

IT Support

Esta es una certificación para técnicos de soporte técnico de nivel básico, técnicos de soporte de escritorio para usuarios finales, estudiantes de TI, pasantes, etc. El examen está dirigido a profesionales de TI de nivel básico y estudiantes de secundaria y post-secundaria inmediata. Los candidatos seleccionados son técnicos de soporte técnico calificados de nivel básico y técnicos de atención al cliente, estudiantes y pasantes con al menos 150 horas de instrucción y experiencia práctica.

Requisitos previos: se espera que los candidatos tengan competencias de lectura y escritura de al menos el nivel de octavo grado. También deben tener dos años de experiencia en el uso de una computadora de escritorio, una computadora portátil o una tableta como usuario final. Además, deben estar familiarizados con el uso de aplicaciones de productividad, como Microsoft Office o Google Docs.

Habilidades interpersonales

Aunque no se prueba específicamente como objetivos discretos, esta certificación espera que los candidatos realicen sus trabajos utilizando las siguientes mejores prácticas interpersonales:

- Demostrar habilidades de comunicación profesional al interactuar con los usuarios.
- Demostrar escucha activa.
- Expresar conceptos técnicos a una audiencia no técnica.
- Comunicarse efectivamente usando vocabulario apropiado a la situación.

Algunos escenarios de la prueba requieren comprender estas mejores prácticas.

Objetivos: CCST IT Support

1. Tareas y responsabilidades laborales de soporte de IT

1.1 Definir conceptos clave de la mesa de ayuda.

- Gestión de colas, gestión del tiempo, sistemas de emisión de tickets, acuerdo de nivel de servicio (SLA), indicadores clave de rendimiento (KPI)

1.2 Preparar documentación para resumir la interacción con el cliente.

- Crear una descripción clara, concisa, objetiva y completa del problema, los pasos para solucionarlo y los resultados obtenidos.
- Documentar de tal manera que la documentación sea útil para futuros interacciones.

1.3 Describe el proceso de resolución de problemas.

- Define el problema.
- Reúna información detallada.
- Identificar una causa probable de la falla.
- Diseñar un plan para resolver el problema.
- Realizar los cambios necesarios para implementar el plan.
- Observar los resultados de los cambios.
- Si el problema no se resuelve, repita el proceso.
- Documentar los cambios realizados para resolver el problema.

2. Problemas de hardware

2.1 Demostrar cómo seguir los procedimientos básicos de seguridad.

- Descarga eléctrica, ESD, incendio, seguridad personal

2.2 Ayudar a los usuarios finales a utilizar herramientas para localizar información sobre su dispositivo.

- **Información:** nombre de host, hardware (procesador, memoria, espacio en disco), versión del sistema operativo, dirección IPv4, dirección IPv6, dirección MAC.
- **Herramientas de Windows:** Administrador de tareas, Información del sistema, Visor de eventos, ipconfig
- **Herramientas de MacOS:** Monitor de actividad, Acerca de esta Mac, Configuración del sistema, Consola, ifconfig

2.3 Ayudar a los usuarios finales a localizar, identificar y comprender las características de varios puertos y cables.

- Puertos de vídeo: HDMI, USB-C, DVI, DisplayPort, VGA
- USB-A, USB-B, USB-C, Micro USB
- Puertos seriales
- RJ-45, UTP, STP
- Tipos comunes de cables de alimentación (escritorio, portátil, móvil)
- Rayo 3/4 (USB-C)
- Convertidores

2.4 Identificar, instalar y actualizar varios componentes en una computadora de escritorio.

- Identificación del procesador y la placa base
- Identificar, instalar y actualizar RAM, periféricos (tarjetas gráficas, tarjetas inalámbricas, tarjetas Bluetooth) y dispositivos de almacenamiento interno (SATA, SSD, NVMe, M2)
- Compatibilidad con interfaces y tarjetas de expansión
- Uso del Administrador de dispositivos para administrar los controladores. • Mejores prácticas de desechos electrónicos para la eliminación de componentes.

2.5 Investigar problemas de hardware que se encuentran comúnmente.

- **Solución de problemas básicos:** enchufar, conectar a la corriente, encender
- **Requisitos de compatibilidad de aplicaciones:** arquitectura del procesador, requisitos de RAM, requisitos de GPU, espacio en disco
- Uso del Administrador de dispositivos para identificar problemas con el hardware
- Indicadores de estado del dispositivo
- Conocimiento de las actualizaciones de firmware (beneficios y peligros)

3. Problemas de conectividad y acceso a recursos

3.1 Ayudar a los usuarios a establecer acceso a recursos basados en la red.

- Conocimientos básicos de servicios de directorio comunes: Active Directory, gestión de acceso basada en la nube (Entra ID y AWS IAM)
- Autenticación multifactor (aplicaciones de autenticación y otros métodos)
- Mapeo de una unidad compartida, incluida SMB y unidad en la nube (súper S3, OneDrive, GoogleDrive, Dropbox, Box, etc.)

Objetivos del examen de técnico de soporte certificado de Cisco

- Uso de Gpupdate/adgpupdate para forzar una actualización de la política de grupo
- Restablecer contraseñas •
- Verificar la membresía en grupos de seguridad y distribución para determinar si hay algún problema.
- Verificación de permisos

3.2 Solucionar problemas de conectividad que se encuentran comúnmente con los periféricos.

- Impresoras: conectividad a la impresora, asistencia al usuario en el uso de un dispositivo multifunción, carga de papel, solución de un atasco de papel, limpieza de la cola de impresión, cambio de tóner.
- Fax
- Auriculares
- Micrófonos
- Unidades externas
- Escáneres
- Cámaras web
- Teclado, mouse, dispositivos señaladores (con cable e inalámbricos)
- Dispositivos de entrada táctiles/interactivos (paneles planos)
- Dispositivos de teleconferencia (pantallas Webex Desk Pro)

3.3 Examinar la conectividad básica del dispositivo final a la red. • Acceso LAN (cableado)

frente a WLAN • Propósito del DNS •

Propósito del DHCP

(reconocimiento de direcciones IP autoasignadas (APIPA))

- Propósito de DHCPv6 (reconocer una dirección de enlace local en lugar de una dirección global)
- Rangos de direcciones IP (¿está en la subred correcta, pública y privada)?
- Puerta de enlace predeterminada
- SSID de red inalámbrica

• Usar los siguientes comandos para verificar la conectividad

◊ Ipconfig/Ifconfig

◊ Traceroute/tracert

◊ Hacer silbido

◊ Nslookup

◊ Netstat

◊ Ping6

◊ Trazaruta6

◊ Iproute2 (añadir ip, ss)

• Propósito de un firewall y cómo podría afectar la conectividad

4. Problemas con el sistema operativo y las aplicaciones

4.1 Ayudar a los usuarios a resolver problemas del sistema operativo Windows.

- Configuración de pantalla, múltiples pantallas, brillo
- Códigos BitLocker
- Actualizaciones de Windows y aplicaciones
- Borrar la memoria caché del navegador

- Terminar procesos con el Administrador de tareas
- Ayudar al cliente a realizar copias de seguridad y restaurar datos personales con herramientas basadas en la nube (OneDrive)
- Secuencia de inicio, inicio en modo seguro
- Gestión de energía
- Funciones de accesibilidad

4.2 Ayudar a los usuarios a resolver problemas del sistema operativo MacOS.

- Configuración de pantalla, múltiples pantallas, brillo
- Permitir a las aplicaciones los permisos necesarios
- Montaje de unidades externas
- Borrar la memoria caché del navegador
- Lanzamiento aéreo
- Terminar procesos con Activity Monitor
- Ayudar al cliente a realizar copias de seguridad y restaurar datos personales con la nube. herramientas basadas (iCloud y Time Machine)
- Gestión de energía
- Funciones de accesibilidad

4.3 Ayudar a los usuarios a resolver problemas de dispositivos móviles.

- Reiniciar el teléfono, teléfono no carga, conectividad, configuración de correo electrónico, móvil aplicaciones, software de colaboración, conocimientos básicos de MDM
- Sistema operativo del dispositivo: iOS, Android

4.4 Describir la terminología de virtualización y nube.

- Proveedores de nube (Amazon Web Services (AWS), Microsoft Azure y Google Cloud Platform (GCP)
- Máquinas virtuales e hipervisores
- Reconocer modelos de nube para dirigir el incidente al equipo adecuado

4.5 Ayudar a los usuarios a resolver problemas comunes de las aplicaciones.

- Instalación en Marketplace o aplicación aprobada
 - ◊ Fuentes no confiables/desconocidas
- Aplicaciones de productividad, colaboración y correo electrónico

5. Amenazas y prevenciones comunes

5.1 Describir las amenazas a la seguridad del usuario final, realizar una investigación básica, y escalar al equipo apropiado.

- **Amenazas:** phishing, malware, spam, intentos de acceso no autorizados, suplantación de identidad
- Ayudar al usuario a ejecutar un análisis de malware.
- Contraseñas seguras y buenas prácticas en materia de contraseñas.

5.2 Reconocer cómo evitar ser víctima de ataques de ingeniería social.

- Conciencia de que un técnico de la mesa de ayuda es un objetivo principal para la ingeniería social. ataques
- Phishing, suplantación de identidad, etc.

5.3 Reconocer cómo las políticas de la empresa y las pautas de confidencialidad protegen datos del usuario.

- Identificar información confidencial, de propiedad y de identificación personal (PII) datos

6. Herramientas de trabajo

6.1 Utilice software de acceso remoto para conectarse a dispositivos de usuario final y realizar Tareas de soporte remoto.

- Escritorio remoto, asistencia remota, Cisco WebEx, administración remota, Visor de equipo , Computación en red virtual (VNC), PC en cualquier lugar

6.2 Utilice herramientas de solución de problemas adecuadas para investigar un problema y actualizarlo documentación interna con hallazgos.

- IA: consulta a la IA para investigar un problema, limitaciones de la IA, consideraciones éticas para IA, riesgos de privacidad y seguridad, diferencia entre IA predictiva y generativa
- Utilizar los resultados del motor de búsqueda
- Foros técnicos
- Artículos de la base de conocimientos (internos y de la industria)