Objetivos do exame Core 2 de certificação CompTIA A+

NÚMERO DO EXAME: CORE 2 (220-1102)

Sobre o exame

Os candidatos são incentivados a usar este documento a fim de se prepararem para o exame de certificação CompTIA A+ 220-1102. Para receber uma certificação CompTIA A+, é necessário ser aprovado em dois exames: Core 1 (220-1101) e Core 2 (220-1102). Os exames de certificação CompTIA A+ Core 1 (220-1101) e Core 2 (220-1102) verificarão se o candidato aprovado possui o conhecimento e as habilidades necessárias para:

- Instalar, configurar e executar a manutenção de equipamentos de informática, dispositivos móveis e software para usuários finais
- Consertar componentes com base nos requisitos do cliente
- Compreender os conceitos básicos de rede e aplicar métodos básicos de segurança cibernética para mitigar ameaças
- Diagnosticar, resolver e documentar problemas de hardware e software de forma correta e segura
- Aplicar habilidades de solução de problemas e fornecer suporte ao cliente usando habilidades de comunicação apropriadas
- Compreender os conceitos básicos de scripts, tecnologias de nuvem, virtualização e implantações de vários sistemas operacionais em ambientes corporativos

Isso equivale a 12 meses de experiência prática trabalhando em uma função de técnico de suporte, técnico de suporte de desktop ou função de técnico de serviço de campo. Esses exemplos de conteúdo destinam-se a esclarecer os objetivos do exame, portanto, não devem ser considerados como uma lista completa de todo o conteúdo deste exame.

CREDENCIAMENTO DE EXAMES

O exame CompTIA A+ Core 2 (220-1102) é credenciado pela ANSI para demonstrar conformidade com a norma ISO 17024 e, como tal, passa por revisões e atualizações regulares dos objetivos do exame.

ELABORAÇÃO DO EXAME

Os exames da CompTIA resultam de workshops especializados e focados no assunto e pesquisas abrangentes em toda a indústria quanto às habilidades e conhecimentos exigidos de um profissional de TI de nível inicial.

POLÍTICA DE USO AUTORIZADO DE MATERIAIS DA CompTIA

A CompTIA Certifications, LLC não está afiliada a, nem autoriza, endossa ou admite o uso de qualquer conteúdo fornecido por sites de treinamento externos não autorizados (também conhecidos como "brain dumps"). Os candidatos que usarem esses materiais como preparação para qualquer exame da CompTIA terão suas certificações anuladas e serão suspensos de futuros testes de acordo com o contrato do candidato CompTIA. Com o intuito de comunicar com maior clareza as políticas dos exames CompTIA referentes ao uso de materiais de estudo não autorizados, a CompTIA encaminha todos os candidatos à certificação para as Políticas do Exame de Certificação da CompTIA. Leia todas as políticas da CompTIA antes de iniciar o processo de estudo para qualquer exame CompTIA. Os candidatos serão obrigados a respeitar o contrato do candidato CompTIA. Se um candidato não tiver a certeza se determinado material de estudo é considerado não autorizado (conhecido como "brain dump"), deverá entrar em contato com a CompTIA pelo e-mail examsecurity@comptia.org para confirmação.

OBSERVAÇÃO

As listas de exemplos fornecidas em formato de marcadores não são listas abrangentes. Outros exemplos de tecnologias, processos ou tarefas pertinentes a cada objetivo podem ser incluídos no exame, embora não estejam listados ou cobertos neste documento de objetivos. A CompTIA revisa constantemente o conteúdo de seus exames e atualiza as questões para assegurar que sejam atuais e que a segurança de suas perguntas estejam protegidas. Quando necessário, publicaremos exames atualizados baseados nos objetivos existentes. Lembre-se que todos os materiais de preparação dos exames ainda serão válidos.

DETALHES DO TESTE

Exame exigido	A+ Core 2 (220-1102)
Número de questões	No máximo 90
Tipos de perguntas	Múltipla escolha e baseadas em desempenho
Duração do teste	90 minutos
Experiência recomendada	12 meses de experiência prática com técnico de suporte, técnico de suporte de desktop ou função de técnico de serviço de campo
Pontuação de aprovação	700 (em uma escala de 100 a 900)

OBJETIVOS DO EXAME (DOMÍNIOS)

A tabela abaixo lista os domínios medidos por este exame e o peso que cada um representa.

DOMÍNIO		PORCENTAGEM DO EXAME
1.0	Sistemas operacionais	31%
2.0	Segurança	25%
3.0	Resolução de problemas de software	22%
4.0	Procedimentos operacionais	22%
Total		**100%**

NOTA SOBRE O WINDOWS 11

As versões do Microsoft® Windows® que não são o fim do Suporte Mainstream (conforme determinado pela Microsoft), até e incluindo o Windows 11, são áreas de conteúdo pretendidas da certificação. Como tal, os objetivos em que uma versão específica do Microsoft Windows não é indicada no título do objetivo principal podem incluir conteúdo relacionado ao Windows 10 e Windows 11, no que se refere à função de trabalho.

1.0 Sistemas operacionais

1.1 Identifique os recursos básicos das edições do Microsoft Windows.

- **Edições do Windows 10**
  - Home
  - Pro
  - Pro para estações de trabalho
  - Corporativo
- **Diferenças de recursos**
  - Acesso ao domínio vs. grupo de trabalho
  - Estilos de área de trabalho/ interface do usuário
  - Disponibilidade de Protocolo de áreas de trabalho remotas (RDP)
  - Limitações de suporte à memória de acesso randômico (RAM)
  - BitLocker
  - gpedit.msc
- **Caminhos de atualização**
  - Atualização no local

1.2 Considerando um cenário, use a ferramenta de linha de comando apropriada da Microsoft.

- **Navegação**
  - cd
  - dir
  - md
  - rmdir
  - Entradas de navegação da unidade:
    - C: ou D: ou x:
- **Ferramentas da linha de comandos**
  - ipconfig
  - ping
  - hostname
  - netstat
  - nslookup
  - chkdsk
  - net user
  - net use
  - tracert
  - format
  - xcopy
  - copy
  - robocopy
  - gpupdate
  - gpresult
  - shutdown
  - sfc
  - [nome do comando] /?
  - diskpart
  - pathping
  - winver

1.3 Considerando um cenário, use recursos e ferramentas do sistema operacional (SO) Microsoft Windows 10.

- **Gerenciador de tarefas**
  - Serviços
  - Inicialização
  - Desempenho
  - Processos
  - Usuários
- **Snap-in do Console de Gerenciamento Microsoft (MMC)**
  - Visualizador de eventos (eventvwr.msc)
  - Gerenciamento de disco (diskmgmt.msc)
  - Agendador de tarefas (taskschd.msc)
  - Gerenciador de dispositivos (devmgmt.msc)
  - Gerenciador de certificados (certmgr.msc)
  - Usuários e grupos locais (lusrmgr.msc)
  - Monitor de desempenho (perfmon.msc)
  - Editor de diretiva de grupo (gpedit.msc)
- **Ferramentas adicionais**
  - Informações do sistema (msinfo32.exe)
  - Monitor de recursos (resmon.exe)
  - Configuração do sistema (msconfig.exe)
  - Limpeza de disco (cleanmgr.exe)
  - Desfragmentação de disco (dfrgui.exe)
  - Editor do Registro (regedit.exe)

1.4 Considerando um cenário, use o utilitário apropriado do Painel de Controle do Microsoft Windows 10.

- **Opções de internet**
- **Dispositivos e impressoras**
- **Programas e recursos**
- **Rede e central de compartilhamento**
- **Sistema**
- **Windows Defender Firewall**
- **Correio**
- **Som**
- **Contas de usuários**
- **Gerenciador de dispositivos**
- **Opções de indexação**
- **Ferramentas administrativas**
- **Opções do explorador de arquivos**
  - Mostrar arquivos ocultos
  - Ocultar extensões
  - Opções gerais
  - Ver opções
- **Opções de energia**
  - Hibernar
  - Planos de energia
  - Inativar/suspender
  - Em espera
  - Escolher o que o fechamento da tampa faz
  - Ativar inicialização rápida
  - Suspensão seletiva do Barramento universal serial (USB)
- **Facilidade de acesso**

1.5 Considerando um cenário, use as configurações apropriadas do Windows.

- **Tempo e Idioma**
- **Atualização e segurança**
- **Personalização**
- **Aplicativos**
- **Privacidade**
- **Sistema**
- **Dispositivos**
- **Rede e Internet**
- **Jogos**
- **Contas**

1.6 Considerando um cenário, configure os recursos de rede do Microsoft Windows em um cliente/desktop.

- **Configuração de domínios vs. grupos de trabalho**
  - Recursos compartilhados
  - Impressoras
  - Servidores de arquivos
  - Unidades mapeadas
- **Configurações de firewall do SO local**
  - Restrições e exceções de aplicativos
  - Configuração
- **Configuração de rede do cliente**
  - Esquema de endereçamento de protocolo de internet (IP)
  - Configurações do Sistema de nomes de domínio (DNS)
  - Máscara de sub-rede
  - Gateway
  - Estático vs. dinâmico
- **Estabelecer conexões de redes**
  - Rede privada virtual (VPN)
  - Sem fio
  - Com fio
  - Rede de área local sem fio (WWAN)
- **Configurações de proxy**
- **Rede pública vs. rede privada**
- **Navegação do explorador de arquivos — caminhos de rede**
- **Conexões e limitações medidas**

1.7 Considerando um cenário, aplique os conceitos de instalação e configuração do aplicativo.

- **Requisitos do sistema para aplicativos**
  - Requisitos de aplicativos dependentes de 32 bits vs. 64 bits
  - Placa gráfica dedicada vs. integrada
  - Requisitos de Memória de acesso randômico de vídeo (VRAM)
  - Requisitos de RAM
  - Requisitos da unidade central de processamento (CPU)
  - Tokens de hardware externo
  - Requisitos de armazenamento
- **Requisitos do SO para aplicativos**
  - Compatibilidade do aplicativo ao SO
  - SO de 32 bits vs. 64 bits
- **Métodos de distribuição**
  - Mídia física vs. para download
  - ISO montável
- **Outras considerações para novos aplicativos**
  - Impacto no dispositivo
  - Impacto na rede
  - Impacto na operação
  - Impacto nos negócios

1.8 Explique os tipos comuns de SO e seus propósitos.

- **SOs de estação de trabalho**
  - Windows
  - Linux
  - macOS
  - SO Chrome
- **SOs de celular/tablet**
  - iPadOS
  - iOS
  - Android
- **Vários tipos de sistema de arquivos**
  - Nova tecnologia de sistema de arquivos (NTFS)
  - Tabela de alocação de arquivos de 32 bits (FAT32)
  - Terceiro sistema de arquivos estendido (ext3)
  - Quarto sistema de arquivos estendido (ext4)
  - Sistemas de arquivos para Apple (APFS)
  - Tabela de alocação de arquivos extensível (exFAT)
- **Limitações do ciclo de vida do fornecedor**
  - Fim da vida útil (EOL)
  - Limitações de atualização
- **Preocupações de compatibilidade entre SOs**

1.9 Considerando um cenário, execute instalações e atualizações do SO em um ambiente de SO diversificado.

- **Métodos de inicialização**
  - USB
  - Meios ópticos
  - Rede
  - Unidades de estado sólido/flash
  - Baseado na Internet
  - Unidade externa/intercambiável
  - Disco rígido interno (partição)
- **Tipo de instalações**
  - Upgrade
  - Partição de recuperação
  - Limpar instalação
  - Implementação de imagens
  - Instalação de reparo
  - Instalação de redes remotas
  - Outras considerações
    - Drivers de terceiros
- **Particionamento**
  - Tabela de partição GUID [Identificador global exclusivo] (GPT)
  - Registro mestre de inicialização (MBR)
- **Formato da unidade**
- **Considerações de atualização**
  - Arquivos de backup e preferências do usuário
  - Suporte a aplicativos e drivers/ compatibilidade com versões anteriores
  - Compatibilidade de hardware
- **Atualizações de recursos**
  - Ciclo de vida do produto

1.10 Identifique recursos e ferramentas comuns do SO mac/SO desktop.

- **Instalação e desinstalação de aplicativos**
  - Tipos de arquivo
    - .dmg
    - .pkg
    - .app
  - Loja de aplicativos
  - Processo de desinstalação
- **ID Apple e restrições corporativas**
- **Melhores práticas**
  - Backups
  - Antivírus
  - Atualizações/patches
- **Preferências do sistema**
  - Displays
  - Redes
  - Impressoras
  - Scanners
  - Privacidade
  - Acessibilidade
  - Time Machine
- **Recursos**
  - Vários desktops
  - Controle da missão
  - Acesso às Chaves
  - Spotlight
  - iCloud
  - Gestos
  - Localizador
  - Disco remoto
  - Plataforma
- **Utilitário de disco**
- **FileVault**
- **Terminal**
- **Forçar encerramento**

1.11 Identifique recursos e ferramentas comuns do SO cliente/desktop Linux.

- **Comandos comuns**
  - ls
  - pwd
  - mv
  - cp
  - rm
  - chmod
  - chown
  - su/sudo
  - apt-get
  - yum
  - ip
  - df
  - grep
  - ps
  - man
  - top
  - find
  - dig
  - cat
  - nano
- **Melhores práticas**
  - Backups
  - Antivírus
  - Atualizações/patches
- **Ferramentas**
  - Shell/terminal
  - Samba

2.0 Segurança

2.1 Resuma as múltiplas medidas de segurança e suas finalidades.

- **Segurança física**
  - Entrada de controle de acesso
  - Leitor de crachá
  - Vigilância de vídeo
  - Sistemas de alarme
  - Sensor de movimento
  - Travas de porta
  - Bloqueios de equipamentos
  - Guardas
  - Postes de segurança
  - Cercas
- **Segurança física para funcionários**
  - Key fobs
  - Smart cards
  - Chaves
  - Biometria
    - Leitor de retina
    - Scanner de impressão digital
    - Leitor de impressão digital
  - Iluminação
  - Magnetômetros
- **Segurança lógica**
  - Princípio do menor privilégio
  - Listas de controle de acesso (ACLs)
  - Autenticação multifator
  - E-mail
  - Tokens físicos
  - Soft token
  - Serviço de mensagens curtas
  - Chamada de voz
  - Aplicação de autenticadores
- **Gerenciamento de dispositivos móveis (MDM)**
- **Active Directory**
  - Script de login
  - Domínio
  - Política do grupo/Atualizações
  - Unidades organizacionais
  - Diretório inicial
  - Redirecionamento de pastas
  - Grupos de segurança

2.2 Compare e diferencie os protocolos de segurança sem fio e os métodos de autenticação.

- **Protocolos e criptografia**
  - Acesso protegido WiFi versão 2 (WPA2)
  - WPA3
  - Protocolo de integridade de chave temporal
  - Padrão de Criptografia Avançado
- **Autenticação**
  - Serviço de usuário discado de autenticação remota (RADIUS)
  - Sistema de controle de acesso ao controlador de acesso adicional (TACACS+)
  - Kerberos
  - Multifator

2.3 Considerando um cenário, detecte, remova e previna o malware usando as ferramentas e métodos apropriados.

- **Malware**
  - Trojan
  - Rootkit
  - Vírus
  - Spyware
  - Ransomware
  - Keylogger
  - Vírus do setor de inicialização
  - Criptomineradores
- **Ferramentas e métodos**
  - Modo de recuperação
  - Antivírus
  - Antimalware
  - Firewalls de software
  - Treinamento antiphishing
  - Educação do usuário sobre ameaças comuns
  - Reinstalação do SO

2.4 Explique os ataques, ameaças e vulnerabilidades comuns de engenharia social.

- **Engenharia social**
  - Phishing
  - Vishing
  - Shoulder surfing (Olhar sobre os ombros)
  - Whaling
  - Tailgating (Acompanhamento não autorizado)
  - Personificação
  - Dumpster diving (hackers que vasculham lixo)
  - Evil twin
- **Ameaças**
  - Negação de serviço distribuído (DDoS)
  - Negação de serviço (DoS)
  - Ataque de dia zero
  - Spoofing
  - Ataque on-path
  - Ataque de força bruta
  - Ataque de dicionário
  - Ameaça interna
  - Injeção de Linguagem de consulta estruturada (SQL)
  - Cross-site scripting (XSS)
- **Vulnerabilidades**
  - Sistemas não compatíveis
  - Sistemas não corrigidos
  - Sistemas desprotegidos (antivírus ausente/ firewall ausente)
  - SOs EOL
  - Traga seu próprio aparelho (BYOD)

2.5 Considerando um cenário, gerencie e defina as configurações básicas de segurança no SO Microsoft Windows.

- **Antivírus Defender**
  - Ativar/desativar
  - Definições atualizadas
- **Firewall**
  - Ativar/desativar
  - Segurança de porta
  - Segurança dos aplicativos
- **Usuários e grupos**
  - Conta local vs. Microsoft
  - Conta padrão
  - Administrador
  - Usuário convidado
  - Usuário avançado
- **Opções de login do SO**
  - Nome de usuário e senha
  - Número de identificação pessoal (PIN)
  - Impressão digital
  - Reconhecimento facial
  - Logon único (SSO)
- **NTFS vs. permissões de compartilhamento**
  - Atributos de arquivo e pasta
  - Herança
- **Executar como administrador vs. usuário padrão**
  - Controle de conta do usuário (UAC)
- **BitLocker**
- **BitLocker To Go**
- **Sistema de arquivos criptografados (EFS)**

2.6 Considerando um cenário, configure uma estação de trabalho para atender às práticas recomendadas de segurança.

- **Criptografia de dados inativos**
- **Melhores práticas em relação a senhas**
  - Requisitos de complexidade
    - Comprimento
    - Tipos de caracteres
  - Requisitos de expiração
  - Senhas do Sistema básico de entrada/saída(BIOS)/ Interface unificada de firmware extensível (UEFI)
- **Práticas recomendadas para o usuário final**
  - Use bloqueios de proteção de tela
  - Faça logoff quando não estiver em uso
  - Proteja/cuide do hardware essencial (por exemplo, notebooks)
  - Proteja informações de identificação pessoal (PII) e senhas
- **Gerenciamento de contas**
  - Restringir permissões de usuário
  - Restringir os horários de login
  - Desabilitar contas de convidado
  - Usar o bloqueio de tentativas com falha
  - Usar o limite de tempo/bloqueio de tela
- **Alterar conta/senha do administrador padrão**
- **Desabilitar autoexecução**
- **Desativar reprodução automática**

2.7 Explicar métodos comuns para proteger dispositivos móveis e incorporados.

- **Bloqueios de tela**
  - Reconhecimento facial
  - Códigos PIN
  - Impressão digital
  - Padrão
  - Passar o dedo (swiping)
- **Limpezas remotas**
- **Aplicadores de localizadores**
- **Atualização de SO**
- **Criptografia de dispositivo**
- **Aplicações de backup remotas**
- **Restrições às tentativas de acesso falhadas**
- **Antivírus/Antimalware**
- **Firewalls**
- **Políticas e procedimentos**
  - BYOD vs. propriedade da empresa
  - Requisitos de segurança dos perfis
- **Internet das Coisas (IoT)**

2.8 Considerando um cenário, use métodos comuns de destruição e descarte de dados.

- **Destruição física**
  - Perfuração
  - Trituração
  - Desmagnetização
  - Incineração
- **Reciclagem ou reaproveitamento de melhores práticas**
  - Apagar/limpar
  - Formatação de baixo nível
  - Formatação padrão
- **Conceitos de terceirização**
  - Fornecedor terceirizado
  - Certificação de destruição/reciclagem

2.9 Considerando um cenário, defina as configurações de segurança apropriadas em redes sem fio e com fio de escritório em casa/escritório pequeno (SOHO).

- **Configurações do roteador doméstico**
  - Alterar senhas padrão
  - Filtro de IP
  - Atualizações do firmware
  - Filtro de conteúdo
  - Disposição física/locais seguros
  - Reservas de Protocolo de configuração de host dinâmico (DHCP)
  - IP estático de rede de longa distância (WAN)
  - Plugar e ligar universal (UPnP)
  - Sub-rede filtrada
- **Específico wireless**
  - Alterar o identificador do conjunto de serviços (SSID)
  - Desabilitar o broadcast de SSID
  - Configurações de criptografia
  - Desabilitar acesso de convidado
  - Alterar canais
- **Configurações de firewall**
  - Desabilitar portas não utilizadas
  - Encaminhamento/mapeamento de portas

2.10 Considerando um cenário, instale e configure navegadores e configurações de segurança relevantes.

- **Download/instalação do navegador**
  - Fontes confiáveis
    - Hashing
  - Fontes não confiáveis
- **Extensões e plug-ins**
  - Fontes confiáveis
  - Fontes não confiáveis
- **Gerenciadores de senhas**
- **Conexões/sites seguros — certificados válidos**
- **Configurações**
  - Bloqueador de pop-up
  - Limpar dados de navegação
  - Limpar o cache
  - Modo de navegação privada
  - Sincronização de dados de login/navegador
  - Bloqueadores de anúncios

3.0 Resolução de problemas de software

3.1 Considerando um cenário, solucione problemas comuns do SO Windows.

- **Sintomas comuns**
  - Tela azul da morte (BSOD)
  - Desempenho lento
  - Problemas de inicialização
  - Desligamentos frequentes
  - Serviços não iniciam
  - Falha de aplicações
  - Avisos de memória baixa
  - Avisos de recursos do controlador USB
  - Instabilidade do sistema
  - Nenhum SO encontrado
  - Carga de perfil lento
  - Perda da configuração da hora
- **Etapas comuns de solução de problemas**
  - Reiniciar
  - Reiniciar serviços
  - Desinstalar/reinstalar/atualizar aplicativos
  - Adicionar recursos
  - Verificar os requisitos
  - Verificação de arquivos do sistema
  - Reparar Windows
  - Restaurar
  - Refazer imagem
  - Reverter atualizações
  - Reconstruir perfis do Windows

3.2 Considerando um cenário, solucione problemas comuns de segurança do computador pessoal (PC).

- **Sintomas comuns**
  - Não é possível acessar a rede
  - Alertas de área de trabalho
  - Alertas falsos sobre proteção antivírus
  - Sistema alterado ou arquivos pessoais
    - Arquivos ausentes/ renomeados
  - Notificações indesejadas no SO
  - Falhas de atualizações do SO
- **Sintomas relacionados ao navegador**
  - Pop-ups aleatórios/frequentes
  - Avisos de certificado
  - Redirecionamento

3.3 Considerando um cenário, use os procedimentos de melhores práticas para remoção de malware.

1. **Investigar e verificar os sintomas de malware**
2. **Colocar o sistema infectado em quarentena**
3. **Desabilitar a restauração do sistema no Windows**
4. **Corrigir sistemas infectados**
   a. Atualizar o software antimalware
   b. Técnicas de varredura e remoção (modo seguro, ambiente pré-instalação)
5. **Agendar análises e efetuar atualizações**
6. **Habilitar restauração do sistema e criar um ponto de restauração no Windows**
7. **Instruir o usuário final**

3.4 Considerando um cenário, solucione problemas comuns do SO e aplicativo para dispositivos móveis.

- **Sintomas comuns**
  - Aplicativo não inicia
  - O aplicativo não fecha/trava
  - Aplicativo não atualiza
  - Demora para responder
  - SO não atualiza
  - Problemas de duração da bateria
  - Reinicializações aleatórias
  - Problemas de conectividade
    - Bluetooth
    - Wi-Fi
    - Comunicação a curta distância (NFC)
    - AirDrop
  - A tela não gira automaticamente

3.5 Considerando um cenário, solucione problemas comuns de segurança de aplicativos e SO móveis.

- **Preocupações com segurança**
  - Origem do pacote Android (APK)
  - Modo de desenvolvedor
  - Acesso root/Desbloqueio Jailbreak
  - Bootleg/aplicativo malicioso
    - Falsificação de aplicativo
- **Sintomas comuns**
  - Alto tráfego de rede
  - Tempo de resposta lento
  - Notificação de limite de uso de dados
  - Conectividade à internet limitada
  - Sem conectividade à internet
  - Número elevado de anúncios
  - Avisos de segurança falsos
  - Comportamento inesperado do aplicativo
  - Arquivos/dados pessoais vazados

4.0 Procedimentos operacionais

4.1 Considerando um cenário, implemente as melhores práticas associadas à documentação e suporte ao gerenciamento de informações dos sistemas.

- **Sistemas de emissão de tíquetes**
  - Informação do usuário
  - Informação de dispositivo
  - Descrição dos problemas
  - Categorias
  - Gravidade
  - Níveis de escalação
  - Comunicação escrita clara e concisa
    - Descrição do problema
    - Notas de progresso
    - Resolução do problema
- **Gerenciamento de ativos**
  - Listas de inventário
  - Sistema de banco de dados
  - Tags e IDs de ativos
  - Ciclo de vida de compras
  - Garantia e licenciamento
  - Usuários atribuídos
- **Tipos de documentos**
  - Política de uso aceitável (AUP)
  - Diagrama de topologia de rede
  - Requisitos de conformidade regulamentar
    - Telas de apresentação
  - Comunicação de incidentes
  - Procedimentos operacionais padrão
    - Procedimentos para instalação personalizada do pacote de software
  - Lista de verificação de configuração de novo usuário
  - Lista de verificação de encerramento do usuário final
- **Base de conhecimento/artigos**

4.2 Explique as melhores práticas básicas da gestão de mudanças.

- **Processos de negócios documentados**
  - Plano de reversão
  - Teste de sandbox
  - Funcionário responsável
- **Gestão de mudanças**
  - Formulários de solicitação
  - Propósito da mudança
  - Escopo da mudança
  - Data e hora da mudança
  - Sistemas afetados/impacto
  - Análises de risco
    - Nível de risco
  - Aprovação do Comitê de Mudanças
  - Aceitação do usuário final

4.3 Considerando um cenário, implemente métodos de backup e recuperação da estação de trabalho.

- **Backup e recuperação**
  - Completo
  - Incremental
  - Diferencial
  - Sintético
- **Teste de backup**
  - Frequência
- **Esquemas de rotação de backup**
  - No local vs. fora do local
  - Avô-pai-filho (GFS)
  - Regra de backup 3-2-1

4.4 Considerando um cenário, use procedimentos de segurança comuns.

- **Pulseiras de descarga eletrostática (ESD)**
- **Tapetes ESD**
- **Aterramento do equipamento**
- **Manuseio de energia adequado**
- **Manuseamento e armazenamento de componentes adequados**
- **Sacos antiestáticos**
- **Conformidade com regulamentos governamentais**
- **Segurança pessoal**
  - Desconectar energia antes de reparar o computador
  - Técnicas de elevação
  - Segurança contra incêndio elétrico
  - Óculos de segurança
  - Máscara de filtragem de ar

4.5 Resuma os impactos ambientais e dos controles ambientais locais.

- **Ficha de dados de segurança do material (MSDS)/documentação para manuseio e descarte**
  - Descarte correto da bateria
  - Descarte correto do toner
  - Descarte correto de outros dispositivos e ativos
- **Consciência da temperatura e do nível de umidade e ventilação adequadas**
  - Localização/disposição de equipamentos
  - Limpeza de pó
  - Ar comprimido/vácuo
- **Picos de energia, eventos de subtensão e falhas de energia**
  - Backup da bateria
  - Proteção contra pico de energia

4.6 Explique a importância do conteúdo/atividade proibido(a) e conceitos de privacidade, licenciamento e política.

- **Resposta a incidentes**
  - Cadeia de custódia
  - Informar a administração/aplicação da lei, conforme necessário
  - Cópia da unidade (integridade e preservação dos dados)
  - Documentação do incidente
- **Licenciamento/gerenciamento de direitos digitais (DRM)/contrato de licença de usuário final (EULA)**
  - Licenças válidas
  - Licenças não expiradas
  - Licença de uso pessoal x licença de uso corporativo
  - Licença de código aberto
- **Dados regulamentados**
  - Transações de cartões de crédito
  - Informações pessoais emitidas pelo governo
  - PII
  - Dados de saúde
  - Requisitos de retenção de dados

4.7 Considerando um cenário, use as técnicas de comunicação e profissionalismo apropriados.

- **Aparência e trajes profissionais**
  - Use o traje necessário correspondente a determinado ambiente
    - Formal
    - Casual de negócios
- **Usar linguagem adequada e evitar jargões, acrônimos, gírias quando aplicável**
- **Manter uma atitude positiva/projetar confiança**
- **Escutar ativamente, anotar, evitar interromper o cliente**
- **Ser culturalmente sensato**
  - Usar títulos profissionais apropriados, quando aplicável
- **Ser pontual (se estiver atrasado, contate o cliente)**
- **Evitar distrações**
  - Chamadas pessoais
  - Mensagens de texto/sites de redes sociais
  - Interrupções pessoais
- **Lidar com clientes ou situações difíceis**
  - Não discutir com clientes ou ficar na defensiva
  - Evitar ignorar problemas dos clientes
  - Evitar ser crítico
  - Esclarecer as afirmações dos clientes (colocar questões de resposta livre para restringir o escopo do problema, reafirmar o problema ou questão para garantir compreensão)
  - Não divulgar experiências por meio de redes sociais
- **Definir e cumprir expectativas/prazos e comunicar o progresso com o cliente**
  - Oferecer opções de reparo/substituição, conforme necessário
  - Fornecer documentação apropriada sobre os serviços prestados
  - Acompanhar o cliente/usuário posteriormente para perceber o nível de satisfação
- **Lidar apropriadamente com materiais confidenciais e privados dos clientes**
  - Localizado em um computador, área de trabalho, impressora, etc.

4.8 Identifique os fundamentos do script.

- **Tipos de arquivos de script**
  - .bat
  - .ps1
  - .vbs
  - .sh
  - .js
  - .py
- **Casos de uso para scripts**
  - Automação básica
  - Reinicializar máquinas
  - Remapear unidade de rede
  - Instalação de aplicativos
  - Backups automatizados
  - Coleta de informações/dados
  - Iniciar atualizações
- **Outras considerações ao usar scripts**
  - Introdução involuntária de malware
  - Alterar inadvertidamente as configurações do sistema
  - O navegador ou o sistema travam devido ao manuseio incorreto de recursos

4.9 Considerando um cenário, use as tecnologias de acesso remoto.

- **Métodos/ferramentas**
  - RDP
  - VPN
  - Computação em rede virtual (VNC)
  - Shell Seguro (SSH)
  - Monitoramento e gerenciamento remoto (RMM)
  - Assistência remota da Microsoft (MSRA)
  - Ferramentas de terceiros
    - Software de compartilhamento de tela
    - Software de videoconferência
    - Software de transferência de arquivos
    - Software de gerenciamento de área de trabalho
- **Considerações de segurança de cada método de acesso**

Lista de acrônimos CompTIA A+ Core 2 (220-1102)

Veja abaixo uma lista de acrônimos presentes no exame CompTIA A+ Core 2 (220-1102). Os candidatos são incentivados a rever a lista completa e a obter conhecimentos de todos os acrônimos listados como parte de um programa de preparação abrangente para o exame.

Acrônimo	Definição
AAA	Authentication, Authorization, and Accounting
AC	Alternating Current
ACL	Access Control List
ADF	Automatic Document Feeder
AES	Advanced Encryption Standard
AP	Access Point
APFS	Apple File System
APIPA	Automatic Private Internet Protocol Addressing
APK	Android Package
ARM	Advanced RISC [Reduced Instruction Set Computer] Machine
ARP	Address Resolution Protocol
ATA	Advanced Technology Attachment
ATM	Asynchronous Transfer Mode
ATX	Advanced Technology Extended
AUP	Acceptable Use Policy
BIOS	Basic Input/Output System
BSOD	Blue Screen of Death
BYOD	Bring Your Own Device
CAPTCHA	Completely Automated Public Turing Test to Tell Computers and Humans Apart
CD	Compact Disc
CDFS	Compact Disc File System
CDMA	Code-Division Multiple Access
CERT	Computer Emergency Response Team
CIFS	Common Internet File System
CMD	Command Prompt
CMOS	Complementary Metal-Oxide Semiconductor
CPU	Central Processing Unit
CRL	Certificate Revocation List
DC	Direct Current
DDoS	Distributed Denial of Service
DDR	Double Data Rate

Acrônimo	Definição
DHCP	Dynamic Host Configuration Protocol
DIMM	Dual Inline Memory Module
DKIM	DomainKeys Identified Mail
DMA	Direct Memory Access
DMARC	Domain-based Message Authentication, Reporting, and Conformance
DNS	Domain Name System
DoS	Denial of Service
DRAM	Dynamic Random-Access Memory
DRM	Digital Rights Management
DSL	Digital Subscriber Line
DVI	Digital Visual Interface
DVI-D	Digital Visual Interface-Digital
ECC	Error Correcting Code
EFS	Encrypting File System
EMI	Electromagnetic Interference
EOL	End-of-Life
eSATA	External Serial Advanced Technology Attachment
ESD	Electrostatic Discharge
EULA	End-User License Agreement
exFAT	Extensible File Allocation Table
ext	Extended File System
FAT	File Allocation Table
FAT12	12-bit File Allocation Table
FAT16	16-bit File Allocation Table
FAT32	32-bit File Allocation Table
FSB	Front-Side Bus
FTP	File Transfer Protocol
GFS	Grandfather-Father-Son
GPS	Global Positioning System
GPT	GUID [Globally Unique Identifier] Partition Table
GPU	Graphics Processing Unit
GSM	Global System for Mobile Communications
GUI	Graphical User Interface

Acrônimo	Definição
GUID	Globally Unique Identifier
HAL	Hardware Abstraction Layer
HAV	Hardware-assisted Virtualization
HCL	Hardware Compatibility List
HDCP	High-bandwidth Digital Content Protection
HDD	Hard Disk Drive
HDMI	High-Definition Multimedia Interface
HSM	Hardware Security Module
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I/O	Input/Output
IaaS	Infrastructure as a Service
ICR	Intelligent Character Recognition
IDE	Integrated Drive Electronics
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IMAP	Internet Mail Access Protocol
IOPS	Input/Output Operations Per Second
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IPS	In-plane Switching
IPSec	Internet Protocol Security
IR	Infrared
IrDA	Infrared Data Association
IRP	Incident Response Plan
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITX	Information Technology eXtended
KB	Knowledge Base
KVM	Keyboard-Video-Mouse
LAN	Local Area Network
LC	Lucent Connector
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LED	Light-emitting Diode
MAC	Media Access Control/Mandatory Access Control
MAM	Mobile Application Management
MAN	Metropolitan Area Network
MBR	Master Boot Record
MDM	Mobile Device Management
MFA	Multifactor Authentication
MFD	Multifunction Device
MFP	Multifunction Printer
MMC	Microsoft Management Console
MOU	Memorandum of Understanding
MSDS	Material Safety Data Sheet
MSRA	Microsoft Remote Assistance
MX	Mail Exchange
NAC	Network Access Control
NAT	Network Address Translation
NDA	Non-disclosure Agreement
NetBIOS	Networked Basic Input/Output System
NetBT	NetBIOS over TCP/IP [Transmission Control Protocol/Internet Protocol]
NFC	Near-field Communication
NFS	Network File System
NIC	Network Interface Card
NTFS	New Technology File System
NVMe	Non-volatile Memory Express
OCR	Optical Character Recognition
OLED	Organic Light-emitting Diode
ONT	Optical Network Terminal
OS	Operating System
PaaS	Platform as a Service
PAN	Personal Area Network
PC	Personal Computer
PCIe	Peripheral Component Interconnect Express
PCL	Printer Command Language
PE	Preinstallation Environment
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PoE	Power over Ethernet
POP3	Post Office Protocol 3
POST	Power-on Self-Test
PPP	Point-to-Point Protocol
PRL	Preferred Roaming List
PSU	Power Supply Unit
PXE	Preboot Execution Environment
RADIUS	Remote Authentication Dial-in User Service
RAID	Redundant Array of Independent (or Inexpensive) Disks
RAM	Random-access Memory
RDP	Remote Desktop Protocol
RF	Radio Frequency
RFI	Radio Frequency Interference
RFID	Radio Frequency Identification
RJ11	Registered Jack Function 11
RJ45	Registered Jack Function 45
RMM	Remote Monitoring and Management
RTO	Recovery Time Objective
SaaS	Software as a Service
SAN	Storage Area Network

Acrônimo	Definição
SAS	Serial Attached SCSI [Small Computer System Interface]
SATA	Serial Advanced Technology Attachment
SC	Subscriber Connector
SCADA	Supervisory Control and Data Acquisition
SCP	Secure Copy Protection
SCSI	Small Computer System Interface
SDN	Software-defined Networking
SFTP	Secure File Transfer Protocol
SIM	Subscriber Identity Module
SIMM	Single Inline Memory Module
S.M.A.R.T.	Self-monitoring Analysis and Reporting Technology
SMB	Server Message Block
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SODIMM	Small Outline Dual Inline Memory Module
SOHO	Small Office/Home Office
SPF	Sender Policy Framework
SQL	Structured Query Language
SRAM	Static Random-access Memory
SSD	Solid-State Drive
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-on
ST	Straight Tip
STP	Shielded Twisted Pair
TACACS	Terminal Access Controller Access-Control System
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol

Acrônimo	Definição
TFTP	Trivial File Transfer Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TN	Twisted Nematic
TPM	Trusted Platform Module
UAC	User Account Control
UDP	User Datagram Protocol
UEFI	Unified Extensible Firmware Interface
UNC	Universal Naming Convention
UPnP	Universal Plug and Play
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
UTM	Unified Threat Management
UTP	Unshielded Twisted Pair
VA	Vertical Alignment
VDI	Virtual Desktop Infrastructure
VGA	Video Graphics Array
VLAN	Virtual LAN [Local Area Network]
VM	Virtual Machine
VNC	Virtual Network Computer
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VRAM	Video Random-access Memory
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WISP	Wireless Internet Service Provider
WLAN	Wireless LAN [Local Area Network]
WMN	Wireless Mesh Network
WPA	WiFi Protected Access
WWAN	Wireless Wide Area Network
XSS	Cross-site Scripting

CompTIA A+ Core 2 (220-1102)
Lista de hardware e software proposta

**A CompTIA incluiu esta lista de exemplo de hardware e software para ajudar os candidatos a se prepararem para o exame A+ Core 2 (220-1102). Esta lista também pode ser útil para as empresas de treinamento que desejam criar um componente laboratorial para sua oferta de treinamento. As listas com marcadores abaixo de cada tópico são listas de exemplo e não são exaustivas.

Equipamento

- Tablet/smartphone da Apple
- Tablet/smartphone Android
- Tablet Windows
- Chromebook
- Notebook Windows/notebook Mac/notebook Linux
- Desktop Windows/desktop Mac/desktop Linux
- Servidor Windows com Active Directory e gerenciamento de impressão
- Monitores
- Projetores
- Roteador/Opção SOHO
- Ponto de acesso
- Telefone de voz sobre IP (VoIP)
- Impressora
  - Laser/jato de tinta
  - Sem fio
  - Impressora 3D
  - Térmica
- Proteção contra pico de energia
- Fonte de energia ininterrupta (UPS)
- Dispositivos inteligentes (dispositivos da Internet das Coisas [IoT])
- Servidor com um hipervisor
- Bloco de inserção
- Painel de conexões
- Webcams
- Alto-falantes
- Microfones

Peças sobressalentes/hardware

- Placas-mãe
- RAM
- Discos rígidos
- Fontes de energia
- Placas de vídeo
- Placas de som
- Placas de rede
- Placas de interface de rede sem fio (NICs)
- Ventoinhas/dispositivos de refrigeração/dissipador de calor
- CPUs
- Conectores/cabos variados
  - USB
  - Interface de mídia de alta definição (HDMI)
  - DisplayPort
  - Interface visual digital (DVI)
  - Padrão de gráficos de vídeo (VGA)
- Adaptadores
  - Adaptador Bluetooth
- Cabos de rede
- Conectores/cabos de rede não finalizados
- Adaptadores de corrente alternada (AC)
- Unidades ópticas
- Parafusos/afastadores
- Caixas
- Kit de manutenção
- Mouses/teclados
- Teclado-vídeo-mouse (KVM)
- Cabo do console
- Unidade de estado sólido (SSD)

Ferramentas

- Chave de fendas
- Multímetro
- Alicates
- Alicate de inserção (punch down)
- Alicate de crimpagem
- Testador da fonte de energia
- Decapador de cabos
- Kit de ferramentas padrão para técnicos
- Pulseira de descarga eletrostática (ESD)
- Pasta térmica
- Testador de cabos
- Toner de cabo
- Analisador de Wi-Fi
- Tecnologia de conexão série avançada (SATA) para conectores USB

Software

- SOs
  - Linux
  - SO Chrome
  - Microsoft Windows
  - macOS
  - Android
  - iOS
- Disco do ambiente de pré-instalação (PE)/disco compacto executável (CD)
- Software antivírus
- Software de virtualização
- Antimalware
- Software de driver

CompTIA