CompTIA A+ Examen de Certificación Core 2 Objetivos

NÚMERO DE EXAMEN: CORE 2 (220-1102)

CompTIA

Acerca del examen

Se recomienda que los candidatos usen este documento como ayuda para prepararse para el examen de certificación de CompTIA A+ 220-1102. Para recibir la certificación CompTIA A+, debe aprobar dos exámenes: Core 1 (220-1101) y Core 2 (220-1102). El examen de certificación CompTIA A+ Core 1 (220-1101) y Core 2 (220-1102) verificará que el candidato aprobado tenga los conocimientos y las habilidades requeridas para lo siguiente:

- Instalar, configurar y mantener computadoras, dispositivos móviles y software para usuarios finales
- Verificar componentes basado en los requerimientos del cliente
- Comprender los fundamentos de las redes y aplicar métodos básicos de ciberseguridad para mitigar amenazas
- Diagnosticar, resolver y documentar, en forma adecuada y segura, problemas comunes de hardware y software
- Aplicar habilidades de resolución de problemas y brindar soporte al cliente, usando habilidades de comunicación adecuadas
- Comprender los fundamentos de las secuencias de comandos, tecnologías en la nube, virtualización e implementación de múltiples sistemas operativos en entornos corporativos

Esto es equivalente a 12 meses de experiencia práctica, trabajando en servicio de ayuda, técnico de servicio de escritorio o técnico de servicio de campo. Estos ejemplos de contenido pretenden aclarar los objetivos de la prueba y no se deben interpretar como un listado completo de todos los contenidos de este examen.

ACREDITACIÓN DEL EXAMEN

El examen CompTIA A+ Core 2 (220-1102) tiene acreditación de ANSI para demostrar cumplimiento con el Estándar ISO 17024 y, como tal, recibe revisiones y actualizaciones regulares a los objetivos del examen.

DESARROLLO DEL EXAMEN

Los exámenes de CompTIA resultan de talleres de expertos del área temática y resultados de encuestas de toda la industria con respecto a las habilidades y conocimientos necesarios para un profesional de TI de nivel básico.

POLÍTICA DE USO DE MATERIALES AUTORIZADOS de CompTIA

CompTIA Certifications, LLC no está afiliado con y no autoriza, aprueba o tolera la utilización de cualquier contenido proporcionado por otros sitios de capacitación no autorizados (conocidos como “brain dumps”). A las personas que utilicen este tipo de materiales en la preparación de cualquier examen CompTIA se les anularán los certificados y será suspendida la realización de futuras pruebas en concordancia con el Acuerdo para Candidatos de CompTIA. En un esfuerzo por comunicar de manera más clara las políticas de exámenes de CompTIA en relación con el uso de materiales de estudio autorizados, CompTIA dirige a todos los candidatos de certificación a las Políticas de Examen de Certificación CompTIA. Revise todas las políticas CompTIA antes de comenzar el proceso de estudio para cualquier examen CompTIA. Se requerirá que los candidatos cumplan el Acuerdo de Candidato CompTIA. Si un candidato tiene una pregunta acerca de qué materiales de estudio se consideran no autorizados (conocidos como “brain dumps”), él/ella deberá comunicarse con CompTIA al correo electrónico examsecurity@comptia.org para confirmar.

RECUERDE

Las listas de ejemplos proporcionadas en formato con viñetas no son listas completas. Otros ejemplos de tecnologías, procesos o tareas relativas a cada objetivo también pueden ser incluidos en el examen, aunque no estén enumerados o cubiertos en este documento de objetivos. CompTIA revisa constantemente el contenido de nuestros exámenes y actualiza las preguntas de las pruebas para asegurar que nuestros exámenes sean actuales y la seguridad de las preguntas esté protegida. Cuando sea necesario, publicaremos exámenes actualizados, basados en objetivos de examen existentes. Sepa que todos los materiales relacionados de preparación para el examen serán válidos.

DETALLES DE LA PRUEBA

Examen requerido	A+ Core 2 (220-1102)
Número de preguntas	90 como máximo
Tipos de preguntas	Selección múltiple y basadas en la ejecución
Longitud de la prueba	90 minutos
Experiencia recomendada	12 meses de experiencia práctica como técnico de servicio de ayuda, técnico de servicio de escritorio o técnico de servicio de campo
Calificación para aprobación	700 (en escala de 100-900)

OBJETIVOS DEL EXAMEN (DOMINIOS)

La siguiente tabla enumera los dominios medidos en este examen y el grado en el que están representados.

DOMINIO		PORCENTAJE DEL EXAMEN
1.0	Sistemas operativos	31%
2.0	Seguridad	25%
3.0	Solución de problemas de software	22%
4.0	Procedimientos operativos	22%
Total		**100%**

NOTA SOBRE WINDOWS 11

Las versiones de Microsoft® Windows® que no sean objeto de Soporte estándar (según sea determinado por Microsoft), que incluye a Windows 11, son áreas de contenido previsto de la certificación. Como tal, los objetivos en que no se indica una versión específica de Microsoft Windows en el título del objetivo principal pueden incluir contenido relacionado con Windows 10 y Windows 11, en cuanto se relaciona con el rol de trabajo.

1.0 Sistemas operativos

1.1 Identificar características básicas de las ediciones de Microsoft Windows.

- **Ediciones de Windows 10**
  - Home
  - Pro
  - Pro para estaciones de trabajo
  - Enterprise
- **Diferencias de funciones**
  - Acceso a dominio versus grupo de trabajo
  - Estilos de escritorio/interfaz del usuario
  - Disponibilidad de Protocolo de Escritorio Remoto (RDP)
  - Limitaciones de soporte para Memoria de acceso aleatorio (RAM)
  - BitLocker
  - gpedit.msc
- **Rutas de actualización**
  - Actualización incluida

1.2 Dado un escenario, usar las herramientas de línea de comando apropiadas de Microsoft.

- **Navegación**
  - cd
  - dir
  - md
  - rmdir
  - Entradas de navegación en unidad:
    - C: o D: o x:
- **Herramientas de línea de comando**
  - ipconfig
  - ping
  - hostname
  - netstat
  - nslookup
  - chkdsk
  - net user
  - net use
  - tracert
  - format
  - xcopy
  - copy
  - robocopy
  - gpupdate
  - gpresult
  - shutdown
  - sfc
  - [nombre de comando] /?
  - diskpart
  - pathping
  - winver

1.3 Dado un escenario, usar las características y herramientas del sistema operativo (OS) Microsoft Windows 10.

- **Administrador de tareas**
  - Servicios
  - Inicio
  - Desempeño
  - Procesos
  - Usuarios
- **Complemento Consola de administración de Microsoft (MMC)**
  - Visor de eventos (eventvwr.msc)
  - Administración de disco (diskmgmt.msc)
  - Programador de tareas (taskschd.msc)
  - Administrador de dispositivos (devmgmt.msc)
  - Administrador de certificados (certmgr.msc)
  - Usuarios y Grupos locales (lusrmgr.msc)
  - Monitor de desempeño (perfmon.msc)
  - Editor de política de grupo (gpedit.msc)
- **Herramientas adicionales**
  - Información del sistema (msinfo32.exe)
  - Monitor de recursos (resmon.exe)
  - Configuración del sistema (msconfig.exe)
  - Liberador de espacio en disco (cleanmgr.exe)
  - Desfragmentador de disco (dfrgui.exe)
  - Editor de registro (regedit.exe)

1.4 Dado un escenario, usar la utilidad Panel de control de Microsoft Windows 10.

- **Opciones de Internet**
- **Dispositivos e Impresoras**
- **Programas y características**
- **Red y Centro para compartir**
- **Sistema**
- **Windows Defender Firewall**
- **Correo electrónico**
- **Sonido**
- **Cuentas de usuario**
- **Administrador de dispositivos**
- **Opciones de indexación**
- **Herramientas administrativas**
- **Opciones del Explorador de archivos**
  - Ver archivos ocultos
  - Ocultar extensiones
  - Opciones generales
  - Opciones de vista
- **Opciones de energía**
  - Hibernar
  - Planes de energía
  - Dormir/suspender
  - Modo de espera
  - Elegir la acción del cierre de la tapa
  - Encender inicio rápido
  - Suspensión selectiva de Bus Serial Universal (USB)
- **Facilidad de acceso**

1.5 Dado un escenario, utilizar la configuración adecuada de Windows.

- **Hora e idioma**
- **Actualización y seguridad**
- **Personalización**
- **Aplicaciones**
- **Privacidad**
- **Sistema**
- **Dispositivos**
- **Red e internet**
- **Juegos**
- **Cuentas**

1.6 Dado un escenario, configurar las funciones de red de Microsoft Windows en un cliente/computadora de escritorio.

- **Grupo de trabajo vs. Configuración de dominio**
  - Recursos compartidos
  - Impresoras
  - Servidores de archivos
  - Unidades asignadas
- **Configuración de firewall de sistema operativo local**
  - Restricciones y excepciones de aplicaciones
  - Configuración
- **Configuración de red del cliente**
  - Esquemas de Direccionamiento del protocolo de Internet (IP)
  - Configuración del sistema de nombres de dominio (DNS)
  - Máscara de subred
  - Puerta de enlace
  - Estático vs. dinámico
- **Establecer conexiones de red**
  - Red Privada Virtual (VPN)
  - Redes inalámbricas
  - Con cable
  - Red de Área Amplia Inalámbrica (WWAN)
- **Configuración de proxy**
- **Red pública vs. Red privada**
- **Navegación en Explorador de archivos – rutas de red**
- **Conexiones medidas y limitaciones**

1.7 Dado un escenario, aplicar los conceptos de instalación y configuración de aplicaciones.

- **Requerimientos del sistema para aplicaciones**
  - Requerimientos de aplicaciones dependientes de 32 bits vs. 64 bits
  - Tarjetas gráficas dedicadas vs. integradas
  - Requerimientos de Memoria de Acceso Aleatorio de Video (VRAM)
  - Requerimientos de RAM
  - Requerimientos de unidad de procesamiento central (CPU)
  - Tokens de hardware externo
  - Requisitos de almacenamiento
- **Requerimientos del sistema operativo para aplicaciones**
  - Compatibilidad de aplicaciones con el sistema operativo
  - 32 bits vs. 64 bits
- **Métodos de distribución**
  - Medios físicos vs. descargables
  - ISO montable
- **Otras consideraciones para aplicaciones nuevas**
  - Impacto en dispositivo
  - Impacto en la red
  - Impacto en funcionamiento
  - Impacto en el negocio

1.8 Explicar tipos comunes de OS y sus objetivos.

- **Sistema operativo de estación de trabajo**
  - Windows
  - Linux
  - macOS
  - Chrome OS
- **Sistemas operativos de teléfono celular/tabletas**
  - iPadOS
  - iOS
  - Android
- **Varios tipos de sistemas de archivos**
  - Nuevo Sistema de Tecnología de Archivos (NTFS)
  - Tabla de Asignación de Archivos 32 (FAT32)
  - Tercer sistema de archivos extendido (ext3)
  - Cuarto sistema de archivos extendido (ext4)
  - Sistemas de archivos Apple (APFS)
  - Tabla de Asignación de Archivos Ampliada (exFAT)
- **Limitaciones del ciclo de vida del proveedor**
  - End of life (EOL)
  - Limitaciones de actualización
- **Preocupaciones de compatibilidad entre sistemas operativos**

1.9 Dado un escenario, realizar instalaciones y actualizaciones de OS en un entorno de OS diverso.

- **Métodos de arranque**
  - USB
  - Medios ópticos
  - Red
  - Unidades flash/de estado sólido
  - Basado en internet
  - Unidad de disco externa/ intercambiables en caliente
  - Unidad de disco duro interno (partición)
- **Tipos de instalaciones**
  - Actualización
  - Partición de recuperación
  - Instalación limpia
  - Despliegue de imagen
  - Instalación de reparación
  - Instalación de red remota
  - Otras consideraciones
    - Controladores de terceros
- **Partición**
  - Tabla de partición GUID [Identificador Único Global] (GPT)
  - Registro de arranque maestro (MBR)
- **Formato de unidad**
- **Consideraciones de actualización**
  - Archivos de copia de seguridad y preferencias del usuario
  - Soporte/compatibilidad hacia atrás de soporte de aplicaciones y controladores
  - Compatibilidad de hardware
- **Actualizaciones de funciones**
  - Ciclo de vida del producto

1.10 Identificar características y herramientas comunes en los sistemas operativos macOS/escritorio.

- **Instalación y desinstalación de aplicaciones**
  - Tipos de archivo
    - .dmg
    - .pkg
    - .app
  - App Store
  - Proceso de desinstalación
- **Restricciones corporativas y de Apple ID**
- **Mejores prácticas**
  - Copias de seguridad
  - Antivirus
  - Actualizaciones/parches
- **Preferencias del sistema**
  - Pantallas
  - Redes
  - Impresoras
  - Escáneres
  - Privacidad
  - Accesibilidad
  - Máquina de tiempo
- **Características**
  - Múltiples escritorios
  - Control de misión
  - Cadena de claves
  - Primer plano
  - iCloud
  - Gestos
  - Finder
  - Disco remoto
  - Dock
- **Utilidad de disco**
- **FileVault**
- **Terminal**
- **Salida forzada**

1.11 Identificar características y herramientas comunes en los sistemas operativos Linux cliente/escritorio.

- **Comandos comunes**
  - ls
  - pwd
  - mv
  - cp
  - rm
  - chmod
  - chown
  - su/sudo
  - apt-get
  - yum
  - ip
  - df
  - grep
  - ps
  - man
  - top
  - find
  - dig
  - cat
  - nano
- **Mejores prácticas**
  - Copias de seguridad
  - Antivirus
  - Actualizaciones/parches
- **Herramientas**
  - Shell/terminal
  - Samba

2.0 Seguridad

2.1 Resumir diversas medidas de seguridad y sus objetivos.

- **Seguridad física**
  - Vestíbulo de control de acceso
  - Lector de gafetes
  - Vigilancia con video
  - Sistema de alarma
  - Sensores de movimiento
  - Cerraduras de puerta
  - Bloqueos de equipos
  - Guardias
  - Pilotes
  - Rejas
- **Seguridad física para personal**
  - Key fobs
  - Tarjetas inteligentes
  - Claves
  - Biométricos
    - Escáner de retina
    - Escáner de huellas digitales
    - Escáner de palmas
  - Iluminación
  - Magnetómetros
- **Seguridad lógica**
  - Principio de menor privilegio
  - Lista de Control de Acceso (ACL)
  - Autenticación de Multifactores (MFA)
  - Correo electrónico
  - Hard token
  - Soft token
  - Servicio de Mensajes Cortos (SMS)
  - Llamada de voz
  - Aplicación de autenticador
- **Gestión de dispositivos móviles (MDM)**
- **Directorio activo**
  - Comandos de inicio de sesión
  - Dominio
  - Política de grupo/ Actualizaciones
  - Unidades de la organización
  - Carpeta particular
  - Redirección de carpeta
  - Grupos de seguridad

2.2 Comparar y contrastar protocolos de seguridad inalámbrica y métodos de autenticación.

- **Protocolos y cifrado**
  - Acceso Protegido Wi-Fi 2 (WPA2)
  - WPA3
  - Protocolo Temporal de Integridad de Clave (TKIP)
  - Estándar de Cifrado Avanzado (AES)
- **Autenticación**
  - Servidor de Autenticación Remota de Usuario por Acceso Telefónico (RADIUS)
  - Controlador de Acceso a Terminal Sistema de Control (TACACS+)
  - Kerberos
  - Multifactor

2.3 Dado un escenario, detectar, eliminar y evitar malware usando las herramientas y métodos adecuados.

- **Malware**
  - Troyanos
  - Rootkit
  - Virus
  - Spyware
  - Ransomware
  - Keylogger
  - Virus del sector de arranque
  - Cryptominer
- **Herramientas y métodos**
  - Modo de recuperación
  - Antivirus
  - Antimalware
  - Cortafuegos de software
  - Capacitación antiphishing
  - Educación del usuario respecto de amenazas comunes
  - Reinstalación del OS

2.4 Explicar ataques, amenazas y vulnerabilidades comunes de ingeniería social.

- **Ingeniería social**
  - Phishing
  - Vishing
  - Fisgoneo
  - Whaling
  - Infiltración
  - Suplantación
  - Buscar en la basura
  - Evil twin
- **Amenazas**
  - Denegación de servicio distribuido (DDoS)
  - Denegación de Servicio (DoS)
  - Ataque de día cero
  - Spoofing
  - Ataque en ruta
  - Ataque con fuerza bruta
  - Ataque de diccionario
  - Amenazas internas
  - Inyección de Lenguaje estructurado de consulta (SQL)
  - Secuencias de comandos entre sitios (XSS)
- **Vulnerabilidades**
  - Sistemas que no cumplen con los estándares
  - Sistemas sin parches
  - Sistemas no protegidos (que no tienen antivirus/firewall)
  - EOL OSs
  - Trae Tu Propio Dispositivo (BYOD)

2.5 Dado un escenario, administrar y establecer la configuración básica de seguridad en el sistema operativo Microsoft Windows.

- **Defender Antivirus**
  - Activar/desactivar
  - Definiciones actualizadas
- **Firewall**
  - Activar/desactivar
  - Seguridad de puertos
  - Seguridad de la aplicación
- **Usuarios y grupos**
  - Cuenta local vs. Microsoft
  - Cuenta estándar
  - Administrador
  - Usuario invitado
  - Usuario avanzado
- **Opciones de inicio de sesión en OS**
  - Nombre de usuario y contraseña
  - Número de Identificación Personal (PIN)
  - Huella digital
  - Reconocimiento facial
  - Inicio de sesión único (SSO)
- **Permiso NTFS vs. de recursos compartidos**
  - Atributos de archivo y de carpeta
  - Legado
- **Ejecutar como administrador vs. como usuario estándar**
  - Control de cuenta de usuario (UAC).
- **BitLocker**
- **BitLocker To Go**
- **Sistema de Archivos de Cifrado (EFS)**

2.6 Dado un escenario, configurar una estación de trabajo para satisfacer las mejores prácticas de seguridad.

- **Cifrado de datos en reposo**
- **Mejores prácticas de contraseñas**
  - Requerimientos de complejidad
    - Longitud
    - Tipos de caracteres
  - Requerimientos de vencimiento
  - Contraseñas de Configuración de Sistema básico de entrada/salida (BIOS)/Interfaz de Firmware Extensible Unificada (UEFI)
- **Mejores prácticas de usuario final**
  - Uso de bloqueos de protector de pantalla
  - Cerrar sesión cuando no esté en uso
  - Asegurar/proteger hardware esencial (por ejemplo, computadoras portátiles)
  - Asegurar información de identificación personal (PII) y contraseñas
- **Administración de cuentas**
  - Restringir los permisos del usuario
  - Restringir las horas de inicio de sesión
  - Deshabilitar cuenta de invitados
  - Bloqueo por intentos fallidos
  - Tiempo límite/bloqueo de pantalla
- **Cambiar cuenta de usuario/ contraseña de administrador predeterminado**
- **Deshabilitar ejecución automática**
- **Deshabilitar AutoPlay**

2.7 Explicar los métodos comunes para asegurar dispositivos móviles y dispositivos embebidos.

- **Bloqueos de pantallas**
  - Reconocimiento facial
  - Códigos PIN
  - Huella digital
  - Patrón
  - Deslizamiento rápido
- **Limpiezas remotas**
- **Aplicaciones de ubicación**
- **Actualizaciones del OS**
- **Cifrado de dispositivos**
- **Aplicaciones de copia de seguridad remota**
- **Restricciones de intentos de inicio de sesión fallidos**
- **Antivirus/Antimalware**
- **Firewalls**
- **Políticas y procedimientos**
  - BYOD vs. propiedad corporativa
  - Requisitos de perfil de seguridad
- **Internet de las cosas (IoT)**

2.8 Dado un escenario, usar los métodos apropiados de destrucción y eliminación de datos.

- **Destrucción física**
  - Taladrarlos
  - Triturar
  - Desmagnetizar
  - Incineración
- **Mejores prácticas de reciclaje o readaptación**
  - Borrado/eliminación
  - Formato de bajo nivel
  - Formato estándar
- **Conceptos de externalización**
  - Proveedor de terceros
  - Certificación de destrucción/reciclaje

2.9 Dado un escenario, establecer la configuración adecuada de seguridad en redes inalámbricas y cableada de oficina pequeña/oficina en el hogar (SOHO).

- **Configuración de router de hogar**
  - Cambiar contraseñas predeterminadas
  - Filtrado IP
  - Actualizaciones de firmware
  - Filtrado de contenido
  - Ubicación física/lugares seguros
  - Reservas de Protocolo de Configuración Dinámica de Servidor (DHCP)
  - IP de red de área ampliada estática (WAN)
  - Enchufar y Usar Universal (UPnP)
  - Subred analizada
- **Inalámbrica específica**
  - Cambiar el identificador de conjunto de servicios (SSID)
  - Deshabilitar transmisión SSID
  - Configuración de cifrado
  - Deshabilitar cuenta de invitados
  - Cambiar canales
- **Configuración de firewall**
  - Deshabilitar puertos no usados
  - Reenviar/visualizar puerto

2.10 Dado un escenario, instalar y configurar parámetros de seguridad de navegadores.

- **Descarga/instalación de navegador**
  - Fuentes confiables
    - Hashing
  - Fuentes no confiables
- **Extensiones y complementos**
  - Fuentes confiables
  - Fuentes no confiables
- **Administradores de contraseñas**
- **Conexiones/lugares seguros – certificados válidos**
- **Configuración**
  - Bloqueador de ventanas emergentes
  - Borrar datos de navegación
  - Borrar caché
  - Modo de navegación privado
  - Inicio de sesión/sincronización de datos de navegador
  - Bloqueadores de publicidad

3.0 Solución de problemas de software

3.1 Dado un escenario, solucionar problemas comunes del sistema operativo Microsoft Windows.

- **Síntomas comunes**
  - Pantalla Azul de la Muerte (BSOD)
  - Desempeño lento
  - Problemas de arranque
  - Apagados frecuentes
  - Servicios no se inician
  - Bloqueos de aplicación
  - Advertencias de baja memoria
  - Advertencias de recursos de controlador USB
  - Inestabilidad del sistema
  - No se encuentra sistema operativo
  - Carga lenta del perfil
  - Desfase de hora
- **Pasos comunes de solución de problemas**
  - Reiniciar
  - Reiniciar servicios
  - Desinstalar/reinstalar/actualizar aplicaciones
  - Agregar recursos
  - Verificar requerimientos
  - Comprobador de archivos del sistema
  - Reparar Windows
  - Restaurar
  - Reimagen
  - Revertir actualizaciones
  - Reconstruir perfiles de Windows

3.2 Dado un escenario, solucionar problemas comunes de seguridad de computadoras personales (PC).

- **Síntomas comunes**
  - No se puede acceder a la red
  - Alertas de escritorio
  - Alertas falsas sobre protección de antivirus
  - Sistema o archivos personales alterados
    - Archivos faltantes/ renombrados
  - Notificaciones no deseadas en el OS
  - Fallas en actualizaciones del sistema operativo
- **Síntomas relacionados con el navegador**
  - Ventanas emergentes aleatorias/ frecuentes
  - Advertencias de certificados
  - Redirección

3.3 Dado un escenario, usar los mejores procedimientos para eliminar malware.

1. **Investigar y verificar síntomas de malware**
2. **Poner en cuarentena sistemas infectados**
3. **Deshabilitar la Restauración de Sistema en Windows**
4. **Remediar sistemas infectados**
   a. Actualizar el software antimalware
   b. Técnicas de escaneo y eliminación (por ejemplo, modo seguro, entorno previo a la instalación)
5. **Programar escaneos y ejecutar actualizaciones**
6. **Habilitar Restauración de sistema y crear un punto de restauración en Windows**
7. **Educar al usuario final**

3.4 Dado un escenario, solucionar problemas comunes de aplicación y sistemas operativos móviles.

- **Síntomas comunes**
  - Aplicación no se inicia
  - Aplicación no se cierra/se bloquea
  - Aplicación no se actualiza
  - Respuesta lenta
  - Sistema operativo no se actualiza
  - Problemas con la vida de la batería
  - Reinicios aleatorios
  - Problemas de conectividad
    - Bluetooth
    - WiFi
    - Comunicación de campo cercano (NFC)
    - AirDrop
  - La pantalla no gira automáticamente

3.5 Dado un escenario, solucionar problemas comunes de seguridad de aplicación y sistemas operativos móviles.

- **Preocupaciones de seguridad**
  - Fuente de paquete Android (APK)
  - Modo de desarrollador
  - Acceso a root/jailbreak
  - Aplicación falsificada/maliciosa
    - Suplantación de aplicación
- **Síntomas comunes**
  - Alto tráfico en red
  - Tiempo de respuesta lento
  - Notificación de límite de uso de datos
  - Conectividad de internet limitada
  - Sin conectividad de internet
  - Alto número de publicidad
  - Falsas advertencias de seguridad
  - Comportamiento inesperado de aplicaciones
  - Archivos/datos personales filtrados

4.0 Procedimientos operativos

4.1 Dado un escenario, implementar las mejores prácticas asociadas con documentación y gestión de información de sistemas de apoyo.

- **Sistemas de tickets**
  - Información del usuario
  - Información de dispositivos
  - Descripción de problemas
  - Categorías
  - Gravedad
  - Niveles de escalamiento
  - Comunicación escrita clara y concisa
    - Descripción del problema
    - Notas de progreso
    - Resolución del problema
- **Administración de activos**
  - Listas de inventario
  - Sistema de bases de datos
  - Etiquetas e identificación de activos
  - Ciclo de vida de adquisiciones
  - Garantía y licencia
  - Usuarios asignados
- **Tipos de documentos**
  - Política de Uso Aceptable (AUP)
  - Diagramas de topología de red
  - Requerimientos de cumplimiento regulatorio.
    - Pantallas de presentación
  - Informes de incidentes
  - Procedimientos operacionales estándar
    - Procedimientos para instalación personalizada de paquetes de software
  - Lista de verificación para configuración de nuevos usuarios
  - Lista de verificación para finalización de usuario final
- **Base de conocimientos/artículos**

4.2 Explicar las mejores prácticas básicas de administración de cambios.

- **Procesos documentados de negocios**
  - Rollback plan
  - Pruebas en Sandbox
  - Miembro responsable del personal
- **Administración de cambios**
  - Formularios de solicitudes
  - Objetivo del cambio
  - Alcance del cambio
  - Hora y fecha del cambio
  - Sistemas afectados/impacto
  - Análisis de riesgo
    - Nivel de riesgo
  - Aprobaciones de la junta de cambio
  - Aceptación del usuario final

4.3 Dado un escenario, implementar métodos de copia de seguridad y recuperación en estaciones de trabajo.

- **Copia de seguridad y recuperación**
  - Completa
  - Incremental
  - Diferencial
  - Sintética
- **Prueba de copia de seguridad**
  - Frecuencia
- **Esquemas de rotación de copias de seguridad**
  - En el sitio vs. fuera del sitio
  - Grandfather-father-son (GFS)
  - Regla de copias de seguridad 3-2-1

4.4 Dado un escenario, usar los procedimientos de seguridad comunes.

- **Cintas de descarga electrostática (ESD)**
- **Tapetes antiestáticos**
- **Puesta a tierra del equipo**
- **Manejo correcto de energía**
- **Manejo y almacenamiento apropiado de los componentes**
- **Bolsas antiestáticas**
- **Cumplimiento de regulaciones gubernamentales**
- **Seguridad personal**
  - Desconectar fuente de energía antes de reparar la computadora personal
  - Técnicas de elevación
  - Seguridad contra incendios eléctricos
  - Gafas de seguridad
  - Máscara para filtro de aire

4.5 Resumir los impactos ambientales y controles ambientales locales.

- **Hoja de datos de seguridad de materiales (MSDS)/ Documentación para manejo y eliminación**
  - Eliminación adecuada de baterías
  - Eliminación adecuada de tóner
  - Eliminación adecuada de otros dispositivos y activos
- **Conocimiento de nivel de temperatura y humedad y ventilación adecuada**
  - Lugar/ubicación de equipos
  - Limpieza de polvo
  - Aire comprimido/vacío
- **Sobrevoltaje de fuente de energía, eventos de bajas de voltaje y fallas de alimentación**
  - Respaldo de batería
  - Supresor de sobrevoltaje

4.6 Explicar la importancia del contenido/actividad prohibida y los conceptos de privacidad, licencia y políticas.

- **Respuesta a incidentes**
  - Cadena de custodia
  - Informar a gerencia/instituciones de cumplimiento de la ley, según sea necesario
  - Copia de unidad (integridad y preservación de datos)
  - Documentación de incidentes
- **Gestión de licencias/derechos digitales (DRM)/acuerdo de licencia del usuario final (EULA)**
  - Licencias válidas
  - Licencias no vencidas
  - Licencia de uso personal vs. licencia de uso corporativo
  - Licencia de código abierto
- **Datos regulados**
  - Transacciones con tarjetas de crédito
  - Información personal generada por el gobierno
  - PII
  - Datos de cuidado de salud
  - Requerimientos de retención de datos

4.7 Dado un escenario, usar técnicas de comunicación adecuadas y profesionalismo.

- **Apariencia y vestuario profesional**
  - Coincidir la vestimenta requerida del entorno dado
    - Formal
    - De negocios casual
- **Usar lenguaje adecuado y evitar la jerga, siglas, cuando sea aplicable**
- **Mantener una actitud positiva/ confianza en el proyecto**
- **Escuchar atentamente (tomar notas) y evitar interrumpir al cliente**
- **Ser culturalmente sensible**
  - Usar títulos profesionales apropiados, cuando aplique
- **Llegar a tiempo (si se retrasa, contactar al cliente)**
- **Evitar distracciones**
  - Llamadas personales
  - Sitios de medios sociales/ mensajes de texto
  - Interrupciones personales
- **Lidiar con un cliente o situación difícil**
  - No discutir con el cliente y/o ponerse a la defensiva
  - Evitar descartar los problemas del cliente
  - Evitar formular juicios
  - Aclarar las declaraciones del cliente (realizar preguntas abiertas para reducir el alcance del problema, repetir el problema o preguntar para verificar que haya entendido)
  - No divulgar las experiencias a través de medios de redes sociales
- **Establecer y cumplir expectativas/ cronograma y comunicar el estado al cliente**
  - Ofrecer opciones de reparación/ reemplazo, según sea necesario
  - Proporcionar documentación apropiada sobre los servicios ofrecidos
  - Dar seguimiento con el cliente / usuario en una fecha posterior para verificar la satisfacción
- **Tratar apropiadamente materiales confidenciales y privados de los clientes**
  - Ubicados en una computadora, escritorio, impresora, etc.

4.8 Identificar los fundamentos de las secuencias de comandos.

- **Tipos de archivo de secuencias de comandos**
  - .bat
  - .ps1
  - .vbs
  - .sh
  - .js
  - .py
- **Usar casos para scripting**
  - Automatización básica
  - Reiniciar máquinas
  - Reasignar unidades de red
  - Instalación de aplicaciones
  - Copias de seguridad automáticas
  - Recopilación de información/ datos
  - Inicio de actualizaciones
- **Otras consideraciones cuando se usan scripts**
  - Introducción casual de malware
  - Cambio casual de configuración del sistema
  - Bloqueos de navegador o el sistema por mal manejo de recursos

4.9 Dado un escenario, usar tecnologías de acceso remoto.

- **Métodos/herramientas**
  - RDP
  - VPN
  - Computadora de red virtual (VNC)
  - Shell seguro (SSH)
  - Monitoreo y gestión remota (RMM)
  - Asistencia remota de Microsoft (MSRA)
  - Herramientas de terceros
    - Software para compartir pantallas
    - Software para videoconferencias
    - Software para transferencia de archivos
    - Software de gestión de escritorio
- **Consideraciones de seguridad de cada método de acceso**

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

La siguiente es una lista de acrónimos que aparecen en el examen CompTIA A+ Core 2 (220-1102). Se insta a los candidatos a revisar la lista completa y alcanzar un conocimiento práctico de todas las siglas listadas, como parte de un programa completo de preparación para el examen.

Acrónimo	Definición
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

Acrónimo	Definición
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

Acrónimo	Definición
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

Acrónimo	Definición
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

Acrónimo	Definición
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

Lista de software y hardware propuesta para CompTIA A+ Core 2 (220-1102)

**CompTIA ha incluido esta lista de muestra de hardware y software para ayudar a los candidatos a preparar el examen A+ Core 1 (220-1101). Esta lista también puede ser útil para las empresas de capacitación que desean crear un componente de laboratorio en su oferta de capacitación. Las listas con viñetas debajo de cada tema son listas de muestra y no están completas.

Equipos

- Tableta/teléfono inteligente Apple
- Tableta/teléfono inteligente Android
- Tableta Windows
- Chromebook
- Computadora portátil Windows / Computadora portátil Mac / Computadora portátil Linux
- Computadora de escritorio Windows / Computadora de escritorio Mac / Computadora de escritorio Linux
- Servidor Windows con Directorio Activo y Administración de Impresión
- Monitores
- Proyectores
- Router/switch SOHO
- Punto de acceso
- Teléfono de voz sobre protocolo de Internet (VoIP)
- Impresora
  - Láser/inyección de tinta
  - Redes inalámbricas
  - Impresora 3-D
  - Térmica
- Supresor de sobrevoltaje
- Fuente de alimentación ininterrumpida (UPS)
- Dispositivos inteligentes (Internet de las cosas (IoT))
- Servidor con hipervisor
- Bloque de conexiones
- Patch panel
- Cámaras web
- Altavoces
- Micrófonos

Hardware/repuestos

- Tarjetas madre
- RAM
- Discos duros
- Fuentes de energía
- Tarjetas de video
- Tarjetas de sonido
- Tarjetas de red
- Tarjetas de Interfaz de Red inalámbrica (NIC)
- Ventiladores/dispositivos de enfriamiento/disipador de calor
- CPU
- Conectores/cables variados
  - USB
  - Interfaz de multimedia de alta definición (HDMI)
  - DisplayPort
  - Interfaz Digital Visual (DVI)
  - Matriz de Gráficos de Vídeo (VGA)
- Adaptadores
  - Adaptador Bluetooth
- Cables de red
- Cables de red/conectores sin terminar
- Adaptadores de corriente alterna (CA)
- Unidades ópticas
- Tornillos/separadores
- Gabinetes
- Kit de mantenimiento
- Mouse/teclados
- Teclado-video-mouse (KVM)
- Cable de consola
- Unidad de estado sólido (SSD)

Herramientas

- Destornillador
- Multímetro
- Cortadores de cable
- Herramienta ponchadora de cable
- Pinza de compresión para cable
- Probador de fuente de energía
- Pelador de cable
- Caja de herramientas estándar para técnicos
- Cinta de descarga electrostática (ESD)
- Pasta térmica
- Tester de cable
- Tóner de cable
- Analizador Wi-Fi
- Conectores de Tecnología Avanzada Serial (SATA) a USB

Software

- OS
  - Linux
  - Chrome OS
  - Microsoft Windows
  - macOS
  - Android
  - iOS
- Disco/disco compacto (CD) de entorno previo a la instalación (PE)
- Software antivirus
- Software de virtualización
- Anti-malware
- Software de controladores

CompTIA