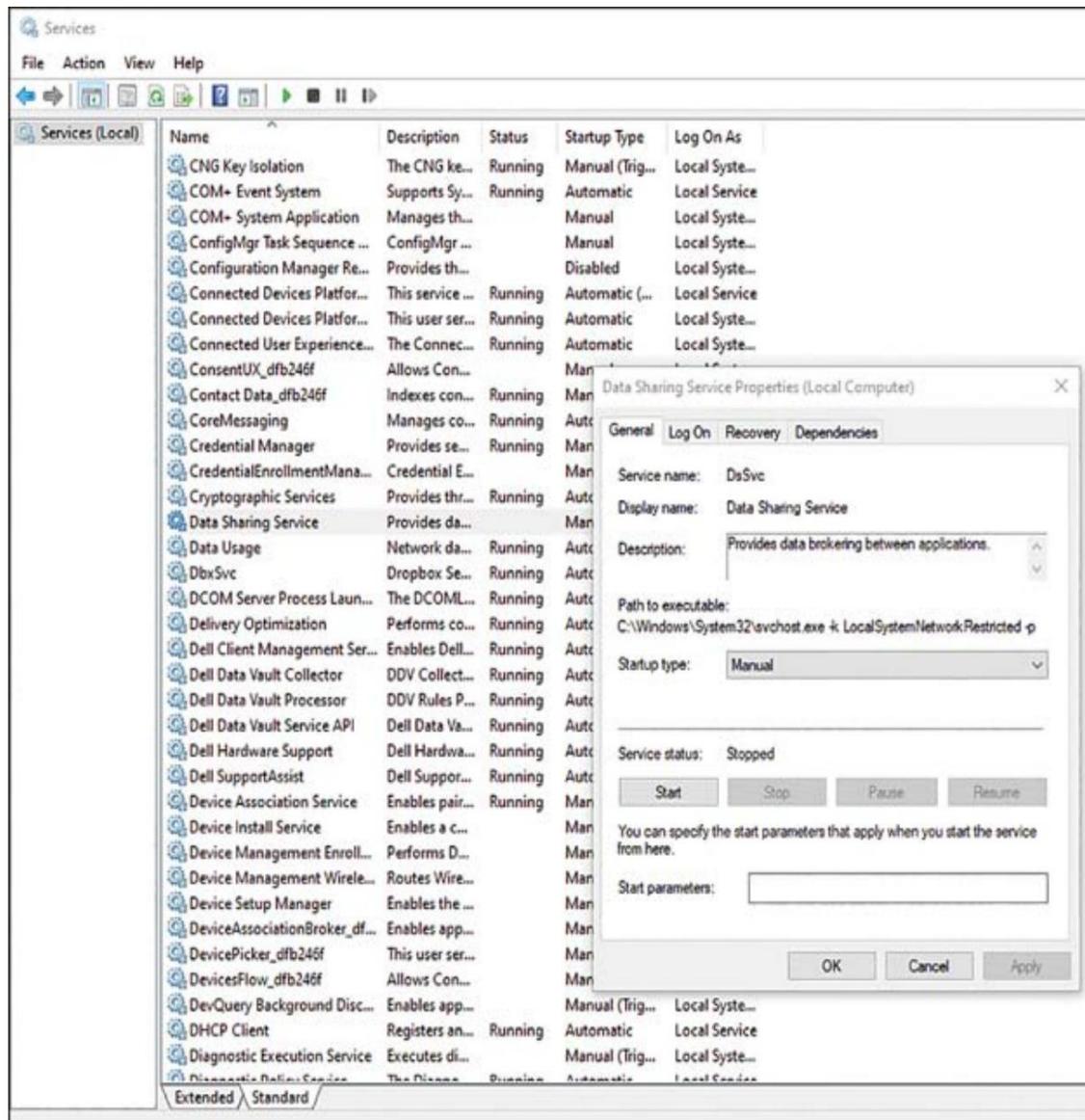


Figura 8-3 Gerente de Serviços

Outras abordagens possíveis incluem o uso do Windows Recovery (WinRE) no menu de configuração avançada. (Isso funciona no Windows 10 e 11.) Três maneiras possíveis de acessar o WinRE são as seguintes:

- Na tela de login, clique em Desligar; em seguida, mantenha pressionada a tecla Shift enquanto seleciona Reiniciar.
- Clique em **Iniciar > Configurações > Atualização e segurança > Recuperação**. Em Inicialização avançada, clique em Reiniciar agora.
- Initialize na mídia de recuperação.

Outra opção é inicializar no modo de segurança e solucionar problemas dos serviços.

Se os problemas persistirem, tente executar o Verificador de arquivos do sistema (em um modo elevado) e reinicie.

A Restauração do sistema (**Configurações > Windows Update > Opções avançadas**) pode ser usada se os esforços anteriores falharem. Um último recurso é redefinir o PC (**Configurações > Atualização e segurança > Recuperação**).

Falhas no aplicativo

Os aplicativos podem se comportar mal ou travar por vários motivos. Os aplicativos são escritos para funcionar com o software do sistema operacional, e aplicativos bem escritos raramente apresentam problemas nesse ambiente. Tenha em mente, no entanto, que o software do sistema operacional está sendo constantemente atualizado por motivos de segurança e outros, e geralmente ocorre um atraso entre o sistema operacional e as revisões do aplicativo. Durante esse atraso de atualização, muitas possibilidades podem dar errado.

A Microsoft está constantemente atualizando o Windows 10 com códigos e patches que funcionam com aplicativos específicos. Esses patches não são necessariamente instalados automaticamente. Você pode personalizar essas atualizações nas configurações do Windows Update. Para acessar essas configurações no Windows 10, vá para **Iniciar > Configurações > Atualização e segurança**. Se necessário, a guia Opções avançadas está disponível.

Também disponível na página Atualização e segurança em Configurações está a ferramenta Solução de problemas, que oferece uma maneira de o Windows 10 autodiagnosticar e reparar problemas.

Para acessar essas configurações no Windows 10, vá para **Iniciar > Configurações > Atualização e segurança > Solução de problemas**. As opções para gerenciar como executar a solução de problemas automaticamente estão disponíveis na lista suspensa.

Se você encontrar erros de aplicativo, verifique também com os desenvolvedores do aplicativo se há atualizações disponíveis. Os “patches” de software são pequenas atualizações que podem corrigir problemas conhecidos até que uma atualização de versão completa esteja disponível. Se os patches não estiverem disponíveis e o software for essencial para os negócios, talvez seja necessário reverter a atualização do sistema operacional para melhorar o desempenho. Claro, as atualizações acontecem por um motivo; se surgirem problemas de segurança ao reverter uma atualização, resolva-os de outra forma, se possível.

Drivers para dispositivos periféricos e placas de vídeo e gráficas podem ser outra fonte de problemas de aplicativos. As atualizações do Windows geralmente incluem os drivers, mas os fabricantes também os possuem. Desinstalar um driver e substituí-lo geralmente pode resolver um problema.

Avisos de pouca memória

Se o Windows emitir um aviso informando “Seu computador está com pouca memória”, a causa provável é que não existem recursos de memória suficientes para todas as tarefas que o computador está tentando executar. O computador pode estar com poucos recursos (consulte o [Capítulo 3, “Hardware”](#), para saber mais sobre como adicionar RAM) ou algum aplicativo (ou até mesmo um vírus) pode estar exigindo mais capacidade de processamento do que deveria. A [Figura 8-4](#) descreve as etapas a seguir que tratam dos avisos de pouca memória ajustando a memória virtual alocada.

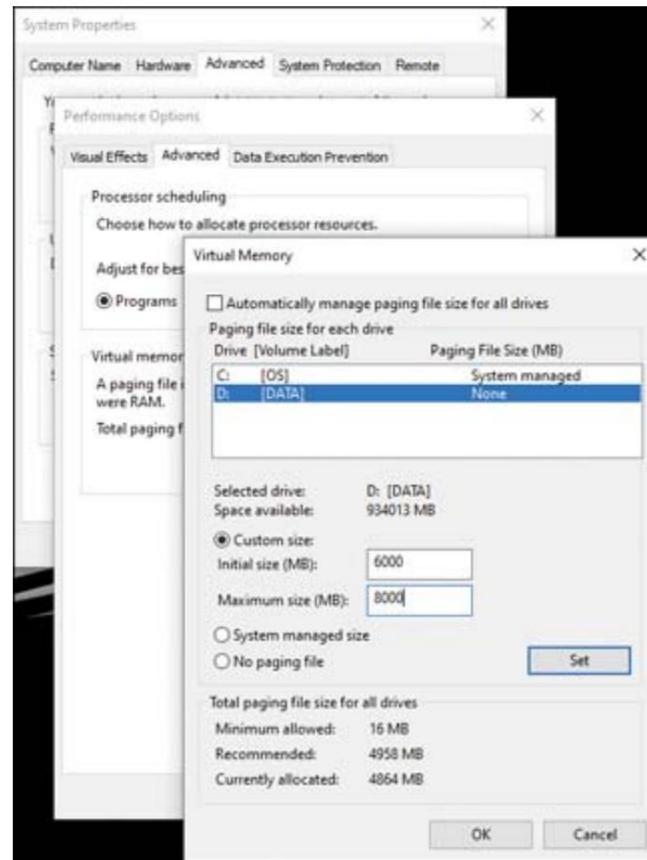


Figura 8-4 Memória virtual

A primeira etapa para lidar com esse aviso é visitar o Gerenciador de Tarefas e ver onde os recursos estão sendo alocados. Se aplicativos não utilizados ou desnecessários estiverem abertos e exigirem espaço de memória e tempo de CPU, desligue-os para liberar recursos. À medida que os aplicativos são fechados, mais memória fica disponível. Se um aplicativo não reconhecido estiver usando memória, pesquise o aplicativo ou serviço para ver se é necessário. Se nenhuma informação estiver disponível, a verificação de vírus ou **malware** é uma boa ideia.

Outra opção é aumentar a memória virtual, o que significa atribuir algum espaço no disco rígido para funcionar como RAM.

Para aumentar a memória virtual, siga estas etapas:

Etapa 1. Pressione Windows+X e selecione **Sistema**.

Etapa 2. Selecione **Configurações avançadas do sistema**. Isso abre a página Propriedades do sistema.

Etapa 3. Selecione a guia **Avançado** e escolha **Configurações** sob o Guia Desempenho para abrir a janela Opções de desempenho.

Etapa 4. Escolha a guia **Avançado** e selecione **Alterar** em Memória virtual para acessar as configurações de alocação.

Controlador USB

O aviso “Not Enough USB Controller Resources” indica que muitos dispositivos USB (ou, mais provavelmente, hubs) estão tentando acessar um número limitado de terminais no controlador USB. Isso é mais comum em dispositivos USB 3.0 do que em dispositivos USB 2.0 porque, em termos bastante simplificados, o USB 3.0 pode exigir mais recursos.

Veja a seguir soluções rápidas para esse problema:

- Desconecte hubs ou dispositivos desnecessários do computador para liberar terminais no controlador.
- Se possível, mova alguns dispositivos ou hubs externos das portas USB 3.0 para USB 2.0 (ou simplesmente use um cabo USB 2.0 do computador para um hub USB). Isso deve liberar algum acesso ao controlador.
- Adicione um controlador de host USB em um slot PCIe.
- Reinstale os controladores host de barramento serial universal.

Para saber mais sobre como reinstalar os controladores de host USB, consulte <https://thegeekpage.com/not-enough-usb-controller-resources/fix>.

Para solucionar problemas de USB, siga estas etapas:

Etapa 1. Desligue o dispositivo (e o computador, se o dispositivo for interno) e substitua o cabo de dados por um substituto que esteja funcionando. Se um dispositivo USB estiver conectado a uma porta USB frontal ou a uma porta USB em um suporte de placa, verifique as conexões do cabo de cabeçalho USB na placa-mãe.

Etapa 2. Ligue o dispositivo ou computador.

Etapa 3. Teste o dispositivo ao longo do tempo. Se o dispositivo funcionar corretamente, o problema está resolvido.

Etapa 4. Se as etapas 1 a 3 não resolverem o problema, use os dados originais cabo e tente conectá-lo a uma porta interna ou externa diferente.
Repita as etapas 2–3.

Etapa 5. Tente as etapas de 1 a 4 novamente, mas desta vez use um conector de alimentação ou adaptador CA de substituição.

Passo 6. Quando você encontrar o componente defeituoso, o problema cessará. Se o problema não for resolvido com diferentes cabos de dados, conectores ou fontes de alimentação/adaptadores CA, o próprio dispositivo precisará ser substituído.

Instabilidade do sistema

Os problemas subjacentes que causam instabilidade do sistema podem ser os mesmos ou semelhantes aos problemas mencionados nas seções anteriores. No entanto, se o PC estiver lento ou intermitentemente lento e se RAM adicional (ou gerenciamento de arquivo de paginação), gerenciamento de programa de inicialização e atualizações não resolverem o problema, você poderá executar mais algumas etapas:

- Libere espaço em disco em Configurações de armazenamento (**Configurações > Sistema > Armazenamento**).
- Pausar a sincronização. A sincronização do OneDrive, Dropbox ou outro armazenamento em nuvem pode consumir recursos intermitentemente, causando tráfego lento e carregamento lento de aplicativos. Tente pausar temporariamente a sincronização e verifique a melhoria do desempenho.
- Verifique/verifique se há problemas de vírus ou malware.
- Atualizações e alterações recentes podem ser o problema. Restaurar a partir de um ponto de restauração do sistema pode remover programas problemáticos sem remover seus arquivos pessoais.

Nenhum sistema operacional encontrado

Se um sistema operacional não puder ser localizado, inicialize no BIOS/UEFI e verifique se o computador está procurando o SO no local correto. A unidade que hospeda o sistema operacional deve estar na primeira opção para inicializar.

Cabos soltos são outro problema comum que pode causar falhas na inicialização. Se as configurações da opção de inicialização estiverem corretas no BIOS/UEFI, verifique os cabos;

às vezes, os cabos parecem conectados, mas não estão encaixados corretamente.

Redefinir o BIOS/UEFI também é uma opção. O menu BIOS-UEFI tem opções para restaurar os padrões.

Carregamento Lento do Perfil

Um perfil de usuário contém configurações personalizadas para dispositivos como mouse e teclado, aplicativos baseados no Windows e arquivos e configurações da área de trabalho.

Às vezes, um usuário percebe que um perfil carrega muito mais lentamente do que outros perfis.

Um motivo para um perfil de carregamento lento é que muitos arquivos e pastas grandes são armazenados na área de trabalho e precisam ser carregados como parte do perfil.

Armazenar esses arquivos grandes em Meu computador ou em outra unidade reduz o tempo de carregamento.

Para verificar o tamanho de um perfil de usuário, use a caixa de diálogo Executar ou a ferramenta de pesquisa e digite **sysdm.cpl**. Isso abre o menu Propriedades do sistema na [Figura 8-5](#).

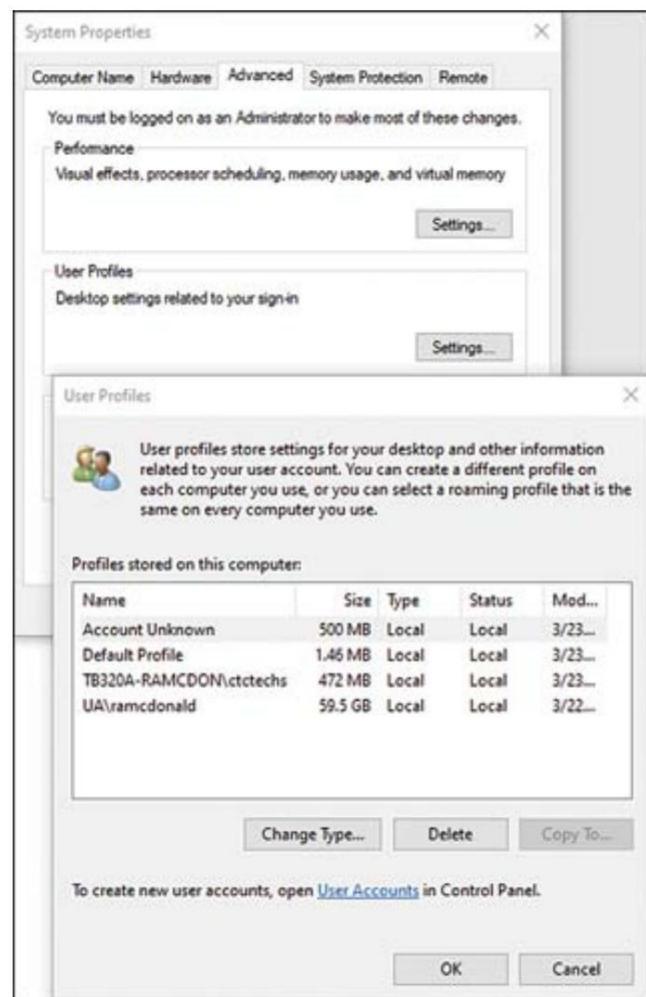


Figura 8-5 Verificando Perfis de Usuário

No menu Propriedades do sistema, selecione a guia Avançado e selecione Configurações em Perfis de usuário. As informações de Perfis de usuário são exibidas conforme mostrado na segunda janela da [Figura 8-5](#).

Observação

Um perfil é muito maior que os outros. Nesse caso, você deve sugerir a esse usuário que a limpeza da área de trabalho provavelmente evitará problemas de perfil lento.

Desvio de tempo

O desvio de tempo ocorre quando o relógio de um computador ou servidor não coincide com os relógios de outros computadores com os quais ele interage. Isso pode causar vários problemas que podem ser difíceis de detectar. Por exemplo, os logs de eventos usados para solucionar problemas podem ter carimbos de data/hora errados, e outros computadores ou servidores, locais ou na Web, podem enfrentar problemas de transação segura ou problemas de autenticação.

A solução fácil aqui é definir a hora de um computador para alinhar com a hora usada pelo Instituto Nacional de Padrões e Tecnologia (NIST), encontrado em www.time.gov. Este site ainda fornece um cálculo da diferença entre o relógio do dispositivo e o horário do NIST. Use este relógio para redefinir a hora no computador.

Uma rede de computadores deve ter todos os seus dispositivos funcionando ao mesmo tempo. Isso pode ser feito estabelecendo um servidor de relógio em uma rede e executando o NTP (Network Time Protocol) em todos os dispositivos.

As configurações de hora, bem como a opção de sincronizar manualmente o relógio, são encontradas em **Configurações > Sistema > Data e hora**, conforme mostra a [Figura 8-6](#). Observe que, no exemplo, a origem da configuração de hora é o servidor localizado em <http://time.windows.com>.

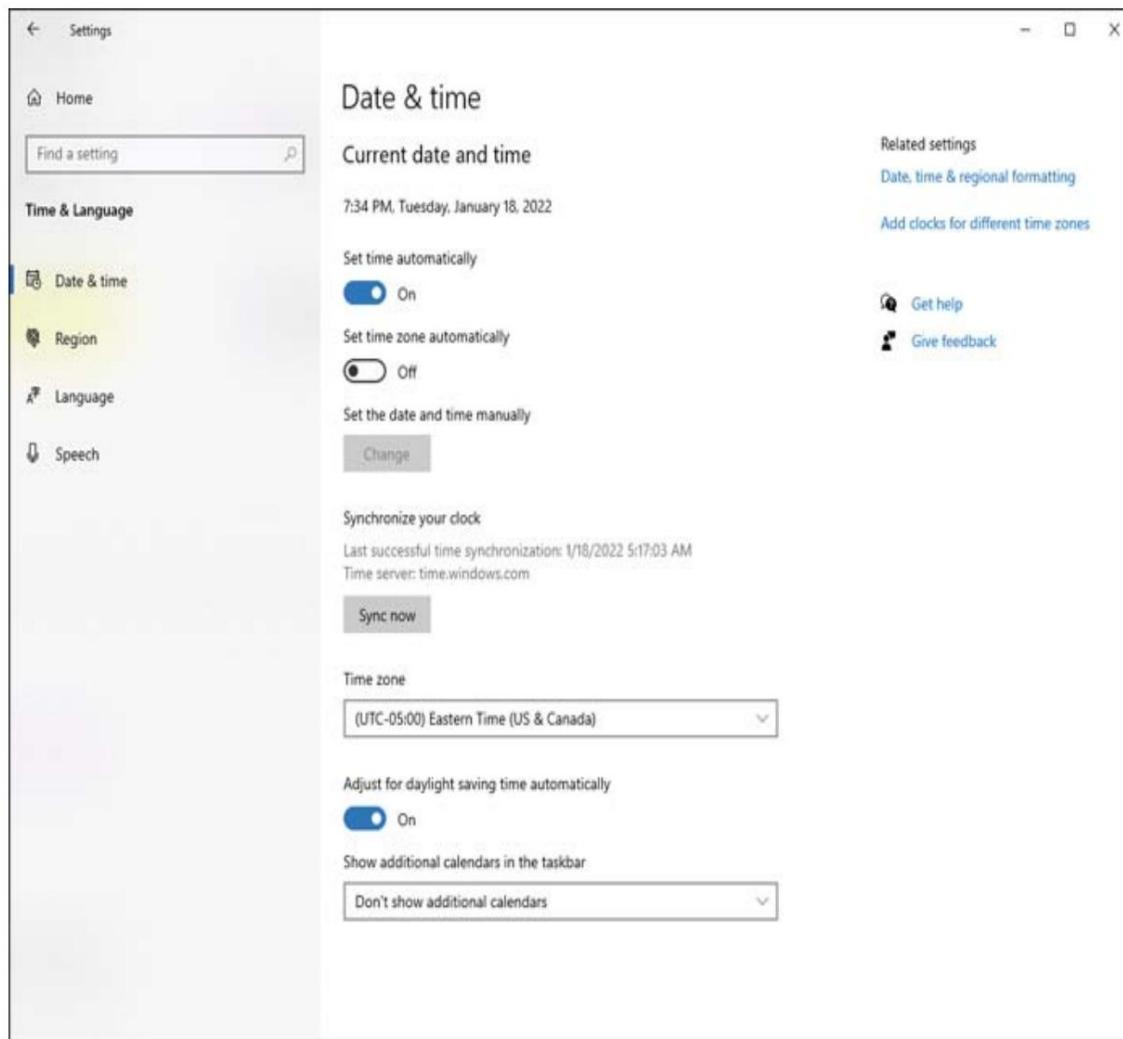


Figura 8-6 Configurações de hora

Etapas comuns de solução de problemas Esta

seção lista as etapas comuns de solução de problemas do sistema operacional Windows descritas ao longo do livro. A lista começa com os primeiros passos simples e progride por etapas cada vez mais complexas. Você deve estar familiarizado com essas etapas para os exemplos que poderá ver no exame A+.

- **Reinicialização:** a reinicialização é sempre um bom primeiro passo, especialmente se o dispositivo estiver em execução por um longo período de tempo.
- **Reinic peace os serviços:** no menu Executar, digite **services.msc** ou **services** na barra de pesquisa e abra o aplicativo Serviços. Selecione o aplicativo e pare ou reinicie conforme necessário.

- **Desinstalar/reinstalar/atualizar aplicativos:** Vá para o aplicativo Microsoft Store, selecione Conta e, em seguida, selecione Atualizações de aplicativos. A loja pode atualizar aplicativos automaticamente.
- **Adicione recursos:** lembre-se sempre, poucas ações podem melhorar o desempenho de um PC de forma mais substancial do que adicionar mais RAM.
- **Verifique os requisitos:** Novas versões de software e atualizações de hardware podem tornar obsoletas as especificações atuais. Problemas de RAM, armazenamento e fonte de alimentação podem se infiltrar em um sistema atualizado.
- **Execute uma verificação de arquivo do sistema:** Selecione Windows+X/PowerShell (Admin). Digite **sfc /scannow** (incluir o espaço após sfc).
- **Reparar o Windows:** Reiniciar enquanto pressiona F11 (na maioria das máquinas) abre as opções avançadas de inicialização do Windows 10. Selecione **Solução de problemas > Opções avançadas > Reparo de inicialização.**
- **Execute a Recuperação do Windows (WinRE):** Clique em Iniciar > Configurações > Atualização e Segurança > Recuperação. Em Inicialização avançada, clique em **Reiniciar agora.**
- **Execute uma restauração do sistema:** Pressionar Reboot+F11 (na maioria das máquinas) abre as opções avançadas de inicialização do Windows 10. Selecione **Solução de problemas > Opções avançadas > Restauração do sistema.**
- **Reimage:** Pressionar Reboot+F11 (na maioria das máquinas) abre as opções avançadas de inicialização do Windows 10. Selecione **Solução de problemas > Opções avançadas > Recuperação da imagem do sistema.**
- **Reverter atualizações:** Reiniciar + F11 (na maioria das máquinas) abre as opções avançadas de inicialização do Windows 10. Selecione **Solução de problemas > Opções avançadas > Desinstalar atualizações.**

Recriar perfis do Windows

Os perfis de usuário contêm planos de fundo e arquivos da área de trabalho, ícones e outros dados pessoais que podem sobrecarregar um perfil e fazer com que ele carregue lentamente durante a inicialização. Se outros perfis carregarem rapidamente, muitos dados podem ser o problema. Gerencie os dados do perfil reduzindo os dados no perfil ou removendo-os.

Observação

A remoção de um perfil não é possível enquanto se trabalha dentro dele. Em vez disso, você deve acessar um perfil diferente (ou criar outro, se necessário).

É possível excluir um perfil sem excluir uma conta de usuário. Quando você terminar de excluir um perfil, reiniciar gera um novo perfil para o conta de usuário.

As etapas para recriar um perfil do Windows são as seguintes (consulte a [Figura 8-5](#)):

Etapa 1. Para excluir um perfil de usuário, use a caixa de diálogo Executar ou a ferramenta de pesquisa e digite **sysdm.cpl**. Isso abre o menu Propriedades do sistema mostrado na [Figura 8-5](#).

Etapa 2. No menu Propriedades do sistema, selecione a guia **Avançado** e escolha **Configurações** em Perfis de usuário. As informações de Perfis de Usuário são exibidas, como na segunda janela da [Figura 8-5](#).

Etapa 3. Selecione o perfil e clique no botão **Excluir**.

Etapa 4. No Editor do Registro (regedit na barra de pesquisa), exclua o perfil de usuário encontrado no final do seguinte caminho:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsN T\CurrentVersion\ProfileList.

Etapa 5. Reinicie.

Solução de problemas comuns de segurança do PC

220-1102: Objetivo 3.2: Dado um cenário, solucionar problemas comuns de segurança de computadores pessoais (PC).



Esta seção ajuda você a lidar com problemas de segurança do PC, incluindo sintomas comuns de infecções por malware e ferramentas de software para combater o malware.

Atenção especial é dada à conectividade de rede, pois esse é um dos problemas mais comuns enfrentados pelos técnicos de TI.

Sintomas comuns Tentar

cobrir todos os problemas de segurança do PC que você pode encontrar no campo é uma missão tola. Em vez disso, esta seção aborda os problemas de segurança mais comuns relacionados ao PC que podem aparecer em uma questão de exame A+, dando atenção especial ao acesso à rede.

Antes de fazer qualquer outra coisa, verifique a conectividade em outros dispositivos na rede. Se nenhum dos dispositivos puder se conectar, tome estas medidas.

No Windows 10, um ícone de X vermelho aparece na barra de tarefas ao lado do ícone de rede quando surgem problemas de conectividade. Às vezes, a falha não é da rede: as configurações de segurança podem não permitir o acesso à rede.

A primeira etapa é verificar a conectividade em outros dispositivos na rede. Se apenas um dispositivo for afetado, desconecte-o de sua rede sem fio e reconecte-o. Para uma rede com fio, reinicie o computador.

Outras tarefas de solução de problemas relacionadas ao acesso à rede são as seguintes:

- Verifique o nome da rede designada ou desejada. Um ponto de acesso pode estar inativo, causando problemas de autenticação em outro ponto de acesso.
- No Windows 10, clique no ícone de rede na barra de tarefas para abrir a janela Status da rede. Um botão Solução de problemas aparece lá se você não estiver conectado.
- Para problemas de conexão com qualquer sistema operacional, desligue o modem de banda larga ou dispositivo de acesso, aguarde cerca de um minuto e ligue o modem ou dispositivo novamente. Em seguida, desligue o roteador, aguarde cerca de um minuto e ligue o roteador novamente. Se o problema for com o modem de banda larga ou dispositivo de acesso, isso deve resolver o problema. Se isso não resolver o problema, entre em contato com o ISP; o problema pode estar na rede do ISP.

A Tabela 8-3 descreve outros problemas de segurança que podem surgir e sugere abordagens para repará-los. Certifique-se de conhecer esses sintomas para o exame 220-1102.

**Tabela 8-3** Sintomas comuns de problemas de segurança do PC**Sintoma Possíveis Causas**

Sem acesso à rede	Problemas de conectividade com a Internet que não afetam todos os computadores e dispositivos na rede podem ser causados por malware. Execute solucionadores de problemas para reparar o problema. Se o problema persistir, verifique os sistemas.
Alertas de área de trabalho	O centro de notificações e ações rápidas é facilmente acessado na barra de tarefas ao lado da hora e da data. As notificações podem ser editadas em Configurações > Sistema > Notificações e ações . As opções incluem notificações de conectividade, VPN, rede e configurações, bem como notificações de aplicativos. As atualizações do sistema operacional também podem ser enviadas aqui. Uma verificação regular do centro de notificações e ações rápidas pode ajudar a evitar que pequenos problemas se transformem em grandes problemas.
Alertas falsos	Os alertas de segurança do Windows Defender ou do seu sistema operacional podem indicar infecção por malware ou outros problemas. Às vezes, os alertas que aparecem sem nenhuma notificação no Defender ou na Central de Ações são tentativas de infectar seu sistema, induzindo-o a clicar em um link de phishing no pop-up. Escaneie o sistema. Programas antivírus desonestos parecem programas antivírus legítimos, mas na verdade são projetados para infectar seu sistema ou usuários de phishing para obter informações pessoais. Desinstale qualquer programa desse tipo e verifique o computador.

Sintoma Possíveis Causas

Sistema alterado ou arquivos pessoais	As infecções por malware podem renomear arquivos do sistema (como msconfig, regedit e taskmgr) que podem ajudar a bloquear malware.
	Os arquivos podem desaparecer ou ser renomeados em seus dispositivos de armazenamento se estiverem corrompidos, infectados com malware, ocultos inadvertidamente ou movidos automaticamente por um programa sem o consentimento do usuário. Os arquivos que realmente desapareceram e não foram movidos ou ocultos artificialmente podem ser recuperados com software de recuperação que verifica o disco rígido em busca de arquivos que não estão mais registrados na tabela de alocação de arquivos, os dados do dispositivo de armazenamento que rastreiam onde os arquivos começam e terminam. Arquivos infectados por malware não excluídos podem reinfetar um sistema se não forem devidamente limpos antes do uso.

Notificações indesejadas podem ser facilmente gerenciadas no Windows 10 por meio de notificações acessando **Configurações > Sistema > Notificações e ações** nesta página operacional do Windows e de aplicativos individuais instalados.

Falhas de atualização do sistema operacional	Um motivo comum para a falha das atualizações do sistema operacional é a falta de espaço em disco. Certifique-se de que haja amplo espaço livre em disco disponível; algumas atualizações podem ser bem grandes. Certifique-se também de que as atualizações automáticas não sejam bloqueadas pelas configurações de proteção antivírus.
--	--

Sintomas relacionados ao navegador

Muitas

vezes, o desempenho do navegador preferido pode indicar problemas com infecção por malware ou aplicativos fraudulentos no dispositivo. A Tabela 8-4 lista os problemas do navegador e suas possíveis causas.

Tabela 8-4 Sintomas relacionados ao navegador

Sintoma Possíveis Causas

Sintoma Possíveis Causas

Aleatório ou pop-ups frequentes Se o navegador tiver o bloqueio de pop-up ativado, mas os pop-ups ainda estiverem aparecendo, o sistema pode estar infectado com malware. Se muitos pop-ups forem exibidos rapidamente na tela e continuarem aparecendo mesmo depois de fechados, é quase certo que o sistema está infectado e precisa ser verificado imediatamente.

Certificado Sistemas operacionais e navegadores usam certificados digitais para obtidos de forma fraudulenta de terceiros de aplicativos e sites de malware para lançar ataques de malware.

sequestro de navegador, mediante navegar no navegador e alterando a configuração da página inicial do seu navegador é alterada sem sua permissão. Alguns aplicativos gratuitos oferecem a alteração da página inicial do navegador durante a instalação, mas você pode ativar ou desativar a alteração. Se um aplicativo alterar a página inicial do navegador sem notificá-lo, pode ser um malware. Escaneie o sistema.

Procedimentos de melhores práticas para remoção de malware

220-1102: Objetivo 3.3: Dado um cenário, use os procedimentos de melhores práticas para remoção de malware.



A remoção de malware será uma tarefa comum para um técnico de suporte no futuro previsível. Essas etapas são práticas recomendadas a serem seguidas sempre que a tarefa é realizada.

Siga este procedimento de sete etapas para remover malware e saiba bem para o exame A+:

Etapa 1. Investigue e verifique os sintomas de malware. Use a [Tabela 8-4](#) para identificar os sintomas.



Etapa 2. Colocar em quarentena os sistemas infectados. Desconecte o sistema de redes com e sem fio e suspeite de qualquer mídia que tenha tocado o sistema como possivelmente infectada.

Etapa 3. Desative a Restauração do sistema no Windows. Desative a Restauração do sistema neste ponto para que não seja executado e crie um ponto de restauração com arquivos infectados antes que o sistema seja limpo. Alguns programas de malware usam a Restauração do sistema para infectar novamente os sistemas. A Restauração do sistema foi projetada para ajudar na recuperação de erros do usuário ou travamentos do sistema, e não para espalhar malware.

Etapa 4. Remendar os sistemas infectados. Use um sistema diferente para alterar senhas de acesso à rede, comércio eletrônico e mídia social. Faça backup dos dados, caso o sistema precise ser reformatado.
Verifique se há malware no backup antes de reinstalá-lo. Esse processo envolve as seguintes subetapas:

- a. Atualização do software antimalware:** Para atualizar o antimalware em um sistema em quarentena, baixe os arquivos de atualização offline em um sistema diferente, copie-os para uma unidade flash USB e instale as atualizações no sistema em quarentena.

b. Usando técnicas de escaneamento e remoção (como Safe

Modo e ambiente de pré-instalação): execute verificações e remova ameaças no modo de segurança ou WinRE. Se o software antivírus/antimalware de um sistema em quarentena não puder ser atualizado, os próprios aplicativos poderão estar infectados ou bloqueados por malware.

Baixe os arquivos necessários para criar um CD ou disco anti-malware inicializável em USB ou uma unidade USB em um sistema diferente.

Etapa 5. Agende verificações e execute atualizações. Atualize o anti-malware e software antivírus e execute verificações completas com ambos. Se a fonte de infecção for conhecida pelo nome, primeiro use uma ferramenta de remoção específica (se disponível) e faça verificações completas. Digitalize com mais de uma ferramenta para garantir que a infecção foi removida.

Etapa 6. Quando o sistema estiver limpo, ative a Restauração do sistema e crie um ponto de restauração no Windows sem copiar os arquivos infectados. Esta etapa envolve simplesmente reativar a Restauração do sistema e criar manualmente um ponto de restauração limpo no Windows.

Etapa 7. Educar o usuário final. Discuta os princípios para evitar infecções por malware com os usuários finais. Se o vetor de infecção (a forma como o vírus acessou o computador, como por e-mail, pen drives ou um aplicativo baixado) for conhecido, discuta-o especificamente. Também forneça orientação geral para computação segura (por exemplo, evitar o uso de unidades flash USB órfãs, não abrir anexos de fontes desconhecidas, usar software antivírus em tempo real e verificar os sistemas semanalmente).

Solucionar problemas do SO móvel comum e Problemas de aplicativos

220-1102: Objetivo 3.4: Dado um cenário, solucionar problemas comuns de sistemas operacionais móveis e aplicativos.



A [Tabela 8-5](#) descreve alguns dos problemas comuns de aplicativos e sistemas operacionais móveis, juntamente com algumas etapas prováveis de solução de problemas a serem executadas.



Tabela 8-5 Sintomas comuns de SO móvel e problemas de aplicativos

Sintoma	Etapa(s) de solução de problemas
O aplicativo falha ao iniciar	Exclua o aplicativo e reinstale-o.

Sintoma	Etapa(s) de solução de problemas
O aplicativo falha ao excluir o aplicativo e reinstalá-lo, fechar ou travar Force a parada do aplicativo (os métodos variam de acordo com o telefone ou dispositivo).	Limpe o cache e os dados do aplicativo (menu Configurações).
O aplicativo falha ao atualizar	Se o aplicativo pausar durante a atualização, um arquivo pode ter sido corrompido em trânsito. Exclua o aplicativo e repita os procedimentos de download e instalação.
O aplicativo demora para responder	Se a reinicialização não corrigir esse problema, verifique o armazenamento disponível e exclua os dados antigos ou não utilizados. Quando um telefone se aproxima da capacidade de armazenamento, ele pode ficar lento.
SO falha ao atualizar	Este é provavelmente um problema de armazenamento. Verifique se há espaço e libere espaço suficiente para o download e o lançamento da atualização.
Surgem problemas de vida útil da bateria	Muitos recursos executados em segundo plano podem limitar a duração da bateria de um telefone ou dispositivo. Por exemplo: <ul style="list-style-type: none">■ Faça uso das informações e configurações de otimização da bateria, como o Modo de baixo consumo de energia.■ Reduza o brilho da tela.■ Identifique aplicativos que usam mais energia e gerencie-os.■ Desligue os sons de alerta e as vibrações.■ Carregue o telefone ou dispositivo antes que fique sem energia. Uma estratégia é reduzir ocasionalmente a bateria até 10 a 15 por cento da capacidade e, em seguida, carregá-la totalmente.

Sintoma	Etapa(s) de solução de problemas
Telefone ou dispositivo reinicia aleatoriamente	Feche todos os aplicativos que não estiverem em uso. Determine se um aplicativo instalado é o problema reiniciando no modo de segurança, removendo o aplicativo mais recente e reiniciando. Se o problema persistir, repita para outros aplicativos recentes.
A tela não acessa o centro de controle (com um iPhone, deslize para baixo a partir do canto superior direito; em um dispositivo Android, deslize de cima para baixo). Toque no ícone de bloqueio de rotação para alternar a configuração.	Verifique também as configurações de exibição e certifique-se de que a exibição é padrão e não ampliada; o zoom pode impedir que a tela gire.
Conectividade	
Problemas	
Sintoma	Etapa(s) de solução de problemas
Bluetooth	Tanto para iPhone quanto para Android, a solução mais comum é "esquecer" o dispositivo que está falhando ao emparelhar do cache.
Wi-fi	Verifique se a força do sinal é boa. Às vezes, afastar-se de um sinal forte ativa os dados do celular e interrompe a conexão Wi-Fi. Verifique as redes e a autenticação. Esteja ciente de que multidões em grandes eventos podem sobrecarregar os sistemas de dados Wi-Fi (e celulares).
Campo próximo	Certifique-se de que o NFC esteja ativado no Centro de controle (para modelos de comunicação do iPhone até 11 - em modelos subsequentes, (NFC)) NFC está sempre ativado e nenhuma configuração está disponível). NFC é bom para apenas alguns centímetros. Para conectar, certifique-se de que o leitor e o telefone estejam quase se tocando.

Sintoma	Etapa(s) de solução de problemas
AirDrop	<p><i>Para iPhone/iPad:</i></p> <p>Certifique-se de que o dispositivo receptor seja compatível e detectável.</p> <p>O AirDrop funciona apenas quando o dispositivo receptor está ligado e sua tela está ativa.</p> <p>AirDrop usa Bluetooth e Wi-Fi; verifique se eles estão ativados.</p> <p>Verifique se o modo avião está desativado.</p>

Para todos os problemas da [Tabela 8-5](#), os primeiros passos são os mesmos:

Etapa 1. Remova os acessórios e as baterias externas.

Etapa 2. Reinicie o telefone ou dispositivo.

Etapa 3. Atualize o sistema operacional e os aplicativos.

Às vezes, as atualizações do sistema operacional afetam as funções dos aplicativos instalados.

Telefones e outros dispositivos móveis podem funcionar de várias maneiras inesperadas.

A [Tabela 8-5](#) descreve vários problemas e suas possíveis soluções.

Observação

Essas etapas pressupõem que o telefone ou dispositivo foi reiniciado e atualizado.

Solucionar problemas do SO móvel comum e

Problemas de segurança de aplicativos



220-1102: Objetivo 3.5: Dado um cenário, solucionar problemas comuns de sistema operacional móvel e segurança de aplicativos.

Devido ao seu armazenamento limitado, memória e dependência de rede sem fio e celular, os dispositivos móveis estão sujeitos a muitos problemas que não afetam os dispositivos mais robustos. Os problemas de segurança a seguir, que podem aparecer no exame, refletem os desafios do uso diário de dispositivos móveis.

Preocupações com segurança



Como sempre, as práticas de segurança são um tópico importante do exame A+. As preocupações listadas nas seções a seguir são maneiras pelas quais os hackers podem tentar contornar as configurações de segurança.

Origem do pacote Android (APK)

Como acontece com qualquer software para um dispositivo, uma importante prática de segurança é verificar a confiabilidade da fonte de um arquivo antes de fazer o download. Os arquivos de **origem do Android Package (APK)** podem ser corrompidos por hackers e distribuídos. Usuários incautos podem baixar involuntariamente arquivos APK carregados com malware ou cavalos de Tróia que estão prontos para serem instalados em seu sistema Android.

Modo de desenvolvedor

O modo de desenvolvedor está disponível no Windows 10 e no sistema operacional móvel Android. O objetivo do modo Desenvolvedor é permitir que alguém desenvolvendo aplicativos teste os aplicativos. O modo de desenvolvedor no Windows é encontrado em **Configurações > Atualização e segurança > Para desenvolvedores**. Em dispositivos Android, varia de acordo com a versão, mas o modo Desenvolvedor é intencionalmente complicado para evitar que os usuários entrem accidentalmente no ambiente do telefone.

Explorar o modo Desenvolvedor não é necessariamente perigoso, mas a experiência do usuário é diferente naquele ambiente e é necessário cautela.

Acesso root/Jailbreak

Fazer o **jailbreak** de um iPhone OS significa obter acesso aos arquivos raiz com o objetivo de personalizar o iOS, adicionar portabilidade entre provedores de celular,

e possivelmente ignorando paywalls para aplicativos. O jailbreak é feito principalmente por hackers amadores que gostam de personalizar telefones.

Embora o jailbreak não seja ilegal, ele pode fornecer acesso a comportamentos ilegais. Ainda assim, o jailbreak envolve sérios riscos. Ignorar o design seguro do fabricante adiciona riscos inerentes ao malware. Além disso, alterar o código e instalar outro software provavelmente causará instabilidade no iOS e muitas vezes anula a garantia do fabricante.

Os dispositivos Android são relativamente fáceis de fazer root (ou seja, obter acesso root) para que os usuários possam instalar diferentes sistemas operacionais e continuar a usar suas conexões de dados e celulares. Por outro lado, obter o mesmo tipo de acesso a um dispositivo iOS requer o jailbreak, o que significa que o dispositivo pode ser impedido de receber atualizações futuras.

O **acesso root** não autorizado pode ser perigoso e é um risco incorrido quando os usuários baixam aplicativos que não vêm do Google Play. Esses aplicativos não seguem corretamente as regras de permissão e podem elevar as permissões sem o conhecimento ou consentimento do usuário. A execução de um dispositivo no modo Desenvolvedor (usado para desenvolvimento e teste de software e serviço) desativa a maioria das proteções. Nas versões atuais do Android, várias etapas são necessárias para ativar o modo de desenvolvedor, portanto, é difícil fazer isso acidentalmente.

Fazer o jailbreak de um dispositivo iOS ou fazer root em um dispositivo Android coloca o dispositivo e suas informações em risco muito maior do que com um dispositivo funcionando normalmente.

Falsificação de aplicativos piratas/maliciosos

A **falsificação de aplicativos** ocorre quando um aplicativo malicioso imita um aplicativo legítimo e engana os usuários para que revelem senhas ou outras informações confidenciais enquanto interagem com o aplicativo falso. Este processo é semelhante a um ataque de phishing. A falsificação de aplicativos pode ser sofisticada e exige que os usuários estejam sempre cientes de como estão compartilhando informações confidenciais.

A falsificação também pode ser usada para gerar anúncios extras e invadir a experiência do usuário com pop-ups.

Sintomas comuns



Os seguintes sintomas devem ser familiares; muitos são semelhantes aos problemas de PC abordados na primeira seção deste capítulo. Esses sintomas indicam problemas em PCs e dispositivos móveis que podem ocorrer como resultado de problemas de segurança. Quando o usuário experimenta esses sintomas, é hora de aumentar a conscientização sobre os hábitos de segurança, verificar se há atualizações e verificar se há vírus. Algumas novas etapas de solução de problemas e correções seguem esta lista:

- Tráfego de rede alto
- Tempo de resposta lento
- Notificação de limite de uso de dados
- Conectividade limitada à Internet
- Sem conectividade com a Internet
- Alto número de anúncios
- Falsos avisos de segurança
- Comportamento inesperado do aplicativo
- Arquivos ou dados pessoais vazados

Velocidades de dados lentas

Velocidades de dados lentas podem ser causadas por vários fatores:

- **Sem conexão com uma rede celular:** verifique o indicador de rede na parte superior do smartphone ou tablet equipado com celular para determinar o tipo de conexão de rede.
- **Um sinal de celular ou Wi-Fi fraco:** Com Wi-Fi, mude para um sinal SSID mais forte, se possível. Com 4G e 5G, use um scanner de torre de celular para localizar uma torre de celular mais forte.

- **Limites de velocidade do plano de dados “ilimitados” após atingir os limites de velocidade ou dados por período de cobrança:** alguns provedores que oferecem planos de dados “ilimitados” reduzem drasticamente a velocidade depois que um determinado nível de dados é transferido durante um período de cobrança. Verifique o uso de dados e configure um aviso a ser exibido antes de atingir essa meta. Como alternativa, considere mudar para um plano diferente.

Dados/arquivos pessoais vazados

Para evitar que arquivos ou dados pessoais sejam descobertos se seu dispositivo móvel for perdido, siga estas etapas:

Etapa 1. Ative a criptografia.

Etapa 2. Ative as opções para bloquear e limpar seu dispositivo em caso de perda.

Etapa 3. Evite se conectar a redes Wi-Fi abertas.

Etapa 4. Use uma VPN para conexões seguras se precisar usar um Wi-Fi aberto rede.

Etapa 5. Desative os serviços de tethering Wi-Fi ou compartilhamento de conexão se eles não estiverem em uso.

Transmissão de dados acima do limite

Exceder a quantidade de dados incluídos em seu plano de celular pode ser caro. Para evitar contas inesperadas, verifique periodicamente o uso de dados. No Android, vá para **Configurações > Conexões > Uso de dados**. Role para baixo para ver quais aplicativos estão usando mais dados. Certifique-se de que Definir limite de dados esteja ativado para definir um limite e fornecer um aviso sobre exceder o limite.

No iOS, vá para **Configurações > Celular > Uso de dados celulares**. Use os controles deslizantes para desativar qualquer aplicativo que não deva usar conexões de celular. Desative os dados de celular se não houver permissão de dados no período atual.

Se você observar quantidades incomuns de uso de dados, o dispositivo pode estar infectado com malware.

Usuários móveis e técnicos têm uma ampla variedade de ferramentas de software disponíveis para ajudar a aumentar o desempenho e a segurança, incluindo o seguinte:

- **Antimalware:** os dispositivos Android e iOS podem ser protegidos com aplicativos antimalware – alguns gratuitos e outros pagos – dos mesmos fornecedores que protegem os sistemas de desktop e laptop. Todo dispositivo móvel deve ser protegido, pelo menos porque um dispositivo móvel pode ser usado como um vetor de infecção para qualquer outro dispositivo ao qual ele se conecte.

Verifique o Google Play e a App Store para aplicativos antimalware da AVAST, AVG, Kaspersky Labs, Norton, McAfee, Bitdefender, AVIRA, ESET e muitos outros.

- **Verificador de aplicativos:** os **verificadores** de aplicativos monitoram as permissões e o uso de aplicativos. Durante o processo de instalação de um aplicativo, o usuário vê uma longa lista de permissões concedidas ao aplicativo. Um scanner de aplicativo pode ajudar a determinar se um aplicativo é seguro de usar.

Restauração de fábrica/instalação limpa

Antes de aposentar um dispositivo ou eliminar aplicativos que possam colocar a privacidade em risco, execute uma redefinição de fábrica no dispositivo. Isso pode ser seguido por uma instalação limpa dos aplicativos desejados, se necessário.

Se o dispositivo ainda não estiver criptografado, configure um PIN para criptografar automaticamente o dispositivo.

Para Android:

Etapa 1. Certifique-se de que Fazer backup dos meus dados e Restauração automática estejam ativados.

Etapa 2. Vá para **Configurações > Pessoal > Backup e redefinição > Dados de fábrica Redefinir.**

Etapa 3. Revise os avisos e clique em **Redefinir dispositivo**.

O dispositivo retorna à sua configuração de fábrica. Todos os dados e atualizações do dispositivo são removidos do dispositivo. Para restaurar os dados no dispositivo, usando os dados de backup do Google na etapa 1, siga as etapas na tela.

Para iOS:

Etapa 1. Instale a versão mais recente do iTunes em seu PC host ou computador macOS.

Etapa 2. Inicie o iTunes.

Etapa 3. Conecte seu dispositivo ao computador por meio do cabo de carregamento/sincronização.

Confie no dispositivo ou insira uma senha, se solicitado.

Etapa 4. Selecione seu dispositivo.

Etapa 5. Faça backup de seu conteúdo. Certifique-se de selecionar **Transferir compras** para conteúdo

adquirido no iTunes, faça backup dos dados de saúde e atividade armazenados em seu dispositivo de forma criptografada e inicie o backup.

Etapa 6. Para apagar o dispositivo, vá para **Resumo > Restaurar**.

Etapa 7. Toque em **Restaurar** novamente para apagar seu dispositivo e recarregá-lo para o original condição de fábrica.

Antes de desinstalar um aplicativo iOS com comportamento inadequado, tente atualizá-lo.

Tarefas de preparação para exames

Conforme mencionado na Introdução, você tem várias opções para se preparar para o exame: os exercícios aqui; [Capítulo 10, “Preparação Final”](#); e as questões de simulação de exame no software de teste prático Pearson Test Prep.

Revise todos os tópicos principais

Revise os tópicos mais importantes do capítulo, indicados pelo ícone Tópico principal na margem externa da página. A [Tabela 8-6](#) lista esses tópicos-chave e o número da página em que cada um é encontrado.



Tabela 8-6 Tópicos-chave para o [Capítulo 8](#)

Tópico principal elemento	Descrição elemento	Página Número
Lista	Causas de erros BSOD	651
Lista	Resolvendo erros BSOD	652
Tabela 8-2	Desempenho lento/lento do sistema Causas e Soluções	652
Tabela 8-3	Sintomas comuns de problemas de segurança do PC	665
Lista	Procedimento de sete etapas para remover malware	667
Tabela 8-5	Sintomas comuns de sistema operacional móvel e Problemas de aplicativos	669
Seção	Preocupações com segurança	670
Seção	Sintomas comuns	672

Complete as tabelas e listas da memória

Imprima uma cópia do [Apêndice C, “Tabelas de Memória”](#) (encontrado online), ou pelo menos a seção deste capítulo, e complete as tabelas e listas de memória.

O [Apêndice D, “Respostas das tabelas de memória”](#), também on-line, inclui tabelas e listas preenchidas para verificar seu trabalho.

Definir termos-chave

Defina os seguintes termos-chave deste capítulo e verifique suas respostas no glossário:

[tela azul da morte \(BSOD\)](#)

[Modo de segurança](#)

[Malware de restauração](#)

[do sistema](#)

[software anti-malware](#)

[Bluetooth](#)

comunicação de campo próximo (NFC)

Jailbreaking da origem do pacote

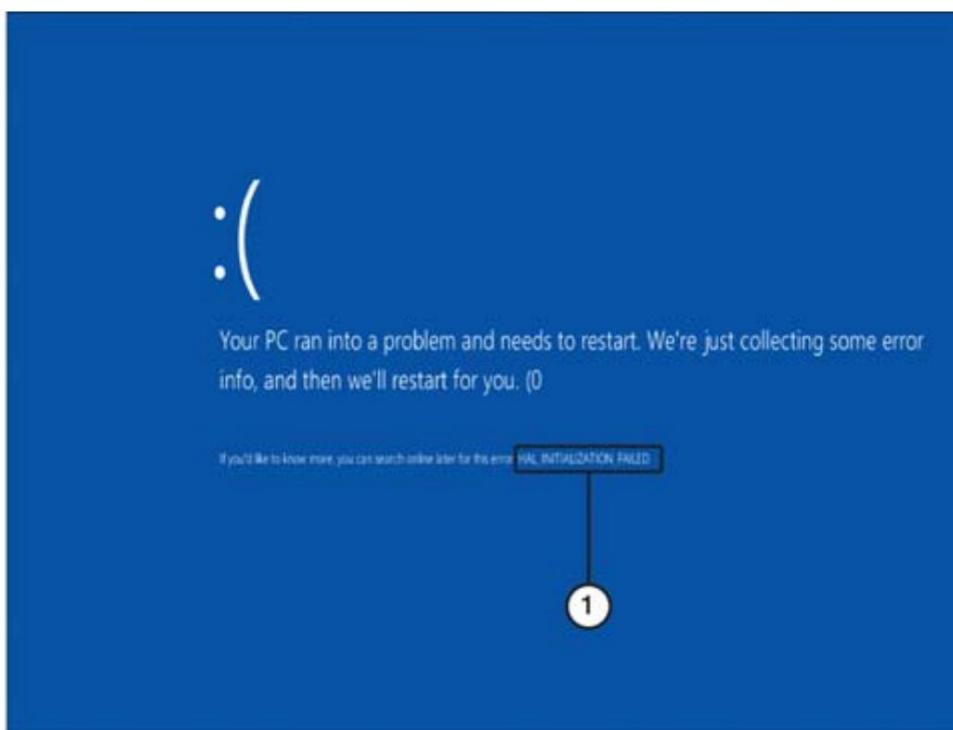
Android (APK)

acesso root

falsificação de aplicativo

Responder a perguntas de revisão

1. Qual sistema operacional está exibindo esta mensagem?



1. STOP error message

a. uma. Mac OS

b. Windows 10

c. Linux

d. Android

2. Por que a falta de espaço livre está causando problemas para o sistema?

- uma.** O disco rígido está ficando sem espaço e não pode armazenar nenhum mais arquivos.
- b.** Pelo menos 10 por cento de espaço livre é necessário para um arquivo de troca. **c.** O disco rígido não tem espaço livre suficiente para atualizar para a versão mais recente do sistema operacional. **d.** Os aplicativos precisam de mais espaço para serem executados.
- 3.** Como você tenta reparar um arquivo BOOTMGR ausente ou corrompido em um sistema Windows?
- uma.** Use as opções de Recuperação do Sistema.
- b.** Use as opções avançadas de inicialização. **c.** Reinicie o computador e edite o programa de inicialização do BIOS/UEFI.
- d.** Baixe um novo arquivo BOOTMGR da Internet.
- 4.** Qual dos procedimentos a seguir melhor descreve como acessar o Gerenciador de Tarefas? **uma.** Pressione Ctrl+R.
- b.** Pressione Ctrl+Alt+Delete e selecione Gerenciador de Tarefas. **c.** Pressione Ctrl+R e selecione Gerenciador de Tarefas. **d.** Pressione Alt+F1 e selecione Gerenciador de Tarefas.
- 5.** Qual das opções a seguir pode ser a causa do baixo desempenho do sistema em um computador com Windows? (Escolha todas as que se aplicam.) **a.** A unidade que contém a paginação e os arquivos temporários está quase cheia. **b.** Poeira e sujeira estão restringindo o fluxo de ar e a CPU está superaquecendo. **c.** Muitos serviços estão configurados para iniciar automaticamente durante comece.
- d.** Os requisitos mínimos de memória foram atendidos, mas não excedido.
- 6.** Coloque as etapas do processo de remoção de malware em ordem, correspondendo cada uma das descrições a seguir a uma das etapas a seguir (incluindo as duas partes da etapa 4).
-

Etapa	Descrição
1.	
2.	
3.	
4a.	
4b.	
5.	
6.	
7.	

a. Agende verificações e execute atualizações. **b.** Desative a Restauração do sistema (no Windows). **c.** Atualize o software antimalware. **d.** Colocar em quarentena os sistemas infectados. **e.** Educar o usuário final. **f.** Ative a Restauração do sistema e crie um ponto de restauração (no Windows). **g.** Investigue e verifique os sintomas de malware. **h.** Escaneie e use técnicas de remoção (modo de segurança, ambiente de pré-instalação).

7. Em qual dos seguintes locais você encontra os arquivos de log que

Windows cria para descrever informações, avisos e erros em seu sistema? **uma.**

Gerenciador de dispositivos **b.** Visualizador de eventos

c. localizador

d. Ambiente de Recuperação

8. A restauração do sistema é usada para fazer qual das opções a

seguir? **uma.** Restaure o sistema para sua configuração original.

- b.** Remova os aplicativos que não são da Microsoft Store e reinstale os aplicativos que são da Microsoft Store.
- c.** Use uma imagem do sistema para restaurar o computador ao seu estado original doença.
- d.** Crie um ponto de restauração com o qual restaurar o computador para um ponto anterior no tempo.

9. Qual utilitário do Windows é usado para desativar quaisquer programas e serviços executados quando o computador é inicializado? **a.** uma. regedit **b.** msconfig **c.** sfc

- d.** msinfo32

10. Qual das opções a seguir pode gerar um erro STOP/BSOD em um computador desktop local?

- a.** uma. Hardware incompatível/defeituoso **b.** Uma infecção por vírus
- c.** Problemas de configuração do registro **d.** Um servidor de nuvem remoto interrompendo uma conexão durante um download

11. Qual das opções a seguir é a solução mais comum para um dispositivo móvel não emparelhado com um dispositivo Bluetooth conhecido no cache?

- a.** Use criptografia em seus dispositivos móveis. **b.** Limpe o cache escolhendo “esquecer” o dispositivo. **c.** Use uma VPN sempre que possível. **d.** Desative o compartilhamento de Wi-Fi.

12. Quais dos seguintes problemas podem ocorrer quando você instala aplicativos de terceiros em um dispositivo móvel? (Escolha todas as que se aplicam.) **a.** Utilização de recursos inesperadamente alta **b.** Acesso raiz não autorizado

- c.** Rastreamento de localização não autorizado
- d.** Ativação não autorizada de câmera ou microfone

Capítulo 9

Procedimentos operacionais

Este capítulo aborda os nove objetivos do exame A+ 220-1102 relacionados a procedimentos operacionais, com foco em segurança, controles ambientais, gerenciamento de mudanças, documentação, privacidade e outros conceitos. Mesmo as redes mais bem planejadas apresentam problemas, e uma importante habilidade de TI é saber como reconhecer problemas e gerenciá-los para um impacto mínimo na rede. Esses objetivos podem abranger 22% das questões do exame:

- **Núcleo 2 (220-1102): Objetivo 4.1:** Dado um cenário, implementar as melhores práticas associadas à documentação e gerenciamento de informações de sistemas de suporte.
- **Núcleo 2 (220-1102): Objetivo 4.2:** Explicar as melhores práticas básicas de gerenciamento de mudanças.
- **Núcleo 2 (220-1102): Objetivo 4.3:** Dado um cenário, implemente métodos de backup e recuperação da estação de trabalho.
- **Núcleo 2 (220-1102): Objetivo 4.4:** Dado um cenário, use procedimentos de segurança comuns.
- **Núcleo 2 (220-1102): Objetivo 4.5:** Resumir os impactos ambientais e os controles ambientais locais.
- **Núcleo 2 (220-1102): Objetivo 4.6:** Explicar a importância do conteúdo/atividade proibida e dos conceitos de privacidade, licenciamento e política.

- **Núcleo 2 (220-1102): Objetivo 4.7:** Dado um cenário, use técnicas de comunicação adequadas e profissionalismo.
- **Núcleo 2 (220-1102): Objetivo 4.8:** Identificar os fundamentos do script.

- **Núcleo 2 (220-1102): Objetivo 4.9:** Dado um cenário, use tecnologias de acesso remoto.

Até este ponto, o foco deste livro tem sido as habilidades técnicas de hardware e software que se espera que um técnico certificado A+ tenha em uma posição de TI. No entanto, um funcionário bem-sucedido no campo técnico também deve ser adepto da comunicação e das habilidades organizacionais. Este capítulo enfoca essas “habilidades interpessoais” que muitas vezes fazem a diferença entre um técnico adequado e um funcionário valioso. O script e o uso de tecnologias remotas também são abordados.

“Eu já sei disso?” Questionário

O “Eu já sei disso?” questionário permite avaliar se você precisa ler o capítulo inteiro. A [Tabela 9-1](#) lista os principais títulos deste capítulo e a seção “Eu já sei disso?” perguntas do questionário que cobrem o material desses títulos para que você possa avaliar seu conhecimento nessas áreas específicas. As respostas para a pergunta “Eu já sei disso?” questionário aparecem no Apêndice A, “Respostas para a pergunta ‘Eu já sei disso?’ Questionários e perguntas de revisão.

Tabela 9-1 “Eu já sei disso?” Mapeamento de seção para pergunta

Seção de Tópicos Fundamentais	Perguntas
Melhores práticas e documentação	1
Mudar a gestão	2
Métodos de backup e recuperação da estação de trabalho	3
Explicar os procedimentos comuns de segurança	4–7
Impactos Ambientais e Controles Apropriados	8
Abordando Conteúdo/Atividade Proibida e Privacidade, Licenciamento e Conceitos de Política	9–12
Técnicas de Comunicação e Profissionalismo	13
Noções básicas de script	14–15

Seção de Tópicos Fundamentais	Perguntas
Tecnologias de acesso remoto	16

CUIDADO

O objetivo da autoavaliação é avaliar seu domínio dos tópicos deste capítulo. Se você não souber a resposta a uma pergunta ou tiver certeza apenas parcial da resposta, marque essa pergunta como errada para fins de autoavaliação. Dar a si mesmo crédito por uma resposta que você adivinhou corretamente distorce os resultados de sua autoavaliação e pode lhe dar uma falsa sensação de segurança.

1. Jennifer pediu um documento mostrando as LANs e endereços IP no edifício. Que tipo de documento ela solicitou? **uma.** Diretório de endereços IP **b.** Topologia lógica **c.** Diretório Netspace **d.** topologia física

2. Enrique foi convidado a participar de uma reunião para relatar como as mudanças de rede propostas afetarão seu grupo de trabalho. Qual termo descreve melhor a reunião da qual ele participará?
 - uma.** Reunião de impacto do escopo
 - b.** mesa redonda do CIO
 - c.** Reunião de gerenciamento de mudança
 - d.** Reunião de prevenção de desastres

3. Qual conceito é abordado na regra 3-2-1? **uma.**
 - Procedimentos de conectividade de rede **b.**
 - Procedimentos de segurança elétrica **c.** Procedimentos de senha administrativa **d.** Procedimentos de backup de dados

- 4.** De acordo com os códigos de construção, a que cada tomada aterrada usada para computadores se conecta?
- uma.** O circuito neutro no armário de fiação **b.** Um tubo de cobre enterrado no subsolo **c.** O corte do circuito de fio quente
d. Uma UPS na sala do servidor
- 5.** Gina estava atualizando placas gráficas em 10 PCs em um escritório de design. Depois de remover os cartões抗igos, ela teve que usar uma tesoura antes de instalar os novos. Por que ela precisaria de uma tesoura em sua bolsa de tecnologia? **uma.** Para cortar as abas plásticas dos conectores de alimentação **b.** Para cortar etiquetas “instaladas em” anotando a data para enviar de volta ao fabricante
c. Para cortar a fita do plástico-bolha em torno dos novos cartões **d.** Para abrir sacos antiestáticos
- 6.** Qual é a finalidade de uma pulseira ESD?
- uma.** Para igualar o potencial **b.** Para selar sacos antiestáticos **c.** Para aterrizar as fontes de alimentação do PC enquanto desconectado **d.** Para eliminar a interferência eletromagnética nas linhas de fibra
- 7.** Quando a instalação de uma estação de trabalho cria um risco de tropeço, qual melhor prática não está sendo praticada? **uma.** Gerenciamento de cabos **b.** Prevenção de desastres **c.** Política de uso aceitável **d.** Auto-aterramento
- 8.** Eric se depara com uma caixa contendo um produto químico em uso no prédio que se derramou no corredor principal do depósito. O que ele deve fazer antes de varrer?
uma. Ligue 911
b. Isolar a área e evacuar o prédio

- c.** Consulte a folha quente química
 - d.** Consulte o MSDS
- 9.** Jacob está chateado porque pode usar um determinado aplicativo em apenas três de seus quatro computadores. Seu quarto computador é capaz de executá-lo, mas ele não quer pagar mais. Qual das opções a seguir o impede de adicionar o aplicativo à máquina sem pagar mais? (Escolha dois.)
 - uma.** DRM
 - b.** RGPD
 - c.** EULA
 - d.** PHI
- 10.** Qual não é um tipo de dado regulamentado?
 - uma.** PCI
 - b.** RGPD
 - c.** DRM
 - d.** PII
- 11.** Qual é o nome de um conjunto de procedimentos que um investigador segue ao examinar um incidente de tecnologia?
 - uma.** Resposta a incidentes
 - b.** AUP
 - c.** DRM
 - d.** EULA
- 12.** Quais dos seguintes são exemplos de como lidar adequadamente com materiais confidenciais e privados de um cliente? (Escolha dois.)
 - uma.** Mary pede a uma cliente que leve sua bolsa para longe do trabalho área.
 - b.** Bob desliga o celular ao falar com os clientes. **c.** Alexandria está atendendo em um consultório médico e pede que os arquivos do seguro sejam removidos da estação de trabalho.

- d.** Ali recusa uma oferta para almoçar no funcionário com desconto cantina.
- 13.** Qual dos seguintes é um exemplo de falta de profissionalismo em um ambiente de atendimento ao cliente?
- uma.** Vestindo shorts cáqui para trabalhar no departamento de TI de um banco **b.** Pedir a um cliente com sotaque que repita o que disse **c.** Usar o celular para pedir opinião a um colega **d.** Esclarecendo as declarações do cliente
- 14.** A qual linguagem de programação está associada a extensão de arquivo .sh?
- uma.** Python
b. PowerShell
c. 3-2-1
d. Linux
- 15.** Qual dos seguintes cria um túnel seguro sobre um público rede?
- uma.** Telnet
b. VPN
c. EULA
d. FISPQ
- 16.** Qual dos seguintes é um aplicativo proprietário de compartilhamento de área de trabalho?
- uma.** DRM
b. RDP
c. EULA
d. FISPQ

Tópicos Fundamentais

Melhores práticas e documentação

220-1102
Exam

220-1102: Objetivo 4.1: Dado um cenário, implementar as melhores práticas associadas à documentação e gerenciamento de informações de sistemas de suporte.

Um técnico deve ser um bom comunicador, e uma das formas mais importantes de comunicação em uma carreira de TI é fornecer documentação. Qualquer técnico experiente pode contar histórias de como a documentação adequada poderia ter economizado tempo e dinheiro em um trabalho. Esta seção explica como diferentes tipos de documentação ajudam a manter uma organização em funcionamento por muito tempo depois que um técnico sai do prédio.

Sistemas de Bilhetagem

Os sistemas de tíquetes de suporte técnico vêm em uma ampla variedade de formatos. Cada empresa ou instituição deve ter o cuidado de escolher um sistema que faça com que os processos técnicos funcionem sem problemas e ajude os clientes, sejam clientes ou colegas de trabalho, a sentir que suas necessidades são atendidas e os problemas são resolvidos de maneira profissional.

Alguns sistemas de suporte exigem o recebimento de informações por telefone; outros requerem a iniciação do cliente online. Cada organização deve determinar o que funciona melhor em seu próprio ambiente. Esta seção não aborda o melhor estilo de sistema de suporte, mas examina sete áreas de conteúdo que são comuns à maioria das solicitações de documentação de suporte.

Informação do usuário

Obter os nomes corretos é importante, é claro, mas coletar informações do usuário sobre onde os usuários trabalham ou como eles estão usando a tecnologia que está sendo suportada. Esta informação informa o técnico de suporte sobre a natureza do problema.

Informação de dispositivo

Seja específico sobre o dispositivo em questão. A identificação de um dispositivo ou software específico que não está funcionando economizará um tempo valioso se uma visita ao local for necessária. A localização, o número de identificação e o nome de uma pessoa de contato são úteis.

Descrição dos Problemas

Descrições precisas são essenciais. Dizer que um dispositivo “não está funcionando direito” não ajuda muito. “Minha conexão de rede é irregular e cai a cada poucos minutos” faz muito mais para isolar o problema e identificar a ajuda adequada.

Categorias

Forneça uma lista de categorias de problemas para os usuários escolherem, com uma opção Outro no final. A maioria dos usuários não está ciente das categorias ou especialidades de suporte que a equipe de suporte usa, portanto, fornecer uma lista é útil. Veja a seguir exemplos de categorias em um ticket de suporte:

- Suporte à conta de usuário (senha, login e suporte a permissões)
- Acesso à rede/Internet
- Slack ou e-mail
- Suporte de software (listando os nomes dos softwares suportados)

Gravidade

A gravidade ajuda a equipe de suporte a priorizar os tíquetes para que os problemas mais críticos sejam atendidos primeiro. Os níveis geralmente se parecem com esta lista, incluindo breves descrições da prioridade necessária para ajudar o cliente a obter o suporte adequado:

- **Urgente:** o trabalho de produção normal foi interrompido. Isso geralmente afeta um escritório inteiro se ocorrer uma interrupção.
- **Alta:** Alguma perda de capacidade para executar tarefas normais de trabalho.
- **Média:** Inconveniência para trabalhadores ou clientes, mas a empresa está conseguindo sobreviver em níveis abaixo do padrão.

- **Baixo:** Sem impacto na capacidade de trabalho, mas pode ser necessária manutenção.

Níveis de escalonamento

Dependendo do tamanho e escopo de um centro de suporte, diferentes níveis (ou níveis) de suporte são oferecidos. Problemas comuns que são bastante fáceis de resolver são atribuídos a um nível baixo; problemas mais complexos que requerem habilidades especiais de suporte e experiência podem ser escalados para níveis mais altos. A seguir estão os três níveis mais comuns:

- **Nível 0:** O cliente/cliente pode resolver o problema com ferramentas e documentação online. Um exemplo é usar um utilitário para redefinição de senha.
- **Nível 1:** Um agente tem acesso a software de suporte e scripts de suporte (etapas predefinidas para ajudar os usuários). Um exemplo é iniciar um script com "A máquina está conectada e ligada?" e, em seguida, passando para detalhes mais técnicos.
- **Nível 2 (ou superior):** A equipe de suporte emprega habilidades especializadas e geralmente mais experiência. Exemplos são especialistas em software e especialistas em rede.

Comunicação clara, concisa e escrita

Habilidades de comunicação escrita e oral também são habilidades técnicas importantes. Comunicar-se calma e prestativamente com os clientes e outras equipes de suporte é uma parte importante do que faz um bom técnico de suporte. Uma comunicação clara nessas áreas é essencial:

- **Descrição do problema:** envolve obter exemplos e detalhes sobre como o problema está se manifestando para o usuário.
- **Notas de progresso:** várias pessoas podem estar tentando resolver um problema, especialmente se um problema foi escalado. É essencial garantir que todos estejam trabalhando com as mesmas informações.
- **Resolução do problema:** Esta é a etapa de comunicação mais difícil. Depois de trabalhar para resolver um problema e fazer o usuário voltar ao trabalho, os técnicos muitas vezes enfrentam pressão para passar para o próximo problema. No entanto,

a documentação completa do problema ajudará a equipe de suporte a reconhecer problemas futuros com dispositivos ou identificar áreas onde o treinamento é necessário.

As organizações de

gerenciamento de ativos de todos os tipos precisam ser responsáveis pelo dinheiro e outros recursos que gastam em tecnologia. O termo *ativo* é utilizado porque o equipamento costuma ser caro e considerado parte do valor da empresa.

As *listas de inventário* contêm um histórico detalhado de todo o hardware e software adquiridos para uso da empresa.

Um *sistema de banco de dados* rastreia os ativos no estoque. Dependendo do tamanho da organização, essa tarefa pode ser gerenciada desde um pequeno banco de dados, como uma simples planilha, até um banco de dados especializado, com equipe designada para acompanhar os ativos para fins técnicos, orçamentários e tributários. O banco de dados deve contabilizar quando os ativos foram adquiridos, como e onde foram usados e, eventualmente, como foram descartados.

O departamento de TI geralmente deve receber e documentar equipamentos com etiquetas de ativos duráveis. Essas tags geralmente são personalizadas, incluindo o nome da organização junto com um código de barras e um número de série usado para criar um banco de dados de ativos. Eles geralmente são feitos de um poliéster metalizado que deve durar enquanto o ativo do computador estiver em uso.

Uma etiqueta de patrimônio permite que a empresa rastreie quem está atribuído ao dispositivo e quem é o responsável pelo equipamento. Esse banco de dados também é usado para rastrear informações de garantia e reparos. Usar um leitor de código de barras é a maneira mais conveniente de acompanhar o equipamento enquanto ele está em uso na empresa.

O ciclo de *vida de aquisição* descreve um método para planejar as compras e a expectativa de vida dos ativos técnicos adquiridos para a empresa. Isso geralmente é feito para compras maiores, como servidores, switches e grandes implementações de software, mas não tanto para consumíveis, como cabos e teclados. O ciclo de vida pode variar amplamente, dependendo do ativo. Por exemplo, os servidores podem ter uma expectativa de vida de alguns anos antes que as novas tecnologias precisem ser substituídas, enquanto a infraestrutura que contém o servidor - rack, ventiladores de resfriamento e backups de bateria - pode ter uma vida útil mais longa.

expectativa de ciclo de vida. O departamento de TI é responsável por documentar o fim de sua utilidade quando o equipamento sai do estoque e é vendido, doado ou destruído.

Garantia e licenciamento precisam ser rastreados como ativos porque agregam valor ao equipamento. As informações de garantia podem ajudar no planejamento do ciclo de vida da aquisição, bem como evitar compras desnecessárias de máquinas quebradas.

Os contratos de licenciamento devem ser rastreados para que os usuários não percam a conformidade e percam o acesso aos serviços fornecidos pela licença ou se tornem responsáveis pelo uso indevido.

Conforme mencionado anteriormente, tags e bancos de dados podem ser usados para rastrear usuários designados de ativos. É surpreendentemente fácil perder o controle dos ativos quando ocorrem mudanças de pessoal ou reorganizações da empresa. A atribuição de usuários também é uma forma de atribuir a responsabilidade pela segurança do ativo, diminuindo a chance de roubo ou uso indevido dos ativos da empresa.

Tipos de documentos Vários

documentos padrão são essenciais para um departamento de TI.

A documentação da infraestrutura de rede e endereçamento, política de uso e procedimentos de conformidade são descritos nas seções a seguir.

Política de Uso Aceitável (AUP)

Uma **política de uso aceitável (AUP)**, no que diz respeito aos procedimentos de segurança e proteção do usuário, é projetada para manter uma rede protegida contra intrusos externos.

O uso aceitável vai ainda mais longe quando se trata de práticas recomendadas de computador dentro de uma empresa. Cada organização deve definir o que considera ser o uso aceitável de seus recursos de computação dentro de sua rede. Por exemplo, as redes governamentais geralmente não estão disponíveis para uso privado, portanto, o e-mail privado pode não ser permitido em computadores de trabalho. O uso inapropriado da Web tem sido um problema nos locais de trabalho desde que a Internet se tornou comum nos negócios.

Para proteção legal da empresa, regras de uso aceitável precisam ser estabelecidas e então aceitas pelos usuários (geralmente com uma assinatura). um AUP

documento é muitas vezes assinado durante o processo de integração quando um funcionário é contratado.

Diagramas de Topologia de Rede

Quando um técnico é chamado a um prédio para atender um computador ou uma rede de computadores, uma das primeiras tarefas é entender como a rede deve funcionar. Um **diagrama de topologia de rede** é essencialmente um mapa de uma rede que mostra como o equipamento está fisicamente organizado no edifício e logicamente conectado como uma rede.

Um diagrama de topologia física usa ícones de representação para representar tipos de equipamentos, como laptops, PCs, servidores, pontos de acesso sem fio, switches e roteadores. Também pode mostrar como os computadores e as impressoras estão organizados, bem como os cabos físicos que os conectam. A Figura 9-1 mostra um exemplo de diagrama de topologia física básica com computadores conectados em uma rede.

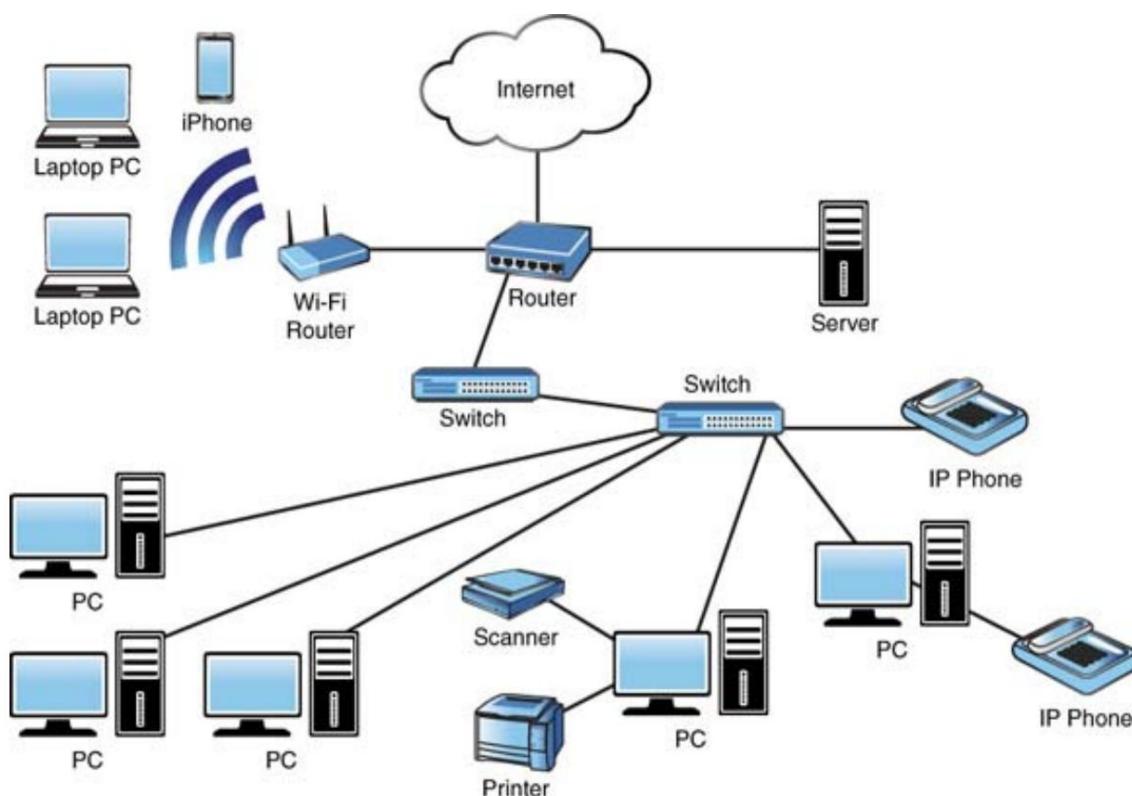


Figura 9-1 Um Diagrama de Topologia Física

Um *diagrama de topologia física* também mapeia as portas de acesso sem fio e os armários de fiação. O diagrama pode “aumentar o zoom” e representar uma única sala ou andar. Os técnicos podem usar um diagrama de topologia física para localizar um dispositivo para o qual foram chamados. Os técnicos também podem usar o diagrama para ver quais outros equipamentos, como impressoras, câmeras de segurança e interruptores, estão em uso e onde encontrá-los. Como alternativa, as topologias físicas podem “diminuir o zoom” e fornecer o design geral de um edifício, incluindo armários de fiação nos andares e o ponto de presença (PoP) para conectividade com o ISP. Essas folhas cortadas devem ser afixadas em armários de fiação seguros, mas, por motivos de segurança, não devem ser disponibilizadas ao público em geral.

Um *diagrama de topologia lógica* descreve o design de uma rede, incluindo como os computadores são agrupados em redes locais (LANs). Um diagrama lógico pode incluir um mapa básico de armários de fiação e áreas gerais do edifício, mas em vez de se concentrar em computadores, esse diagrama aponta endereços IP de rede. Isso é benéfico porque a solução de problemas de conectividade com a Internet é uma parte importante do dia de trabalho de TI; saber em qual rede os dispositivos devem estar economiza tempo na solução de problemas. [A Figura 9-2](#) mostra um diagrama de topologia lógica de uma instalação médica.

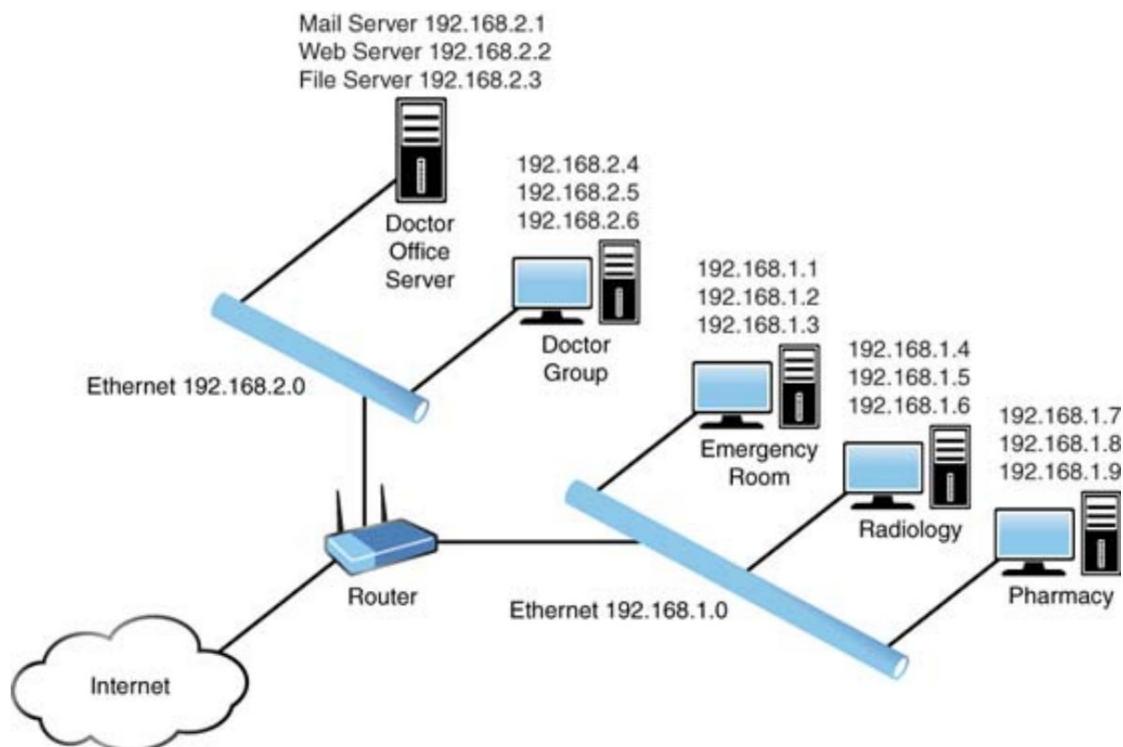


Figura 9-2 Um Diagrama de Topologia Lógica

Política Regulatória e de Conformidade

A conformidade com os regulamentos do governo local é uma parte necessária do trabalho legal e seguro com eletrônicos e tecnologia. Muitos regulamentos regem os locais de trabalho e variam em diferentes áreas. Por exemplo, a reciclagem de eletrônicos está sujeita às leis locais de descarte, e as preocupações com a privacidade dos dados do cliente estão cada vez mais sujeitas ao escrutínio regulatório. Os códigos de construção para projetos elétricos e de ventilação também estão sujeitos às regras locais.

É importante conscientizar todos os usuários de tecnologia sobre os procedimentos e documentários. Considere algumas maneiras pelas quais isso ocorre:

- **Telas iniciais:** essas telas exibem logotipos ou políticas que dão as boas-vindas a um usuário na inicialização ou no login. Estes podem ser acompanhados por uma caixa de seleção exigindo o reconhecimento de certas regras antes que o usuário possa acessar os recursos da empresa.
- **Relatórios de incidentes:** Quando uma regra ou lei é violada, um relatório de incidente é necessário para que a empresa possa rastrear suas responsabilidades legais. Isso permite que a empresa planeje o treinamento e cumpra as leis conforme necessário.
- **Procedimentos operacionais padrão (SOP):** A maioria das grandes organizações possui um manual de SOP, às vezes conhecido como política ou manual do funcionário, para documentar as maneiras adequadas de uma empresa fazer negócios. Estes são frequentemente atualizados e se tornam objeto de treinamento recorrente dos funcionários. Seguem exemplos de procedimentos em um SOP:
 - Procedimentos para rastrear o licenciamento de instalações de software
 - políticas de senha
 - Novas listas de verificação de configuração do usuário
 - Políticas de rescisão de usuário final

Base de conhecimento e artigos

Leitura e pesquisa também são habilidades técnicas. Ser técnico de informática é estar em constante aprendizado, e um bom técnico sabe

como encontrar respostas para problemas incomuns. Manter uma biblioteca de artigos e links para recursos úteis é essencial.

Um whitepaper é um tipo de recurso comum em campos técnicos. Um whitepaper difere de outros tipos de redação, pois se concentra em um tópico técnico complexo e tenta torná-lo compreensível para o leitor comum. As empresas geralmente publicam whitepapers sobre novas tecnologias ou produtos que estão apresentando ao público para que possam influenciar os tomadores de decisão. As bases de conhecimento também podem consistir em links para fóruns de suporte comumente acessados, onde colegas profissionais de TI buscam e fornecem suporte técnico.

A maneira mais fácil de acessar artigos e white papers da base de conhecimento é acessar o site de suporte de um produto ou pesquisar um tópico. Um exemplo de site de suporte à documentação é o site de documentação do AWS CloudFormation, em <https://docs.aws.amazon.com/cloudformation/index.xhtml>.

Mudar a gestão



220-1102: Objetivo 4.2: Explicar as melhores práticas básicas de gerenciamento de mudanças.

A mudança é uma força constante no campo de TI. Essa força precisa ser bem gerenciada para que a mudança possa melhorar os processos na organização e evitar perigos potenciais. Por exemplo, se um gerente de dados deseja fazer alterações em um sistema de software de gerenciamento de empréstimos em um banco, o gerente deve primeiro certificar-se de que o departamento de marketing, que pode depender dos dados do empréstimo, tenha um software que funcione com o novo sistema. Caso contrário, melhorar a gestão de empréstimos pode causar problemas para o departamento de marketing.

O gerenciamento de mudanças é o processo de preparação e controle de mudanças em uma rede, incluindo planejamento, pessoal, organização e obtenção de feedback das partes interessadas afetadas. O gerenciamento de mudanças é estudado por organizações de TI e de negócios, como o Departamento de Tecnologia da Informação

Infrastructure Library (ITIL) e ISO/IEC 20000, que produzem diretrizes de processo de mudança para seus membros.

Processos e práticas de negócios documentados

Saber como uma empresa executa suas diversas tarefas pode ajudar a criar um mapa de como a mudança deve ser implementada. Não se pode presumir que todos possam ficar sem serviços enquanto a rede estiver inativa. Além disso, provavelmente também existe uma enorme sobreposição no uso da rede. Por exemplo, mudanças no final da produção de um negócio podem impactar involuntariamente outras partes. Um gerente de TI pode acreditar que um servidor antigo é inútil, sem perceber que ele serve como um servidor de backup para outro departamento.

Mesmo pequenas mudanças em uma rede precisam ter uma implementação bem planejada. O gerenciamento de mudanças coloca o planejamento em primeiro plano e envolve o pessoal de TI e os usuários de toda a organização. É importante que todos os usuários de uma rede estejam cientes das mudanças que virão e entendam, a partir de uma análise detalhada, como essas mudanças impactarão suas funções. Por exemplo, uma alteração de software feita para beneficiar as funções de vendas ou marketing pode ter um efeito adverso sobre como a contabilidade rastreia as despesas da empresa. Compreender o impacto total de uma mudança em toda a organização é essencial, e esse conhecimento deve ser levado aos membros do conselho de mudança.

Muitas partes de uma organização usam a infraestrutura de TI de maneiras diferentes, e é necessário ter um documento que registre como ela é usada. Isso significa criar um registro de quem usa a rede, quais partes usam e como impactam outros usuários.

Plano de reversão

O **plano de reversão** (também chamado de plano de reversão) é um documento que permite que os administradores de alteração restarem a rede para o nível de serviço que estava presente antes da alteração. Às vezes, mesmo os melhores planos podem ter consequências não intencionais em uma rede ou uma atualização planejada pode falhar. Quando isso acontece, é importante ter um documento exato que conte todas as etapas planejadas e registre os códigos de configuração necessários para voltar ao normal.

Teste de Sandbox

Uma sandbox digital, como um ambiente de máquina virtual (VM), é uma área off-line onde mudanças e ideias podem ser testadas antes de serem aplicadas em redes de produção ao vivo. Ao replicar o ambiente de trabalho em um sandbox, qualquer falha na mudança pode ser identificada antes da implementação.

Funcionário responsável

Uma pessoa designada geralmente coordena as mudanças com as partes interessadas em toda a organização. Essa pessoa, chamada de líder de mudança, pode comunicar as mudanças planejadas a diferentes departamentos para que possam verificar possíveis impactos ou problemas que possam causar consequências não intencionais a outras partes da rede ou organização.

Gerenciamento de

mudanças Conforme definido anteriormente, o gerenciamento de mudanças é o processo de preparação e controle de mudanças em uma rede, incluindo planejamento, pessoal, organização e obtenção de feedback das partes interessadas afetadas. Quando ocorrem mudanças, é importante registrar o que foi mudado e como foi realizado. A documentação da mudança pode incluir um plano de retorno a ser implementado caso surjam problemas em uma data futura. Este documento precisa estar disponível para qualquer pessoa que queira fazer mais alterações na rede. As seções a seguir documentam alguns dos detalhes mais refinados do gerenciamento de mudanças.

Formulários de Solicitação

Os departamentos que desejam planejar ou implementar alterações em sua parte de uma rede maior devem enviar um formulário, geralmente localizado no manual de procedimentos operacionais padrão, à pessoa designada responsável pelas alterações na rede geral. O formulário deve exigir descrições da mudança proposta, os custos (tanto técnicos quanto financeiros) e os benefícios da mudança. O formulário pode então ser usado como base para comunicação com outras partes interessadas na organização.

Finalidade da Mudança

A clareza de propósito é essencial para uma mudança ou migração de rede bem-sucedida. Primeiro, conhecer o propósito do projeto ajuda a limitar o escopo da mudança e evita que ela fique maior do que o necessário. Em segundo lugar, os usuários serão incomodados, então eles precisam ser incluídos no processo para identificar problemas e ajudar a tornar a mudança bem-sucedida.

Escopo da mudança

O escopo refere-se à extensão do *impacto* de uma mudança. O escopo deve ser determinado para que todos os usuários e gerentes afetados não percam repentinamente a capacidade de trabalhar quando uma mudança é implementada. Definir o escopo de uma mudança significa criar um plano detalhado discriminando processos e configurações que permanecerão os mesmos após a mudança (por exemplo, configurações de aplicativos necessárias para executar funções principais), hardware ou software que desaparecerá e as mudanças que têm um resultado misto (significando algum benefício, como eficiência, mas também algumas desvantagens, como demissões de funcionários leais).

Data e Hora da Alteração

Certifique-se de anunciar a data e a hora de uma mudança com bastante antecedência para que outras pessoas também possam planejar. Esses planos geralmente exigem que as alterações ocorram durante o período de inatividade à noite, quando o menor número de usuários será afetado, especialmente se houver uma interrupção do sistema esperada.

Sistemas Afetados/Impacto

Um objetivo fundamental no gerenciamento cuidadoso da mudança é evitar problemas não intencionais para vários sistemas que estão em vigor. Por exemplo, escolher a hora de uma mudança é importante; fazer uma alteração ao mesmo tempo em que uma folha de pagamento está sendo processada pode causar problemas não apenas para a folha de pagamento, mas também para os funcionários que dependem de contracheques em dia. Assim, é importante identificar todos os sistemas que serão afetados pelas mudanças e mitigar o impacto em suas tarefas.

Análise de risco

Algum nível de risco está sempre presente ao fazer alterações em uma rede. Um objetivo do gerenciamento de mudanças é identificar os riscos e mitigá-los.

Exemplos de riscos para os quais os gerentes de TI planejam incluem atrasos,

qualidade esperada e uso de mais recursos. Quando os riscos são identificados, gerentes e planejadores podem trabalhar para neutralizá-los.

Um gerente de mudança pode atribuir um nível de risco de categorias de alto, médio e baixo risco e, em seguida, gerenciar os recursos da equipe de acordo com o impacto potencial na organização.

A análise de risco geralmente é realizada usando métodos de análise qualitativos ou quantitativos. Uma avaliação de risco qualitativa pode envolver brainstorming, grupos focais, pesquisas e processos semelhantes para determinar o valor e avaliação de ativos para a organização. A incerteza também é estimada, permitindo uma projeção relativa do risco qualitativo para cada ameaça. Os níveis de risco podem receber um valor numérico com base em sua posição em uma matriz de risco/mapa de aquecimento que representa a probabilidade (de muito baixo a muito alto) e o impacto (de muito baixo a muito alto). Valores numéricos podem ser atribuídos a cada estado (muito baixo = 1, baixo = 2, moderado = 3 e assim por diante) para executar uma análise quase quantitativa, mas como as categorias são atribuídas subjetivamente, o resultado permanece qualitativo. Uma avaliação quantitativa é menos subjetiva; o processo requer a atribuição de um valor a todos os vários componentes. Para realizar uma avaliação de risco quantitativa, uma estimativa de perdas potenciais é calculada.

Aprovações do Conselho de

Mudanças O conselho de mudanças (também conhecido como conselho consultivo de mudanças, ou CAB) é um grupo reunido de áreas da organização que serão impactadas pelas mudanças planejadas. A tarefa do conselho de mudança é analisar as solicitações de mudança (RFCs) e estudar os benefícios e riscos da implementação de mudanças. O gerente de mudança trabalha sob a autoridade do conselho de mudança e dá aprovação para que o gerente prossiga com o trabalho necessário a ser feito. Os membros do conselho de mudança geralmente são funcionários de nível de liderança que entendem o impacto que as mudanças solicitadas terão no trabalho em suas respectivas áreas.

Aceitação do usuário final

Os usuários finais da rede serão os árbitros finais de sucesso ou falha na migração de mudança. Aqueles que planejam e implementam a mudança devem ser informados, mas como todos os usuários terão uma função, eles precisam ser

envolvido também. Os gerentes podem precisar agendar o tempo de treinamento e os usuários podem ter que aceitar e suportar uma curva de aprendizado. Quanto mais propriedade eles puderem ter no processo, maior a probabilidade de os usuários tolerarem as dificuldades do processo.

Métodos de backup e recuperação da estação de trabalho



220-1102: Objetivo 4.3: Dado um cenário, implemente métodos de backup e recuperação da estação de trabalho.

Ao longo deste livro, mencionamos que os dados costumam ser o ativo mais importante que uma empresa deve proteger. A perda ou violação de dados pode paralisar uma empresa e derrubá-la. Desastres, por definição, são repentinos e causam grandes danos. Eles geralmente são movidos pela natureza e não podem ser evitados. O melhor que uma organização pode esperar ao planejar um desastre é ter um sistema que possa falhar bem e fornecer um caminho razoável para a recuperação.

Restaurar e recuperar

Existem quatro tipos principais de backup de dados:



- **Completo:** um backup completo faz backup de todo o conteúdo do computador ou da unidade selecionada em outro local ou local de rede. Como todos os arquivos são copiados, esse backup leva mais tempo e usa mais espaço de armazenamento.
- **Incremental:** Esses backups copiam apenas os dados que foram alterados desde o último backup. Se um backup completo for executado todo sábado, um backup incremental poderá ser executado todos os dias da semana, registrando um dia de atividade de cada vez. Dessa forma, os backups são atuais, mas um backup completo não precisa ser executado todos os dias.

- **Diferencial:** Esses backups registram dados alterados desde o último backup completo. Esses backups podem ser feitos com frequência para garantir que os backups de dados sejam muito atuais.

Um backup diferencial inclui todos os dados que foram alterados desde o último backup completo, independentemente se ou quando o último backup diferencial foi feito, porque esse backup não redefine o bit de arquivamento, um atributo de arquivo usado para rastrear alterações incrementais em arquivos para esse fim do backup. Um backup incremental inclui todos os dados que foram alterados desde o último backup incremental. Um backup incremental está incompleto para recuperação completa sem um backup completo válido e todos os backups incrementais desde o último backup completo. Por exemplo, se o servidor falhar na quinta-feira, serão necessárias quatro fitas: o backup completo de sexta-feira e as fitas incrementais de segunda, terça e quarta-feira. Um backup completo copia todos os arquivos selecionados e redefine o bit de arquivamento.

- **Sintético:** Esses backups são semelhantes aos backups completos, exceto pelo fato de serem realmente reconstruídos no software a partir de um backup completo anterior e, em seguida, modificados com os backups incrementais que ocorreram desde o backup completo. O benefício é a redução das necessidades de armazenamento para dados de backup.

Teste de backup

Testar backups é importante: o pior momento para descobrir que seus backups agendados não estão funcionando corretamente é quando eles são necessários para recuperar dados. Testar backups garante que os dados necessários estejam disponíveis quando um backup for necessário. Ele também permite que a equipe de TI pratique a restauração para que eles tenham essa habilidade quando for mais necessário.

Cada organização deve determinar a frequência necessária de testes.

Testar não apenas os dados, mas também a infraestrutura, como fontes de alimentação de backup, é um bom plano.

Nos dias em que os backups em fita eram executados, testar os backups era uma tarefa demorada. Graças ao armazenamento em nuvem, soluções de armazenamento conectado à rede (NAS) e virtualização, o processo é muito mais fácil hoje.

Opções de recuperação de conta É

fácil perder o controle de todas as contas que as pessoas mantêm em suas vidas digitais diárias. À medida que aumentamos os papéis do trabalho digital e da recreação em nossas vidas diárias com compras, transações bancárias, assinaturas de TV, armazenamento online, registros médicos e acesso a redes onde trabalhamos, a necessidade de contas e autenticação se torna mais vital. Perder o acesso a uma conta pode resultar em qualquer coisa, desde uma mera inconveniência que requer um processo de recuperação de senha, até um desastre total após o corte de serviços financeiros ou médicos.

A recuperação de conta pode assumir várias formas, dependendo da conta e de quem é responsável pela sua guarda. Não importa quem seja o responsável, os titulares de contas inteligentes sabem como sair do problema antes que o problema ocorra.

Ter um plano para recuperar sua vida digital se laptops ou telefones forem perdidos, roubados ou destruídos permite que você se recupere rapidamente e mantenha os registros seguros até que os dispositivos voltem a ficar online.

A maioria das contas pessoais de fornecedores pode ser recuperada de várias maneiras:

- Enviar um endereço de e-mail da conta na página de login e receber um link de recuperação de senha enviado por e-mail
- Fazer com que um agente de suporte técnico redefina uma conta com uma senha temporária que deve ser redefinida no login
- Respondendo a perguntas secretas com respostas fornecidas durante a configuração da conta

Por exemplo, assinantes de contas de usuário online da Microsoft no Windows podem ter suas contas encerradas se a Microsoft detectar sinais de atividade incomum.

Quando uma conta é desativada, os usuários podem entrar em sua conta da Microsoft e seguir as instruções para obter um código de segurança. Da mesma forma, um banco pode bloquear um cartão de crédito se detectar padrões de compra incomuns; então, ou o banco entra em contato com o cliente ou o titular da conta deve entrar em contato com um agente do banco para verificar as compras.

No trabalho, os usuários contam com o administrador do sistema para ajudá-los a voltar a ficar online. Windows Active Directory e quase todos os outros sistemas de nível empresarial

as soluções de servidor possuem ferramentas administrativas para recuperar contas de usuário excluídas.

Os dados são frágeis por natureza e muitos problemas podem surgir, resultando em dados corrompidos ou inutilizáveis em um computador ou dispositivo móvel. Nossa crescente dependência de dados torna os backups essenciais até mesmo para usuários domésticos. Felizmente, fazer backup de qualquer dispositivo de computação está mais fácil do que nunca.

Windows, Linux e macOS têm sistemas implementados para tornar o backup e, se necessário, a restauração de dados um processo bastante rotineiro. Várias maneiras de fazer backup de imagens estão disponíveis, incluindo backup na nuvem, usando um serviço de backup e criando um sistema de armazenamento conectado à rede (NAS) para uma rede.

Existem três níveis de backup de dados. Eles estão listados aqui e descritos com mais detalhes nas seções a seguir:

- **Imagen do sistema:** Fazendo uma cópia de um disco inteiro, incluindo o imagem do Windows
- **Backup em nível de arquivo:** backup ou arquivamento de arquivos, como documentos, relatórios e imagens
- **Backup de aplicativos críticos:** backup de aplicativos necessários para restaurar os negócios após um desastre

Imagen do sistema

Um backup de imagem do sistema inclui tudo na unidade, incluindo o sistema operacional (que é a imagem do sistema). Esse backup pode ser usado para restaurar um computador com falha se ocorrer uma falha. Este é um backup completo e também é conhecido como um “instantâneo” de tudo em uma unidade em um determinado momento. A hora do instantâneo torna-se o ponto de restauração no processo de recuperação.

Após a instalação do sistema operacional, os arquivos de dados são recuperados. Se o espaço de backup for um problema, fazer um backup de imagem do sistema pode não ser a melhor escolha: o sistema operacional ocupa um espaço considerável e provavelmente já existe uma cópia do sistema operacional que pode ser simplesmente reinstalada. Nos últimos anos, no entanto, os preços de armazenamento caíram e o processo do sistema operacional para backup foi simplificado, portanto, fazer backup com uma imagem do sistema é uma escolha mais comum agora. [O Capítulo 8, “Solução de problemas de software”,](#) detalha esse processo.

Backup em nível de arquivo

Os arquivos geralmente são os dados salvos pelos usuários quando eles usam aplicativos. Os backups de arquivo podem ser documentos, arquivos de mídia (como vídeo ou música) e imagens. Manter apenas os dados ocupa menos espaço do que fazer backup dos aplicativos também. Assim como no sistema operacional, a maioria dos aplicativos pode ser restaurada dos discos originais ou baixada novamente; então os arquivos podem ser recuperados. Consulte o [Capítulo 8](#) para obter detalhes do procedimento.

Aplicações Críticas

Determinar quais arquivos são considerados críticos varia de acordo com a organização, mas geralmente esses são os primeiros arquivos que serão restaurados após um desastre, para que as operações voltem a funcionar. Isso pode ser feito com uma imagem do sistema ou com máquinas virtuais (VMs) que podem ser carregadas para execução rápida.

Esquemas de rotação de backup

É importante gerenciar e organizar backups de dados de maneira que permita acesso confiável aos dados atuais e históricos. Para garantir que os dados estejam seguros e acessíveis, planeje onde e quando os dados serão arquivados, conforme explicado nas seções a seguir.

Backups no local x fora do local



Onde os dados são armazenados é uma consideração vital. Armazená-lo em pelo menos dois locais evita uma possível perda de dados devido a incêndio, inundação, erro humano ou falhas do sistema. Manter uma cópia dos dados de backup no local garante fácil acesso diariamente. O armazenamento no local pode ser em servidores, discos rígidos armazenados, fitas de backup ou outras mídias de armazenamento.

Manter uma cópia redundante dos dados de backup fora do local protege contra um desastre físico que apague dados importantes. O armazenamento externo pode estar em uma nuvem ou pode envolver backup de mídia em outro data center longe o suficiente para não ser afetado pelos mesmos incêndios, inundações ou tempestades que poderiam

prejudicar o centro de dados primário. Manter os dados remotos offline também protege contra hackers.

A maneira mais fácil de fazer backup de dados em estações de trabalho é usar uma unidade externa (disco rígido ou unidade flash USB) com backup redundante na nuvem.

Para um backup de unidade externa, monte uma unidade flash USB (ou um disco rígido externo) e arraste os arquivos para a janela da unidade. Desmonte/ejete a unidade USB e armazene a unidade flash. Em seguida, copie os arquivos para uma unidade flash para backup.

Os utilitários de backup e histórico de arquivos do Windows e o Time Machine no macOS fazem backup facilmente de arquivos e imagens do sistema em discos rígidos externos. Com um disco rígido externo conectado a uma porta USB, inicie o utilitário de backup e selecione a unidade. Quando o backup for concluído, armazene a unidade em um ambiente seguro e seco até que o próximo backup seja executado. Os backups agendados devem ser executados nos horários em que o sistema estiver ocioso, como durante a noite e nos finais de semana. A [Figura 9-3](#) mostra as primeiras etapas do backup do Windows 10 usando o utilitário Histórico de arquivos para armazenar ou recuperar arquivos.

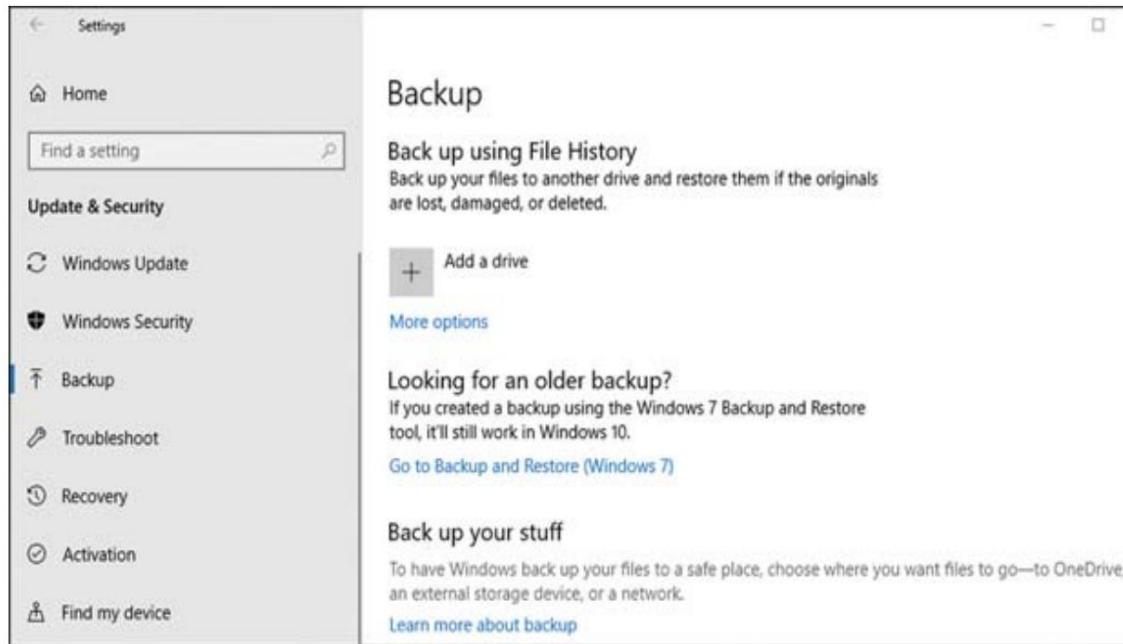


Figura 9-3 Backup do Windows 10

O macOS inclui o Time Machine, um utilitário de backup automático que pode criar backups de hora em hora por 24 horas e que salva esses backups de hora em hora como diários

backups e mantém versões semanais e mensais. Vá para Preferências do Sistema para habilitar e configurar o Time Machine:

Etapa 1. Conecte um disco externo adequado a um sistema macOS (consulte a [Figura 9-4](#)).

Neste exemplo, Rick Bup é um drive externo conectado via USB.



Figura 9-4 Utilitário de backup do macOS Time Machine

Etapa 2. Clique em Disco de backup.

Etapa 3. Na nova janela exibida, marque a caixa **Criptografar backups** para proteger o backup (consulte o encarte da [Figura 9-5](#)).

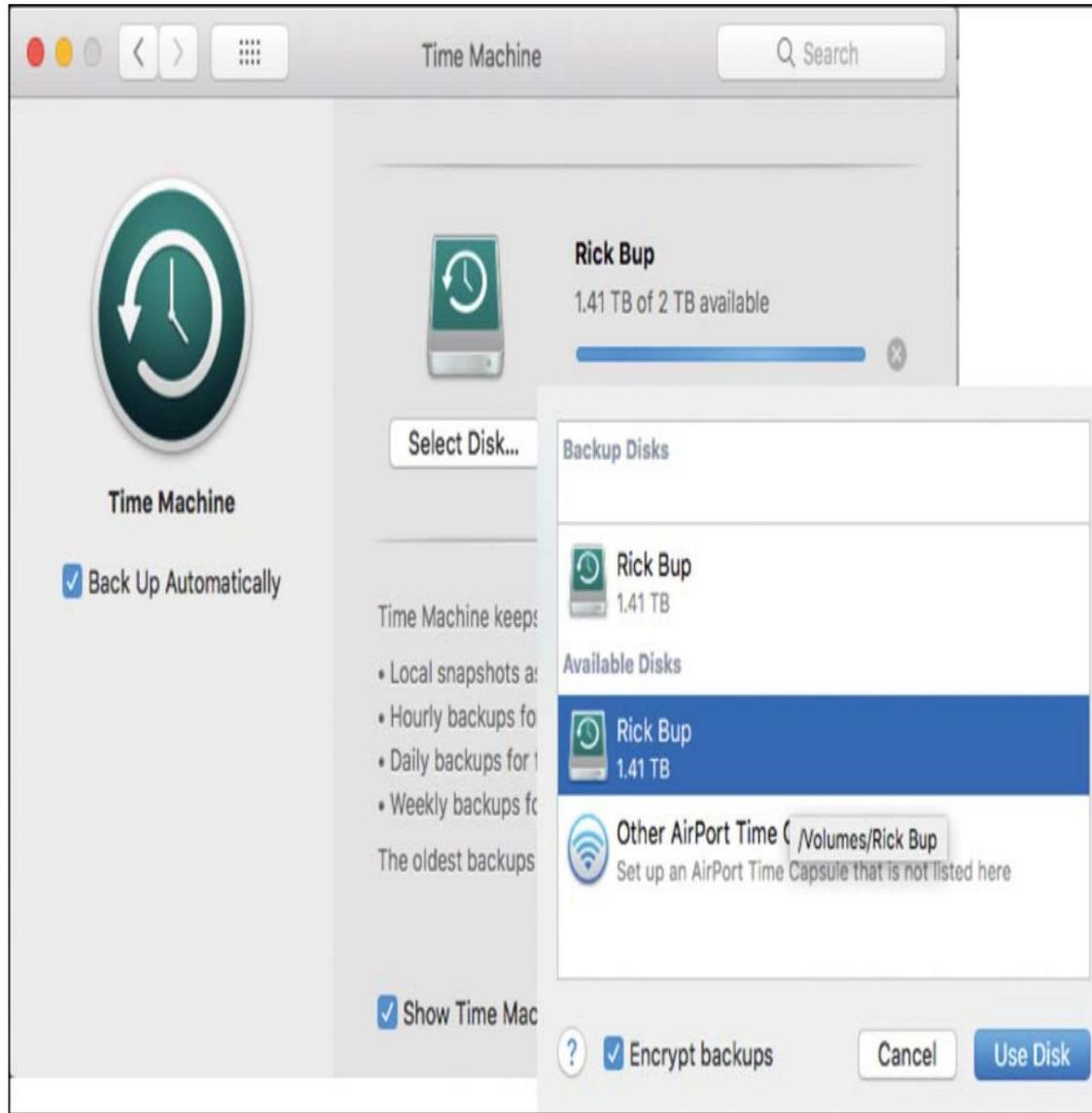


Figura 9-5 Selecionando e criptografando um disco externo (Rick Bup) em Máquina do tempo

Etapa 4. Digite uma senha, confirme-a e digite uma dica de senha. Clique **Criptografar disco.**

Etapa 5. Verifique se o Time Machine está ativado. Depois que o disco selecionado é criptografado, o backup é iniciado.

O Linux inclui vários utilitários que podem ser usados para backups. Isso inclui os utilitários tar e rsync de linha de comando. Outros, incluindo grsync (que é uma GUI para rsync), duplicidade (que está disponível como um utilitário de linha de comando

e também como uma GUI chamada Deja Dup), estão disponíveis no repositório para uma distribuição Linux ou nos fornecedores.

Observação

A página BackupYourSystem no Ubuntu Linux (<https://help.ubuntu.com/community/BackupYourSystem>) fornece uma grande lista de ferramentas de backup baseadas em linha de comando e GUI que também funcionam com outras distribuições do Linux.

O processo de backup de arquivos ou imagens na nuvem pode ser gerenciado por um serviço de backup em nuvem que sincroniza as unidades de acordo com a programação que você escolher. A seguir, nomes comuns no provedor de nuvem cada vez mais lotado arena:

- Amazon Drive
- Dropbox
- Google Drive
- Aplicativo OneDrive no Windows

Essas opções fornecem níveis variados de espaço de armazenamento, serviços de criptografia e preços. Cada um tem um nível introdutório para uso pessoal que oferece espaço de armazenamento gratuito ou com desconto e planos maiores para clientes de nível empresarial.

Todos esses serviços imitam uma unidade flash ou unidade externa montando uma unidade virtual na área de trabalho para acessar arquivos. Como em qualquer outra janela de unidade no computador, os arquivos podem ser copiados ou movidos simplesmente arrastando-os de ou para a janela da unidade na nuvem. Os dados do usuário também podem ser acessados por meio da página da web do provedor. A [Tabela 9-2](#) compara o armazenamento de arquivos na nuvem com o armazenamento local.

Tabela 9-2 Comparando nuvem x armazenamento local

Fator	Armazenamento na nuvem	Armazenamento Local	Vantagem

Fator	Armazenamento na nuvem	Armazenamento Local	Vantagem
meios de comunicação	Rede	Fita, CD, USB, discos rígidos	Nenhum
Custo	Assinatura conforme a necessidade	Hardware, utilitários, custos de localização externa e despesas administrativas	Nuvem
Acessibilidade	Acesso sob demanda	Deve estar fisicamente em arquivos armazenados e protegidos em um local separado	Nuvem
Segurança	Seguro, mas requer Web Acesso	Seguro quando manuseado corretamente	Nenhum
Flexibilidade	Capacidade para trás upar qualquer computador ou arquivo; restaura arquivos sob demanda	Capacidade de fazer backup apenas de computadores locais; requer acesso físico para restaurar arquivos	Nuvem

Como você pode ver na [Tabela 9-2](#), há vantagens crescentes no uso da nuvem, mas os benefícios do armazenamento local seguro não desapareceram completamente. Adicione a essa mistura a possibilidade de nuvens internas, e as linhas ficam ainda menos nítidas. Um bom plano de backup não se restringe a nenhuma dessas opções e envolve aproveitar os benefícios de cada uma.

Esquema Rotacional de Backup Avô-Pai-Filho (GFS)

O método de rotação **avô-pai-filho (GFS)** descreve a manutenção de três gerações diferentes, ou tipos de backups, em vários locais. O nome é simplesmente uma maneira fácil de lembrar que backups completos (avô—talvez um backup mensal armazenado redundantemente fora do local) podem ser combinados com um backup semanal (pai—também enviado fora do local) e um backup incremental diário (filho).

Esse esquema é popular devido ao uso mínimo de tempo e armazenamento para backups menores.

O aumento do uso de armazenamento em nuvem simplifica o processo de armazenamento externo para que o armazenamento de todos os três tipos de backup no local e externo possa ser feito facilmente.

3-2-1 Regra de Rotação de Backup

A **regra** ou esquema de backup 3-2-1 é uma maneira fácil de definir a prática de manter backups:

- **3:** Mantenha uma cópia primária mais duas cópias de backup dos dados.
- **2:** Mantenha dois métodos de armazenamento para os dados (por exemplo, local e nuvem).
- **1:** Mantenha um backup local fora do local, em caso de incêndio ou danos causados por tempestades em uma instalação.

Explicar os procedimentos comuns de segurança



220-1102: Objetivo 4.4: Dado um cenário, use procedimentos de segurança comuns.

A segurança no local de trabalho deve ser a principal preocupação de todos os funcionários em todos os níveis de uma organização. A maioria das organizações possui planos e procedimentos de segurança que se aplicam diretamente ao trabalho executado por um técnico de PC.

Esses técnicos precisam estar cientes não apenas da segurança e proteção dos dados, mas também da segurança física. Esta seção aborda os procedimentos básicos de segurança comuns para um técnico de PC.

A segurança do computador envolve manter os computadores protegidos contra falhas e manter os técnicos seguros enquanto trabalham em um ambiente perigoso. Os seguintes conceitos são abordados nesta seção:

- Prevenção de descarga eletrostática
- Trabalhando com eletricidade com segurança
- Manuseio de lixo tóxico
- Proteger a segurança pessoal e física

Aterramento do Equipamento/Manuseio de Energia Adequado

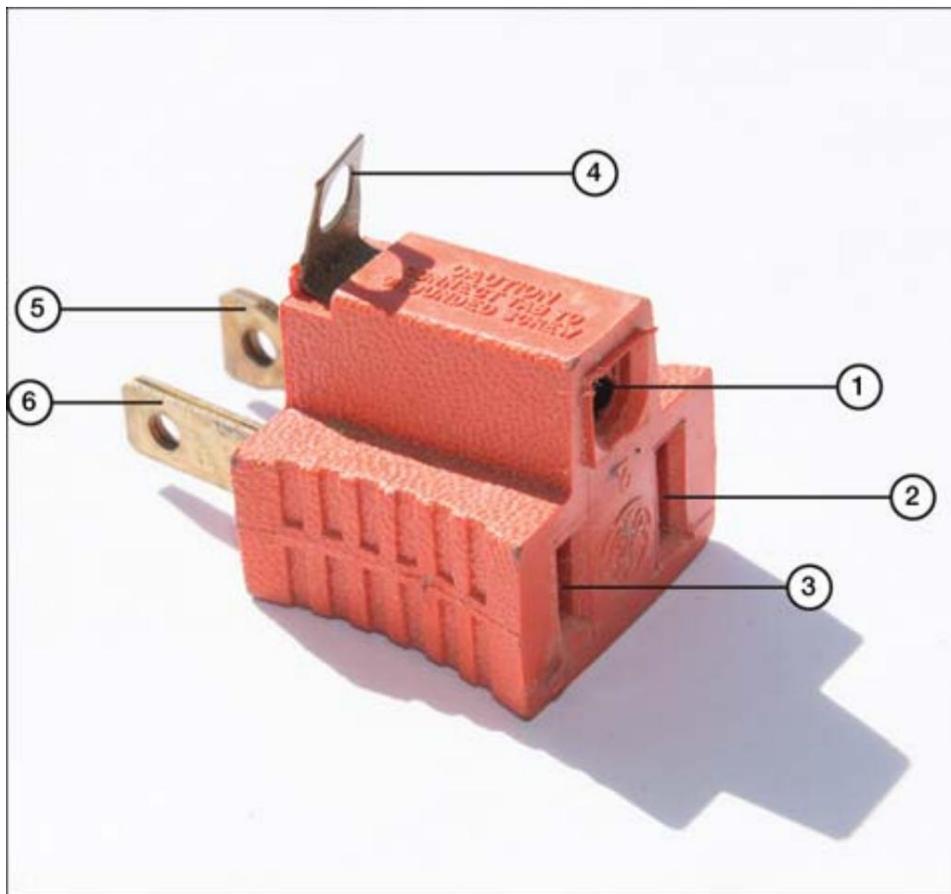


Os códigos de construção exigem que todos os edifícios com serviços elétricos sejam aterrados. *Aterrar* um sistema elétrico significa fazer uma conexão direta do serviço elétrico do edifício à terra, de modo que a tensão perigosa de surtos de linha e descargas atmosféricas encontre seu caminho para a terra, em vez de ferir pessoas, danificar equipamentos ou causar um incêndio. Cada tomada aterrada em um edifício tem uma conexão direta com um eletrodo de aterramento de metal que penetra vários metros na terra. O uso de tomadas de aterramento adequadas fornece um elemento de segurança para o usuário e para o computador. A Figura 9-6 mostra uma tomada comum aterrada. As tomadas aterradas têm três pinos em quase todas as áreas do mundo.



Figura 9-6 Uma tomada comum aterrada (Imagen © Jason Kolenda, Shutterstock)

Quando uma tomada aterrada não estiver disponível, um adaptador aterrado para não aterrado (consulte a [Figura 9-7](#)) pode ser usado para configurações temporárias se o loop no adaptador puder ser conectado a um aterramento de trabalho (como um parafuso de aterramento ou fio de cobre). fio enrolado em um tubo de metal).

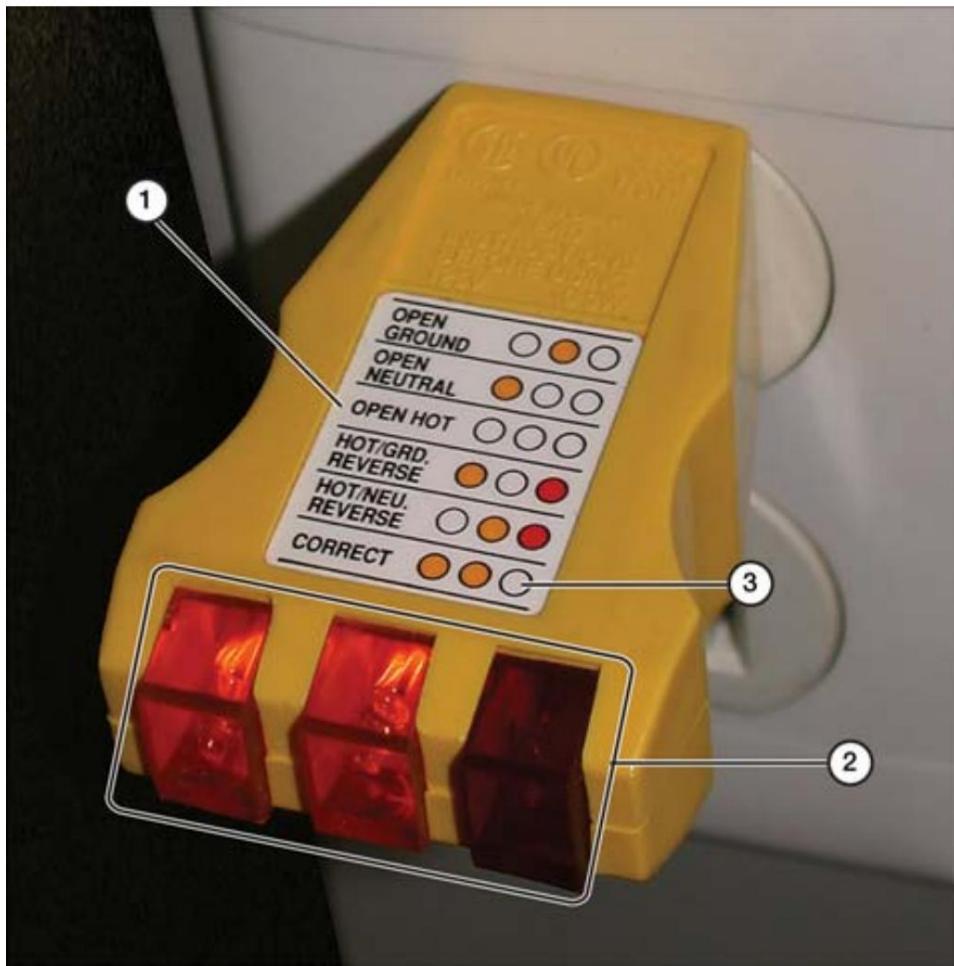


- | | |
|----------------------|------------------|
| 1. Ground connector | 4. Ground loop |
| 2. Neutral connector | 5. Neutral prong |
| 3. Hot connector | 6. Hot prong |

Figura 9-7 Usando um parafuso de aterramento ou fio para fornecer um seguro
Conexão para Equipamentos Aterrados

Nos Estados Unidos, as tomadas elétricas de 120 V CA aterradas são exigidas pelo código desde 1962. Portanto, um problema mais provável em ambientes residenciais e de escritório é a possibilidade de uma tomada aterrada instalada incorretamente: uma em que a linha de aterramento não se conecta a um terra.

A maneira mais fácil de determinar a fiação adequada do prédio, incluindo o aterramento, é usar um testador de tomadas elétricas, como o mostrado na [Figura 9-8](#).



1. Outlet tester legend
2. Test lights
3. Legend indicates wiring is correct

Figura 9-8 Usando um testador elétrico para determinar se uma tomada está devidamente conectado e aterrado (aterrado)

Manuseio e armazenamento adequados de componentes



Durante a construção, atualização, reparo ou desmontagem de equipamentos eletrônicos e de informática, muitas oportunidades potenciais surgem para que o equipamento seja danificado ou destruído por **descarga eletrostática (ESD)**.

ESD é o inimigo silencioso dos equipamentos de informática. O ESD pode ser muito baixo para ser detectado por humanos, mas ainda é forte o suficiente para danificar componentes eletrônicos. O corpo humano constantemente acumula eletricidade estática – mesmo quando está sentado em uma mesa. Além disso, quanto mais seca for a atmosfera, mais facilmente a eletricidade estática se acumula. A [Tabela 9-3](#) mostra o potencial de ESD em diferentes níveis de umidade e atividades.

Tabela 9-3 ESD por atividade e umidade relativa

Atividade	Relativo Umidade
55% 40% 10%	
Atividades normais	
andar no tapete	7500 V 15.000 V 35.000 V
Andar em piso vinílico	3.000 V 5.000 V 12.000 V
Tarefas de Reparo e Embalagem de Bancadas	
Concluindo tarefas típicas de trabalhador em uma bancada eletrônica	400V 800V 6000V
Removendo chips de computador de um tubo de plástico	400V 700V 2000V
Removendo chips de computador de uma bandeja de vinil	2.000 V 4.000 V 11.500 V
Removendo chips de computador de isopor	3500 V 5000 V 14.500 V
Removendo um pacote de bolhas de uma placa de circuito impresso (placa-mãe, placa de vídeo e assim por diante)	7.000 V 20.000 V 26.500 V
Embalar placas-mãe, placas de vídeo ou outras placas de circuito impresso em uma caixa forrada de espuma	5.000 V 11.000 V 21.000 V

O equipamento pode ser danificado por ESD de 700 V ou superior. A Tabela 9-3 demonstra que mesmo atividades comuns podem causar níveis de ESD que são perigosos para os componentes. À medida que a umidade diminui, a tensão liberada durante o ESD sobe.

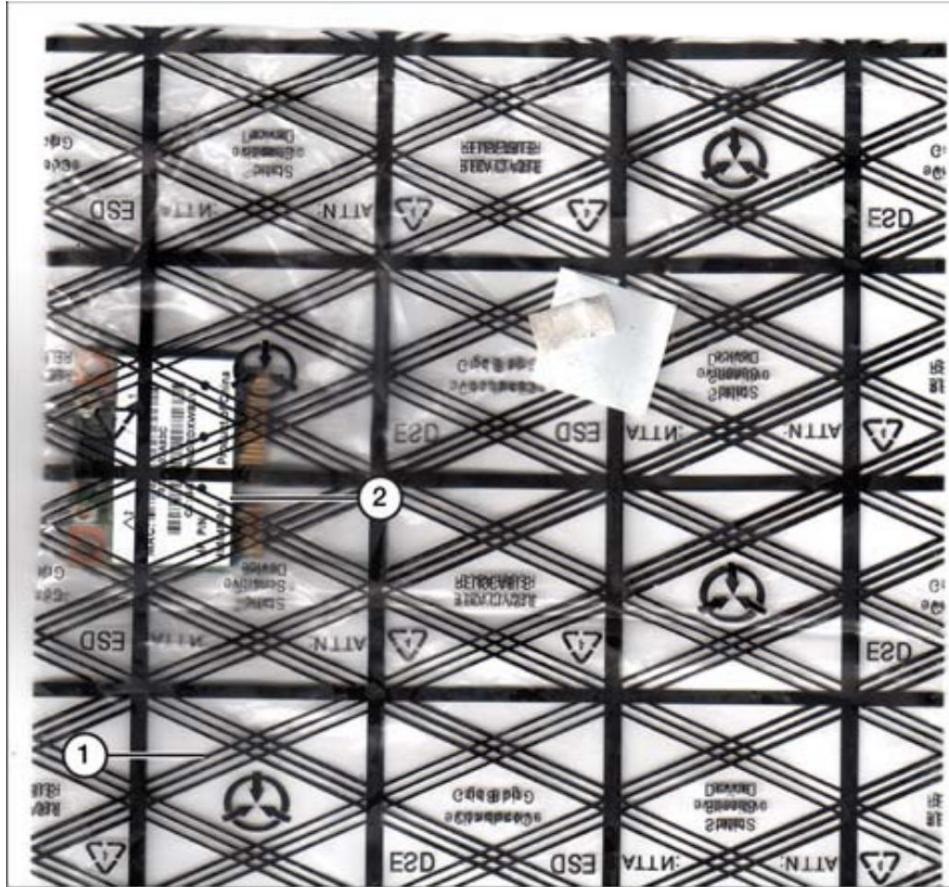
Sem proteção ESD, a eletricidade estática procura descarregar para qualquer outra coisa que tenha um potencial elétrico diferente, especialmente itens metálicos, como placas de circuito. Pegar casualmente uma placa de vídeo cara pode danificá-la. Esse dano pode causar uma falha completa ou problemas intermitentes difíceis de solucionar. Torne as coisas mais fáceis para você, empregando medidas antiestáticas em todos os momentos. Existem quatro chaves para a proteção:

- sacos antiestáticos
- Correias ESD
- tapetes ESD
- Auto-aterramento

Bolsas Antiestáticas

Ao remover um componente de um computador, coloque-o imediatamente em um saco antiestático e coloque-o de lado (consulte a Figura 9-9). As peças nunca devem ficar fora de um saco antiestático. Sacos de plástico bolha normais não constituem proteção antiestática, portanto, certifique-se de usar sacos antiestáticos adequados.

Alguns plásticos-bolha são antiestáticos e são rotulados como tal.



1. Antistatic bag
2. micro PCIe card inside anti-static bag

Figura 9-9 Usando uma bolsa antiestática para proteger um microPCIe Wireless Adaptador de rede

Depois de colocar um item em um saco antiestático, coloque-o em uma caixa protetora para evitar danos por impacto físico.

Correias ESD

Uma pulseira ESD é projetada para equalizar o potencial elétrico do usuário e do dispositivo ao qual a pulseira está presa, como o interior de um computador.

A equalização do potencial elétrico evita a ESD porque a ESD é o movimento da eletricidade entre dois objetos com potencial elétrico diferente.

Uma pulseira ESD tem duas peças:

- Uma tira elástica ou de velcro com um fecho de metal embutido apoiado por uma placa de metal.
- Um cabo flexível enrolado com um encaixe correspondente em uma extremidade e um clipe crocodilo na outra extremidade. O encaixe contém um resistor de 1 megohm, que pode ajudar a prevenir ferimentos em caso de descarga elétrica.

Para usar corretamente uma pulseira ESD, siga estas etapas:

Passo 1. Coloque o elástico ou tira de velcro em torno de um pulso, com o placa de metal plana contra a pele.

Etapa 2. Ajuste a alça até que a placa de metal permaneça no lugar enquanto você move o pulso.

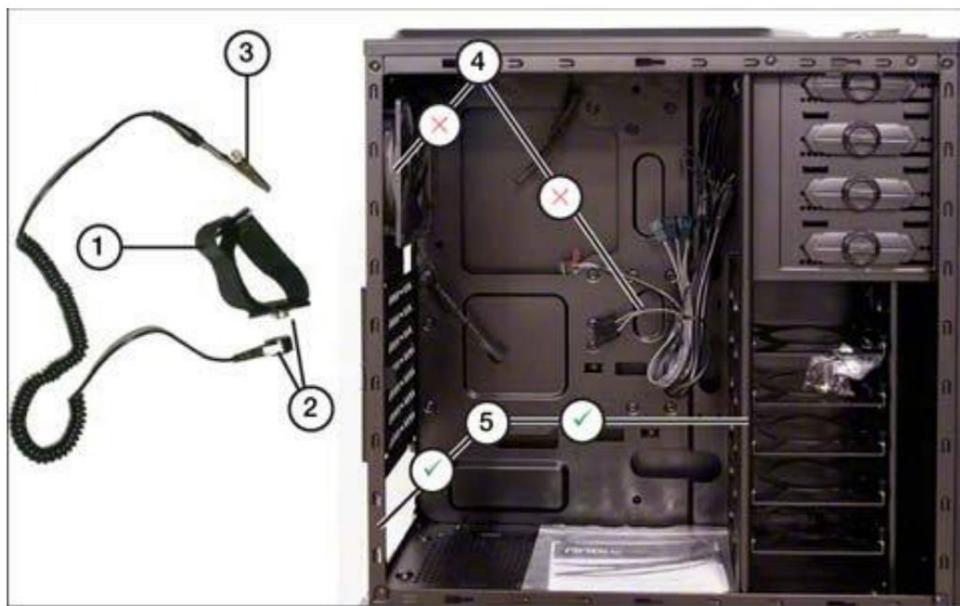
Etapa 3. Encaixe o cabo na alça em volta do pulso.

Etapa 4. Abra o cabo crocodilo e prenda-o no metal não pintado do objeto que você está consertando.

A tira ao redor do pulso com a placa de metal, encaixe e cabo equaliza o potencial elétrico entre você e o objeto que você está consertando, para evitar ESD.

[A Figura 9-10](#) ilustra uma alça ESD típica e os locais adequados para conectá-la a um computador.





1. Adjustable wrist strap
2. Snap cable to wrist strap
3. Clamp alligator clip to unpainted metal components on the device being serviced
4. Not suitable (plastic fan or coated wires)
5. Suitable (metal chassis frame or drive bay frame)
Green check (indicates suitable locations for strap)
Red X (not suitable locations)

Figura 9-10 Usando uma cinta ESD para evitar danos ESD quando Trabalhando em Eletrônica

Tapetes ESD

O próximo nível de proteção para reparos e atualizações de bancada é usar um tapete ESD. Um tapete ESD pode ser conectado a um dispositivo que está sendo reparado usando um dos seguintes métodos:

- Um cabo com um clipe jacaré
- Um cabo com um laço projetado para ser mantido no lugar por um parafuso de caixa, mas com o cabo preso ao tapete em vez de ao seu pulso

Como acontece com uma alça ESD, a extremidade do cabo que se encaixa no tapete tem um resistor de 1 megohm embutido.

O tapete ESD mostrado na [Figura 9-11](#) é empacotado com uma alça ESD. Algumas versões usam material antifadiga adequado para uso em pisos.



1. Resistors built into cables
2. Attach this clip to equipment being serviced

Figura 9-11 Usando um tapete ESD para proteção adicional contra ESD prejudicial

Auto-Aterramento

Em alguns casos, pode ser necessário trabalhar em equipamentos sem qualquer proteção ESD. Nesses casos, o autoaterramento é uma forma de proteger o equipamento que está sendo trabalhado.

O autoaterramento envolve tocar em um componente de metal próximo antes de tocar no dispositivo que está sendo reparado (por exemplo, tocar em uma parte de metal de uma cadeira antes de pegar um componente ou abrir o dispositivo). Antes de abrir um computador, você pode se auto-atarrar tocando em uma parte não pintada do gabinete com as duas mãos antes de instalar ou desinstalar um componente. Faça isso sempre antes de tocar em um componente. Se nenhuma outra opção antiestática estiver disponível, esta técnica pode ser usada como último recurso.

Observação

Lembre-se de manter o computador desconectado enquanto estiver trabalhando dentro dele. Desconecte a alimentação ou desligue o computador usando o botão liga/desliga (se

existe um) antes de trabalhar no sistema. Você pode não saber se a tomada CA está conectada corretamente. Simplesmente desconectando a energia, você elimina qualquer chance de choque.

Outras precauções de segurança e ESD a serem tomadas

Ao trabalhar com eletrônicos, considere estas precauções:

- Ao manusear componentes ou cartões, segure-os pela borda ou suporte. Não toque nos chips, contatos ou outros circuitos.
- Ao manusear componentes, permaneça parado. Não arraste os pés ou mova-se mais do que o necessário ao instalar ou remover o componente.
- Remova as joias e use roupas protetoras. Em alguns laboratórios, os técnicos usam macacões de náilon antiestático. Para a pessoa comum, usar sapatos com sola de borracha também pode ajudar a prevenir ESD.
- Se possível, trabalhe em uma área sem carpete. O carpete é talvez a principal causa de alto potencial elétrico que leva à ESD.
- Evite usar ferramentas alimentadas por CA perto de um computador. Use dispositivos alimentados por bateria (como um multímetro) somente quando necessário.

Conformidade com os regulamentos do governo local

A conformidade com os regulamentos do governo local é uma parte necessária do trabalho legal e seguro com eletrônicos e tecnologia. Verifique com o município local os locais de reciclagem de eletrônicos recomendados que estejam em conformidade com a certificação ISO 14001. Siga também os regulamentos para ventilação e outras questões do local de trabalho.



Segurança pessoal

Nesta seção, discutimos métodos para manter um técnico de bancada seguro enquanto trabalha em computadores e equipamentos eletrônicos.

Desconecte a energia primeiro

A eletricidade é um perigo para computadores e humanos. Aproxime-se com cuidado de qualquer encontro com eletricidade. Certifique-se sempre de desconectar a energia antes de reparar um PC.

Remover joias

Remova joias de todos os tipos (anéis, colares, brincos e assim por diante) antes de trabalhar no computador. Não permita que joias entrem em contato com nenhum componente.

Técnicas de Levantamento

Use técnicas seguras de elevação para evitar lesões. Ao levantar um item grande ou pesado, fique perto do item, agache-se dobrando os joelhos, segure o item com firmeza, mantenha as costas retas e levante lentamente com as pernas, não com as costas. Certifique-se de não torcer o corpo e mantenha o item próximo ao corpo, para ajudar a evitar lesões nas costas. Ao mover itens, é melhor armazená-los na altura da cintura para que seja necessário levantá-los o mínimo possível. A Administração de Segurança e Saúde Ocupacional (OSHA) tem muitas diretrizes e recomendações para segurança física no local de trabalho; consulte www.osha.gov.

Limitações de peso

Conheça suas limitações de peso, para evitar lesões. Levantar itens pesados incorretamente pode causar muitos tipos de lesões. Como regra geral, se um item pesar mais de um quarto do seu peso corporal, você deve pedir a ajuda de outra pessoa. Aproxime-se de uma caixa e mova-a levemente, para avaliar se é necessária ajuda para movê-la com segurança. A elevação está entre as causas mais comuns de acidentes de trabalho.

Segurança Contra Incêndio Elétrico

Com a segurança contra incêndio elétrico, as medidas mais seguras são as preventivas. Os edifícios devem ser equipados com detectores de fumaça e extintores de incêndio. O tipo adequado de extintor de incêndio para um incêndio elétrico é um extintor de Classe C. Os extintores de incêndio BC à base de CO₂ são comuns e relativamente seguros para os seres humanos, mas podem causar danos aos computadores. Se o equipamento precisar ser mais protegido, um extintor ABC Halotron deve ser usado. Salas de servidores e centros de dados geralmente são protegidos por um sistema maior de proteção especial contra riscos que usa o sistema de agente limpo FM-200. Este agente limpo não causa danos aos servidores e outros equipamentos caros e também é seguro para humanos.

Se você vir um incêndio elétrico, use o extintor adequado e tente apagá-lo. Se o incêndio for grande demais para você controlar, disque o número de emergência do seu país (911 nos Estados Unidos). Em seguida, evacue o prédio. Posteriormente, você pode notificar a administração do prédio, seu supervisor ou outras pessoas das instalações. Se o incêndio envolver um fio elétrico energizado, ele deve ser desligado na fonte. Não tente fazer isso com as mãos desprotegidas e certifique-se de que seus pés estejam secos e que você não esteja em pé na água. Use uma vara, tábua ou corda de madeira. Se isso não for possível, entre em contato com o supervisor ou a administração do prédio para que eles possam desligar a energia em outra junção.

Se você encontrar uma pessoa aparentemente inconsciente debaixo de um fio energizado, não toque na pessoa. Novamente, tente mover o fio energizado com uma vara de madeira ou objeto semelhante. Nunca use nada de metal e não toque em nada de metal enquanto estiver fazendo isso. Depois de mover o fio, ligue para o 911 e contate imediatamente seus superiores. Enquanto espera, tente administrar os primeiros socorros à pessoa.

Siga sempre a política da empresa e os regulamentos do governo local para lidar com emergências.

Gerenciamento de cabos

O gerenciamento de cabos é ainda mais importante fora de um computador do que dentro dele. O roteamento de cabos de alimentação e cabos de dados dentro de um PC é importante para fornecer um bom fluxo de ar para resfriamento. No entanto, os cabos fora do computador podem ser um risco de tropeçar. Quaisquer cabos USB externos devem ser roteados de modo que não

não interfira na atividade normal dos funcionários. Mais importante, os cabos de rede devem ser estacionários e roteados longe das áreas de passagem.

Os governos locais têm regras sobre como os fios de rede e telecomunicações devem ser instalados, e muitos municípios exigem uma licença para instalar qualquer um desses cabos. Ao passar cabos de rede para novos computadores, primeiro verifique os regulamentos locais e veja se um instalador licenciado é necessário para conformidade com os regulamentos do governo local. Certifique-se de que os cabos não representem perigo de tropeçar e, se possível, não estejam perto de quaisquer dispositivos elétricos ou fios.

Óculos de segurança

Use óculos de segurança ao realizar reparos, limpeza ou atualizações do computador para evitar lesões oculares causadas por poeira, sujeira, parafusos soltos ou porcas, solda ou outras ameaças. O padrão dos EUA para óculos de trabalho de proteção é ANSI Z87.1-2010. Os protetores oculares que atendem a esse padrão podem ser classificados para aplicações sem impacto ou de impacto (Z87+), portanto, escolha de acordo com os riscos envolvidos em sua aplicação específica.

Em outros países, determine os padrões relevantes para proteção industrial ao selecionar óculos de segurança.

Máscara de filtro de ar

Se um trabalho que está sendo executado requer usinagem de metal, polimento, lixamento, soldagem, processamento de resíduos, reciclagem ou pintura como parte ou todo o seu trabalho relacionado à tecnologia, uma máscara de filtro de ar pode ser necessária para segurança.

Os padrões do Instituto Nacional de Segurança e Saúde Ocupacional dos EUA (NIOSH) para respiradores com filtro de partículas incluem as seguintes séries de filtros:

- **N:** Não resistente a óleo
- **R:** Resistente ao óleo
- **P:** À prova de óleo

As classificações mais altas disponíveis são P100 (99,97% de eficiência contra aerossóis de partículas de óleo e não óleo, para atender aos padrões HEPA), R95 (95% de eficiência contra aerossóis de partículas de óleo e não óleo) e N95 (95% de eficiência contra aerossóis particulados). Alguns filtros também podem bloquear ozônio.

Verifique os tipos de perigo particulado associados a uma tarefa antes de selecionar um filtro da série R ou da série N, ou escolha um filtro P100. Algumas máscaras podem aceitar qualquer um desses tipos de filtro.

Impactos Ambientais e Controles Apropriados



220-1102: Objetivo 4.5: Resumir os impactos ambientais e os controles ambientais locais.

O equipamento de TI não está restrito a data centers climatizados, e um profissional de TI deve estar ciente de como diferentes ambientes podem afetar o desempenho de um computador ou rede.

Para o exame 220-1102, você precisa saber como controlar a temperatura e a umidade, o que é um MSDS e como usá-lo e como lidar com poeira e detritos quando se trata de computadores.

Ficha de Dados de Segurança do Material (MSDS)



Uma **folha de dados de segurança de material (MSDS)** é um documento que fornece informações sobre substâncias específicas, como o toner no cartucho de toner de uma impressora a laser. Qualquer produto que usa produtos químicos é obrigado a ter um MSDS. Um MSDS inclui as seguintes informações:

- Tratamento adequado se uma pessoa entrar em contato ou ingerir a substância

- Como lidar com derramamentos
- Como manusear e descartar adequadamente a substância
- Como e onde armazenar a substância

Observação

O termo *MSDS* foi atualizado para *SDS* (Safety Data Sheet). Ambos os termos são vistos em uso comum, mas SDS é o padrão atual.

GORJETA

As classificações de proteção pessoal MSDS são projetadas para informar o consumidor sobre a maneira segura de manusear o material.

As recomendações para as classificações A–D são as seguintes:

- **Classificação A:** Óculos de segurança
- **Classificação B:** Óculos e luvas de segurança
- **Classificação C:** Óculos de segurança, luvas e avental
- **Classificação D:** Protetor facial, proteção para os olhos, luvas e avental

A maioria das empresas tem seus documentos MSDS online. Por exemplo, acessar www.hp.com/us-en/hp-information/sustainable-impact/document-reports.xhtml e pesquisar HP MSDS leva você a todos os documentos MSDS para cartuchos de tinta Hewlett-Packard, cartuchos de toner, produtos de limpeza, projetor digital e lâmpadas de impressora, baterias e assim por diante. Os documentos MSDS geralmente estão no formato PDF, portanto, certifique-se de ter o Adobe Reader ou outro leitor de PDF instalado.

Geralmente, as substâncias que contêm produtos químicos devem ser armazenadas em local fresco e seco, longe da luz solar. “Cool” significa na extremidade inferior da diretriz da OSHA, cerca de 68 graus Fahrenheit (20 graus Celsius). Muitas vezes, isso envolve um armário de armazenamento que fica longe da área de trabalho geral e

fora do sistema de filtragem de ar. Esse armário também costuma ser menos úmido do que outras partes do edifício.

No que diz respeito ao descarte, qualquer substância com MSDS não deve ser jogada fora quando você terminar de usá-la. Geralmente deve ser reciclado de acordo com os procedimentos documentados no MSDS. Essa reciclagem pode ocorrer interagindo com o município local (no caso de baterias) ou devolvendo os itens diretamente ao fabricante ou fornecedor (no caso de cartuchos de tinta/toner).

Saiba o que fazer quando alguém for afetado adversamente por um produto que contém produtos químicos. Uma pessoa pode ter irritação na pele ao entrar em contato com partículas de toner ou um limpador usado em um teclado ou mouse. Como técnico, é seu trabalho descobrir como ajudar essa pessoa.

Se você não tiver acesso direto ao MSDS, entre em contato com o departamento de instalações de sua organização ou com o gerenciamento do prédio. Talvez a equipe de limpeza use um agente de limpeza específico com o qual você não esteja familiarizado e apenas o departamento de instalações tenha recebido o MSDS para isso. É melhor revisar proativamente todos os documentos MSDS, mas, neste caso, você provavelmente não terá acesso ao documento. Colabore com o departamento de instalações para fornecer à pessoa afetada os primeiros socorros adequados e, se necessário, leve a pessoa ao pronto-socorro. Por fim, remova o dispositivo afetado (se for um teclado ou mouse, por exemplo) e substitua-o por um dispositivo semelhante até que o dispositivo original seja limpo adequadamente.



Manuseio/Descarte de Resíduos Tóxicos

O exame de certificação CompTIA A+ aborda três tipos de manuseio seguro de lixo tóxico relacionado a computadores:

- baterias
- Toner
- Outros dispositivos e ativos, como monitores CRT, celulares e tablets

As seções a seguir fornecem orientações sobre o manuseio de resíduos tóxicos.

Reciclagem de baterias

Certifique-se de descartar as baterias corretamente. Baterias de níquel-cádmio (Ni-Cad), níquel-hidreto metálico (NiMH) e íon-lítio (Li-Ion) para celulares, computadores e outros eletrônicos não devem ser descartadas como lixo; nem as células de chumbo-ácido usadas em unidades de backup de bateria UPS. Se esses itens não forem reciclados adequadamente, eles se tornarão lixo tóxico.

Essas baterias podem ser recicladas com segurança de várias maneiras, para evitar ameaças ambientais:



- Para pequenas quantidades de baterias recarregáveis ou dispositivos que contenham baterias recarregáveis, use uma estação de descarte de reciclagem (como uma estação de coleta em uma loja de eletrônicos).
- Para grandes quantidades de baterias recarregáveis, dispositivos ou dispositivos UPS com baterias, entre em contato com um reciclador de eletrônicos em sua área.
- Algumas baterias podem ser devolvidas diretamente ao fabricante para reciclagem.

- Durante o armazenamento e transporte, certifique-se de que os contatos da bateria não se toquem. Verifique e siga os regulamentos relativos ao envio de baterias Li-Ion, que representam um risco potencialmente alto de incêndio e explosão em alguns ambientes.

Toner

Frascos de toner e cartuchos para impressoras e copiadoras a laser devem ser reciclados em vez de descartados. Ao contrário das baterias, os usuários podem ganhar dinheiro ou créditos para compras adicionais reciclando frascos de toner e cartuchos em lojas locais de material de escritório ou lojas de reciclagem de toner.

Embora os cartuchos de jato de tinta não sejam reconhecidos como lixo tóxico, eles também não devem ser descartados; eles podem ser entregues para crédito no material de escritório

lojas ou remanufaturadores de cartuchos de jato de tinta. Alguns fabricantes incluem uma etiqueta pré-paga na caixa que contém a tinta, para facilitar a devolução.

Depois de remover o cartucho de toner antigo, use um aspirador de toner especialmente projetado para remover o toner solto de dentro da impressora antes de inserir o novo cartucho.

Celulares e tablets

Conforme mencionado anteriormente, baterias de celulares e tablets devem ser recicladas. Mas antes de descartar esses dispositivos, certifique-se de que todos os dados pessoais ou da empresa sejam excluídos com segurança e o cartão SIM removido. Os dados a serem verificados incluem contatos, mensagens, downloads, fotos e correios de voz. Os dados do navegador também devem ser limpos.

Sensibilização e Adequação do Nível de Temperatura e Umidade Ventilação

Você deve estar ciente das medições de temperatura e umidade em seu prédio. Você também deve estar pensando em partículas transportadas pelo ar e ventilação adequada. Coletivamente, a OSHA se refere a isso como tratamento de ar. O tratamento do ar envolve a remoção de contaminantes do ar e o controle da temperatura e umidade do ambiente. Embora nenhuma política governamental específica cubra isso, as recomendações sugerem uma faixa de temperatura de 68 a 76 graus Fahrenheit (20 a 24 graus Celsius) e uma faixa de umidade entre 20% e 60%. Lembre-se de que um nível de umidade mais alto significa uma chance menor de ESD, mas as condições podem ficar um pouco desconfortáveis para os trabalhadores; um compromisso deve ser buscado. Se a organização usar manipuladores de ar para aquecer, resfriar e movimentar o ar, será um pouco difícil manter a umidade muito acima de 25 a 30 por cento.

Ventilação adequada

Uma organização deve usar exaustão local (para remover os contaminantes gerados pelos processos da organização) e introduzir um suprimento adequado de ar externo fresco por meio de ventilação natural ou mecânica. Para o tratamento do ar, as organizações devem usar dispositivos de filtragem, limpadores eletrônicos e, possivelmente, tratamentos químicos ativados com carvão ou outro

absorventes (isto é, materiais usados para absorver gases indesejados). A maioria dos sistemas de filtragem usa carvão e filtros HEPA. Esses filtros devem ser substituídos em intervalos regulares. Dutos de ar e abafadores devem ser limpos regularmente, e o isolamento dos dutos deve ser inspecionado periodicamente.

Se um nível considerável de partículas no ar permanecer, podem ser adquiridos gabinetes de filtragem de ar portáteis que também usam carvão e filtros de ar HEPA ou que possivelmente utilizam luz ultravioleta para eliminar partículas. Esses gabinetes são comumente encontrados em instalações de reparo de computadores devido à quantidade de poeira e detritos nos computadores que aguardam reparos. Algumas organizações até fornecem máscaras ou respiradores para seus funcionários.

Sistemas de Ar Comprimido e Vácuo

Uma bancada de PC pode ser equipada com sistema de ar comprimido e sistema de vácuo. Dessa forma, o técnico de PC pode soprar a poeira e a sujeira de um computador enquanto, ao mesmo tempo, o aspira. Caso contrário, a melhor abordagem geralmente é levar o computador para fora ao limpá-lo.

Surtos de energia, eventos de baixa tensão e falhas de energia O fornecimento confiável de energia em um nível consistente é essencial para proteger equipamentos eletrônicos, como computadores e televisões. Mesmo em comunidades com fornecimento de energia de qualidade, picos e quedas de energia colocam os computadores em perigo. Uma tomada elétrica pode estar conectada corretamente (consulte a seção “Aterramento do equipamento”, anteriormente neste capítulo), mas outras ameaças podem afetar o bem-estar de computadores ou outros dispositivos conectados à tomada:

- picos de energia
- Eventos de subtensão
- Falhas de energia

supressores de surto

Um supressor de surto é projetado para impedir que surtos de energia danifiquem o equipamento conectado a ele. **Surtos de energia** são definidos como eventos de sobretensão que não duram mais de 50 ms e podem atingir níveis de tensão de até 6.000 V e 3.000 A.

Os supressores de surto são classificados em joules para indicar a quantidade de energia que um supressor de surto pode absorver antes de falhar. Todos os outros fatores sendo iguais, quanto maior a taxa de joule, melhor. No entanto, lembre-se de que uma unidade com vários varistores de óxido metálico (MOVs) em cada cabo de alimentação pode fornecer melhor proteção do que um único grande MOV.

Os MOVs absorvem picos de energia e se desgastam gradualmente. Embora muitos (mas não todos) supressores de surto tenham luzes que indicam quando a proteção falhou, apenas alguns modelos param de fornecer energia se a proteção falhar.

Preste atenção em quantos computadores estão conectados a um supressor de pico. Adicione as classificações combinadas de potência ou volt-amp dos dispositivos a serem conectados ao supressor de pico e compare com o máximo que o supressor de pico pode suportar. Normalmente, um supressor de pico pode lidar com dois computadores básicos e dois monitores. No entanto, um dispositivo de alta potência, como uma impressora a laser, deve ter seu próprio supressor de pico.

Os supressores de pico devem ser substituídos a cada três a cinco anos ou logo após um evento que danifique os MOVs, como um raio próximo, oscilações frequentes de energia, marcas de queimadura ou fumaça em qualquer tomada da unidade.

Unidades de backup de bateria



Falhas de energia (perda total de energia) e eventos de subtensão (quedas de tensão sustentadas de até metade da saída nominal) impedem o funcionamento de computadores e periféricos. Infelizmente, se os computadores e periféricos ficarem sem energia no meio de backups, atualizações ou relatórios, os arquivos podem ser corrompidos.

A solução é usar uma fonte de alimentação ininterrupta (UPS) de backup de bateria.

As unidades de backup de bateria são classificadas de duas maneiras: volt-amps (VA) e Watts (W). Diferentes unidades de backup de bateria com a mesma classificação de potência podem variar em termos de classificação VA. No entanto, o cálculo usual para comparar as classificações de W e VA é assumir que $VA \times 0,60 = W$. Portanto, um no-break com classificação de 1.000 VA fornece cerca de 600 W de potência.

Além de fornecer energia suficiente para operar os dispositivos conectados (como um computador, um monitor e dispositivos USB, mas não uma impressora a laser), um no-break precisa ser capaz de funcionar com bateria por um período de tempo adequado antes que o no-break o desligue. Isso é chamado de tempo de execução. Alguns fornecedores e sites de terceiros (por exemplo, [www.easycalculation.com/physics/classical physical/ups-power-requirement.php](http://www.easycalculation.com/physics/classical%20physical/ups-power-requirement.php)) fornecem calculadoras que usam watts de entrada ou consumo de amperagem para calcular o tamanho do no-break necessário. Para aumentar o tempo de execução, selecione uma unidade com uma classificação VA ou W maior.

Observação

Não use as tomadas alimentadas por bateria em um no-break para dispositivos como impressoras a laser. Esses dispositivos que consomem muita energia podem esgotar rapidamente a bateria do no-break ou danificar a unidade. Para esses dispositivos, use as tomadas com supressão de surto que não estejam conectadas à bateria.

A Tabela 9-4 fornece uma revisão rápida do que o exame 220-1102 exige que você saiba sobre como lidar com picos de energia, blecautes e quedas de energia.



Tabela 9-4 Condições Elétricas e Medidas de Proteção

Tipo de Elétrico Doença	Descrição	protetor A medida
Surto de energia Evento de sobretensão com duração inferior a 50ms. Até 6000V e 3000A.	Supressor de surtos	
Subtensão Queda de tensão sustentada de até metade da tensão evento. normal. Pode durar de minutos a horas do	UPS	
Falha de energia Perda total de energia por um longo período de tempo.	UPS ou gerador	

Abordagem de Conteúdo/Atividade Proibida e Conceitos de privacidade, licenciamento e política

220-1102
Exam

220-1102: Objetivo 4.6: Explicar a importância do conteúdo/atividade proibida e dos conceitos de privacidade, licenciamento e política.

Os administradores de rede enfrentam vários desafios para manter uma rede segura e protegida. Embora muitas ferramentas e procedimentos sejam usados para evitar o uso indevido de recursos, incidentes de segurança estão prestes a acontecer. Nem todos vêm de fora da rede. Na verdade, algumas das ameaças mais perigosas vêm de usuários dentro da organização que violam regras de segurança ou regras de uso aceitável.

Gerenciar o conteúdo, a atividade e a privacidade do usuário é um desafio porque nem todos os usuários e gerentes entendem esses conceitos da mesma maneira. Uma organização deve criar uma política bem definida que especifique o que é e o que não é uso e prática aceitável. A política também deve definir as consequências do não cumprimento dos padrões da organização durante o uso de seus equipamentos. Esta seção detalha o processo de resposta a incidentes de violação.

Para fins de estudo do processo de resposta a incidentes, o conteúdo e a atividade proibidos podem ser definidos da seguinte forma:

- Qualquer conteúdo armazenado em um computador, dispositivo móvel ou rede pertencente ou gerenciado pela empresa que seja contrário à política organizacional
- Qualquer atividade realizada ou recebida por um computador, dispositivo móvel ou rede pertencente ou gerenciado pela empresa que seja contrária à política organizacional

Quando se descobre que alguém agiu de forma inadequada, ter uma resposta e um processo em vigor protege tanto a organização quanto os usuários.

Key
Topic

Resposta a incidentes

A resposta a incidentes é o conjunto de procedimentos que qualquer investigador segue ao examinar um incidente de tecnologia. A resposta inicial e a documentação são importantes porque as informações e evidências coletadas orientam o resto do processo.

Primeira Resposta

Quando um incidente é relatado, a primeira tarefa do respondente é identificar exatamente o que aconteceu. O respondente deve primeiro *identificar* se este é um problema simples que requer solução de problemas ou um incidente que precisa ser escalado. A chave para qualquer solução de problemas é entender qual problema precisa ser resolvido.

Por exemplo, se uma pessoa tiver conteúdo proibido em um computador, isso pode ser considerado um incidente. Como parte da primeira resposta, o incidente deve ser encaminhado ao supervisor do infrator, relatando exatamente o que foi encontrado. Informações protegidas por direitos autorais, malware, conteúdo impróprio e informações roubadas podem ser considerados proibidos.

Após a identificação do problema, o incidente deve ser *comunicado através dos canais apropriados*. A denúncia por meio dos canais adequados pode incluir a aplicação da lei se o incidente envolver fraude ou a segurança das informações privadas do cliente. Em seguida, devem ser tomadas medidas para garantir a *preservação dos dados/dispositivo*. Isso geralmente significa fazer um backup da imagem do computador usando um software especial para garantir a integridade e preservação dos dados. No entanto, dependendo das políticas da organização, uma abordagem melhor pode ser deixar tudo como está e esperar por um especialista em computação forense ou um analista de segurança. É importante preservar a cena para que um especialista possa coletar evidências.

Documentação

Documentar tudo o que for encontrado e tudo o que acontecer após o relatório inicial é essencial. Se a organização não tiver formatos de relatórios definidos, é apropriado anotar os detalhes e tirar fotos.

Toda e qualquer informação deve estar disponível para o supervisor. Se o socorrista conseguir resolver o problema e nenhum outro especialista for necessário,

o processo de documentação pode continuar até a conclusão da tarefa (e além, enquanto monitora o sistema). A documentação deve incluir quaisquer processos, procedimentos e treinamento de usuários que possam ser necessários para evitar um incidente semelhante no futuro.

Cadeia de Custódia

Se for necessário preservar evidências, uma maneira de fazer isso é estabelecer uma **cadeia de custódia**, a documentação cronológica ou a trilha em papel das evidências. Deve ser iniciado no início de qualquer investigação e deve incluir o rastreamento do processo de evidência/documentação; identificar quem tinha a custódia das provas, até o processo judicial (se necessário); e verificar se a evidência não foi modificada ou adulterada.

Observação

Um técnico de PC normalmente não se envolve muito com as investigações, mas o exame A+ cobre os conceitos básicos de incidente/primeira resposta, documentação e cadeia de custódia.



Licenciamento/Gerenciamento de direitos digitais (DRM)/Contrato de licença de usuário final (EULA)

Todos os tipos de problemas de licenciamento de software podem complicar sua vida como técnico de PC. É importante perceber que o descuido com o licenciamento pode colocar sua empresa em risco financeiro e legal.

A seguir, alguns problemas a serem observados:

- As limitações criadas pelo gerenciamento de direitos digitais (DRM)
- Contratos de licença de usuário final (EULAs)
- Código aberto x licenças comerciais
- Licenças pessoais x corporativas

DRM

Gerenciamento de direitos digitais (DRM) é o termo geral para mecanismos de software ou serviço que limitam os direitos do usuário final de copiar, transferir ou usar software ou mídia digital. A seguir estão alguns exemplos de DRM:

- Restrições na reprodução de música digital quando a música foi gravada em um CD de áudio, como no Apple Music
- Limites no número de sistemas que podem usar um aplicativo ao mesmo tempo, como Adobe Creative Cloud ou Microsoft Office 365

Ao atualizar um sistema que executa aplicativos baseados em DRM, é importante determinar com antecedência como a atualização pode afetar os problemas de DRM. Em alguns casos, mudar para um novo sistema operacional pode ser transparente para o sistema DRM; em outros casos, o sistema DRM pode exigir que o usuário confirme a licença.

Ao remover de serviço um sistema que está executando aplicativos baseados em DRM, é importante determinar com antecedência como mover corretamente os aplicativos baseados em DRM ou arquivos limitados por DRM para outro sistema. A autorização pode precisar ser removida do sistema antes que um novo sistema possa ser autorizado a usar o aplicativo.

EULA

Um **contrato de licença de usuário final (EULA)** restringe como um aplicativo pode ser usado e quais direitos de transferência estão disponíveis. Se um aplicativo foi pré-instalado em um sistema, seu licenciamento pode não permitir que o aplicativo seja movido para outro sistema. Certifique-se de verificar o EULA de um aplicativo específico ou de um sistema operacional com aplicativos integrados para determinar o que pode ser feito legalmente com o sistema operacional e os aplicativos quando o computador original for retirado de serviço ou atualizado para um novo sistema operacional.

Compreendendo o código aberto e as licenças comerciais

De acordo com o site da Open Source Initiative (<https://opensource.org/osd>):

Geralmente, o software de código aberto é um software que pode ser acessado, usado, alterado e compartilhado livremente (em forma modificada ou não modificada) por qualquer pessoa.

O software de código aberto é feito por muitas pessoas e distribuído sob licenças que cumprem com a Definição de código aberto.

As distribuições do sistema operacional Linux (conhecidas como *distros*) e os aplicativos Linux são alguns dos exemplos mais conhecidos de software de código aberto.

O software de código aberto pode ser usado para fins comerciais e pode até ser vendido. No entanto, **as licenças de código aberto** exigem que os vendedores de software de código aberto não limitem os direitos dos compradores de usar, alterar ou compartilhar o software. Por exemplo, os direitos obtidos quando a Empresa A passa a usar o Software X devem ser repassados à Empresa B quando a Empresa A vende qualquer versão do Software X, e assim por diante. Esses direitos incluem o código-fonte.

Observação

O site da Open Source Initiative oferece uma variedade de licenças aprovadas pela OSI que podem ser usadas como modelos para licenciamento; consulte <https://opensource.org/licenses>.

A maioria dos softwares comerciais que não sejam de código aberto podem ser chamados de código fechado. Por exemplo, Microsoft Windows, Apple macOS, Adobe Creative Cloud e Microsoft Office são exemplos de sistemas operacionais e aplicativos que usam licenças comerciais. Ao contrário de uma licença de código aberto, que permite o uso, modificação e compartilhamento gratuitos do código-fonte, as licenças comerciais não cobrem o código-fonte (as instruções reais usadas para fazer o software).

Eles também limitam como os licenciados podem usar o código objeto (o programa). Por exemplo, as assinaturas da Adobe Creative Cloud podem ser usadas em dois computadores (por exemplo, um trabalho e um computador doméstico ou de viagem), mas não ao mesmo tempo. Se um terceiro computador tiver a Adobe Creative Cloud instalada, a Adobe permite que os aplicativos da Creative Cloud sejam executados no dispositivo adicional se as licenças dos outros computadores forem desativadas pela Creative Cloud.

Licenças pessoais x empresariais

Licenças de **uso pessoal** são licenças de software fornecidas para computadores adquiridos em lojas de varejo ou online e aplicativos baixados ou empacotados projetados para uso por indivíduos. Essencialmente, essas licenças limitam o uso de

o software para um ou um número muito pequeno de computadores na mesma casa (por exemplo, utilitários antivírus projetados para até cinco Windows, macOS ou dispositivos móveis).

As licenças de uso corporativo podem diferir das licenças de software pessoal de várias maneiras:

- O software coberto pelas licenças corporativas inclui recursos de gerenciamento e segurança projetados para a empresa.
- O software coberto por licenças corporativas tem regras muito diferentes para atualizações de software do que o software com licença pessoal.
- O software coberto por licenças corporativas pode ser licenciado por estação, por dispositivo, por processador ou de outras formas.
- Algumas licenças de software pessoal, como o Microsoft Office Home and Student, são especificamente proibidas de serem usadas nos negócios.

A empresa pode enfrentar multas graves se os termos de licenciamento de software não forem seguidos. Um supervisor deve ser notificado se um técnico for solicitado a violar os termos de uma licença.

Licenças válidas e licenças não expiradas

Uma *licença válida* significa que o usuário concordou com os termos de uso do desenvolvedor de software. Isso também é conhecido como *licenciamento baseado em assinatura*. Esses termos podem incluir um contrato de pagamento recorrente com base no tempo ou no número de usuários. O acordo também deve detalhar como o software ficará inutilizável se a assinatura não for renovada.

Uma alternativa ao licenciamento por assinatura é uma *licença que não expira*, também conhecida como *licença perpétua*. Esta licença simples concede ao usuário permissão contínua para um aplicativo, sem prazo de validade.

Dados regulamentados

Quatro tipos de dados são regulamentados e devem ser protegidos pelos administradores de rede. Eles são listados com o acrônimo primeiro porque é assim que eles são referidos no campo:



- **PII:** informações de identificação pessoal, como nome de uma pessoa, endereço, número da carteira de habilitação, números de cartão de crédito e número do seguro social
- **PCI:** Padrões da indústria de cartões de pagamento que estão em vigor para proteger os dados dos titulares de cartão de crédito, incluindo números de cartão e endereço e informações de crédito
- **GDPR:** Regulamento Geral de Proteção de Dados, promulgado na Europa para proteger vários tipos de dados, incluindo saúde, biometria, genética e histórico criminal
- **PHI:** informações de saúde protegidas (uma parte da lei HIPAA), que abrange o estado de saúde, bem como métodos de pagamento, números de contas e beneficiários

Qualquer organização que detenha ou use esse tipo de informação é responsável por protegê-la contra ladrões de identidade. Muitos casos graves (e muito caros) de violação de dados aconteceram na história recente, e alguns deles tiveram efeitos prejudiciais nas empresas que perderam dados. A função de um técnico de informática na proteção de dados inclui o seguinte:

- Configurando sistemas para usar armazenamento em nuvem seguro em vez de informações confidenciais armazenadas localmente em laptops e dispositivos móveis
- Configurar e usar criptografia forte em redes sem fio e sistemas de ponto de venda (POS)
- Usando criptografia de disco completo, como BitLocker, BitLocker To Go ou produtos semelhantes em laptops e dispositivos móveis que armazenam ou acessam dados confidenciais
- Configuração de firewalls de hardware e software para proteger dados confidenciais
- Educar os usuários sobre métodos para remover informações de identificação pessoal de documentos, fotos e outros arquivos que possam ser compartilhados ou publicados online

Obviamente, é importante proteger os usuários e a organização acompanhando os desenvolvimentos recentes no conhecimento e na aplicação dessas políticas e práticas recomendadas. Compreendê-los é necessário para o A+ exame.

Técnicas de Comunicação e Profissionalismo



220-1102: Objetivo 4.7: Dado um cenário, use técnicas de comunicação adequadas e profissionalismo.

De todas as habilidades técnicas que os técnicos de suporte de PC devem ter em seu kit de ferramentas, fortes habilidades de comunicação estão entre as mais duradouras e vitais. Não importa qual versão do software ou geração de hardware esteja em uso, é necessária uma comunicação escrita e oral eficaz para identificar e documentar problemas e treinar os usuários sobre como funcionar em seu ambiente técnico. Os empregadores classificam consistentemente a comunicação como a “habilidade leve” mais desejável (em oposição à habilidade técnica forte) que procuram ao contratar novos funcionários. Esta seção destaca aspectos de comunicação e profissionalismo esperados de um técnico de suporte de PC.

Aparência e vestuário profissionais Os técnicos de

suporte de TI projetam a imagem de sua organização quando são chamados para prestar suporte a um cliente, seja esse cliente um cliente ou um colega de trabalho. Cada organização tem sua própria cultura e as expectativas de aparência (barba, cabelo, tatuagens e assim por diante) podem variar bastante. É importante estar ainda mais atento a isso ao visitar clientes fora da organização.

O traje, ou a escolha da roupa, também faz parte da cultura de uma organização. O ponto principal a ter em mente com a escolha da roupa é que ela reflete respeito pelo ambiente em que você estará trabalhando mais do que envolve conforto pessoal ou declarações de moda.

Alguns empregadores optam por fornecer aos técnicos algum tipo de uniforme para que possam ser facilmente reconhecidos. Outras empresas simplesmente oferecem diretrizes, como as seguintes:

- **Formal:** Isso significa calça social, camisa social e gravata. Esse traje é mais frequentemente exigido ao apoiar instituições que têm as mesmas expectativas para todos os funcionários, como instituições governamentais ou financeiras.
- **Business casual:** este termo é um pouco menos definido e varia de acordo com a região. Na maioria das vezes, significa calças de veludo cotelê ou cáqui (não jeans), ou talvez jeans limpos e intactos com uma camisa de colarinho. O empregador deve definir essas expectativas no início do processo de contratação, mas se elas não forem claras, os técnicos devem apostar no lado seguro: vestir-se bem é sempre melhor do que vestir-se mal quando se trabalha com outras pessoas.

Use linguagem adequada e evite jargões, acrônimos e gírias quando aplicável . Usar linguagem adequada é uma maneira de inspirar confiança nas pessoas que você está tentando ajudar. Linguagem adequada é aquela que é habitual e profissional em seu ambiente de trabalho. Xingar e xingar nunca são considerados aceitáveis, mesmo que algumas pessoas no trabalho falem dessa maneira. Fale claramente e de forma simples, concisa e respeitosa.

Use o inglês adequado e evite gírias. Evite também jargões e siglas de informática, como WPA3 ou TCP/IP, que podem confundir o cliente.

Mantenha uma atitude positiva/confiança no projeto Os clientes

observam os técnicos enquanto eles trabalham em seus problemas e podem perder a confiança quando o técnico soa ou parece preocupado. Da mesma forma, um técnico de serviço ruim projeta arrogância ao rejeitar ou ignorar perguntas e comentários; um bom mantém uma atitude de que o problema será resolvido.

Um cliente fica tranquilo quando um técnico tem certeza de que as ferramentas e os recursos certos resolverão o problema.

Ouça ativamente, faça anotações e evite interromper o Cliente

A chave para obter informações de um cliente é *a escuta ativa*, uma habilidade de conversação que inclui fazer contato visual, fazer anotações e encorajar respostas abertas sem interromper. Ouça com atenção o que alguém tem a dizer sobre um problema que está enfrentando. O que a pessoa diz pode fornecer pistas sobre o motivo do problema. Mesmo quando um cliente admite ser uma pessoa não técnica ou mesmo um tecnófobo, ouça com atenção.

Seja culturalmente sensível

Nações, organizações e departamentos têm culturas — formas de comunicação, rituais a seguir e definições de boas maneiras. A sensibilidade cultural ajuda a evitar barreiras a uma boa comunicação. Certifique-se de usar os títulos honoríficos apropriados (Sr., Sra., Sra. e assim por diante), pegue dicas visuais e verbais e use títulos profissionais quando aplicável (médico, professor e assim por diante). Quando uma pessoa tem sotaque e é difícil de entender, concentre-se e peça para a pessoa repetir qualquer coisa que você não entender.

Ser pontual

A pontualidade é provavelmente o ingrediente mais importante no relacionamento com o cliente. Se você tiver que se atrasar, entre em contato com o cliente. Considere também entrar em contato com seu supervisor, dependendo de quanto você está atrasado. Os clientes sempre valorizam muito a confiabilidade.

Evite distrações

Não deixe que seu celular, um evento na TV ou a vista da janela do canto do escritório interfiram entre você e uma solução. Evite distrações e interrupções ao falar com os clientes. Mantenha o foco no que seu cliente está lhe dizendo e a solução será mais fácil de encontrar. Não converse com outros colegas de trabalho enquanto estiver interagindo com os clientes. Não use sites de mídia social ou mensagens de texto para questões não relacionadas ao trabalho; ao enviar uma mensagem de texto pedindo ajuda, certifique-se de que seu cliente saiba por que você está

enviando um texto. Evite interrupções pessoais, exceto em caso de emergência. Respeite o tempo do cliente e economize ligações pessoais para intervalos ou quando o trabalho terminar. Os clientes costumam pagar por hora e merecem cada minuto de sua atenção.

Lidando com Clientes ou Situações Difíceis

Resolver problemas de tecnologia é difícil e os clientes podem tornar isso ainda mais difícil. Estas dicas devem ajudar a mitigar uma situação difícil:

- **Não importa o quão difícil seja o problema (ou o cliente), evite discutir com os clientes ou ficar na defensiva:** o trabalho é resolver o problema do cliente, e fazer isso bem às vezes exige muita paciência.
- **Não minimize ou descarte os problemas dos clientes:** Problemas que parecem simples para um técnico podem ser muito difíceis para um cliente. Lembre-se de que todas as pessoas com um PC quebrado podem estar perdendo dados pessoais ou comerciais valiosos; eles podem até perder dados suficientes para acabar com um negócio.
- **Não importa o quão incorretas sejam suas ações ou quão ruim seja seu julgamento, evite julgar seus clientes:** novamente, concentre-se no problema e procure uma solução. Formar opiniões com base em seus sentimentos pessoais geralmente tem um resultado ruim.
- **Esclareça as declarações do cliente:** faça perguntas abertas ao cliente para identificar melhor o problema e restringir o escopo do problema. Esclareça repetindo o problema para o cliente.
Reafirme a questão para verificar se todos entenderam o problema.
- **Não divulgue experiências nas redes sociais:** O relacionamento com o cliente deve ser valorizado. A fofoca nas mídias sociais diz ao cliente que você não valoriza a privacidade do cliente.

Defina e atenda às expectativas/cronograma e comunique o status com o cliente

Muitas das habilidades de comunicação discutidas nesta seção vêm juntas no processo de estabelecer e atender às expectativas do cliente. Expectativas

e a comunicação pode ser fortalecida de várias maneiras, incluindo as seguintes:

- Entrar pela porta com um sorriso e começar a trabalhar para determinar o problema define o tom da experiência do cliente.
Indique claramente o problema, o plano é corrigi-lo, quanto tempo levará e, se conhecido, quaisquer custos extras. Os clientes sempre apreciam surpresas mínimas.
- Crie um cronograma das etapas e quando você espera cumpri-las. Comunique o status com o cliente com frequência.
- Se aplicável, ofereça diferentes opções de reparo/substituição e permita que o cliente selecione aquela que funciona melhor na situação.
- Fornecer e organizar a documentação adequada de quaisquer serviços e produtos oferecidos. Quando o trabalho estiver concluído, documente o problema, o processo e a solução.
- Acompanhe o cliente em uma data posterior para verificar a satisfação contínua.

Lidar adequadamente com informações confidenciais e Materiais Privados

Seja trabalhando no escritório do cliente ou em uma bancada de trabalho, lembre-se de que as informações do computador do cliente, impressões e outras informações são do cliente e esses dados precisam ser mantidos em sigilo. Em muitos casos, isso não é apenas uma boa prática, mas a lei.

Pedir a um cliente para mover materiais confidenciais como extratos bancários, informações contábeis, documentos jurídicos e outras informações privadas da empresa para outra área protege você de qualquer suspeita posterior. Materiais privados que pertencem pessoalmente ao cliente também devem ser retirados do caminho.

Noções básicas de script



220-1102: Objetivo 4.8: Identificar os fundamentos do script.

Os técnicos de PC geralmente são chamados para trabalhar, configurar e atualizar muitos computadores ou outros dispositivos ao mesmo tempo, e isso pode significar repetir as mesmas tarefas em cada máquina. Aguardar a execução de processos longos ou a instalação de atualizações em cada máquina pode levar muito tempo. Escrever um script com todos os comandos e entradas permite que você execute as atualizações automaticamente, economizando tempo e dinheiro valiosos.

A programação é uma habilidade técnica importante, mas está além do escopo do exame CompTIA A+. No entanto, ser capaz de identificar os fundamentos do script é importante porque a capacidade de executar scripts como técnico ou administrador de PC é um ativo inestimável.

Tipos de arquivo de script

Arquivos de script são arquivos de texto que contêm instruções ou comandos que um computador segue para executar uma tarefa. Eles podem ser comandos de texto simples para um sistema operacional ou podem ser escritos em uma linguagem de script (um tipo limitado de linguagem de programação) que pode ser executado no computador e interpretado pelo sistema operacional. O sistema operacional executa os comandos no script para concluir as tarefas. A [Tabela 9-5](#) identifica e descreve resumidamente as seis linguagens de script comuns necessárias para o exame A+. Você deve ser capaz de reconhecê-los por suas extensões de arquivo.



Tabela 9-5 Linguagens de script básicas

Informações básicas do idioma da extensão

.bastão	arquivo de lote do Windows	Arquivos em lote são arquivos de script estritamente baseados no Windows. Eles são arquivos de texto que contêm comandos ou instruções para o interpretador de linha de comando executar. As instruções em um arquivo em lote podem ser interpretadas apenas pelo sistema operacional Windows.
----------------	----------------------------	--

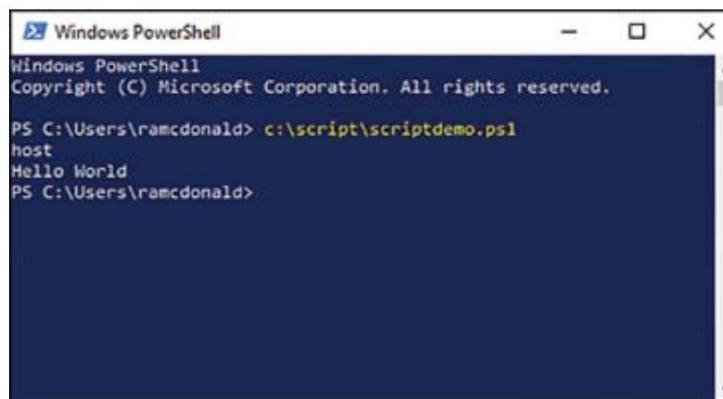
Informações básicas do idioma da extensão

.ps1	PowerShell O Windows PowerShell é uma ferramenta para ajudar técnicos e administradores de rede a automatizar as funções de suporte por meio do uso de scripts e snippets. O Windows 10 e 11 são fornecidos com o PowerShell.
.vbs	VBScript VBScript, uma linguagem de script desenvolvida pela Microsoft, é considerada um subconjunto da linguagem de programação Visual Basic. Ele foi projetado especificamente para uso com o Microsoft Internet Explorer. Dá às páginas da web um nível de interatividade.
.sh	Shell do Linux Um script de shell é um arquivo de texto que contém uma sequência de comandos de linha de comando. Os scripts de shell podem não ser executados corretamente em um sistema Windows. O Linux teve vários shells; BASH (Bourne-Again Shell) é o mais comum deles.
.py	Pitão Python costuma ser uma boa escolha para quem está começando a aprender programação. É relativamente fácil de aprender e os scripts Python podem ser executados na maioria dos sistemas operacionais. Por exemplo, o Windows Shell é conhecido como Python Interactive Shell.
.js	JavaScript JavaScript é uma linguagem de programação que tem muitos usos hoje. É valioso para criar scripts porque pode ser executado em qualquer sistema operacional. Geralmente é escrito em páginas da web para criar interações com o cliente; JavaScript é lido pelo navegador. Criar e executar JavaScript de linha de comando requer a instalação do Node.js.

Os scripts podem ser abertos e lidos ou editados em editores de texto básicos, como Bloco de notas ou em ambientes de programação especiais que auxiliam no

comandos e testes de scripts. Eles geralmente são chamados de shells e são projetados para auxiliar na escrita de scripts. A [Figura 9-12](#) mostra um script básico “Hello World” no Windows PowerShell. Observe que o arquivo foi escrito no bloco de notas e salvo como scriptdemo.ps1, usando a extensão de nome de arquivo para PowerShell. O texto completo do script é:

"Olá Mundo"


 A screenshot of a Windows PowerShell window titled "Windows PowerShell". The window shows the following text output:


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\ramcdonald> c:\script\scriptdemo.ps1
host
Hello World
PS C:\Users\ramcdonald>
```

Figura 9-12 Script básico no Windows PowerShell

Casos de uso para scripts

O objetivo dos scripts é automatizar tarefas comumente executadas por um técnico. O uso de tarefas economiza tempo, não apenas na digitação do script, mas também na garantia da confiabilidade da entrada e na prevenção de consequências não intencionais de códigos incorretos. A [Tabela 9-6](#) lista sete casos de uso comuns em que os scripts são úteis.



Tabela 9-6 Casos de uso para scripts

Caso	Descrição	Exemplos
Executando a automação básica	Economiza tempo inserindo de instalação individualmente ao configurar estações de trabalho de novas máquinas	Usando comandos de scripts

Caso	Descrição	Exemplos
Reiniciando máquinas	Reinicializações sem entrada humana	Instalando atualizações ou patches
Remapeamento de unidades de rede	Redireciona recursos em estações de trabalho	Facilitando o processo de atualização do sistema
Instalando aplicativos	Executa um script com chaves de licença e permissões	Permitindo instalações simultâneas em estações de trabalho
Automatizando backups	Implementa backups agendados	Fazendo backup de várias máquinas com um script
Reunião	Registra o uso de recursos ou logins de usuários de informações/dados	Recursos de monitoramento para planejamento de rede
Iniciando atualizações	Garante a segurança com atualizações e patches agendados	Agendamento de verificações de patches de segurança

Outras considerações de script

Uma frustração comum para pessoas novas em scripts é “digitar de forma exagerada” um script com um caractere ou número errado e ter até mesmo esse tipo de pequeno erro faz com que o script falhe. Todas as linguagens de computador seguem estruturas de comando e sintaxe estritas; embora os shells eliminem parte do fardo, a sintaxe ainda precisa estar correta. Ao inserir um script em um ambiente de produção, verifique se ele foi testado primeiro em um ambiente de sandbox.

Não fazer isso pode resultar em efeitos prejudiciais na rede de produção:

- **Introdução acidental de malware:** isso pode ser feito não verificando os scripts importados com o software de segurança.
- **Alterar inadvertidamente as configurações do sistema:** Lembre-se de que os computadores não questionam o que lhes é dito para fazer. Se instruções de script incorretas alterarem a segurança ou outras configurações do sistema, isso pode abrir a porta para o desastre.

- Falha do **navegador ou do sistema devido ao manuseio incorreto de recursos**: Às vezes, um script mal escrito pode instruir o computador a executar uma tarefa que está além do poder de uma máquina. Se a CPU estiver ocupada executando um loop em um script ruim, ela não terá recursos para outras tarefas importantes. Novamente, o sandbox deve ajudar a evitar esses tipos de erros.

Esta breve introdução ao script abrange os fundamentos mencionados nos objetivos CompTIA A+, mas há muito mais a aprender. Os links a seguir fornecem mais informações sobre scripts no PowerShell, Linux, Python e JavaScript:

<https://docs.microsoft.com/en-us/powershell/scripting/windows-powershell/ise/how-to-write-and-run-scripts-in-the-windows-powershell-ise?view=powershell-7.2> <https://help.ubuntu.com/community/BEGINNERS/BashScripting> www.python.org

www.javascript.com

Tecnologias de acesso remoto



220-1102: Objetivo 4.9: Dado um cenário, use tecnologias de acesso remoto.

Um técnico geralmente precisa acessar computadores clientes ou computadores virtuais remotamente. As máquinas podem estar em outra parte do centro de operações de rede ou nas residências de clientes que trabalham em outras partes do mundo. O acesso remoto permite que um usuário veja e controle o que está acontecendo em outro computador ou dispositivo em um local diferente.

Exemplos de uso do acesso remoto incluem o seguinte:

- Um técnico de suporte acessando o computador de um cliente para solucionar problemas ou atualizar um PC.
- Um administrador de rede ajustando configurações em um servidor em outra parte da rede.

- Um administrador de rede que precisa acessar um roteador, switch, firewall ou outro dispositivo de rede para gerenciar o tráfego. (Esses dispositivos geralmente não possuem teclados ou monitores para entrada ou saída.)

Alguns protocolos e aplicativos são usados há muito tempo para acesso remoto, e os aplicativos de terceiros se tornaram mais comuns. Esta seção descreve exemplos de tecnologia de acesso remoto.

Métodos/Ferramentas

Existem vários métodos para conectar computadores remotos, cada um desenvolvido para uma necessidade ou ambiente especializado. Esta seção discute os métodos mais comuns para acessar remotamente e gerenciar redes e computadores remotos.

RDP

O Remote Desktop Protocol (RDP) foi desenvolvido pela Microsoft para permitir que um usuário se conecte com segurança a um computador remoto para executar serviços ou oferecer suporte a outro usuário. O protocolo permite acesso criptografado com funções de captura de tela, mouse e teclado. Tarefas comuns com as conexões remotas são suporte e gerenciamento de computadores remotos.

O RDP é baseado em um modelo cliente/servidor. O usuário é o cliente e o computador Windows remoto habilita o servidor RDP. O computador remoto fornece uma captura gráfica da tela para o técnico de suporte. O técnico de suporte também pode manipular o mouse e o teclado do computador remoto. Se um trabalhador remoto precisar de suporte técnico, o técnico poderá instruir o trabalhador a habilitar o servidor RDP (se ainda não estiver habilitado) e ver remotamente o que está acontecendo. Isso pode reduzir muito o custo dos serviços de tecnologia em uma empresa.

O RDP é um protocolo proprietário da Microsoft pré-instalado no Windows, mas também estão disponíveis versões macOS e Linux do servidor e do cliente. Para habilitar a Área de Trabalho Remota no Windows 10, vá para **Configurações > Sistema > Área de Trabalho Remota**. Lembre-se que o RDP usa a porta 3389, que precisa ser aberta no firewall. [O Capítulo 6, “Sistemas operacionais”,](#) discute o RDP em detalhes.

O Aplicativo de Conexão de Área de Trabalho Remota do Windows 10 é a ferramenta mais atual para conectar um computador executando o Windows 10 Pro a outro computador ou dispositivo (iOS, Android ou Windows) que também esteja executando o Aplicativo de Área de Trabalho Remota. O dispositivo cliente deve habilitar a Conexão de Área de Trabalho Remota. Para habilitá-lo no Windows 10, vá para **Configurações > Sistema** e escolha Conexão de Área de Trabalho Remota para alternar a configuração de habilitação. No iOS ou Android, abra a Conexão de Área de Trabalho Remota e selecione o PC desejado para a conexão.

Observação

Esse tipo de software é conhecido como software thin client porque apenas o movimento do mouse, a atividade do teclado e as capturas de tela são enviadas pela rede, exigindo uma largura de banda muito baixa. A Citrix, trabalhando com a Microsoft, foi a pioneira do software thin client, mas muitos outros fornecedores agora competem no mercado.

VPN

Uma **conexão de rede privada virtual (VPN)** cria um túnel seguro em uma rede pública, como a Internet, entre dois computadores (consulte “Conexões VPN” no [Capítulo 6](#) para obter mais detalhes).

Computação de rede virtual

A **computação de rede virtual (VNC)** é comum no suporte de desktop. Ele permite que um agente de suporte controle remotamente entradas de mouse e teclado no computador de um cliente.

SSH

Secure Shell (SSH) permite que os dados sejam trocados entre computadores em um canal seguro. Este protocolo oferece uma opção mais segura do que FTP e Telnet. O servidor Secure Shell usa a porta TCP 22.

Monitoramento e gerenciamento remoto

As ferramentas de monitoramento e gerenciamento remoto (**RMM**) permitem que os técnicos monitorem e gerenciem redes remotas. Isso geralmente envolve a instalação de ferramentas especiais chamadas **agentes** que coletam dados e os reportam à equipe de gerenciamento para análise de dados. As soluções RMM são projetadas principalmente para ajudar grandes provedores de serviços de TI gerenciados (MSPs) a gerenciar e administrar remotamente computadores e redes de clientes.

Assistência Remota da Microsoft

A **Assistência Remota da Microsoft (MSRA)** é o utilitário do Windows para oferecer ou aceitar assistência remota. No Windows, pode ser habilitado acessando o menu executar (Windows+R) e digitando **MSRA**.

Assim como acontece com a Conexão de Área de Trabalho Remota, o MSRA deve primeiro ser ativado em Propriedades do Sistema com informações específicas sobre quem tem permissão para se conectar. Se o computador fizer parte de uma rede corporativa, as opções do MSRA podem não estar disponíveis se outros aplicativos de ajuda forem proibidos pelo gerenciamento.

Quando o aplicativo é aberto, aparecem opções para convidar uma conexão ou para aceitar uma solicitação de conexão.

Ferramentas de terceiros

Durante anos, existiu um mercado para ferramentas especializadas ou desenvolvimento terceirizado de serviços de terminal como Telnet e SSH, bem como FTP.

Algumas ferramentas são gratuitas e outras têm software de cliente gratuito, mas software de servidor pago; ainda outros são pagos apenas. Muitas vezes, um download gratuito de 30 dias está disponível para indivíduos, mas não para empresas.

Às vezes, o Windows incorpora ferramentas de terceiros ao sistema operacional, mas as opções disponíveis podem variar daquelas de terceiros que criaram as ferramentas. Por exemplo, PuTTY (www.putty.org) é um aplicativo de código aberto que fornece software de conectividade para conexões Telnet e SSH.

Software de compartilhamento de tela e videoconferência

O software de compartilhamento de tela e videoconferência passou a ser de uso público generalizado durante a pandemia de COVID-19, quando o trabalho e o aprendizado remotos se tornaram a norma. Pré-pandemia, uma distinção mais clara foi feita entre

compartilhamento de tela e videoconferência, mas agora os produtos de software listados aqui são usados para executar ambas as tarefas. Vários produtos ajudam as organizações a compartilhar comunicações e telas, e cada um tem um lugar no mercado. Alguns são muito familiares, como Zoom, Microsoft Teams, Google Meet e Webex da Cisco Systems. Custos, recursos e opções de suporte variam muito.

Software de transferência de arquivos

Vários protocolos usam o SSH como forma de fazer uma conexão segura. Um deles é o Secure File Transfer Protocol (SFTP). O FTP regular, que foi projetado décadas atrás, antes que a segurança fosse uma grande preocupação, pode ser inseguro. O SFTP combate isso fornecendo acesso a arquivos por meio de um fluxo de dados confiável, gerado e protegido por SSH na porta 22.

O FTP usa duas portas durante uma sessão de transferência de arquivos: a porta 21 para iniciar uma conexão e a porta 20 para estabelecer uma conexão para transferir arquivos.

Muitas grandes empresas usam o FTP para gerenciar grandes documentos e arquivos que precisam ser compartilhados com uma força de trabalho distribuída. Serv-U (www.serv-u.com), da SolarWinds, é um provedor comercial de FTP e FileZilla (<https://sourceforge.net/projects/filezilla/>) é um aplicativo FTP de código aberto que funciona para Windows, macOS e Linux.

O gerenciamento de arquivos em nuvem agora está fazendo muito do trabalho que o FTP realizou no passado. Exemplos de provedores de armazenamento em nuvem são Dropbox, Google Drive, Microsoft OneDrive e Amazon Drive. Também há uma aceitação cada vez maior do compartilhamento de documentos baseado em nuvem, como o Google Docs, no qual os documentos são criados e editados em um ambiente de nuvem compartilhado.

A maioria das transferências de arquivos baseadas em nuvem são mais rápidas e fáceis do que com FTP, mas o FTP é amplamente utilizado e fácil de gerenciar, portanto, os técnicos o encontrarão em um futuro previsível.

Software de gerenciamento de área de trabalho

O software de gerenciamento de desktop foi projetado para permitir que os administradores de rede gerenciem o software e as atualizações de software nas máquinas, sejam locais ou remotas. Isso pode significar o gerenciamento de licenças, instalações remotas e patches de segurança em máquinas sob seu controle. Alguns produtos facilitam o gerenciamento de um produto de software em diferentes plataformas de sistema operacional.

Considerações de segurança de cada método de acesso

A segurança tornou-se a preocupação mais importante no campo da tecnologia da informação. Fraquezas que existem há anos estão sendo descobertas – e exploradas – regularmente. Nenhum produto ou sistema discutido nesta seção está imune à sofisticação cada vez maior de hackers privados e patrocinados pelo governo.

As tecnologias mencionadas aqui têm preocupações associadas, mas estão intimamente relacionadas.

Um exemplo famoso da pandemia de COVID-19 fornece uma lição valiosa.

Durante a pandemia, quando o Zoom se tornou o software de reunião remota mais popular em questão de dias ou semanas, os usuários estavam focados em se conectar de forma barata e fácil, e o Zoom realizou ambos. Depois de algumas semanas, no entanto, o *bombardeio de zoom* tornou-se um problema quando pessoas de fora não convidadas puderam entrar e interromper as reuniões. A Zoom se esforçou para criar sistemas de segurança para o produto. Por fim, foram criadas atualizações que exigiam práticas de autenticação seguras discutidas no [Capítulo 7, “Segurança”](#).

O que poderia ter sido feito para mitigar as ameaças à segurança? Em retrospectiva, o mais importante teria sido tornar as preocupações de segurança mais importantes do que “barato e fácil” ao selecionar o software.

Outra prática de segurança comum que melhora a segurança dessas tecnologias remotas é usá-las em uma VPN sempre que possível. Lembre-se de que as VPNs criptografam a comunicação. Juntamente com fortes práticas de autenticação, isso pode ajudar as organizações a se conectarem remotamente e trabalharem em um ambiente seguro.

Tarefas de preparação para exames

Conforme mencionado na Introdução, você tem várias opções para se preparar para o exame: os exercícios aqui; [Capítulo 10, “Preparação Final”](#); e as questões de simulação de exame no software de teste prático Pearson Test Prep.

Revise todos os tópicos principais

Revise os tópicos mais importantes do capítulo, indicados pelo ícone Tópico principal na margem externa da página. [A Tabela 9-7](#) lista esses tópicos-chave e o número da página em que cada um deles é encontrado.



Tabela 9-7 Tópicos-chave para o [Capítulo 9](#)

Tópico principal Elemento	Descrição	Página Número
Gerenciamento de Mudanças de Seção		693
Lista	Restaurar e recuperar	697
Seção	Backups no local x fora do local	700
Seção de Aterramento do Equipamento/Manuseio Adequado de Energia	705	
Seção	Manuseio e armazenamento adequados de componentes	707
Figura 9-10	Usando uma cinta ESD para evitar danos ESD Ao trabalhar em eletrônica	710
Seção	Segurança pessoal	713
Seção	Ficha de Dados de Segurança do Material (MSDS)	715
Seção	Manuseio/Descarte de Resíduos Tóxicos	717
Lista	Métodos adequados para reciclar baterias	717
Seção	Unidades de backup de bateria	720
Tabela 9-4 Condições Elétricas e Medidas de Proteção		721
Seção	Resposta a Incidentes	722
Seção	Licenciamento/gerenciamento de direitos digitais (DRM)/Contrato de licença de usuário final (EULA)	723
Lista	Dados regulamentados	726
Seção	Técnicas de Comunicação e Profissionalismo	727

Tópico principal	Descrição	Página
Elemento		Número
Tabela 9-5	Linguagens de script básicas	731
Tabela 9-6	Casos de uso para scripts	733

Complete as tabelas e listas da memória

Imprima uma cópia do [Apêndice C, “Tabelas de Memória”](#) (encontrado online), ou pelo menos a seção deste capítulo, e complete as tabelas e listas de memória. O [Apêndice D, “Respostas das tabelas de memória”](#), também on-line, inclui tabelas e listas preenchidas para verificar seu trabalho.

Definir termos-chave

Defina os seguintes termos-chave deste capítulo e verifique suas respostas no glossário:

[sistemas de tíquete](#)
[política de uso aceitável \(AUP\)](#)
[diagrama de topologia de rede](#)
[telas iniciais relatórios de](#)
[incidentes gerenciamento de](#)
[mudança plano de reversão](#)
[análise de risco backup completo](#)
[backup incremental backup](#)
[diferencial backup sintético avô-](#)
[pai-filho \(GFS\) 3-2-1 regra de](#)
[backup material de descarga](#)
[eletrostática \(ESD\) ficha de](#)
[dados de segurança \(MSDS\)](#)

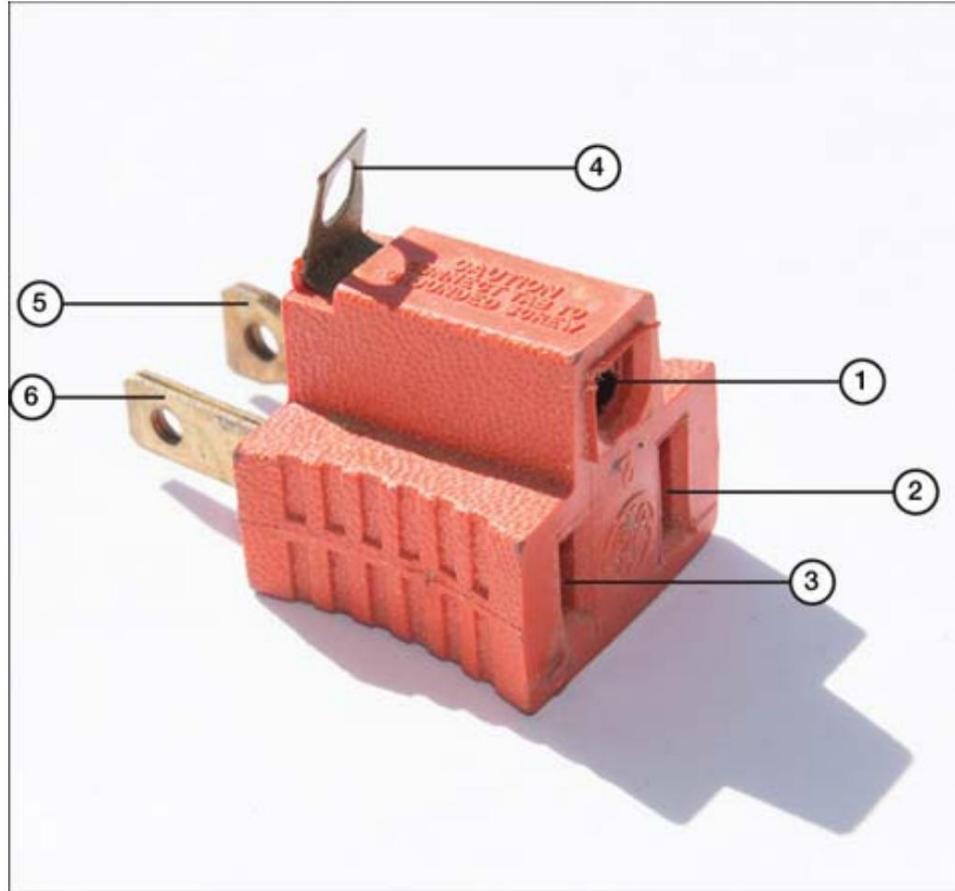
picos de energia
cadeia de custódia
gerenciamento de direitos digitais (DRM)
contrato de licença de usuário final (EULA)
licenças de código aberto licenças de uso
pessoal licenças de uso corporativo

PII

arquivos de
script .bat arquivos
de script .ps1
arquivos de
script .vbs arquivos
de script .sh
arquivos de script .py arquivos de script .js
protocolo de área de trabalho remota
(RDP) rede privada virtual (VPN) computação de rede virtual (VNC)
Secure Shell (SSH)
monitoramento remoto e gerenciamento (RMM)
Assistência Remota da Microsoft (MSRA)

Responder a perguntas de revisão

1. Identifique as partes do plugue na figura a seguir.



a. uma. ponta quente

b. Conector ativo

c. Ponto neutro **d.**

Conector neutro

e. Loop de aterramento

f. Conector de aterramento

2. O objeto na figura a seguir é um testador de tomadas elétricas. O que

este testador de tomada informa sobre a tomada na qual está conectado no momento?



a. O fio terra está com defeito. **b.**

O fio quente está com defeito. **c.** O
fio neutro está com defeito. **d.** Todos
os fios estão corretos.

3. Qual das seguintes afirmações melhor define ESD?

a. Dispositivo de desligamento eletrônico

b. Descarga eletrostática **c.**

Desenvolvimento ambientalmente sustentável **d.**

Diferencial sensível à energia

4. Qual das opções a seguir pode ser usada como proteção contra ESD?

(Escolha todas as que se

aplicam.) **a.** Um saco

antiestático **b.** Um adaptador de 3 fios
para 2 fios **c.** Um tapete ESD

d. Uma pulseira ESD

5. Qual das opções a seguir aumenta a probabilidade de ESD?

- uma.** Carpete no chão
b. Aumentar a umidade da sala **c.**
Aumentando a temperatura ambiente
d. sapatos com sola de borracha
- 6.** Qual das opções a seguir melhor descreve como descartar usados baterias?
- uma.** Abra as baterias e remova cuidadosamente seus núcleos de chumbo antes de reciclar. **b.** Recicle as baterias na lixeira. **c.** Recicle NiMH e Li-Ion na lixeira; As baterias de NiCad podem ser descartadas no lixo.
d. Devolva as baterias a uma loja de eletrônicos para reciclagem.
- 7.** Qual dos seguintes é considerado um perigo ambiental?
- uma.** Celulares e tablets **b.**
baterias UPS
c. Cartuchos de toner
d. Todos esses
- 8.** Qual classe de extintor deve ser usado em um incêndio elétrico?
- uma.** Classe A
b. Classe B
c. Classe C
d. Classe D
- 9.** Ao selecionar uma máscara de filtro de ar, qual categoria oferece o maior nível de proteção?
- uma.** UMA
b. N
c. P
d. R

10. Qual das seguintes afirmações melhor descreve um MSDS (também conhecido como SDS)?

- uma.** Um MSDS fornece acessibilidade simultânea a vários dados fontes.
- b.** Um MSDS fornece informações de segurança sobre armazenamento, derramamentos e exposição acidental a produtos químicos perigosos. **c.** Um MSDS ajuda a proteger os componentes do computador contra danos devido para ESD.
- d.** Um MSDS é um documento legal usado para estabelecer a cadeia de custódia em casos legais.

11. Qual material perigoso é usado para fabricar baterias UPS?

- uma.** Ni-Cad
- b.** NiMH
- c.** Li-Ion
- d.** Chumbo ácido

12. Qual das opções a seguir descreve melhor a função de um no-break em um ambiente de tecnologia? **uma.** Uma UPS é uma bateria de reserva. **b.** Uma UPS é uma classificação para o desempenho do sistema. **c.** Uma UPS é um programa de segurança. **d.** A UPS é uma empresa de entrega de pacotes.

13. Qual das opções a seguir melhor descreve a cadeia de custódia?

- uma.** Cadeia de custódia é a documentação da propriedade de um computador ou componentes de computador.
- b.** Cadeia de custódia é a documentação de quem estava na posse de provas relativas a uma investigação. **c.** Cadeia de custódia é a documentação de como um computador foi consertado, como o que foi feito e quem o fez. **d.** Cadeia de custódia é a documentação da posse de um computador e não está relacionada à propriedade.

- 14.** Qual das opções a seguir melhor descreve o software de código aberto? (Escolha todas as que se aplicam.) **a.** O software de código aberto pode ser usado gratuitamente. **b.** O software de código aberto pode ser usado para fins comerciais. **c.** Software de código aberto pode ser vendido. **d.** O software de código aberto pode ser modificado.
- 15.** Como técnico de informática, o que você pode fazer para ajudar seus clientes a proteger suas informações pessoais? (Escolha todas as que se aplicam.) **a.** Você pode aconselhá-los a armazenar suas informações confidenciais usando armazenamento em nuvem em vez de armazenamento local. **b.** Você pode aconselhá-los a usar a criptografia do BitLocker. **c.** Você pode aconselhá-los a armazenar informações confidenciais no disco rígido de um PC em vez de armazená-las com os arquivos de backup. **d.** Você pode aconselhá-los a usar firewalls para evitar invasões de hackers.
- 16.** Qual das seguintes afirmações descreve a melhor maneira de explicar uma problema para um cliente?
- uma.** Use o máximo de vocabulário técnico possível porque isso faz você parecer experiente e vai impressionar o cliente.
- b.** Explique o menos possível porque o cliente provavelmente não entenderia a explicação, e isso só criaria confusão.
- c.** Explique o problema em termos não técnicos e ofereça-se para mostrar ao cliente qual era o problema e como você o corrigiu.
- d.** Peça ao cliente para não se preocupar com os detalhes e assegure ao cliente que você cuidará do problema.
- 17.** Ellen está trabalhando em uma estação de trabalho no departamento de contabilidade. Em uma aba aberta do navegador, ela percebe um meme com comentários racistas e imagens gráficas. Qual é o próximo passo que Ellen deve dar?
- uma.** Termine de corrigir o problema e avise o usuário que este conteúdo é contra a AUP

b. Chame a segurança corporativa **c.**

Entre em contato com seu supervisor

d. Entre em contato com o supervisor do usuário

18. Fátima estava ajudando Mark, um novo funcionário que estava tendo problemas para acessar as pastas de rede de que precisava para suas novas atribuições.

Quando ela pediu que ele descrevesse os problemas, ela fez anotações, não interrompeu e reapresentou o problema dele com suas próprias palavras para ter certeza de que ela entendeu. Qual habilidade de atendimento ao cliente Fátima estava demonstrando?

uma. Audição presumida **b.**

Sensibilidade cultural **c.** Escuta

ativa **d.** Lidando com um cliente

difícil

19. Martin, um trabalhador de suporte técnico em um macOS help desk, recebeu uma

ligação de suporte de Sarah e logo determinou que o laptop de Sarah precisava ter algumas configurações alteradas. Ele pediu a Sarah que permitisse acesso seguro à área de trabalho dela, e ele conseguiu controlar o mouse e fazer as alterações necessárias. Qual protocolo os computadores de Martin e Sarah provavelmente estavam usando durante a sessão de ajuda? **uma.** Telnet

b. RTP

c. RDP

d. FTP

20. Jess e Hiroko precisam atualizar vários computadores e seu laboratório

gerente escreveu um script básico para acelerar o processo. Eles recebem uma unidade flash com quatro arquivos, mas o que desejam está escrito em um shell para máquinas Linux. Qual extensão de arquivo é provavelmente aquela que eles desejam usar? **uma.** update.js **b.** update.sh **c.** update.py **d.** atualizar.bat

21. Quando Josh não consegue responder a uma pergunta sobre um novo tipo de software que está chegando ao mercado e como seu cliente pode implementá-lo, que ação ele deve tomar?

a. Dar a melhor resposta possível com o conhecimento que tem **b.** Procure um whitepaper online **c.** Envie o cliente para a página da Web do desenvolvedor de software **d.** Encaminhe a pergunta para o chefe dele

22. Carla, que trabalha na folha de pagamento, começou a trabalhar um dia e percebeu que não tinha mais acesso às informações de pagamento do bônus de bem-estar dos funcionários, que eram essenciais para seu trabalho. Mais tarde, ela descobriu que o prestador de cuidados de saúde implementou um novo sistema de relatórios que separava os relatórios contábeis dos registros privados de bem-estar. O que isso é provavelmente um exemplo?

a. Não obter feedback das partes interessadas **b.** Gerenciamento inadequado de senhas **c.** falha de domínio
d. A base de conhecimento não está sendo atualizada

Parte III: Preparação Final

Capítulo 10

Preparação Final

Este capítulo desmistifica o processo de preparação para a certificação e compartilha algumas ideias úteis para garantir que você esteja pronto para os exames. Muitas pessoas ficam ansiosas para fazer exames; nossa esperança é que este capítulo lhe dê as ferramentas para criar confiança para o dia do exame. Uma maneira importante de fazer isso é dar uma olhada detalhada nos exames de certificação reais.

Os primeiros nove capítulos deste livro cobrem as tecnologias, protocolos, conceitos de design e considerações necessárias para passar nos exames CompTIA A+ Core 1 (220-1101) e Core 2 (220-1102). Apesar de ter essas informações detalhadas, a maioria das pessoas precisa de mais preparação do que apenas ler os primeiros nove capítulos deste livro. Este capítulo fornece um conjunto de ferramentas e um plano de estudo para ajudá-lo a concluir sua preparação para os exames.

Este pequeno capítulo tem quatro seções principais. A primeira seção lista as informações e detalhamento dos exames CompTIA A+ 220-1101 e 220-1102. A segunda seção compartilha algumas dicas importantes a serem lembradas para garantir que você esteja pronto para esses exames. A terceira seção discute ferramentas de preparação para exames que podem ser úteis neste ponto do processo de estudo. A seção final deste capítulo apresenta uma sugestão de plano de estudo a ser seguido após a conclusão de todos os capítulos anteriores deste livro.

Observação

O [Apêndice C, “Tabelas de memória”](#) e o [Apêndice D, “Chave de resposta para as tabelas de memória”](#), existem como apêndices digitais no site deste livro.

Você pode acessar este site acessando www.pearsonITcertification.com/register, registrando seu livro, e inserindo o ISBN deste livro: 9780137675944.

Informações do exame

Esses detalhes são importantes para os dois exames que mapeiam para este texto:

- **Códigos de ID do exame:** A+ Core 1 (220-1101) e A+ Core 2 (220-1102)
- **Tipos de perguntas:** perguntas de múltipla escolha e baseadas em desempenho
- **Número de questões:** Máximo de 90 por prova
- **Tempo limite:** 90 minutos por exame
- **Pontuação necessária para aprovação:** 220-1101: 675 (em uma escala de 100–900); 220-1102: 700 (numa escala de 100–900)
- **Idiomas disponíveis (sujeitos a alterações):** inglês, alemão, Japonês, português, chinês simplificado e espanhol
- **Taxa do exame (sujeita a alterações):** US\$ 239 por exame

CompTIA A+ 220-1101 abrange hardware e periféricos de PC, hardware de dispositivo móvel e rede e solução de problemas de hardware e conectividade de rede.

CompTIA A+ 220-1102 abrange a instalação e configuração de sistemas operacionais, incluindo Windows, iOS, Android, macOS e Linux. Ele também aborda a segurança, os fundamentos da computação em nuvem e os procedimentos operacionais.

CompTIA A+ é a credencial de qualificação preferencial para suporte técnico e funções operacionais de TI. É muito mais do que reparar o PC:

- Os candidatos estão mais bem preparados para solucionar problemas e resolver problemas.
- Os técnicos entendem uma ampla variedade de questões, desde redes e sistemas operacionais até dispositivos móveis e segurança.
- A+ suporta a capacidade de conectar os usuários aos dados de que precisam para realizar seus trabalhos, independentemente dos dispositivos que estão sendo usados.

Os candidatos aprovados têm o conhecimento necessário para fazer o seguinte:

- Montar componentes com base nos requisitos do cliente

- Instalar, configurar e manter PCs, dispositivos móveis e software para usuários finais
- Entenda os fundamentos da análise forense de rede e segurança
- Diagnostique, resolva e documente problemas comuns de hardware e software de forma adequada e segura
- Aplicar habilidades de solução de problemas
- Forneça suporte adequado ao cliente
- Entenda os conceitos básicos de script, virtualização, imagem de desktop e implantação

Para uma análise completa dos objetivos do exame para esses domínios de cada exame, baixe o PDF dos objetivos do exame no site da CompTIA (www.comptia.org/certifications/a#examdetails) preenchendo a caixa Obter questões práticas e objetivos do exame, mostrada na [Figura 10-1](#).

Get Practice Questions and Exam Objectives

First Name Last Name
Email Job Description
Select Exam Country

I'm interested in receiving:

Exam Objectives Practice Questions

Training Status

I plan on taking the exam...

I agree to the [Terms of Use & Privacy statement](#).

SUBMIT