



Conceptos básicos del soporte técnico para macOS 10.13

**Soporte técnico y solución de problemas
de macOS High Sierra
Guía de preparación del examen**



Índice

Ventajas de la certificación ACSP	6
Completar el curso	7
Leer el libro	7
Adquirir experiencia con macOS	7
Usar esta guía	7
Características del examen	8
Lección 1: Introducción a macOS	9
Objetivos	9
Preguntas de repaso	9
Respuestas	9
Lección 2: Actualizar, actualizar a una versión importante o reinstalar macOS	9
Objetivos	9
Preguntas de repaso	9
Respuestas	10
Lección 3: Configurar macOS	10
Objetivos	10
Preguntas de repaso	10
Respuestas	11
Lección 4: Usar la interfaz de línea de comandos	11
Objetivos	11
Preguntas de repaso	11
Respuestas	11
Lección 5: Usar Recuperación de macOS	12
Objetivos	12
Preguntas de repaso	12
Respuestas	12
Lección 6: Actualizar macOS	13
Objetivos	13

Preguntas de repaso	13
Respuestas	13
Lección 7: Gestionar cuentas de usuario	15
Objetivos	15
Preguntas de repaso	15
Respuestas.....	15
Lección 8: Gestionar carpetas de inicio de usuario.....	16
Objetivos	16
Preguntas de repaso	16
Respuestas	16
Lección 9: Gestionar la seguridad y la privacidad.....	16
Objetivos	16
Preguntas de repaso	16
Respuestas	17
Lección 10: Gestionar cambios de contraseña	18
Objetivos	18
Preguntas de repaso	18
Respuestas	18
Lección 11: Gestionar el almacenamiento y los sistemas de archivos.....	19
Objetivos	19
Preguntas de repaso	19
Respuestas	19
Lección 12: Gestionar FileVault.....	20
Objetivos	20
Preguntas de repaso.....	20
Respuestas	20
Lección 13: Gestionar los permisos y el uso compartido.....	20
Objetivos	20
Preguntas de repaso	21
Respuestas.....	21

Lección 14: Usar elementos ocultos, funciones rápidas y archivos comprimidos	22
Objetivos.....	22
Preguntas de repaso.....	22
Respuestas	22
Lección 15: Gestionar los recursos del sistema	23
Objetivos.....	23
Preguntas de repaso.....	23
Respuestas	23
Lección 16: Usar metadatos, Spotlight y Siri	24
Objetivos.....	24
Preguntas de repaso.....	24
Respuestas	24
Lección 17: Gestionar Time Machine	25
Objetivos.....	25
Preguntas de repaso.....	25
Respuestas	25
Lección 18: Instalar apps.....	27
Objetivos.....	27
Preguntas de repaso.....	27
Respuestas	27
Lección 19: Gestionar documentos	28
Objetivos	28
Preguntas de repaso.....	28
Respuestas	28
Lección 20: Administrar y resolver problemas de las apps.....	29
Objetivos	29
Preguntas de repaso.....	29
Respuestas.....	30
Lección 21: Administrar ajustes de red básicos	32
Objetivos.....	32

Preguntas de repaso.....	32
Respuestas	32
Lección 22: Administrar ajustes de red avanzados	33
Objetivos	33
Preguntas de repaso.....	33
Respuestas.....	33
Lección 23: Solucionar problemas de red	34
Objetivos	34
Preguntas de repaso	34
Respuestas.....	34
Lección 24: Administrar servicios de red	36
Objetivos	36
Preguntas de repaso	36
Respuestas.....	36
Lección 25: Administrar el uso compartido de servidores y el firewall personal	37
Objetivos.....	37
Preguntas de repaso.....	37
Respuestas.....	38
Lección 26: Resolver problemas con los periféricos	39
Objetivos	39
Preguntas de repaso	39
Respuestas.....	39
Lección 27: Gestionar impresoras y escáneres	40
Objetivos	40
Preguntas de repaso	40
Respuestas.....	40
Lección 28: Resolver problemas del sistema y con el arranque.....	41
Objetivos	41
Preguntas de repaso	41
Respuestas	41

Obtención de la certificación Apple Certified Support Professional

El programa Formación y Certificación de Apple te permite estar a la vanguardia de la tecnología de Apple. La certificación es un estándar de referencia que demuestra tus sólidos conocimientos de las tecnologías de Apple y te proporciona una ventaja competitiva en el mercado laboral actual en continua evolución.

Apple ofrece dos certificaciones de macOS:

- Apple Certified Associate - Mac Integration
- Apple Certified Support Professional (ACSP)

La certificación ACSP está destinada a los profesionales de los centros de asistencia técnica, coordinadores técnicos o usuarios avanzados que prestan ayuda a los usuarios de macOS, administran redes u ofrecen soporte técnico a los usuarios del Mac. Con ella, demuestras que conoces perfectamente el funcionamiento básico de macOS y eres capaz de realizar las siguientes tareas:

- Configurar servicios fundamentales
- Realizar tareas básicas de solución de problemas
- Prestar soporte técnico a usuarios del Mac con diferentes niveles

Para obtener la certificación de ACSP, es imprescindible aprobar el examen Conceptos básicos del soporte técnico para macOS 10.13. Visita la página web [Training and Certification](#) para obtener más información.

Ventajas de la certificación ACSP

La certificación ACSP, además de distinguirti como usuario avanzado y profesional de soporte técnico para el macOS High Sierra, te permite beneficiarte del prestigio de la marca Apple. Después de aprobar el examen de certificación, recibirás un correo electrónico con información sobre lo que tienes que hacer para recibir tu certificado de Apple e instrucciones para pedirlo en formato de papel. El correo electrónico también incluye enlaces a LinkedIn, Facebook y Twitter para que a través de ellos, puedas informar a tus redes de que has obtenido el certificado.

Recibirás también credenciales para registrarte en el Apple Certification Records System (Sistema de registros de certificaciones de Apple), donde puedes:

- Actualizar tu perfil e inscribirte en el [Apple Certified Professionals Registry](#) (Registro de profesionales certificados de Apple) para aparecer como técnico certificado por Apple.
- Revisar tu historial de certificados.
- Descargar el logotipo del certificado para usarlo en tus tarjetas de presentación, currículums, páginas web, etc.
- Permitir a las empresas verificar tus certificaciones.

Recomendaciones para preparar el examen

Para preparar el examen, te recomendamos lo siguiente:

- Completar el curso macOS Support Essentials 10.13.
- Leer el libro de la Apple Training Series *macOS Support Essentials 10.13*, de Arek Dreyer y Adam Karneboge.
- Adquirir experiencia con macOS.
- Leer esta guía y practicar realizando las tareas y contestando a las preguntas de repaso.

Completar el curso

Los proveedores de formación Apple Authorized Training Providers (AATP) ofrecen cursos que te proporcionarán formación práctica sobre macOS. También podrás beneficiarte de la experiencia y conocimientos de los Apple Certified Trainers y de tus compañeros. [LearnQuest](#) es uno de nuestros AATP. Visita su página para encontrar algún curso que te resulte próximo.

Leer el libro

El examen ASCP se basa en el libro de la Apple Training Series *macOS Support Essentials 10.13*. Puedes comprar el libro en distintos sitios:

- iBooks Store: si usas un dispositivo iOS o un Mac, puedes comprar el libro en el iBooks Store.
- Safari Tech Books Online: biblioteca digital bajo demanda que ofrece suscripciones para acceder a la Apple Pro Training Series, además de miles de vídeos y libros de referencia.
- Peachpit: visita el [sitio web de Peachpit](#) para ahorrar un 30 %.

Puede que el libro esté en otros idiomas. Visita el [sitio web de Peachpit](#) para obtener más información.

Adquirir experiencia con macOS

No hay nada más útil que las horas que dediques a aprender la tecnología que hay detrás de macOS. Después de leer el libro, haz el curso, o haz las dos cosas al mismo tiempo, y dedícale tiempo a familiarizarte con macOS para tener más probabilidades de aprobar el examen de certificación.

Usar esta guía

Puedes prepararte por tu cuenta o hacer cursos que no sigan el plan de estudios de Apple Pro Training Series. También puedes prepararte para el examen de certificación practicando las tareas propuestas y respondiendo a las preguntas de repaso de las secciones que figuran a continuación.

Las tareas y las preguntas tratan sobre los conocimientos que se evalúan en el examen ASCP. Aunque en esta guía las tareas y las preguntas de repaso están divididas en diferentes lecciones o áreas de conocimiento, en el examen las preguntas estarán mezcladas.

Características del examen

El examen macOS Support Essentials 10.13 se hace con ordenador y lo ofrecen los proveedores de formación Apple Authorized Training Providers (AATP). Visita la página web de [LearnQuest](#) para encontrar tu AATP más cercano. LearnQuest es un socio de formación de Apple internacional. Si no ves ninguna sesión programada en el centro de formación de LearnQuest que te resulte más cercano, ponte en contacto con ellos para ver si pueden ofrecerte alguna sesión particular. Todos los exámenes de macOS y apps profesionales están disponibles en todos los centros de formación de LearnQuest aunque no ofrezcan el curso correspondiente.

Estas son algunas de las características del examen Conceptos básicos del soporte técnico para macOS 10.13:

- El examen incluye cinco preguntas demográficas que no cuentan para la puntuación. Tienes 5 minutos para contestarlas.
- El examen contiene 100 preguntas técnicas que sí cuentan para la puntuación. Tienes 150 minutos para contestarlas.
- El examen usa de forma aleatoria preguntas de selección múltiple e interactivas.
- La puntuación mínima para aprobar es el 75 %. Las puntuaciones no se redondean.
- Si quieres saber más cosas sobre cómo se puntúa el examen, visita la página web [Training and Certification: Exam and Certification Questions](#).
- No podrás usar ningún material de consulta durante la prueba.
- Algunos exámenes se ofrecen en varios idiomas. Para obtener más información, visita la página [Training and Certification: Localized Apple Certification Exams](#).

Si tienes alguna pregunta sobre los exámenes, visita la página [Training and Certification: Exam and Certification Questions](#).

Parte primera: Instalación y configuración

Lección 1: Introducción a macOS

Objetivos

- Describir macOS.
- Describir las nuevas características de macOS High Sierra 10.13.
- Enumerar las versiones de macOS que pueden usarse en ordenadores Mac que pueden ejecutar también macOS High Sierra 10.13.

Preguntas de repaso

1. ¿Cuál es el sistema de archivos predeterminado para ordenadores Mac con almacenamiento 100 % flash que se ejecuta en macOS High Sierra?
2. ¿Qué estándar del sector permite a los Mac con High Sierra trabajar sin problemas con los vídeos 4K, cada vez más populares?
3. ¿Qué funciones añade Metal 2 a High Sierra?

Respuestas

1. El sistema de archivos predeterminado para los ordenadores Mac con almacenamiento 100 % flash es el Sistema de archivos de Apple (APFS).
2. El estándar High Efficiency Video Coding (HEVC), también denominado H.265, permite a los ordenadores Mac trabajar sin problemas con los vídeos 4K.
3. Metal 2 añade funciones como el aprendizaje automático, la realidad virtual y la compatibilidad con GPU externas, que se usan en apps de entretenimiento y de creatividad profesional.

Lección 2: Actualizar, actualizar a una versión importante o reinstalar macOS

Objetivos

- Describir las diferencias entre una actualización, una actualización a una versión importante y una reinstalación de macOS.
- Describir el instalador de macOS.
- Resolver problemas con una reinstalación o una actualización a una versión importante de macOS.

Preguntas de repaso

1. ¿Cómo puedes obtener el instalador de macOS?
2. ¿Qué diferencias hay entre una actualización, una actualización a una versión importante y una reinstalación de macOS?
3. ¿Cuáles son los requisitos del sistema para poder actualizar a macOS High Sierra?
4. ¿Qué tienes que hacer para poder actualizar a macOS High Sierra?
5. ¿Cómo sabe el instalador de macOS qué actualizaciones de firmware tiene que descargar?
6. ¿Qué puedes usar para resolver los problemas de instalación de macOS?

Respuestas

1. macOS es gratuito para los usuarios que tengan un Mac válido.
2. Las diferencias entre una actualización, una actualización a una versión importante y una reinstalación de macOS son:
 - Actualización de macOS: instala una actualización incremental del sistema operativo del Mac, pero no actualiza el ordenador a la siguiente versión importante.
 - Actualización a una versión importante de macOS: instala la siguiente versión importante independiente.
 - Reinstalación: instala la misma versión importante de macOS en un disco que ya tiene instalado macOS.
3. Los requisitos del sistema para poder actualizar a macOS High Sierra son:
 - OS X Mountain Lion 10.8 o versiones posteriores
 - 2 GB de RAM
 - 14,3 GB de espacio disponible en el disco
4. Para poder actualizar a macOS High Sierra, realiza antes las siguientes tareas:
 - a. Verifica la compatibilidad de las aplicaciones.
 - b. Haz una copia de seguridad de los archivos y carpetas importantes.
 - c. Anota las configuraciones fundamentales.
 - d. Abre la app Actualización de software o entra en el App Store.
5. El instalador usa el número de modelo del Mac para localizar y descargar las actualizaciones de firmware disponibles para él.
6. Usa la barra de menús del instalador de macOS para ver el registro.

Lección 3: Configurar macOS

Objetivos

- Realizar la configuración inicial de macOS.
- Configurar los ajustes del sistema más habituales.
- Identificar e instalar un perfil de configuración.
- Verificar la información del sistema.

Preguntas de repaso

1. ¿Qué herramienta te guía a través del proceso de configuración inicial de macOS High Sierra?
2. ¿Qué prestaciones importantes obtienes si configuras iCloud?
3. ¿Qué prestación puede mejorar de manera significativa la seguridad del ID de Apple en los Mac que tienen activado iCloud?
4. Una vez configurado macOS High Sierra, ¿dónde puedes configurar iCloud?
5. ¿Qué es un perfil? ¿Cómo se gestionan los perfiles?
6. ¿Dónde puedes encontrar información sobre el sistema, las reparaciones y la cobertura de la garantía del Mac?

Respuestas

1. El Asistente de Configuración te guía por el proceso de configuración de macOS High Sierra.
2. iCloud proporciona servicios de comunicación y almacenamiento en la nube para las apps, como Mail, Contactos, Calendarios, Recordatorios, Notas, Safari, Llavero, Fotos y todas las apps que admitan la integración con iCloud. iCloud ofrece también la tecnología Buscar mi Mac, que permite localizar un Mac perdido o robado.
3. La autenticación de doble factor puede mejorar la seguridad del ID de Apple si iCloud está activado.
4. Una vez terminada la configuración de macOS High Sierra, podrás configurar los ajustes de iCloud en el panel de preferencias de Cuentas de Internet o de iCloud.
5. Un perfil es un documento con la extensión .mobileconfig que contiene los ajustes del sistema que ha definido el administrador. Cuando se abre un documento de perfil, macOS High Sierra instala el perfil y configura los ajustes. Puedes gestionar los perfiles instalados en el panel de preferencias Perfiles.
6. Usa la ventana Acerca de este Mac para obtener información sobre el sistema, las reparaciones y la cobertura de la garantía del Mac.

Lección 4: Usar la interfaz de línea de comandos

Objetivos

- Describir cuándo resulta útil la interfaz de línea de comandos.
- Explorar Terminal.

Preguntas de repaso

1. ¿Cuáles son algunas de las ventajas de usar la interfaz de línea de comandos?
2. ¿De qué cuatro partes consta una cadena de comando?
3. ¿Qué comando de terminal tienes que usar para hacer las tareas que se indican a continuación?
 - a. Imprimir el directorio activo
 - b. Elaborar una lista
 - c. Cambiar de directorio
 - d. Indicar el directorio principal
 - e. Indicar la carpeta de inicio del usuario actual
 - f. Crear una carpeta
 - g. Ejecutar el comando con acceso a la cuenta raíz
 - h. Borrar la pantalla de Terminal
4. ¿Qué tecla tienes que usar si quieres completar de forma automática nombres de archivo, de ruta y de comando?

Respuestas

1. La interfaz de línea de comandos ofrece las siguientes ventajas:
 - Más opciones para resolver problemas y realizar tareas administrativas
 - Mayor acceso al sistema de archivos
 - Inicio remoto usando el protocolo Secure Shell (SSH)
 - Capacidad para ejecutar comandos como usuario raíz con sudo

- Posibilidad de automatizar las tareas repetitivas con scripts
 - Capacidad para administrar de forma remota varios ordenadores Mac de forma simultánea con Apple Remote Desktop (ARD)
2. Las cuatro partes que componen una cadena de comando son:
- Nombre del comando
 - Opciones de comando
 - Argumentos
 - Extras
3. Usa estos comandos para realizar las siguientes tareas:
- a. Imprimir el directorio activo: `pwd`
 - b. Elaborar una lista: `ls`
 - c. Cambiar de directorio: `cd`
 - d. Indicar el directorio principal: `..`
 - e. Indicar la carpeta de inicio del usuario actual: `~`
 - f. Crear una carpeta: `mkdir`
 - g. Ejecutar el comando con acceso a la cuenta raíz: `sudo`
 - h. Borrar la pantalla de Terminal: borra o pulsa Control-L
4. Usa la tecla de tabulación para completar de forma automática los nombres de archivo, ruta y comando.

Lección 5: Usar Recuperación de macOS

Objetivos

- Acceder a las utilidades de Recuperación de macOS.
- Volver a instalar macOS desde Recuperación de macOS.
- Crear un disco externo de Recuperación de macOS.

Preguntas de repaso

1. ¿Qué utilidades están disponibles cuando se arranca el ordenador desde Recuperación de macOS?
2. ¿Qué distintas opciones de recuperación y combinaciones de teclas de arranque hay?
3. ¿Cómo puedes crear un disco externo de instalación de macOS?

Respuestas

1. Recuperación de macOS te ofrece las siguientes opciones: Restaurar desde una copia de seguridad de Time Machine, Reinstalar macOS, Obtener ayuda en Internet a través de Safari, Utilidad de Discos, Disco de Arranque, Utilidad Contraseña Firmware, Utilidad de Red, Terminal y Restaurar contraseña.
2. Recuperación de macOS instala diferentes versiones de macOS en función de la combinación de teclas que se use.
 - a. Comando + R: instala la versión de macOS instalada más recientemente.
 - b. Opción + Comando + R: actualiza a la versión de macOS más reciente que sea compatible con el Mac.
 - c. Mayúsculas + Opción + Comando + R: instala la versión de macOS incluida con el Mac.

3. Puedes crear un disco de recuperación de macOS que incluya las herramientas y recursos necesarios para instalar macOS High Sierra con la herramienta de línea de comandos `createinstallmedia` en el instalador de macOS.

Lección 6: Actualizar macOS

Objetivos

- Configurar ajustes de actualización automática de software.
- Actualizar de forma automática el software de Apple.
- Actualizar de forma manual el software de Apple.

Preguntas de repaso

1. ¿Quién puede instalar actualizaciones de software del sistema desde el App Store?
2. ¿Cómo te informa macOS de que hay una actualización de software?
3. ¿Qué apps intenta actualizar la función Actualización de software?
4. ¿Qué app tienes que abrir para iniciar las actualizaciones de software de Apple?
5. ¿Qué elementos se instalan siempre, de forma predeterminada, con las actualizaciones de software automáticas?
6. ¿Qué apps integradas no se instalan de forma automática cuando desinstalas macOS High Sierra y lo vuelves a instalar?
7. ¿Cómo puedes controlar qué aplicaciones de software se actualizarán de forma automática en el Mac?
8. ¿Dónde puedes encontrar actualizaciones de software de Apple si necesitas instalar una de forma manual?
9. ¿Cuál es la mejor manera de saber qué software se ha instalado en el Mac?

Respuestas

1. Los usuarios que tengan cuentas de administrador y estándar pueden instalar actualizaciones del sistema desde el App Store.
2. Cuando las actualizaciones de software están listas para instalar, macOS muestra una notificación de actualizaciones disponibles.
3. Actualización de software de macOS intenta actualizar lo siguiente:
 - El software de Apple instalado actualmente
 - Los paquetes de software de macOS
 - El software que se ha comprado en el App Store
4. Para iniciar las actualizaciones de software, tienes que abrir la app en el App Store.
5. Los archivos del sistema y las actualizaciones de seguridad se instalan por defecto de forma automática cuando están disponibles.
6. iMovie, GarageBand y las apps de productividad, Pages, Keynote y Numbers, no se reinstalan de forma automática si se borra el disco.
7. La automatización de las actualizaciones de software se controla en las preferencias del App Store. Configura los controles parentales de la cuenta del usuario para limitar su capacidad para usar el App Store.

8. Visita <https://support.apple.com/downloads> para localizar y descargar todas las actualizaciones de software de Apple.
9. Información del Sistema muestra el software instalado en el equipo desde el App Store o la app Instalador, y también las instalaciones por defecto de Apple o las de otros fabricantes.

Parte segunda: Cuentas de usuario

Lección 7: Gestionar cuentas de usuario

Objetivos

- Reconocer los distintos tipos de cuentas y atributos de usuario.
- Crear y gestionar cuentas de usuario.
- Configurar los parámetros de inicio de sesión y cambio rápido de usuario.

Preguntas de repaso

1. ¿Cuáles son los tipos de cuentas de usuario local que hay en macOS High Sierra? ¿En qué se diferencian?
2. ¿Qué son los atributos de cuenta?
3. ¿Cómo se puede impedir que una cuenta de usuario tenga acceso total a todas las apps?
4. ¿Para qué sirve el cambio rápido de usuario?

Respuestas

1. Las cuentas de usuario local en macOS son:
 - Administrador: las cuentas de administrador forman parte del grupo de administradores y tienen acceso total a todas las apps, preferencias y ubicaciones de recursos compartidas.
 - Estándar: los usuarios estándar pueden utilizar prácticamente todos los recursos y funciones del Mac pero, por lo general, no pueden cambiar nada que pueda afectar a otros usuarios.
 - Gestionada con controles parentales: una cuenta gestionada es una cuenta estándar que tiene activados los controles parentales.
 - Invitado: la cuenta de invitado predeterminada es similar a la cuenta de usuario estándar, pero no necesita contraseña. Cuando un usuario invitado cierra la sesión, se elimina la carpeta de inicio, además de todos los elementos de la carpeta de inicio que se guardarían normalmente, como los archivos de preferencias o el historial del navegador web.
 - Solo compartir: este tipo de cuenta solo te permite compartir archivos con un usuario que esté en otro ordenador, pero no le permite iniciar sesión en tu Mac.
 - Administrador del sistema (raíz): este tipo de cuenta tiene acceso ilimitado prácticamente a todo en el Mac. Está desactivada de forma predeterminada en macOS.
 - Grupo: las cuentas de grupo son listas de cuentas de usuarios que permiten controlar mejor el acceso a los archivos y a las carpetas.
2. Los atributos de cuenta son datos que sirven para definir una cuenta de usuario. Algunos ejemplos de atributo son: ID de usuario, grupo, nombre de cuenta, nombre completo, shell de inicio de sesión, directorio principal, identificador único universal (UUID), ID de Apple o alias.
3. Puedes usar controles parentales para limitar lo que pueden hacer los usuarios. Entre las limitaciones están: forzar el uso de Finder Simple, limitar las apps, limitar los contenidos en el App Store, configurar límites de tiempo, ajustes de privacidad, etc.
4. El cambio rápido de usuario permite cambiar de cuenta de usuario en el Mac sin que los usuarios tengan que cerrar sesión o salir de las apps.

Lección 8: Gestionar carpetas de inicio de usuario

Objetivos

- Ser capaz de describir las características de las carpetas de inicio de los usuarios.
- Eliminar cuentas de usuario y archivar el contenido de sus carpetas de inicio.
- Migrar y restaurar cuentas de inicio.

Preguntas de repaso

1. ¿Qué carpetas están incluidas de forma predeterminada en la carpeta de inicio de un usuario?
2. ¿Qué opciones puedes elegir al eliminar una cuenta de usuario local?
3. ¿Qué puedes hacer con el Asistente de Migración?
4. ¿Cómo puedes asociar una cuenta de usuario local nueva con una carpeta de inicio de usuario que se ha migrado o restaurado de forma manual en macOS?

Respuestas

1. Las carpetas de inicio de usuario predeterminadas son: Escritorio, Documentos, Descargas, Vídeos, Música, Imágenes y Carpeta Pública.
2. Al eliminar una cuenta de usuario local, tienes tres opciones:
 - a. Guardar la carpeta de inicio en una imagen de disco.
 - b. No cambiar la carpeta de inicio.
 - c. Eliminar la carpeta de inicio.
3. El Asistente de Migración te permite transferir los ajustes, las cuentas de usuario y el contenido desde un ordenador Mac o Windows o desde una copia de seguridad de Time Machine al Mac.
4. Para asociar una cuenta de usuario local con una carpeta de inicio de usuario que se ha migrado o restaurado de forma local, haz lo siguiente:
 - a. Copia la carpeta de inicio del usuario restaurada en la carpeta /Usuarios.
 - b. Abre Preferencias del Sistema y selecciona Usuarios y Grupos.
 - c. Crea una cuenta de usuario local y asígnale el mismo nombre de cuenta que se utilizó con la carpeta de inicio del usuario. macOS te pedirá que asocies la nueva cuenta de usuario local con la carpeta de inicio restaurada.

Lección 9: Gestionar la seguridad y la privacidad

Objetivos

- Ser capaz de describir las distintas clases de contraseña y su uso.
- Gestionar los secretos del Llavero.
- Activar y administrar el llavero de iCloud.
- Gestionar la seguridad del sistema y la privacidad de los usuarios.

Preguntas de repaso

1. ¿Qué clases de contraseña diferentes se pueden usar para proteger un Mac?
2. ¿Qué ítems se pueden guardar en un llavero?
3. ¿Cómo ayuda a proteger la información Acceso a Llaveros?

4. ¿Dónde se almacenan los archivos del llavero?
5. ¿Qué app tienes que usar para configurar el llavero?
6. La autenticación de doble factor seguridad añade más seguridad a tu ID de Apple. ¿Cómo?
7. ¿Cuándo y por qué se usa el código de seguridad de iCloud?
8. ¿Cómo se puede limitar el uso de Servicios de localización?
9. ¿Cómo se puede garantizar la privacidad de las grabaciones de audio que se usan en Dictado?
10. ¿Qué función se puede activar para encontrar un Mac si se pierde?

Respuestas

1. Las distintas clases de contraseña que se pueden usar para proteger el Mac son:
 - a. Contraseña de cuenta de usuario local.
 - b. ID de Apple y contraseña: para iCloud, iTunes y el App Store.
 - c. Contraseñas de llavero: para proteger los componentes de autenticación de los archivos cifrados del llavero.
 - d. Contraseñas de recursos: por ejemplo, el correo electrónico, los sitios web, los servidores de archivos, las apps y las imágenes de disco cifradas.
 - e. Contraseña de firmware: impide arrancar el Mac desde un disco que no sea el disco de arranque designado.
2. Los llaveros sirven para almacenar contraseñas de recursos, certificados, claves, formularios de páginas web y notas seguras. El sistema del llavero también puede almacenar de forma segura la información de autorrelleno de Safari, la configuración de las cuentas de internet y las notas de texto seguras.
3. Acceso a Llaveros usa archivos cifrados, que sirven para guardar de forma segura los ítems. No se puede acceder a ellos a menos que se conozca la contraseña del llavero. Si se olvida la contraseña, el contenido de los archivos se pierde para siempre.
4. Los llaveros se almacenan en diferentes ubicaciones de macOS en función de los usuarios y los recursos.
 - a. Los llaveros de inicio de sesión local están guardados en `/Usuarios/nombre de usuario/Biblioteca/Llavero/login.keychain`.
 - b. Los demás llaveros locales están almacenados en `/Usuarios/nombre de usuario/Biblioteca/Llaveros/otros.keychain`.
 - c. Los llaveros de iCloud están guardados en `/Usuarios/nombre de usuario/Biblioteca/Llaveros/UUID/`.
 - d. Los llaveros del sistema están en `/Biblioteca/Llaveros/System.keychain`.
 - e. Los llaveros de raíz del sistema para las redes de confianza no aparecen por defecto, pero se pueden encontrar aquí: `/Sistema/Biblioteca/Llaveros/`
 - f. Los demás llaveros están en distintas ubicaciones de macOS. No toques estos archivos salvo que alguien en quien confíes te lo indique para resolver un problema.
5. Acceso a Llaveros permite ver y modificar la mayoría de los ítems de un llavero.
6. Con la autenticación de doble factor, solo podrás acceder a la cuenta de tu ID de Apple en dispositivos de confianza, como tu iPhone, iPad o Mac.
7. Si usas un ID de Apple que no tenga activada la autenticación de doble factor, el llavero de iCloud se activa de forma automática. Para poder usar tu ID de Apple en otros dispositivos, tienes que usar el código de seguridad de iCloud.

8. Usa las preferencias de Seguridad y privacidad dentro del panel Privacidad para configurar el acceso de las apps a Servicios de localización, Contactos, Calendarios, Recordatorios y a los servicios para las redes sociales. Cuando una app nueva solicita información considerada como personal, macOS pide permiso al usuario.
9. La opción Dictado mejorado está activada de forma predeterminada. Cuando se usa esta opción, el Mac convierte lo que el usuario le dice en voz alta en texto, pero no envía el texto dictado a Apple. Si se desactiva esta opción, lo que el usuario dice en voz alta se envía a Apple para convertirlo en texto.
10. La función Buscar mi Mac de iCloud permite acceder de forma remota a los servicios de localización del Mac para poder encontrarlo si se pierde.

Lección 10: Gestionar cambios de contraseña

Objetivos

- Cambiar contraseñas que se han descubierto.
- Restablecer contraseñas de usuario perdidas.
- Establecer una contraseña de firmware para impedir inicios de macOS no autorizados.

Preguntas de repaso

1. ¿Cómo se puede cambiar la contraseña de una cuenta de ordenador local?
2. ¿Cómo se puede restablecer la contraseña de cuenta de otro usuario en macOS High Sierra?
3. Si un usuario cambia la contraseña de su cuenta, ¿cómo afecta el cambio a su llavero de inicio de sesión?
4. ¿Cómo se puede restablecer una contraseña de cuenta olvidada si el usuario no puede iniciar sesión en el Mac?
5. ¿Cómo afectará el restablecimiento de la contraseña al llavero de inicio de sesión de ese usuario?
6. ¿Cómo se puede restablecer una contraseña de inicio de sesión con un ID de Apple?
7. ¿Cómo se puede usar Utilidad de Contraseña de Firmware para impedir que los usuarios hagan cambios de contraseña para los que no están autorizados?

Respuestas

1. Las contraseñas de cuentas locales se pueden cambiar en las preferencias de Seguridad y privacidad dentro del panel General.
2. Puedes restablecer las contraseñas de cuenta de otros usuarios en el panel de preferencias Usuarios y grupos. ¿Cómo? Selecciona la cuenta de usuario que quieres cambiar y haz clic en Restablecer contraseña.
3. Si la contraseña de inicio de sesión no coincide con la del llavero de inicio de sesión, macOS crea ítems de llavero vacíos que coinciden con el llavero de inicio de sesión cuando se inicia sesión en el Mac.
4. Puedes utilizar el asistente para restablecer contraseñas que está disponible en Recuperación de macOS.
5. Si la contraseña de inicio de sesión no coincide con la de llavero, macOS crea ítems de llavero vacíos que coinciden con el llavero de inicio de sesión. Si el usuario recuerda su contraseña antigua, podrás recuperar el llavero archivado.
6. La contraseña de inicio de sesión se puede restablecer con un ID de Apple si se indicó este al crear la primera cuenta de usuario siguiendo los pasos del Asistente de Configuración.
7. Las contraseñas de firmware impiden a los usuarios que no tienen la contraseña iniciar sesión desde un disco que no sea el designado como de arranque.

Parte tercera: Archivos del sistema

Lección 11: Gestionar el almacenamiento y los sistemas de archivos

Objetivos

- Reconocer los sistemas compatibles con macOS.
- Gestionar discos, particiones y volúmenes.
- Solucionar problemas y reparar particiones y fallos de los volúmenes.

Preguntas de repaso

1. ¿Cómo se denomina el proceso de aplicar la lógica al almacenamiento en forma de particiones, contenedores y volúmenes?
2. ¿Qué esquemas de partición admite macOS?
3. ¿Cuáles son los principales formatos de volumen compatibles con macOS High Sierra?
4. ¿Cuáles son algunas de las ventajas que ofrece APFS?
5. ¿Cuáles son las cinco maneras con las que se puede expulsar un disco o un volumen desde el Finder?
6. ¿Qué dos apps incluidas en macOS High Sierra se pueden usar para recopilar información sobre los dispositivos de almacenamiento?
7. ¿Para qué sirve la función Primera Ayuda dentro de Utilidad de Discos?

Respuestas

1. El proceso de aplicar lógica al almacenamiento se denomina formateo.
2. macOS admite tres esquemas de partición:
 - a. Mapa de particiones GUID (GPT): es el esquema de partición predeterminado en los ordenadores Mac.
 - b. Mapa de particiones Apple (APM): es el esquema de partición predeterminado que se usaba en los ordenadores Mac anteriores con PowerPC.
 - c. Registro maestro de arranque (MBR): es el esquema de partición predeterminado que usan la mayoría de ordenadores que no son Mac, incluidos los PC compatibles con Windows. Es el esquema de partición que usan por lo general los periféricos que se almacenan en la memoria flash.
3. Los tres formatos de volumen principales que se pueden usar con macOS High Sierra son:
 - APFS: se usa con las unidades de estado sólido (SSD) y otros dispositivos 100 % flash.
 - Mac OS Plus: se usaba con anterioridad a macOS High Sierra. También se denomina HFS Plus.
 - FAT: formato de volumen antiguo que se usaba en los PC con Windows.
 - ExFAT: creado específicamente para los discos de almacenamiento flash grandes con un tamaño superior a los 32 GB.
 - NTFS: el formato de volumen nativo predeterminado de Windows. macOS puede leer volúmenes NTFS, pero no puede escribir ni arrancar desde ellos.
4. APFS realiza operaciones habituales, como copia instantánea de archivos y directorios, ayuda a proteger los datos en caso de cortes del suministro eléctrico o caídas del sistema y protege los archivos con cifrado nativo.

5. Para expulsar un volumen o un disco en el Finder, puedes usar uno de estos cinco métodos:
 - a. Arrastra el icono del disco a la Papelera en el Dock.
 - b. En la barra lateral del Finder, haz clic en Expulsar (el botón pequeño que aparece junto al volumen que quieres expulsar).
 - c. Selecciona el volumen que quieres expulsar y haz clic en Archivo > Expulsar.
 - d. Selecciona el volumen que quieres expulsar y usa la función rápida de teclado Command + E.
 - e. Selecciona el volumen que quieres expulsar y pulsa Control + clic para mostrar un menú emergente. Selecciona Expulsar.
6. Utilidad de Discos e Información del Sistema son las dos apps que se pueden usar indistintamente para recopilar información sobre los dispositivos de almacenamiento.
7. La función Primera Ayuda dentro de Utilidad de Discos sirve para verificar y reparar el esquema de partición y la estructura de directorios de un volumen. Estos elementos contienen la información necesaria para localizar archivos y carpetas en el volumen.

Lección 12: Gestionar FileVault

Objetivos

- Describir cómo puede ayudar FileVault a proteger los datos.
- Activar la protección de FileVault.
- Describir cómo recuperar el acceso a un Mac protegido con FileVault cuando se han perdido todas las contraseñas de las cuentas de usuario locales.

Preguntas de repaso

1. ¿Cómo protege FileVault los datos de usuario?
2. ¿Cómo se puede activar FileVault si no se ha activado cuando lo solicitaba el Asistente de Configuración?
3. ¿De qué dos maneras se puede guardar la clave de recuperación de FileVault cuando se activa en el panel de preferencias Seguridad y privacidad?

Respuestas

1. FileVault usa cifrado de disco completo para evitar accesos no autorizados a la información del disco de arranque.
2. FileVault se puede activar en cualquier momento desde el panel de preferencias Seguridad y privacidad.
3. El modo de recuperación de FileVault ofrece dos maneras de recuperar las contraseñas de FileVault si se pierden:
 - a. Usar el ID de Apple para desbloquear el volumen de FileVault y restablecer la contraseña.
 - b. Registrar la clave generada de forma aleatoria por FileVault.

Lección 13: Gestionar los permisos y el uso compartido

Objetivos

- Describir la propiedad y los permisos de los archivos.
- Explorar las carpetas compartidas predeterminadas de macOS.
- Gestionar de forma segura el acceso a los archivos y las carpetas.

Preguntas de repaso

1. ¿Cómo se puede identificar la propiedad y los permisos de un archivo o una carpeta en el Finder?
2. ¿En qué se diferencian las listas ACL de los permisos del sistema de archivos UNIX estándar?
3. ¿Por qué el nivel raíz (o inicial) de la carpeta de inicio de un usuario es visible para otros?
4. ¿Cómo permite la organización predeterminada del sistema de archivos compartir de forma segura archivos y carpetas locales?
5. ¿Qué característica única tienen los permisos de la carpeta Usuarios/Compartido?

Respuestas

1. La ventana Información del Finder se puede usar para identificar la propiedad y los permisos de un elemento.
2. Las listas de control de acceso (ACL) amplían la arquitectura de permisos UNIX estándar para controlar aún más el acceso a las carpetas y a los archivos. Funcionan de manera similar a los sistemas de archivos NTFS y UNIX basados en Windows.
3. El nivel raíz de la carpeta de inicio de un usuario es visible para otros usuarios para que puedan acceder a la carpeta Pública de uso compartido.
4. Todas las carpetas de inicio incluyen una carpeta Pública que pueden leer otros usuarios y una carpeta de Dropbox en la que pueden escribir. Las demás subcarpetas de la carpeta de inicio de un usuario (excepto la Carpeta Web) tienen permisos de forma predeterminada que impiden a otros usuarios acceder a ellas. La carpeta Compartido está también configurada para que todos los usuarios puedan compartir elementos.
5. La carpeta Compartido está configurada para que todos los usuarios puedan leer y escribir archivos, pero únicamente el propietario de un elemento puede eliminarlo de la carpeta. La configuración de permiso "sticky bit" (bit adhesivo) impide que otros usuarios eliminen elementos de los que no son propietarios.

Parte cuarta: Gestión de datos

Lección 14: Usar elementos ocultos, funciones rápidas y archivos comprimidos

Objetivos

- Acceder a archivos y carpetas ocultos.
- Examinar paquetes.
- Gestionar alias y enlaces.
- Crear y abrir archivos zip e imágenes de disco.

Preguntas de repaso

1. ¿Por qué oculta el Finder algunas carpetas en la raíz del volumen del sistema?
2. ¿Cuáles son los dos métodos utilizados para ocultar elementos en el Finder?
3. ¿Para qué se usan los paquetes en macOS High Sierra?
4. ¿En qué se diferencian los alias y los enlaces simbólicos?
5. ¿En qué casos es preferible usar un archivo comprimido en lugar de una imagen de disco? ¿En qué casos es preferible usar una imagen de disco en lugar de un archivo comprimido?
6. ¿Qué clase de archivo crea el Finder cuando se selecciona la opción Archivar?
7. ¿Cuál es la acción definida como predeterminada para abrir archivos comprimidos zip en macOS High Sierra?

Respuestas

1. El Finder oculta los recursos UNIX tradicionales a los usuarios normales porque no necesitan acceder a esos elementos. Si lo necesitan, pueden usar Terminal.
2. Para ocultar elementos en el Finder, se puede usar uno de estos métodos:
 - a. Añadir un punto al principio de un nombre de archivo.
 - b. Activar la marca de archivo oculto.

Nota: Los dos métodos para ocultar archivos se pueden gestionar desde la línea de comandos.
3. Los paquetes se usan para combinar elementos complejos en carpetas individuales. Los paquetes tienen la ventaja añadida de que se muestran como un solo elemento en el Finder. De esta forma, los desarrolladores pueden combinar recursos en un solo elemento e impedir que los usuarios puedan ver y potencialmente dañar esos recursos si eliminan o mueven archivos.
4. Los alias y los enlaces simbólicos funcionan como accesos directos al elemento original. Sin embargo, un alias contiene información adicional que permite al sistema hacer un seguimiento del elemento original si se cambia el nombre o se mueve dentro del mismo volumen. Por el contrario, si hay algún cambio en un elemento original, el enlace simbólico se rompe.
5. Los archivos comprimidos son mucho más fáciles de crear en el Finder y se pueden usar con los sistemas operativos de otros fabricantes. Las imágenes de disco son más difíciles de crear y gestionar, pero ofrecen más flexibilidad porque se pueden modificar y convertir más fácilmente. Sin embargo, las imágenes de disco de macOS High Sierra no son compatibles con los sistemas operativos de otros fabricantes.
6. La opción Archivar del Finder crea archivos comprimidos.

7. Al hacer doble clic en un archivo comprimido en macOS High Sierra, el sistema descomprime de forma predeterminada los contenidos del archivo en una ubicación próxima a la del archivo comprimido original.

Lección 15: Gestionar los recursos del sistema

Objetivos

- Acceder a archivos y carpetas ocultos.
- Examinar paquetes.
- Gestionar alias y enlaces.
- Crear y abrir archivos zip e imágenes de disco.

Preguntas de repaso

1. ¿Cuáles son las cuatro carpetas de nivel superior predeterminadas que se ven en el Finder?
2. ¿Cuáles son los seis recursos comunes del sistema? ¿Para qué sirve cada uno de ellos?
3. ¿Cuáles son los cuatro dominios de recursos del sistema? ¿Para qué sirve cada dominio?
4. ¿Para qué sirve la carpeta ~/Biblioteca/Contenedores? ¿Qué elementos incluye esa carpeta?
5. ¿Qué pasa cuando un usuario hace doble clic en un archivo de tipo de letra?
6. ¿Cómo se pueden detectar los tipos de letra duplicados?
7. ¿Cómo contribuye Protección de la integridad del sistema (SIP) a proteger los recursos del sistema de macOS High Sierra?

Respuestas

1. Las cuatro carpetas de nivel superior que pueden verse en el Finder son:
 - a. Aplicaciones: las apps a las que tienen acceso los usuarios locales.
 - b. Biblioteca: recursos del sistema a los que tienen acceso los usuarios locales.
 - c. Sistema: recursos del sistema.
 - d. Usuarios: carpetas de inicio de usuario local.
2. Estos son los seis recursos comunes del sistema y su finalidad:
 - a. Extensiones: se anexas al kernel del sistema para proporcionar compatibilidad con los drivers del hardware y de los periféricos.
 - b. Estructuras: bibliotecas de códigos compartidas que proporcionan recursos de software adicionales a las apps y a los procesos del sistema.
 - c. Tipos de letra.
 - d. Archivos de preferencias: información de configuración de las apps y del sistema.
 - e. LaunchAgents y LaunchDaemons: permiten a launchd proporcionar servicios que se inician de forma automática cuando se necesitan al arrancar el sistema o cuando los usuarios inician sesión.
 - f. Registros: archivos de texto que contienen entradas con los errores y progresos de prácticamente todas las apps o servicios del sistema.
3. Estos son los cuatro dominios de recursos del sistema y su finalidad:
 - a. Usuario: contiene las apps y recursos del sistema específicos de cada cuenta de usuario.
 - b. Local: contiene las apps y recursos del sistema disponibles para los usuarios de un Mac local.

- c. Red: opcional. Contiene apps y recursos del sistema que están disponibles para cualquier Mac que tenga uso compartido de redes automático.
 - d. Sistema: contiene apps y recursos del sistema que proporcionan funciones básicas del sistema.
4. La carpeta ~/Biblioteca/Contenedores contiene recursos para las apps de zona protegida. macOS High Sierra crea y mantiene una carpeta contenedora independiente para cada app de zona protegida que pueden abrir los usuarios. Las apps de zona protegida son más seguras porque solo pueden acceder a los elementos que estén dentro de su contenedor. Solo los elementos pensados para compartir se encuentran en las carpetas contenedoras de grupo.
 5. Al hacer doble clic en un archivo de tipo de letra, se abre automáticamente una vista previa del tipo de letra en la app Tipo de letra del libro. Se puede pulsar el botón Instalar tipo de letra desde la vista previa para copiar el tipo de letra en la carpeta ~/Biblioteca/Tipos de letra.
 6. La app Tipo de letra del libro muestra un punto pequeño junto al nombre de los tipos de letra que tienen recursos duplicados.
 7. Protección de la integridad del sistema impide que los usuarios y procesos con acceso de administrador o raíz puedan modificar elementos fundamentales de macOS High Sierra. Entre los elementos protegidos están las carpetas /Sistema, /bin, /sbin y /usr, además de las apps fundamentales de macOS High Sierra.

Lección 16: Usar metadatos, Spotlight y Siri

Objetivos

- Describir de qué forma macOS almacena y usa los metadatos del archivo.
- Usar metadatos, por ejemplo, las marcas y los comentarios, para organizar los archivos.
- Usar Spotlight y Siri para buscar recursos locales y en Internet.

Preguntas de repaso

1. ¿Qué son los metadatos del sistema de archivos? ¿Podrías dar algunos ejemplos?
2. ¿Cuáles son algunas de las marcas de archivo comunes que se usan en macOS High Sierra?
3. ¿Qué son las marcas de sistema de archivos? ¿Dónde están las marcas en la interfaz de usuario?
4. ¿Cómo usa los metadatos el servicio de búsqueda de Spotlight?
5. ¿Dónde almacena Spotlight las bases de datos de los índices de metadatos y sus plug-ins?
6. ¿Cuáles son algunos de los problemas que Spotlight plantea para la privacidad y la seguridad?
7. ¿Cómo se puede resolver un problema cuando la búsqueda de Spotlight no encuentra los elementos correctos?
8. ¿Cómo puedes comprobar que Siri no envía grabaciones de audio a Apple?

Respuestas

1. Los metadatos son información que se ha almacenado fuera de un archivo o una carpeta. Proporcionan información adicional sobre ellos. Algunos ejemplos de metadatos son las marcas, los atributos de archivo ampliados y los permisos.
2. Entre las marcas de archivo frecuentes están la marca de bloqueo, que impide que se introduzcan cambios en los archivos, y la marca de oculto, que oculta el elemento en el Finder.
3. Las marcas del sistema de archivos son una clase de metadatos que permite asignar de forma rápida palabras clave, o “marcas”, a los elementos. Los usuarios pueden personalizar los nombres y los colores de las marcas.

4. El servicio de búsquedas Spotlight crea bases de datos de índices de los metadatos del sistema de archivos para poder ejecutar de forma instantánea búsquedas que, por lo general, llevan mucho tiempo. Las marcas del sistema de archivos están en la barra lateral del Finder, en la búsqueda de Spotlight y en los diálogos que se muestran al abrir o guardar documentos.
5. Las bases de datos de índices de metadatos de Spotlight se almacenan en la raíz de los volúmenes, en una carpeta denominada /.Spotlight-V100. Sin embargo, las bases de datos de los usuarios de FileVault Original se almacenan en la carpeta de inicio cifrada de los usuarios. Por su parte, la app Mail almacena su propia base de datos en la carpeta de inicio de cada usuario ~/Biblioteca/Mail/V2/MailData/Envelope Index. Los plug-ins de Spotlight se encuentran en las carpetas de la Biblioteca, en una carpeta denominada Spotlight.
6. Aunque Spotlight indexa los permisos de archivo y de carpeta, otros usuarios podrán buscar en el contenido de los volúmenes que no son del sistema y que se han anexado de forma local cuando no se tenga en cuenta la propiedad de esos volúmenes.
7. Si experimentas algún problema con las búsquedas de archivos locales, puedes hacer que Spotlight vuelva a generar las bases de datos de los índices. Para ello, elimina las bases de datos y vuelve a iniciar el ordenador o configura las preferencias de Spotlight, como veremos más adelante en esta lección.
8. Si no quieres que Siri envíe archivos de audio a Apple, desactiva el asistente en las preferencias del panel de Siri.

Lección 17: Gestionar Time Machine

Objetivos

- Describir Time Machine.
- Configurar Time Machine para que haga copias de seguridad de los datos.
- Restaurar datos o macOS a partir de una copia de seguridad de Time Machine.

Preguntas de repaso

1. ¿Qué clase de copias de seguridad puedes hacer con Time Machine?
2. ¿Qué discos para destinar las copias de seguridad se pueden usar con Time Machine?
3. ¿Cómo lleva Time Machine un historial de las copias de seguridad del sistema de archivos?
4. ¿Qué tipo de archivos no se incluyen en las copias de seguridad de Time Machine?
5. ¿Por qué no resulta práctico usar Time Machine para hacer copias de seguridad de bases de datos de gran tamaño?
6. ¿Qué función ayuda a Time Machine a restaurar los datos cuando el disco de copia de seguridad de Time Machine no está disponible?
7. ¿De qué cuatro formas diferentes se pueden restaurar los datos a partir de una copia de seguridad de Time Machine?

Respuestas

1. Time Machine permite hacer una copia de seguridad de todos los elementos del Mac, incluidos los archivos del sistema, apps, música, fotos, correos electrónicos y documentos.
2. El formato más utilizado es HFS Plus, pero los formatos Xsan están también admitidos. Las copias de seguridad se pueden hacer desde un disco con formato HFS Plus o APFS a uno HFS Plus; sin embargo, Time Machine no puede hacer una copia de seguridad en un disco con formato APFS.

3. Para ahorrar espacio, Time Machine omite los archivos que no necesitan una copia de seguridad, es decir, aquellos que se pueden volver a crear con una restauración. En términos generales, Time Machine omite los archivos temporales, los índices de Spotlight, los elementos que están en la Papelera y todo lo que pueda considerarse que está en la memoria caché.
4. Time Machine no es práctico con bases de datos que tienen un tamaño considerable porque tiene que hacer una copia de seguridad de todos los archivos de la base de datos cada vez que se produce algún cambio, por muy pequeño que sea, en la base de datos.
5. Los elementos de los que se haya hecho copia de seguridad con anterioridad no estarán disponibles si se ha llenado el volumen para las copias de seguridad y Time Machine ha tenido que eliminar los elementos más antiguos para liberar espacio.
6. Time Machine crea instantáneas locales en el disco de arranque integrado para poder usarlo cuando no está disponible el disco de copia de seguridad.
7. Hay varias maneras de restaurar elementos a partir de una copia de seguridad de Time Machine:
 - Restaurar algunos elementos específicos a partir de una copia de seguridad de Time Machine.
 - Ejecutar la restauración con el Asistente de Migración.
 - Restaurar el sistema entero con Recuperación de macOS.
 - Realizar una restauración manual con el Finder.

Parte quinta: Aplicaciones y procesos

Lección 18: Instalar apps

Objetivos

- Instalar apps desde el App Store.
- Describir el soporte técnico de las apps e identificar problemas de seguridad.
- Instalar apps con paquetes de software y la función de arrastrar y soltar.

Preguntas de repaso

1. ¿Cómo puedes instalar las apps que has comprado en un Mac en otro Mac que también utilices?
2. ¿Cuántos ID de Apple admiten los grupos En familia?
3. ¿Qué tecnologías usa el Mac para proteger a los usuarios cuando instalan apps de otros fabricantes?
4. ¿Qué dos opciones de seguridad se pueden usar con Gatekeeper? ¿Qué opción de Gatekeeper se usa de forma predeterminada en macOS High Sierra?
5. ¿Cómo se pueden instalar las apps que no están en el App Store?
6. ¿Qué tres procedimientos puedes usar para desinstalar las apps?

Respuestas

1. Si usas más de un Mac, puedes habilitar las descargas automáticas de las apps que has comprado en el otro Mac.
2. Los grupos En familia pueden tener un máximo de seis miembros.
3. Para proteger a los usuarios que instalen apps de otros fabricantes, el Mac usa estas tecnologías:
 - Seguridad de los procesos: se trata de mecanismos de seguridad, incluido SIP, que impiden acceder a los recursos si no se cuenta con autorización. Los privilegios para todo el sistema solo se otorgan cuando son necesarios.
 - Zona protegida (sandboxing) para las apps: las apps solo tienen acceso a los elementos que necesitan.
 - Firmas de código: el sistema las usa para comprobar la autenticidad y la integridad del software.
 - Cuarentena de los archivos: en la pantalla aparece un mensaje de aviso cuando se intenta abrir un elemento que se ha descargado de un recurso externo, como Internet, por ejemplo.
 - Detección de malware: macOS posee una lista de software malicioso conocido que se renueva de forma automática con cada actualización de software de macOS.
 - Gatekeeper: usa las firmas de código y pone los archivos en cuarentena para proteger el Mac frente a los ataques de apps maliciosas.
4. Gatekeeper admite las apps descargadas desde:
 - El App Store
 - El App Store y desarrolladores identificados (opción predeterminada)
5. Además del App Store, el software se puede instalar con la función de arrastrar y soltar o los paquetes de instalación.

6. Hay tres formas de desinstalar las apps:
 - a. Usando el Launchpad.
 - b. Arrastrando la app a la Papelera.
 - c. Usando un programa de desinstalación personalizado.

Lección 19: Gestionar documentos

Objetivos

- Usar las funciones de Launch Services y Vista Rápida para abrir documentos.
- Trabajar con apps que admiten las funciones Guardado automático y Versiones.
- Guardar y abrir documentos guardados en iCloud.
- Optimizar el almacenamiento local para tener más espacio en el volumen de sistema.

Preguntas de repaso

1. ¿Cómo se indica en macOS la app que tiene que abrirse al hacer doble clic en un documento?
2. ¿Cómo se inicia Vista Rápida? ¿Qué apps son compatibles con esta función?
3. ¿Qué tecnología permite a Vista Rápida mostrar tantas clases diferentes de archivo?
4. ¿Qué es Guardado automático? ¿Cómo puedes identificar las apps que admiten el Guardado automático?
5. ¿Cuál es el historial de versiones de un archivo que se puede ver cuando se comparte por correo electrónico?
6. ¿Qué apps pueden bloquear documentos?
7. ¿Dónde se pueden configurar las opciones de las funciones Guardado automático y Reanudar?
8. ¿Qué cambio de comportamiento se produce Cuando se actualiza de iCloud a iCloud Drive?
9. ¿Dónde se puede acceder a los elementos almacenados en iCloud Drive?
10. ¿Dónde deben guardarse los documentos en iCloud Drive para poder acceder a ellos desde un dispositivo iOS?
11. Si Escritorio y Documentos de iCloud Drive están activados en un Mac y los activas también en otro, ¿qué les sucede a las carpetas Escritorio y Documentos del usuario?
12. ¿Qué les sucede a las carpetas Escritorio y Documentos del usuario si se desactivan Escritorio y Documentos en iCloud?

Respuestas

1. macOS High Sierra usa la extensión del nombre de archivo del documento para determinar el tipo de documento. El proceso Launch Services tiene una base de datos de apps instaladas y los tipos de documento que pueden abrir.
2. Para iniciar Vista Rápida, es necesario presionar la barra espaciadora después de seleccionar un documento. Las apps compatibles con Vista Rápida son el Finder, Time Machine, Mail y la mayoría de los diálogos del navegador que aparecen al abrir y guardar archivos.
3. Vista Rápida usa plug-ins para poder abrir una vista previa de los documentos. En macOS High Sierra, estos plug-ins se encuentran en las carpetas de Vista Rápida de las carpetas de la Biblioteca.

4. La función Guardado automático permite a las apps compatibles con macOS High Sierra guardar de forma automática los cambios en los documentos de los usuarios. Los usuarios solo tienen que guardar el documento una vez y ya no tienen que volver a preocuparse. Las apps que admiten el Guardado automático muestran la función Duplicar en el menú Archivo en lugar de Guardar como, que es la función predeterminada.
5. Los documentos que se envíen por correo electrónico o que se copien de alguna otra forma en una ubicación compartida no mostrarán ningún historial de versiones.
6. Todas las apps que admitan la función de Guardado automático y el Finder pueden bloquear documentos.
7. Desmarcando la opción “Volver a abrir las ventanas al reiniciar la sesión” en el cuadro de diálogo para verificar el cierre de sesión. Lleva a cabo una de estas acciones en Panel de preferencias General:
 - Desmarca la opción “Cerrar las ventanas al salir de una app”.
 - Selecciona “Preguntar si se guardan los cambios al cerrar los documentos”. Esta opción desactiva el guardado automático.
8. Si se actualiza una cuenta de iCloud para poder usar iCloud Drive, no se podrá acceder directamente a los documentos desde OS X Yosemite 10.10 o versiones anteriores, o desde iOS 8 o versiones anteriores. Si se usa OS X Yosemite 10.10, se puede acceder a los elementos desde la página web de iCloud: www.icloud.com.
9. Los elementos de iCloud Drive están disponibles en el Finder o en las apps que usen los cuadros de diálogo estándar para abrir o guardar archivos en macOS.
10. Los dispositivos con iOS 8 o versiones posteriores podrán acceder a los documentos de iCloud Drive si están almacenados en determinadas carpetas de aplicación. Por ejemplo, Pages para iOS podrá acceder a los documentos de Pages si se han guardado en la carpeta Pages de iCloud Drive.
11. Si Documentos y Escritorio de iCloud se activan en otros Mac, el contenido incluido en las carpetas Escritorio y Documentos de esos ordenadores se moverá a unas subcarpetas dentro de las carpetas Documentos y Escritorio de iCloud. Por ejemplo, si se añade otro Mac que se llama “Mi Mac”, las carpetas Documentos y Escritorio contendrán las subcarpetas “Mi Mac - Escritorio” y “Mi Mac - Documentos”.
12. Cuando se desactiva Escritorio y Documentos en iCloud, los elementos se mueven a una subcarpeta de iCloud Drive, y las carpetas Escritorio y Documentos locales se crean como carpetas vacías para el usuario local. Los usuarios tendrán que ir a iCloud Drive y copiar de forma manual los archivos en las nuevas carpetas de Escritorio y Documentos, que estarán vacías.

Lección 20: Administrar y resolver problemas de las apps

Objetivos

- Describir y prestar soporte técnico a los distintos tipos de app.
- Administrar las extensiones de las apps y los widgets en el Centro de notificaciones.
- Supervisar y controlar procesos y apps.
- Analizar diferentes técnicas para solucionar problemas de las apps.

Preguntas de repaso

1. ¿Por qué resulta útil abrir una app en modo de 32 bits?
2. ¿Qué funcionalidad añaden las extensiones de app en macOS High Sierra?

3. ¿Cómo se pueden instalar nuevas extensiones de app? Y una vez instaladas, ¿cómo se gestiona la visibilidad de las extensiones?
4. ¿Cómo se pueden identificar las apps instaladas en un Mac?
5. En macOS High Sierra, ¿qué app debe usarse para ver las apps que están abiertas?
6. ¿Qué pasos debes seguir cuando soluciones los problemas de una app?
7. ¿De qué tres maneras puedes quitar de manera forzada una app de la interfaz gráfica?
8. ¿Para qué sirve la función de informes de diagnóstico?
9. ¿Dónde se almacenan las preferencias de las apps?
10. ¿Qué formato de archivo se utiliza normalmente con los archivos de preferencias? ¿Cómo se puede ver el contenido de este tipo de archivo?

Respuestas

1. Puedes forzar que una app se abra en modo de 32 bits en la ventana Información del Finder. Este paso es necesario para que las apps de 64 bits sean compatibles con los plug-ins de 32 bits y otros recursos de app antiguos.
2. Las extensiones de apps permiten que apps de distintos desarrolladores interactúen entre ellas como si estuvieran integradas en otra app.
3. Las extensiones se instalan automáticamente porque están empaquetadas en la app que proporciona la extensión. Las extensiones de app se pueden activar o desactivar desde las preferencias de Extensiones.
4. Puedes utilizar Información del Sistema para examinar las ubicaciones donde están las apps y obtener una lista de las que se encuentran instaladas.
5. Usa Monitor de Actividad para supervisar los procesos y las apps abiertos.
6. Estos son los pasos generales de solución de problemas de las apps:
 - a. Reiniciar la app.
 - b. Abrir otro documento que se sabe que se abre correctamente.
 - c. Probar con otra app.
 - d. Probar con otra cuenta de usuario.
 - e. Revisar los informes de diagnóstico y los archivos de registro.
 - f. Eliminar los archivos almacenados en la memoria caché.
 - g. Reemplazar los archivos de preferencias.
 - h. Reemplazar los recursos de las apps.
7. Estas son las tres maneras en que puedes quitar de manera forzada una app de la interfaz gráfica:
 - a. En el diálogo Forzar salida de las aplicaciones
 - b. En el Dock
 - c. En la app Monitor de Actividad
8. La función de informes de diagnóstico crea de forma automática un registro de informe de diagnóstico cuando una app se bloquea o se cuelga. El informe se puede ver de manera inmediata. Se envía a Apple a través de Internet. También puedes consultarlo más tarde en la carpeta Aplicaciones/Utilidades/Consola.

9. Las preferencias de aplicación se almacenan casi siempre en la carpeta de la biblioteca del usuario ~/Biblioteca/Preferencias. Las preferencias de las apps de zona preferida más recientes deben guardarse en la carpeta ~/Biblioteca/Contenedores/*ID del paquete*/Datos/Biblioteca/Preferencias, donde ID del paquete se refiere al identificador de paquete exclusivo para la app.
10. La mayor parte de las preferencias de app son listas de propiedades compuestas de archivos XML con la extensión de nombre de archivo .plist. El contenido de estos archivos se puede ver usando Vista Rápida y se pueden editar con la app de desarrollo Xcode, que está disponible en el App Store.

Parte sexta: Configuración de redes

Lección 21: Administrar ajustes de red básicos

Objetivos

- Describir los conceptos de las redes TCP/IP.
- Configurar y supervisar los ajustes de red.
- Conectarse a una red Wi-Fi.

Preguntas de repaso

1. ¿Qué es una dirección MAC?
2. ¿Para qué sirven las direcciones Internet Protocol v4 (IPv4) y las máscaras de subred?
3. ¿Cómo se construyen las direcciones IPv4?
4. ¿Cómo transfiere la IP mensajes entre ordenadores a través de una red de área amplia (WAN)?
5. ¿Cómo debe usarse el Sistema de nombres de dominio (DNS) para tener un sistema de resolución de nombres de red?
6. ¿Qué debe usarse para identificar una red Wi-Fi?
7. ¿Qué protocolos de autenticación Wi-Fi se pueden usar con macOS High Sierra?
8. ¿Cómo puede macOS High Sierra conectarse a una red Wi-Fi?

Respuestas

1. La dirección de control de acceso al medio (MAC) sirve para identificar una interfaz de red física en una red local.
2. La dirección IP identifica la ubicación de un dispositivo de red. Las direcciones IP son el identificador primario que usa la suite de protocolos de Internet TCP/IP con las redes LAN y WAN. Las máscaras de subred permiten a los dispositivos de red identificar su rango de red local y determinar si los datos de salida van dirigidos a un dispositivo de la red LAN.
3. La mayor parte de direcciones IP y máscaras de subred habituales comparten el formato IPv4. Las direcciones IPv4 son un número de 32 bits representado en cuatro grupos de tres dígitos, denominados octetos, y separados por un punto. Cada uno de los octetos tiene un valor que va de 0 a 255.
4. Los clientes de red usan la máscara de subred para determinar si la dirección IP de destino está en la red LAN. Si no están en la red, asume que la dirección de destino se encuentra en otra red y el cliente envía los datos a la dirección IP del router de red local. El router envía entonces los datos, a través de una conexión WAN, a otro router que considera que está más próximo al destino. Este proceso continúa en todas las conexiones WAN de un router a otro hasta que los datos alcanzan su destino.
5. El Sistema de nombres de dominio se usa para resolver un nombre DNS para las direcciones IP correspondientes.
6. El Identificador de conjunto de servicios, o SSID, sirve para identificar un nombre de red Wi-Fi y su configuración asociada.
7. macOS High Sierra admite redes Wi-Fi autenticadas y usa los siguientes protocolos para su verificación: WEP, WPA/WPA2 Personal y WPA/WPA2 Enterprise, que incluye la autenticación 802.1X.

8. Un Mac nuevo solo podrá conectarse automáticamente con redes Wi-Fi que no tengan ningún mecanismo de autenticación estándar, que se conoce como "red abierta". Sin embargo, un Mac configurado se puede volver a conectar automáticamente a redes Wi-Fi autenticadas, si se ha guardado la información adecuada en el sistema de Llavero.

Lección 22: Administrar ajustes de red avanzados

Objetivos

- Describir la arquitectura de configuración de red de macOS.
- Administrar varias ubicaciones de red e interfaces de servicio.
- Configurar ajustes avanzados de red.

Preguntas de repaso

1. ¿Qué es una ubicación de red? ¿Quién puede acceder a las ubicaciones de red?
2. ¿Qué interfaces y protocolos admite de forma predeterminada macOS High Sierra?
3. ¿Cómo afecta el orden de los servicios de red a la conectividad de red?
4. ¿Cómo puedes saber en las preferencias de Red qué interfaz se está usando con las diferentes actividades de red?
5. ¿Cuál es la forma más fácil de configurar los ajustes de VPN en macOS High Sierra?
6. ¿Cómo se configura el estándar 802.1X en el Mac?

Respuestas

1. Las ubicaciones de red son un estado almacenado de las preferencias de Red que contienen todos los ajustes de interfaz de red. Solo los administradores pueden definir las ubicaciones de red, pero si hay varias ubicaciones, todos los usuarios podrán cambiar entre ellas en el menú Apple.
2. macOS High Sierra admite las siguientes interfaces de red y protocolos:
 - La familia de estándares de interfaz de red de hardware IEEE 802.3 Ethernet
 - La familia de estándares de interfaz de red de hardware IEEE 802.11 para redes inalámbricas (Wi-Fi)
 - Interfaz de red en puente IEEE 1394 FireWire
 - Interfaz de red en puente Thunderbolt
 - Interfaz de red de hardware inalámbrica Bluetooth
 - Redes móviles que usan adaptadores USB o dispositivos iOS con servicio de red móvil (Compartir Internet)
 - Interfaz de red virtual para redes privadas virtuales (VPN) a través del protocolo Layer 2 Tunneling Protocol (L2TP) over Internet Protocol Security (IPSec); IPSec de Cisco; e Internet Key Exchange versión 2 (IKEv2)
 - Transmission Control Protocol/Internet Protocol (TCP/IP), también denominado suite de protocolos de Internet
 - Dynamic Host Configuration Protocol (DHCP)
 - Protocolo Domain Name System (DNS)
 - Protocolos Network Basic Input/Output System (NetBIOS) y Windows Internet Naming Service (WINS)
 - Ethernet autenticado con el protocolo 802.1X

3. La lista del orden de servicios de red se usa para determinar la interfaz de servicio de red primaria si hay más de un servicio activo. Todo el tráfico de red que no puede gestionarse adecuadamente a través de una conexión local con una interfaz de servicio de red activa se envía a la interfaz de servicio de red primaria. Por lo tanto, en la mayoría de los casos, todo el tráfico de la red WAN, el tráfico de Internet y las resoluciones DNS se envían a través de la interfaz de servicio de red primaria.
4. En las preferencias de Red, las interfaces de servicio de red que tienen un indicador de estado de color verde se usan en las actividades de red. Todo el tráfico de red que no se puede gestionar de forma adecuada a través de una conexión local se envía a la interfaz de servicio de red primaria. La interfaz de servicio de red primaria es la interfaz activa que ocupa el primer lugar de la lista.
5. La manera más sencilla de configurar los ajustes de VPN es usar un perfil de configuración que contenga toda la información de configuración de la red VPN pertinente.
6. macOS High Sierra usa dos métodos para configurar 802.1X:
 - a. Con una configuración automática, que consiste en seleccionar una red Wi-Fi que requiera autenticación WPA/WPA2 Enterprise
 - b. Con una configuración semiautomática, que consiste en usar un perfil de configuración 802.1X proporcionado por un administrador

Lección 23: Solucionar problemas de red

Objetivos

- Identificar y resolver problemas con la configuración de la red.
- Comprobar la configuración de red con la preferencias de Red.
- Usar Utilidad de Red como ayuda para resolver los problemas.

Preguntas de repaso

1. ¿Cuáles son los tres problemas más frecuentes que pueden detener los servicios de red en un Mac?
2. ¿Cómo se pueden identificar las direcciones MAC de todas las interfaces de red del Mac?
3. ¿Cómo se puede comprobar la conectividad básica con otro servidor en la red?
4. ¿Cómo se puede verificar que el nombre del host DNS es correcto?
5. ¿Cómo se puede comprobar si el sistema puede conectarse a un servidor de red remoto?

Respuestas

1. Los tres problemas que con más frecuencia pueden interrumpir los servicios de red en un Mac son:
 - a. Problemas locales: por lo general, se deben a que la red se ha configurado de forma incorrecta o a que se han perdido las conexiones de red.
 - b. Problemas de la red: usa los diagnósticos de red para que te ayuden a determinar las posibles causas.
 - c. Problemas de servicio: están relacionados con el dispositivo de red o el servicio al que se está intentando acceder.
2. Puedes ver en el panel Información de Utilidad de Red todas las direcciones Mac de las interfaces de red del ordenador.
3. Usa la pestaña Ping dentro de Utilidad de Red para comprobar la conectividad básica con otro host de red mediante el envío de un paquete de ping y esperando su vuelta.

4. Con la pestaña Lookup dentro de Utilidad de Red, podrás probar la resolución del nombre en el servidor DNS que tengas configurado.
5. La pestaña Traceroute dentro de Utilidad de Red te permite verificar los saltos de red entre el Mac y un servidor remoto.

Parte séptima: Servicios de red

Lección 24: Administrar servicios de red

Objetivos

- Describir cómo accede macOS a los servicios de red compartidos.
- Configurar apps de red de macOS integradas.
- Usar el Finder para navegar por los servicios de archivos de red y acceder a ellos.
- Resolver problemas con los servicios de red compartidos.

Preguntas de repaso

1. ¿Qué relación existe entre los clientes, los servidores y el acceso a los servicios de red?
2. ¿Qué relación hay entre un servicio de red y un puerto de red?
3. ¿Cuál es la interfaz primaria para configurar las apps de servicios de red?
4. ¿De qué manera usa macOS High Sierra los protocolos de descubrimiento dinámico de servicios de red para acceder a los servicios de red?
5. ¿Cuáles son los dos protocolos de descubrimiento dinámico de servicios de red que admite macOS High Sierra?
6. ¿Con qué cinco servicios de archivos de red puedes conectarse desde el cuadro de diálogo “Conectarse al servidor” del Finder?
7. ¿Cómo se incluyen los elementos en la carpeta Red del Finder?
8. ¿De qué dos maneras se puede conectar de forma automática a un recurso compartido de red?
9. Si no puedes conectarte a los servicios de red, ¿qué tres procedimientos de solución de problemas puedes usar?
10. ¿Cómo puedes comprobar que un servicio de red concreto está disponible en un proveedor de servicios?

Respuestas

1. Usa el software de cliente para acceder a los servicios de red proporcionados por el software de servidor. El software de cliente y el de servidor usan protocolos de red y estándares para comunicarse entre sí.
2. Los servicios de red se establecen usando un protocolo de red común. El protocolo especifica el número de puerto TCP o UDP que se usará en las comunicaciones.
3. La preferencia Cuentas de Internet es la interfaz primaria de macOS High Sierra para configurar apps de red integradas.
4. Los dispositivos que ofrecen un servicio de red anuncian su disponibilidad a través de un protocolo de descubrimiento dinámico de servicios de red. Los clientes que busquen estos servicios solicitarán y recibirán esta información para proporcionar al cliente una lista de las opciones de servicios de red disponibles.
5. macOS High Sierra admite Bonjour y Server Message Block (SMB) y también los protocolos dinámicos de descubrimiento de servicios de red antiguos Network Basic Input/Output System (NetBIOS) y Windows Internet Naming Service (WINS).

6. El cuadro de diálogo Conectarse al servidor del Finder permite conectarse a estos servicios y sistemas:
 - Server Message Blocks/Common Internet File System (SMB/CIFS)
 - SMB2/SMB3
 - Apple File Protocol (AFP)
 - Network File System (NFS)
 - Web-based Distributed Authoring and Versioning (WebDAV)
 - Servicios de archivos de red File Transfer Protocol (FTP)
7. El Finder rellena los elementos de la carpeta Red usando la información que proporcionan los protocolos de descubrimiento dinámico de servicios de red. Los ordenadores que ofrecen servicios aparecen como recursos dentro de la carpeta Red y las zonas de descubrimiento de servicios o los grupos de trabajo aparecen como carpetas. Todos los servidores conectados en ese momento aparecerán también en la carpeta Red.
8. Para que al iniciar sesión en el sistema un usuario se conecte automáticamente a un recurso compartido de archivos, arrastra el recurso desde el Finder a las opciones de inicio de sesión de ese usuario en las preferencias del panel Usuarios y grupos. También puedes arrastrar el recurso compartido a la derecha del Dock del usuario y se conectará cuando el usuario haga clic en el icono del recurso compartido en el Dock.
9. Revisa las preferencias del panel Red y las estadísticas de Utilidad de Red e intenta conectarte a distintos servicios de red.
10. Para comprobar si un determinado servicio de red está disponible en un proveedor de servicios, usa primero la pestaña Ping de Utilidad de Red para comprobar la conectividad básica. A continuación, usa la pestaña Port Scan de Utilidad de Red para comprobar si están abiertos los puertos de servicio específicos. Debes limitar siempre la exploración de puertos a aquellos que necesite específicamente el servicio de red que quieras probar.

Lección 25: Administrar el uso compartido de servidores y el firewall personal

Objetivos

- Examinar y activar los servicios de uso compartido de servidores integrados en macOS.
- Examinar y activar los servicios de almacenamiento en caché integrados en macOS.
- Usar las herramientas de compartir pantalla para acceder a otros servidores de red.
- Usar AirDrop para compartir archivos de forma rápida y sencilla.
- Configurar un firewall personal para proteger los servicios compartidos.
- Resolver problemas con los servicios compartidos.

Preguntas de repaso

1. ¿Qué servicios compartidos puede proporcionar macOS High Sierra?
2. ¿Qué es el almacenamiento en caché de contenido?
3. ¿Qué app puede ofrecer uso compartido de la pantalla a petición aunque el servicio Compartir pantalla no se haya activado?
4. ¿Qué servicio de red o servicios se comparten en Compartir pantalla en macOS High Sierra?

5. ¿Qué es AirDrop y cómo se puede saber si se puede usar en un Mac concreto?
6. Si en el navegador de AirDrop no aparecen otros dispositivos que lo tienen activado, ¿qué ajustes del Mac se pueden cambiar para que aparezcan más dispositivos en principio?
7. ¿Cuál es la diferencia básica entre el firewall integrado en macOS de un firewall de red tradicional?
8. ¿Cuáles son los ajustes de configuración del firewall en macOS High Sierra?

Respuestas

1. Estos son los servicios compartidos en macOS:
 - Disco remoto (uso compartido del DVD o del CD)
 - Compartir Pantalla
 - Compartir Archivos
 - Compartir impresora (y escáner)
 - Sesión Remota
 - Gestión Remota (ADR)
 - Eventos Apple Remotos
 - Compartir Internet
 - Compartir Bluetooth
 - Almacenamiento en caché
2. El almacenamiento en caché de contenido es la descarga de software distribuido por Apple y de datos almacenados por los usuarios en iCloud guardando el contenido que ya han descargado los dispositivos locales.
3. La app Mensajes ofrece uso compartido de la pantalla a petición; podrás usarlo cuando no esté activado el servicio compartir pantalla en el sistema.
4. En macOS High Sierra, el uso compartido de la pantalla en Mensajes requiere iMessage. Los usuarios de los dos ordenadores Mac tienen que iniciar sesión en iCloud.
5. AirDrop ofrece una manera fácil y rápida de compartir archivos dentro del alcance de la conexión Bluetooth y Wi-Fi. AirDrop crea una red P2P segura entre dispositivos locales. En el menú Ir del Finder, puedes comprobar si el Mac usa AirDrop.
6. En el último modelo de Mac, hay dos ajustes en la parte de abajo del navegador de AirDrop que controlan la función de descubrimiento de AirDrop. El primer ajuste amplía el descubrimiento de AirDrop de los usuarios que están en tus Contactos a cualquiera que esté dentro del alcance de AirDrop. El segundo ajuste revierte AirDrop al método de descubrimiento anterior y permite al Mac descubrir ordenadores Mac antiguos y los Mac que ejecuten versiones anteriores de los sistemas operativos para el Mac.
7. Con el firewall integrado en macOS High Sierra, las conexiones se aceptan o se rechazan una por una. En ese sentido, se diferencia de los firewalls tradicionales en los que las reglas de acceso se basan en los números de puertos de servicio de red.
8. El firewall en macOS High Sierra está configurado para:
 - Bloquear todas las conexiones entrantes.
 - Permitir de forma automática recibir conexiones entrantes al software integrado.
 - Permitir de forma automática recibir conexiones entrantes al software con firma descargado.
 - Activar el modo encubierto.

Parte octava: Gestión del sistema

Lección 26: Resolver problemas con los periféricos

Objetivos

- Gestionar la conectividad de los dispositivos periféricos.
- Enlazar dispositivos Bluetooth con el Mac.
- Resolver problemas con los dispositivos periféricos y los drivers.

Preguntas de repaso

1. ¿Cuáles son las cuatro tecnologías de bus principales para dispositivos periféricos que admiten los ordenadores Mac con macOS Sierra?
2. ¿Qué es necesario que suceda para que un Mac se comunique con un dispositivo periférico Bluetooth? ¿Dónde se configura este enlace?
3. ¿Qué son los drivers de dispositivo? ¿Cuáles son las tres clases principales de driver?
4. ¿Cómo obtiene compatibilidad macOS High Sierra con dispositivos de otros fabricantes sin necesitar drivers de dispositivo de terceros?
5. ¿Qué puedes deducir de un dispositivo periférico si no aparece en la app Información del Sistema?

Respuestas

1. Las cuatro tecnologías de bus principales que admite macOS High Sierra son:
 - a. Universal Serial Bus (USB)
 - b. FireWire
 - c. Conexión Bluetooth inalámbrica
 - d. Thunderbolt
2. Para que se produzca la comunicación, es necesario enlazar los dispositivos Bluetooth. El enlace del Mac con los dispositivos periféricos Bluetooth debe hacerse en las preferencias de Bluetooth de la app Preferencias del Sistema. Se puede acceder rápidamente a las preferencias de Bluetooth desde el menú de estado de Bluetooth.
3. Los controladores de dispositivo son un tipo de software diseñado especialmente para facilitar la comunicación entre macOS High Sierra y los dispositivos periféricos. Las tres clases principales de driver son:
 - a. Extensiones de kernel
 - b. Plug-ins de estructura
 - c. Apps independientes
4. macOS High Sierra usa drivers genéricos integrados en función de cada clase de dispositivo. Por ejemplo, se pueden usar drivers genéricos con escáneres e impresoras en lugar de los drivers oficiales de otros fabricantes.
5. Si un periférico conectado no aparece en Información del Sistema, probablemente se deba a un problema de hardware. Habrá que resolver el problema por tanto.

Lección 27: Gestionar impresoras y escáneres

Objetivos

- Describir las tecnologías que activan la función de impresión en macOS.
- Configurar macOS para impresoras y dispositivos que no funcionan correctamente.
- Administrar y solucionar problemas con los trabajos de impresión.

Preguntas de repaso

1. ¿Qué es Common UNIX Printing System (CUPS)?
2. ¿Para qué sirven los archivos PostScript Printer Description (PPD)?
3. ¿Cuál es el mejor sitio para obtener drivers de impresora para macOS High Sierra?
4. ¿En qué circunstancias puede un usuario normal (es decir, que no es administrador) configurar una impresora?
5. ¿Cómo se pueden compartir impresoras con otros usuarios?
6. ¿Cómo se selecciona un driver de impresora nuevo para una impresora configurada?
7. Si todas las impresoras configuradas parecen tener problemas, ¿cómo podría solucionarse rápidamente?

Respuestas

1. Common UNIX Printing System (CUPS) gestiona las impresiones en macOS High Sierra, tanto las impresiones desde recursos compartidos como de forma local.
2. Los archivos PostScript Printer Description (PPD) son archivos de controladores de impresora que indican al sistema CUPS cómo debe comunicarse con determinados modelos de impresora.
3. Los controladores de impresión de Apple son la fuente más adecuada para configurar impresoras en macOS High Sierra. Una forma de obtener los controladores de impresora para macOS High Sierra es dejar que el sistema de actualización de software descargue e instale de forma automática los controladores de impresora adecuados. También, se pueden descargar estos drivers en la página web del Soporte técnico de Apple e instalarlos de forma manual.
4. Si damos por supuesto que se ha seleccionado los ajustes de configuración predeterminados de macOS High Sierra, los usuarios normales solo podrán configurar en el cuadro de diálogo Imprimir las impresoras que estén conectadas directamente al ordenador o las que estén dentro de la red local. Además, es preciso que estén instalados los drivers correctos para que los usuarios normales puedan configurar la impresora.
5. El uso compartido de la impresora se puede activar en las preferencias de los paneles panel Imprimir y escanear o Compartir. Es posible que los clientes Windows necesiten drivers adicionales para acceder a las impresoras compartidas del Mac con el protocolo IPP (Internet Printing Protocol).
6. Depende de la impresora. El cuadro de diálogo Opciones y recambios de las preferencias del panel Imprimir y escanear permite en algunas ocasiones seleccionar un nuevo driver de impresora. En muchos casos, para seleccionar un controlador de impresora nuevo para una impresora configurada, tendrá que eliminar la impresora y añadirla otra vez.
7. Si hay problemas con las impresoras, haz Control + clic en la lista de impresoras y selecciona la opción Restablecer sistema de impresión.

Lección 28: Resolver problemas del sistema y con el arranque

Objetivos

- Describir el proceso de arranque de macOS.
- Analizar los archivos esenciales y los procesos necesarios para que el arranque sea correcto.
- Conocer los diferentes modos de arranque de macOS.
- Resolver problemas con el arranque y el inicio de sesión.

Preguntas de repaso

1. ¿Cuáles son las principales fases de inicialización del sistema en macOS High Sierra? ¿Qué señales visuales y acústicas proporcionan estas fases?
2. ¿Para qué sirve el firmware? ¿Qué es Power-On Self-Test (POST)?
3. ¿Para qué sirve `launchd` durante el arranque del Mac?
4. ¿Qué elementos inicia de forma automática `launchd` al arrancar el Mac?
5. ¿Cuáles son las principales fases de sesión de usuario en macOS High Sierra? ¿Qué señales visuales y acústicas proporcionan estas fases?
6. ¿Qué diferencia hay entre los clientes de inicio, los elementos de arranque, los agentes de inicio y los elementos de inicio de sesión?
7. ¿Qué son el reposo seguro y Power Nap?
8. ¿Qué pasa cuando el usuario cierra la sesión?
9. ¿Qué pasa cuando se apaga el Mac?
10. ¿Qué función rápida de teclado se puede usar para arrancar el ordenador en modo seguro?
11. ¿Qué función rápida de teclado se puede usar de forma temporal para seleccionar otro disco de arranque?
12. ¿Qué cambios se producen cuando se inicia macOS High Sierra en modo seguro?
13. ¿Qué elementos no se cargan cuando se inicia macOS High Sierra en modo seguro?

Respuestas

1. Cada fase principal del arranque del sistema se puede indicar con una de estas señales;
 - a. Firmware: encendido. Power On Self Test (POST). Sonido de campanilla de arranque (en función del modelo).
 - b. Booter: el proceso de arranque se inicia. El logotipo de Apple se muestra en el centro de la pantalla principal.
 - c. Kernel: inicio del Kernel. Se muestra la barra de progreso.
 - d. System `launchd`: iniciando los demás elementos. El logotipo de Apple se sustituye por la ventana de inicio de sesión.
2. El firmware inicia el hardware del ordenador Mac y localiza el archivo de inicio en un volumen de sistema. Cuando se enciende un Mac, el POST comprueba el funcionamiento básico del hardware.
3. `launchd` se encarga de iniciar los procesos de macOS High Sierra. También se encarga de la inicialización de macOS High Sierra e inicia el proceso `loginwindow`.
4. Durante la fase de arranque de macOS High Sierra, `launchd` inicia los siguientes clientes y scripts:
 - `/Sistema/Biblioteca/LaunchDaemons`
 - `/Biblioteca/LaunchDaemons`

5. Cada fase principal de una sesión de usuario se puede indicar con estas señales:
 - a. Se muestra la pantalla de inicio de sesión.
 - b. `launchd` carga las apps, como el Finder, una vez autenticado el usuario.
 - c. El entorno de usuario está activo siempre que un usuario inicia sesión en macOS High Sierra.
6. El proceso `launchd` de la cuenta de administrador inicia los clientes y los ítems de arranque durante la fase de inicio del Mac. Los procesos `launchd` de la cuenta de usuario arrancan los agentes y los elementos de inicio de sesión durante el arranque del entorno.
7. Cuando un Mac se queda sin batería, el modo de reposo seguro guarda el estado de macOS High Sierra en una ubicación de almacenamiento permanente. Power Nap permite al Mac reanudarse en modo de bajo consumo. Esto permite al Mac ejecutar actualizaciones de apps y de macOS High Sierra.
8. Cuando el usuario cierra la sesión, el proceso `loginwindow` del usuario lleva a cabo lo siguiente:
 - a. Solicita a las apps de ese usuario que se cierren
 - b. Sale automáticamente de los procesos en segundo plano del usuario
 - c. Ejecuta scripts de cierre de sesión
 - d. Registra el cierre de sesión en el archivo `system.log` principal
 - e. Restablece los permisos de dispositivo y las preferencias a sus valores predeterminados
 - f. Sale de los procesos `loginwindow` y `launchd` del usuario
9. Cuando se apaga el Mac, el proceso `loginwindow` hace que salgan los usuarios y después le indica al kernel que salga de los procesos restantes de macOS High Sierra. Después, el Mac se apaga.
10. Mantén pulsada la tecla Mayúsculas durante el arranque para iniciar el ordenador en modo seguro.
11. Mantén pulsada la tecla Opción durante el arranque para abrir el gestor de arranque. El gestor te permitirá seleccionar de forma temporal otro disco de arranque.
12. El arranque en modo seguro ejecuta estas acciones permanentes:
 - a. Intenta reparar la estructura del volumen de sistema
 - b. Elimina las cachés de extensiones de kernel de terceros (KEXT)
 - c. Borra las cachés de tipos de letra
13. Cuando macOS High Sierra arranca en modo seguro, no carga los KEXT, los agentes de inicio de otros fabricantes, los clientes de inicio de otros fabricantes, los ítems de arranque de otros fabricantes, los tipos de letra de otros fabricantes, los elementos de inicio de sesión de usuario ni los agentes de inicio específicos de usuario.