



Examen de certificación CompTIA A+: Objetivos de Core 2

NÚMERO DE EXAMEN: CORE 2 (220-1002)



Acercas del examen

Se motiva a los candidatos a usar este documento para ayudarlos a prepararse para el Core 2 de CompTIA A+. Para recibir la certificación CompTIA A+, debe aprobar dos exámenes: Core 1 (220-1101) y Core 2 (220-1102). Core 2 CompTIA A+ mide las habilidades necesarias para un profesional de TI de nivel de entrada. Los candidatos exitosos tendrán el conocimiento requerido para:

- Reunir componentes basado en los requerimientos del cliente
- Instalar, configurar y mantener las PC, dispositivos móviles y software para usuarios finales
- Comprender los aspectos básicos de sistemas de redes y seguridad de análisis forense
- Diagnosticar, resolver y documentar, en forma adecuada y segura, problemas comunes de hardware y software
- Aplicar habilidades de resolución de problemas
- Proporcionar soporte adecuado al cliente
- Comprender los aspectos básicos de secuencias de comandos, imagen de computador e implementación

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

CompTIA A+ 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 de conformidad con el Acuerdo para Candidatos de CompTIA. En un esfuerzo por comunicar más claramente 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 acaten el [Acuerdo de Candidato CompTIA](#). Si un candidato tiene una pregunta acerca de si materiales de estudio se consideran no autorizados (también conocidos como “brain dumps”), él/ella debería contactar a CompTIA al examsecurity@comptia.org para confirmar.

POR FAVOR RECUERDE

Las listas de ejemplos proporcionada 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 de prueba. Sepa que todos los materiales relacionados de preparación para el examen serán válidos.

DETALLES DE LA PRUEBA

Examen requerido	Core 2
Número de preguntas	Máximo de 90
Tipos de preguntas	Opción múltiple y basada en desempeño
Duración de la prueba	90 minutos
Experiencia recomendada	12 meses de experiencia como un especialista de apoyo de TI
Calificación para aprobar	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	27%
2.0 Seguridad	24%
3.0 Solución de problemas de software	26%
4.0 Procedimientos operativos	23%
Total	100%



1.0 Sistemas operativos

1.1 Comparar y contrastar tipos comunes de sistemas operativos y sus objetivos.

- **32 bits vs. 64 bits**
 - Limitaciones de RAM
 - Compatibilidad de software
- **Sistemas operativos de estación de trabajo**
 - Microsoft Windows
 - Apple Macintosh OS
 - Linux
- **Sistemas operativos de teléfonos celulares/tabletas**
 - Microsoft Windows
 - Android
 - iOS
 - Chrome OS
- **Limitaciones específicas de los proveedores**
 - Final de la vida
 - Limitaciones de actualización
- **Preocupaciones de compatibilidad entre sistemas operativos**

1.2 Comparar y contrastar características de las versiones de Microsoft Windows.

- **Windows 7**
- **Windows 8**
- **Windows 8.1**
- **Windows 10**
- **Necesidades corporativas vs. personales**
 - Acceso a dominio
 - BitLocker
 - Centro de medios
- BranchCache
- EFS
- **Estilos de escritorio/interfaz del usuario**

1.3 Resumir consideraciones y métodos de actualización generales de sistemas operativos.

- **Métodos de arranque**
 - Disco óptico (CD-ROM, DVD, Blu-ray)
 - Unidad flash/unidad externa (USB/eSATA)
 - Arranque de red (PXE)
 - Disco fijo interno (HDD/SSD)
 - Unidad de disco duro interno (partición)
- **Tipo de instalaciones**
 - Instalación desatendida
 - Actualización incluida
 - Instalación limpia
 - Instalación de reparación
 - Arranque múltiple
 - Instalación de red remota
 - Despliegue de imagen
 - Partición de recuperación
 - Recargar/restaurar
- **Partición**
 - Dinámica
 - Básica
 - Primaria
 - Extendida
 - Lógica
 - GPT
- **Tipos de sistemas de archivos/formateo**
 - ExFAT
 - FAT32
 - NTFS
 - CDFS
 - NFS
 - ext3, ext4
 - HFS
 - Partición de intercambio
 - Formateo rápido vs. formateo completo
- **Cargar controladores alternativos de terceros cuando sea necesario**
- **Grupo de trabajo vs. Configuración de dominio**
- **Configuraciones de hora/ fecha/región/idioma**
- **Instalación de controlador, software y actualizaciones de Windows**
- **Partición de recuperación de fábrica**
- **Unidad de disco de arranque formateada apropiadamente con las particiones/formato correcto**
- **Requisitos previos/ compatibilidad de hardware**
- **Compatibilidad de aplicaciones**
- **Compatibilidad de sistema operativo/ruta de actualización**

1.4 Dado un escenario, aplique las herramientas de línea de comando apropiadas de Microsoft.

- Navegación
 - dir
 - cd
 - ..
- ipconfig
- ping
- tracert
- netstat
- nslookup
- shutdown
- dism
- sfc
- chkdsk
- diskpart
- taskkill
- gpupdate
- gpreresult
- format
- copy
- xcopy
- robocopy
- net use
- net user
- [nombre del comando]/?
- Comandos disponibles con privilegios estándar vs. privilegios administrativos

1.5 Dado un escenario, use las características y herramientas apropiadas de los sistemas operativos de Microsoft.

- Administrativas
 - Administración de equipos
 - Administrador de dispositivos
 - Usuarios y Grupos locales
 - Política de seguridad local
 - Monitor de desempeño
 - Servicios
 - Configuración del sistema
 - Programador de tareas
 - Servicios de componentes
 - Fuentes de datos
 - Administración de impresión
 - Diagnóstico de memoria de Windows
 - Cortafuegos (Firewall) de Windows
 - Seguridad avanzada
 - Visor de eventos
 - Administración de cuentas de usuario
- MSConfig
 - General
 - Arranque
 - Servicios
 - Inicio
 - Herramientas
- Administrador de tareas
 - Aplicaciones
 - Procesos
 - Desempeño
 - Red
 - Usuarios
- Administración de disco
 - Estado de la unidad
 - Montaje
 - Inicio
 - Ampliación de particiones
 - División de particiones
- Reducción de particiones
- Asignar/cambiar letras de unidades de disco
- Agregar unidades de disco
- Agregar matrices
- Espacios de almacenamiento
- Utilidades del sistema
 - Regedit
 - Command
 - Services.msc
 - MMC
 - MSTSC
 - Bloc de notas
 - Explorer
 - Msinfo32
 - DxDiag
 - Desfragmentador de disco
 - Restauración del sistema
 - Actualización de Windows

1.6 Dado un escenario, use las utilidades del Panel de control de Microsoft Windows.

- Opciones de Internet
 - Conexiones
 - Seguridad
 - General
 - Privacidad
 - Programas
 - Avanzada
- Pantalla/Configuración de pantalla
 - Resolución
 - Profundidad de color
 - Frecuencia de actualización
- Cuentas de usuario
 - Dormir/suspender
 - Modo de espera
- Opciones de carpeta
 - Ver archivos ocultos
 - Ocultar extensiones
 - Opciones generales
 - Ver opciones
- Sistema
 - Desempeño (memoria virtual)
 - Configuraciones remotas
 - Protección del sistema
- Cortafuegos (Firewall) de Windows
- Opciones de energía
 - Hibernar
 - Planes de energía
- Administrador de credenciales
- Programas y características
- Grupo Hogar
- Dispositivos e Impresoras
- Sonido
- Solución de problemas
- Red y Centro para compartir
- Administrador de dispositivos
- BitLocker
- Sync Center

1.7 Resumir conceptos de instalación y configuración de aplicaciones.

- **Requerimientos del sistema**
 - Espacio de la unidad
 - RAM
- **Requerimientos del sistema operativo**
 - Compatibilidad
- **Métodos de instalación e implementación**
 - Local (CD/USB)
 - Basado en red
- **Permisos del usuario local**
 - Acceso a carpetas/archivos para instalación
- **Consideraciones de seguridad**
 - Impacto en dispositivo
 - Impacto en la red

1.8 Dado un escenario, configure la red de Windows en una computadora de escritorio de un cliente.

- **Grupo Hogar vs. grupo de trabajo**
- **Configuración de dominio**
- **Recurso compartido de red/ recurso compartido administrativo/ unidades de asignación**
- **Compartir impresora vs. asignación de impresora en red**
- **Establecer conexiones de red**
 - VPN
 - Telefónicas
 - Inalámbricas
 - Cableadas
 - WWAN (Celular)
- **Configuración de proxy**
- **Conexión de Escritorio Remoto**
- **Asistencia remota**
- **Configuraciones de redes de hogar vs. trabajo vs. públicas**
- **Configuración de cortafuegos (firewall)**
 - Excepciones
 - Configuración
 - Habilitar/deshabilitar Cortafuegos (Firewall) de Windows
- **Configurar una dirección IP alternativa en Windows**
 - Asignación de IP
- Máscara de subred
- DNS
- Puerta de enlace
- **Propiedades de tarjeta de red**
 - Medio dúplex/dúplex completo/automático
 - Velocidad
 - Wake-on-LAN
 - QoS
 - BIOS (NIC incorporada)

1.9 Dado un escenario, use características y herramientas del sistema operativo Mac y sistemas operativos de cliente/escritorio Linux.

- **Mejores prácticas**
 - Copias de seguridad programadas
 - Mantenimiento del disco programado
 - Actualizaciones del sistema/App Store
 - Gestión de parches
 - Actualización de controladores/ firmware
 - Actualizaciones de antivirus/ anti-malware
- **Herramientas**
 - Copia de seguridad/Máquina de tiempo
 - Restauración/copia instantánea
 - Despliegue de imagen
 - Utilidades de mantenimiento de disco
 - Shell/Terminal
 - Compartir pantalla
 - Salida forzada
- **Características**
 - Escritorio múltiples/Control de Misión
 - Key Chain
 - Spot Light
 - iCloud
 - Gestures
 - Finder
 - Disco remoto
 - Dock
 - Boot Camp
- **Comandos básicos de Linux**
 - ls
 - grep
 - cd
 - shutdown
 - pwd vs. passwd
 - mv
- cp
- rm
- chmod
- chown
- iwconfig/ifconfig
- ps
- su/sudo
- apt-get
- vi
- dd
- kill



2.0 Seguridad

2.1 Resumir la importancia de las medidas físicas de seguridad.

- Doble puerta de seguridad
- Lectores de gafetes
- Tarjeta inteligente
- Guardia de seguridad
- Bloqueo de puertas
- Bloqueos biométricos
- Token de hardware
- Candados de cable
- Bloqueos de servidor
- Candados USB
- Pantalla de privacidad
- Key fobs
- Lista de control de ingreso

2.2 Explicar los conceptos de seguridad lógica.

- Directorio activo
 - Comandos de inicio de sesión
 - Dominio
 - Política de grupo/Actualizaciones
 - Unidades de la organización
 - Carpeta particular
 - Redirección de carpeta
- Token de software
- Políticas MDM
- Seguridad de puertos
- Filtrado de dirección MAC
- Certificados
- Antivirus/Anti-malware
- Cortafuegos (Firewalls)
- Autenticación de usuario/contraseñas seguras
- Autenticación de multifactores
- Permisos de directorio
- VPN
- DLP
- Listas de control de acceso
- Tarjeta inteligente
- Filtro de correo electrónico
- Fuentes de software de confianza/no confiables
- Principio de menor privilegio

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

- Protocolos y cifrado
 - WEP
 - WPA
 - WPA2
 - TKIP
 - AES
- Autenticación
 - Factor único
 - Multifactor
 - RADIUS
 - TACACS

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

- Malware
 - Ransomware
 - Troyanos
 - Registrador de pulsaciones de teclas
 - Rootkit
 - Virus
- Botnet
- Gusano
- Spyware
- Herramientas y métodos
 - Antivirus
 - Anti-malware
- Consola de recuperación
- Realizar copia de seguridad/restaurar
- Educación del usuario final
- Cortafuegos de software
- Configuración DNS

2.5 Comparar y contrastar ingeniería social, amenazas y vulnerabilidades.

- **Ingeniería social**
 - Phishing
 - Spear phishing
 - Suplantación
 - Fisgoneo
 - Infiltración
 - Buscar en la basura
- **DDoS**
- **DoS**
- **Día cero**
- **Hombre en el medio**
- **Fuerza bruta**
- **Diccionario**
- **Tabla Rainbow**
- **Spoofing**
- **Sistemas que no cumplen con los estándares**
- **Zombie**

2.6 Comparar y contrastar las diferencias de la configuración básica de seguridad del sistema operativo Microsoft Windows.

- **Usuario y grupos**
 - Administrador
 - Usuario avanzado
 - Invitado
 - Usuario estándar
- **Permiso NTFS vs. de recursos compartidos**
 - Permitir vs. denegar
 - Mover vs. copiar carpetas y archivos
 - Atributos de archivos
- **Archivos y carpetas compartidos**
 - Recursos compartidos administrativos v. locales
 - Propagación de permisos
 - Herencia
- **Archivos y carpetas del sistema**
- **Autenticación de usuario**
 - Inicio único de sesión
- **Ejecutar como administrador vs. como usuario estándar**
- **BitLocker**
- **BitLocker To Go**
- **EFS**

2.7 Dado un escenario, implementar mejores prácticas de seguridad para asegurar una estación de trabajo.

- **Mejores prácticas de contraseñas**
 - Configurar contraseñas seguras
 - Vencimiento de contraseñas
 - Contraseña requerida por el protector de pantalla
 - Contraseñas de BIOS/UEFI
 - Solicitar contraseñas
- **Administración de cuentas**
 - Restringir los permisos del usuario
 - Configurar restricciones de horario 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
 - Funciones básicas de Directorio activo
 - Creación de cuentas
 - Eliminación de cuentas
 - Restablecimiento de contraseña/desbloquear cuenta
 - Deshabilitar cuenta
- **Deshabilitar autorun**
- **Cifrado de datos**
- **Gestión de parches/actualizaciones**



2.8 Dado un escenario, implementar métodos para asegurar dispositivos móviles.

- **Bloqueos de pantallas**
 - Bloqueo con huella digital
 - Bloqueo con rostro
 - Bloqueo con deslizamiento
 - Bloqueo con código de contraseña
- **Limpiezas remotas**
- **Aplicaciones de ubicación**
- **Aplicaciones de copia de seguridad remota**
- **Restricciones de intentos de inicio de sesión fallidos**
- **Antivirus/Anti-malware**
- **Gestión de parches/Sistema Operativo**
- **Autenticación biométrica**
- **Cifrado de dispositivo completo**
- **Autenticación de multifactores**
- **Aplicaciones de autenticador**
- **Fuentes de confianza vs. fuentes no confiables**
- **Cortafuegos (Firewalls)**
- **Políticas y procedimientos**
 - BYOD vs. propiedad corporativa
 - Requisitos de perfil de seguridad

2.9 Dado un escenario, implementar métodos apropiados de destrucción y eliminación de datos.

- **Destrucción física**
 - Trituradora
 - Taladro/martillo
 - Electromagnético (desmagnetizar)
 - Incineración
 - Certificado de destrucción
- **Mejores prácticas de reciclaje o readaptación**
 - Formateo de bajo nivel vs. formateo estándar
 - Sobrescribir
 - Borrado de la unidad

2.10 Dado un escenario, configurar seguridad en redes cableadas e inalámbricas SOHO.

- **Específico de red inalámbrica**
 - Cambiar SSID predeterminado
 - Configurar cifrado
 - Deshabilitar transmisión SSID
 - Colocación de antena y punto de acceso
 - Niveles de potencia de radio
 - WPS
- **Cambiar nombres de usuario y contraseñas predeterminados**
- **Habilitar filtrado MAC**
- **Asignar direcciones IP estáticas**
- **Configuración de cortafuegos (firewall)**
- **Reenviar/visualizar puerto**
- **Deshabilitar puertos**
- **Filtrado de contenido/controles parentales**
- **Actualizar firmware**
- **Seguridad física**



3.0 Solución de problemas de software

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

• Síntomas comunes

- Desempeño lento
- Conectividad limitada
- Falla para arrancar
- No se encuentra sistema operativo
- Bloqueos de aplicación
- Pantallas azules
- Pantallas negras
- Problemas de impresión
- Servicios no se pudieron iniciar

- Arranque lento

- Carga lenta del perfil

• Soluciones comunes

- Desfragmentar el disco duro
- Reiniciar
- Terminar tareas
- Reiniciar servicios
- Actualizar configuración de red
- Restablecer imagen/volver a cargar el sistema operativo

- Revertir actualizaciones

- Revertir controladores de dispositivos

- Aplicar actualizaciones

- Reparar aplicación

- Actualizar orden de arranque

- Desactivar servicios/
aplicaciones de Windows

- Desactivar inicio de aplicación

- Arranque seguro

- Reconstruir perfiles de Windows

3.2 Dado un escenario, detectar y resolver problemas comunes de seguridad de PC

• Síntomas comunes

- Elementos emergentes
- Redirección de navegador
- Alertas de seguridad
- Desempeño lento
- Problemas de conectividad a Internet
- Bloqueo de PC/sistema operativo
- Bloqueos de aplicación

- Fallas en actualizaciones
del sistema operativo

- Antivirus malintencionado

- Spam

- Archivos de sistema con
cambio de nombre

- Archivos que desaparecen

- Cambios en permisos de archivo

- Correo electrónico intervenido

- Respuestas de usuarios con
respecto al correo electrónico

- Respuestas automatizada
de correo electrónico por un
remitente desconocido

- Acceso denegado

- Certificado inválido
(CA raíz de confianza)

- Errores de registro de
sistema/aplicación

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

1. Identificar e investigar
síntomas de malware.

2. Poner en cuarentena los
sistemas infectados.

3. Deshabilitar la Restauración
de Sistema (en Windows).

4. Corregir los sistemas infectados.

a. Actualizar el software anti-malware.

b. Escanear y utilizar técnicas
de eliminación (modo seguro,
ambiente de preinstalación).

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, resolver problemas de aplicación y sistemas operativos móviles.

• Síntomas comunes

- Pantalla débil
- Señal inalámbrica intermitente
- Sin conectividad inalámbrica
- Sin conectividad de Bluetooth
- No puede transmitir a monitor externo
- Pantalla táctil no responde
- Aplicaciones no cargan
- Desempeño lento
- No puede descifrar correo electrónico
- Vida de batería extremadamente breve
- Calentamiento excesivo
- Sistema se congela
- No hay sonido de los altavoces
- Respuesta imprecisa de pantalla táctil
- Bloqueo del sistema
- Errores de registro de aplicaciones

3.5 Dado un escenario, resolver problemas de seguridad de aplicaciones y sistema operativo móviles.

• Síntomas comunes

- Caída de la señal/señal débil
- Consumo de energía
- Velocidades de datos lentas
- Conexión no intencionada de WiFi
- Enlace no intencionado de Bluetooth
- Archivos/datos personales filtrados
- Transmisión de datos sobre el límite
- Acceso de cuenta no autorizado
- Rastreo de ubicación no autorizado
- Activación de cámara/micrófono no autorizada
- Alta utilización de recursos



4.0 Procedimientos operativos

4.1 Comparar y contrastar mejores prácticas asociadas con tipos de documentación.

- Diagramas de topología de red
- Knowledge base/artículos
- Documentación de incidentes
- Política regulatoria y de cumplimiento
- Política de uso aceptable
- Política de contraseña
- Administración de inventario
 - Etiquetas de activos
 - Códigos de barra

4.2 Dado un escenario, implementar mejores prácticas de administración de cambios básicos

- Procesos documentados de negocios
- Objetivo del cambio
- Alcance del cambio
- Análisis de riesgo
- Planificación para el cambio
- Aceptación del usuario final
- Junta de cambio
 - Aprobaciones
- Plan de retroceso
- Cambios en documentos

4.3 Dado un escenario, implementar métodos básicos de prevención y recuperación de desastres.

- Copia de seguridad y recuperación
 - Nivel de imagen
 - Nivel de archivo
 - Aplicaciones esenciales
- Prueba de copia de seguridad
- UPS
- Protector de sobrevoltaje
- Copias de seguridad con almacenamiento en nube vs. almacenamiento local
- Opciones de recuperación de cuenta

4.4 Explicar procedimientos comunes de seguridad.

- Puesta a tierra del equipo
- Manejo y almacenamiento apropiado de los componentes
 - Bolsas antiestáticas
 - Correas antiestáticas
 - Tapetes antiestáticos
 - Autoconexión a tierra
- Manejo de desechos tóxicos
 - Baterías
 - Tóner
 - CRT
 - Teléfonos celulares
 - Tabletillas
- Seguridad personal
 - Desconectar fuente de energía antes de reparar la computadora personal
 - Remover las piezas de joyería
 - Técnicas de elevación
 - Limitaciones de peso
 - Seguridad contra incendios eléctricos
 - Manejo de cables
 - Gafas de seguridad
 - Máscara para filtro de aire
- Cumplimiento de regulaciones gubernamentales



4.5 Explicar impactos ambientales y controles apropiados.

- Documentación de MSDS para manejo y desecho
- Conocimiento de nivel de temperatura y humedad y ventilación adecuada
- Sobrevoltaje de fuente de energía, apagones parciales, apagones
 - Respaldo de batería
 - Supresor de sobrevoltaje
- Protección de partículas en el aire
 - Gabinetes
 - Máscara/filtro de aire
- Polvo y desechos
 - Aire comprimido
 - Vacío
- Cumplimiento de regulaciones gubernamentales

4.6 Explicar los procesos de abordar contenido/actividad prohibida, y los conceptos de privacidad, licencia y políticas.

- Respuesta a incidentes
 - Primera respuesta
 - Identificar
 - Reportar a través de los canales apropiados
 - Preservación de datos/dispositivo
 - Uso de documentación/cambios en documentación
 - Cadena de custodia
- Rastreo de evidencia/documentación de procesos
- Otorgamiento de licencia/DRM/EULA
 - Licencia de código abierto vs. comercial
 - Licencia personal vs. licencias empresariales
- Datos regulados
 - PII
 - PCI
- GDPR
- PHI
- Seguir todas las políticas y mejores prácticas de seguridad

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

- 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/texto
- Hablar con compañeros de trabajo mientras interactúa con clientes
- 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 diferentes opciones de reparación/reemplazo, si corresponde
 - Proporcionar documentación apropiada sobre los servicios ofrecidos
 - Dar seguimiento con el cliente/usuario en una fecha posterior para verificar la satisfacción
- Tratar apropiadamente con 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
- .py
- .js

- **Variables de entorno**

- **Sintaxis de comentario**

- **Construcción de secuencias de comandos básicos**

- Bucles básicos
- Variables

- **Tipos de datos básicos**

- Enteros
 - Cadenas
-

4.9 Dado un escenario, usar tecnologías de acceso remoto.

- **RDP**

- **Telnet**

- **SSH**

- **Herramientas de terceros**

- Función de compartir pantalla
- Recurso compartido de archivo

- **Consideraciones de seguridad de cada método de acceso**

Siglas de CompTIA A+

A continuación, hay una lista de siglas que aparecen en los exámenes de CompTIA A+. 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.

SIGLAS	EXPLICACIÓN	SIGLAS	EXPLICACIÓN
AC	Alternating Current	CGA	Computer Graphics and Applications
ACL	Access Control List	CIDR	Classless Inter-Domain Routing
ACPI	Advanced Configuration Power Interface	CIFS	Common Internet File System
ADF	Automatic Document Feeder	CMOS	Complementary Metal-Oxide Semiconductor
ADSL	Asymmetrical Digital Subscriber Line	CNR	Communications and Networking Riser
AES	Advanced Encryption Standard	COMx	Communication port (x=port number)
AHCI	Advanced Host Controller Interface	CPU	Central Processing Unit
AP	Access Point	CRT	Cathode-Ray Tube
APIPA	Automatic Private Internet Protocol Addressing	DaaS	Data as a Service
APM	Advanced Power Management	DAC	Discretionary Access Control
ARP	Address Resolution Protocol	DB-25	Serial Communications D-Shell Connector, 25 pins
ASR	Automated System Recovery	DB-9	Serial Communications D-Shell Connector, 9 pins
ATA	Advanced Technology Attachment	DBaaS	Database as a Service
ATAPI	Advanced Technology Attachment Packet Interface	DC	Direct Current
ATM	Asynchronous Transfer Mode	DDoS	Distributed Denial of Service
ATX	Advanced Technology Extended	DDR	Double Data Rate
AUP	Acceptable Use Policy	DDR RAM	Double Data Rate Random Access Memory
A/V	Audio Video	DFS	Distributed File System
BD-R	Blu-ray Disc Recordable	DHCP	Dynamic Host Configuration Protocol
BIOS	Basic Input/Output System	DIMM	Dual Inline Memory Module
BD-RE	Blu-ray Disc Rewritable	DIN	Deutsche Industrie Norm
BNC	Bayonet-Neill-Concelman	DLT	Digital Linear Tape
BSOD	Blue Screen of Death	DLP	Digital Light Processing or Data Loss Prevention
BYOD	Bring Your Own Device	DMA	Direct Memory Access
CAD	Computer-Aided Design	DMZ	Demilitarized Zone
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart	DNS	Domain Name Service or Domain Name Server
CD	Compact Disc	DoS	Denial of Service
CD-ROM	Compact Disc-Read-Only Memory	DRAM	Dynamic Random Access Memory
CD-RW	Compact Disc-Rewritable	DRM	Digital Rights Management
CDFS	Compact Disc File System	DSL	Digital Subscriber Line
CERT	Computer Emergency Response Team	DVD	Digital Versatile Disc
CFS	Central File System, Common File System, or Command File System	DVD-RAM	Digital Versatile Disc-Random Access Memory
		DVD-ROM	Digital Versatile Disc-Read Only Memory
		DVD-R	Digital Versatile Disc-Recordable
		DVD-RW	Digital Versatile Disc-Rewritable

SIGLAS	EXPLICACIÓN	SIGLAS	EXPLICACIÓN
DVI	Digital Visual Interface	HTTP	Hypertext Transfer Protocol
DVI-D	Digital Visual Interface-Digital	HTTPS	Hypertext Transfer Protocol Secure
ECC	Error Correcting Code	I/O	Input/Output
ECP	Extended Capabilities Port	IaaS	Infrastructure as a Service
EEPROM	Electrically Erasable Programmable Read-Only Memory	ICMP	Internet Control Message Protocol
EFS	Encrypting File System	ICR	Intelligent Character Recognition
EIDE	Enhanced Integrated Drive Electronics	IDE	Integrated Drive Electronics
EMI	Electromagnetic Interference	IDS	Intrusion Detection System
EMP	Electromagnetic Pulse	IEEE	Institute of Electrical and Electronics Engineers
EPROM	Erasable Programmable Read-Only Memory	IIS	Internet Information Services
EPP	Enhanced Parallel Port	IMAP	Internet Mail Access Protocol
ERD	Emergency Repair Disk	IMEI	International Mobile Equipment Identity
eSATA	External Serial Advanced Technology Attachment	IMSI	International Mobile Subscriber Identity
ESD	Electrostatic Discharge	IP	Internet Protocol
EULA	End User License Agreement	IPConfig	Internet Protocol Configuration
EVGA	Extended Video Graphics Adapter/Array	IPP	Internet Printing Protocol
Ext2	Second Extended File System	IPS	Intrusion Prevention System
exFAT	Extended File Allocation Table	IPSec	Internet Protocol Security
FAT	File Allocation Table	IR	Infrared
FAT12	12-bit File Allocation Table	IrDA	Infrared Data Association
FAT16	16-bit File Allocation Table	IRP	Incident Response Plan
FAT32	32-bit File Allocation Table	IRQ	Interrupt Request
FDD	Floppy Disk Drive	ISA	Industry Standard Architecture
FPM	Fast Page Mode	ISDN	Integrated Services Digital Network
FSB	Front-Side Bus	ISO	International Organization for Standardization
FTP	File Transfer Protocol	ISP	Internet Service Provider
FQDN	Fully Qualified Domain Name	JBOD	Just a Bunch of Disks
GDDR	Graphics Double Data Rate	KB	Knowledge Base
GDI	Graphics Device Interface	KVM	Kernel-based Virtual Machine
GUI	Graphical User Interface	KVM	Keyboard-Video-Mouse
GUID	Globally Unique Identifier	LAN	Local Area Network
GPS	Global Positioning System	LBA	Logical Block Addressing
GPT	GUID Partition Table	LC	Lucent Connector
GPU	Graphics Processing Unit	LCD	Liquid Crystal Display
GSM	Global System for Mobile Communications	LDAP	Lightweight Directory Access Protocol
HAL	Hardware Abstraction Layer	LED	Light Emitting Diode
HAV	Hardware Assisted Virtualization	LPD/LPR	Line Printer Daemon/Line Printer Remote
HCL	Hardware Compatibility List	LPT	Line Printer Terminal
HDCP	High-Bandwidth Digital Content Protection	LVD	Low Voltage Differential
HDD	Hard Disk Drive	MAC	Media Access Control/Mandatory Access Control
HDMI	High Definition Media Interface	MAN	Metropolitan Area Network
HIPS	Host Intrusion Prevention System	MAPI	Messaging Application Programming Interface
HPFS	High Performance File System	mATX	Micro Advanced Technology Extended
HTML	Hypertext Markup Language	MAU	Media Access Unit/Media Attachment Unit
HTPC	Home Theater PC	MBR	Master Boot Record
		MBSA	Microsoft Baseline Security Analyzer

SIGLAS	EXPLICACIÓN	SIGLAS	EXPLICACIÓN
MDM	Mobile Device Management	PCIe	Peripheral Component Interconnect Express
MFA	Multifactor Authentication	PCIX	Peripheral Component Interconnect Extended
MFD	Multifunction Device	PCL	Printer Control Language
MFP	Multifunction Product	PCMCIA	Personal Computer Memory Card International Association
MicroDIMM	Micro Dual Inline Memory Module	PE	Preinstallation Environment
MIDI	Musical Instrument Digital Interface	PGA	Pin Grid Array
MIME	Multipurpose Internet Mail Extension	PGA2	Pin Grid Array 2
MIMO	Multiple Input Multiple Output	PGP	Pretty Good Protection
MMC	Microsoft Management Console	PII	Personally Identifiable Information
MP3	Moving Picture Experts Group Layer 3 Audio	PIN	Personal Identification Number
MP4	Moving Picture Experts Group Layer 4	PHI	Personal Health Information
MPEG	Moving Picture Experts Group	PKI	Public Key Infrastructure
MSConfig	Microsoft Configuration	PnP	Plug and Play
MSDS	Material Safety Data Sheet	PoE	Power over Ethernet
MT-RJ	Mechanical Transfer Registered Jack	POP3	Post Office Protocol 3
MUI	Multilingual User Interface	PoS	Point of Sale
NaaS	Network as a Service	POST	Power-On sSelf-tTest
NAC	Network Access Control	POTS	Plain Old Telephone Service
NAS	Network-Attached Storage	PPM	Pages Per Minute
NAT	Network Address Translation	PPP	Point-to-Point Protocol
NetBIOS	Networked Basic Input/Output System	PPTP	Point-to-Point Tunneling Protocol
NetBEUI	Networked Basic Input/Output System Extended User Interface	PRI	Primary Rate Interface
NFC	Near Field Communication	PROM	Programmable Read-Only Memory
NFS	Network File System	PS/2	Personal System/2 connector
NIC	Network Interface Card	PSTN	Public Switched Telephone Network
NiCd	Nickel Cadmium	PSU	Power Supply Unit
NiMH	Nickel Metal Hydride	PVA	Patterned Vertical Alignment
NLX	New Low-profile Extended	PVC	Permanent Virtual Circuit
NNTP	Network News Transfer Protocol	PXE	Preboot Execution Environment
NTFS	New Technology File System	QoS	Quality of Service
NTLDR	New Technology Loader	RADIUS	Remote Authentication Dial-In User Server
NTP	Network Time Protocol	RAID	Redundant Array of Independent (or inexpensive) Discs
NTSC	National Transmission Standards Committee	RAM	Random Access Memory
NVMe	Non-volatile Memory Express	RAS	Remote Access Service
OCR	Optical Character Recognition	RDP	Remote Desktop Protocol
OEM	Original Equipment Manufacturer	RF	Radio Frequency
OLED	Organic Light Emitting Diode	RFI	Radio Frequency Interference
OS	Operating System	RFID	Radio Frequency Identification
PaaS	Platform as a Service	RGB	Red Green Blue
PAL	Phase Alternating Line	RIP	Routing Information Protocol
PAN	Personal Area Network	RIS	Remote Installation Service
PAT	Port Address Translation	RISC	Reduced Instruction Set Computer
PC	Personal Computer	RJ-11	Registered Jack Function 11
PCI	Peripheral Component Interconnect	RJ-45	Registered Jack Function 45
PCI	Payment Card Industry		

SIGLAS	EXPLICACIÓN	SIGLAS	EXPLICACIÓN
RMA	Returned Materials Authorization	TKIP	Temporal Key Integrity Protocol
ROM	Read-Only Memory	TLS	Transport Layer Security
RPO	Recovery Point Objective	TN	Twisted Nematic
RTC	Real-Time Clock	TPM	Trusted Platform Module
RTO	Recovery Time Objective	UAC	User Account Control
SaaS	Software as a Service	UDF	User Defined Functions or Universal Disk Format or Universal Data Format
SAN	Storage Area Network	UDP	User Datagram Protocol
SAS	Serial Attached SCSI	UEFI	Unified Extensible Firmware Interface
SATA	Serial Advanced Technology Attachment	UNC	Universal Naming Convention
SC	Subscription Channel	UPnP	Universal Plug and Play
SCP	Secure Copy Protection	UPS	Uninterruptible Power Supply
SCSI	Small Computer System Interface	URL	Uniform Resource Locator
SCSI ID	Small Computer System Interface Identifier	USB	Universal Serial Bus
SD card	Secure Digital Card	USMT	User State Migration Tool
SEC	Single Edge Connector	UTM	Unified Threat Management
SFC	System File Checker	UTP	Unshielded Twisted Pair
SFF	Small Form Factor	UXGA	Ultra Extended Graphics Array
SFTP	Secure File Transfer Protocol	VA	Vertical Alignment
SIM	Subscriber Identity Module	VDC	Volts DC
SIMM	Single In-Line Memory Module	VDI	Virtual Desktop Infrastructure
SLI	Scalable Link Interface or System Level Integration or Scanline Interleave Mode	VESA	Video Electronics Standards Association
S.M.A.R.T.	Self-Monitoring, Analysis, and Reporting Technology	VFAT	Virtual File Allocation Table
SMB	Server Message Block	VGA	Video Graphics Array
SMTP	Simple Mail Transfer Protocol	VLAN	Virtual LAN
SNMP	Simple Network Management Protocol	VM	Virtual Machine
SoDIMM	Small Outline Dual Inline Memory Module	VNC	Virtual Network Computer
SOHO	Small Office/Home Office	VoIP	Voice over Internet Protocol
SP	Service Pack	VPN	Virtual Private Network
SPDIF	Sony-Philips Digital Interface Format	VRAM	Video Random Access Memory
SPGA	Staggered Pin Grid Array	WAN	Wide Area Network
SRAM	Static Random Access Memory	WAP	Wireless Access Protocol/Wireless Access Point
SSD	Solid State Drive	WEP	Wired Equivalent Privacy
SSH	Secure Shell	WIFI	Wireless Fidelity
SSID	Service Set Identifier	WINS	Windows Internet Name Service
SSL	Secure Sockets Layer	WLAN	Wireless Local Area Network
SSO	Single Sign-on	WMN	Wireless Mesh Network
ST	Straight Tip	WPA	Wireless Protected Access
STP	Shielded Twisted Pair	WPA2	WiFi Protected Access 2
SXGA	Super Extended Graphics Array	WPS	WiFi Protected Setup
TACACS	Terminal Access Controller Access-Control System	WUXGA	Wide Ultra Extended Graphics Array
TCP	Transmission Control Protocol	WWAN	Wireless Wide Area Network
TCP/IP	Transmission Control Protocol/Internet Protocol	XGA	Extended Graphics Array
TDR	Time Domain Reflectometer	ZIF	Zero-Insertion-Force
TFTP	Trivial File Transfer Protocol	ZIP	Zigzag Inline Package

Lista propuesta de hardware y software para A+

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

EQUIPOS

- Tableta/teléfono inteligente Apple
- Tableta/teléfono inteligente Android
- Tableta/teléfono inteligente 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
- Proyector
- Router/switch SOHO
- Punto de acceso
- Teléfono VoIP
- Impresora
 - Láser/de tinta
 - Inalámbricas
 - Impresora 3D
- Supresor de sobrevoltaje
- UPS
- Auriculares VR
- Dispositivos inteligentes (Dispositivos IoT)

HARDWARE/REPUESTOS

- Tarjetas madre
- RAM
- Discos duros

- Fuentes de energía
- Tarjetas de video
- Tarjetas de sonido
- Tarjetas de red
- NIC inalámbrico
- Ventiladores/dispositivos de
enfriamiento/disipador de calor
- CPU
- Conectores/cables variados
 - USB
 - HDMI
 - Etc.
- Adaptadores
- Cables de red
- Cables de red/conectores sin terminar
- Adaptador AC
- Unidades ópticas
- Tornillos/separadores
- Gabinetes
- Kit de mantenimiento
- Mouse/teclados
- KVM
- Cable de consola

HERRAMIENTAS

- Destornilladores
- Multímetro
- Cortadores de cable
- Herramienta ponchadora de patch panel
- Pinza de compresión para cable
- Probador de fuente de energía

- Pelador de cable
- Caja de herramientas estándar
para técnicos
- Correa antiestática
- Pasta térmica
- Probador de cable
- Cable tonal
- Analizador WiFi
- Conectores SATA a USB

SOFTWARE

- Sistemas operativos
 - Linux
 - Chrome OS
 - Microsoft Windows
 - Mac OS
 - Android
 - iOS
- PE Disk/Live CD
- Software antivirus
- Software de virtualización
- Anti-malware
- Software de controladores