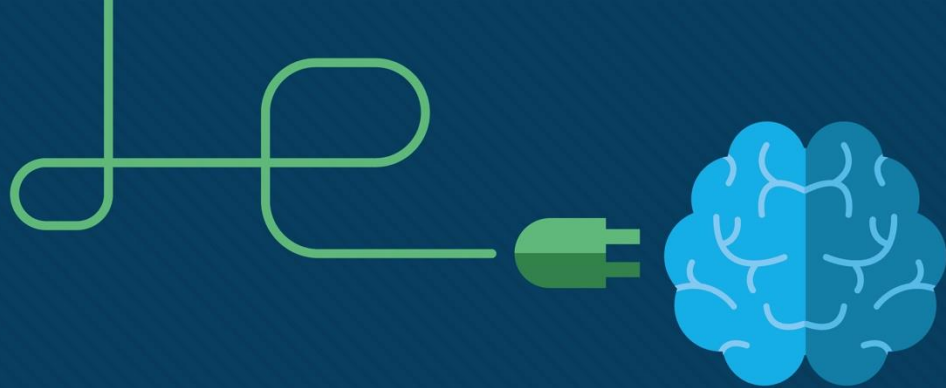




Capítulo 12: Sistemas operativos móviles, Linux y macOS

IT Essentials v7.0



Capítulo 12: Secciones y objetivos

▪ 12.1 Sistemas operativos móviles

Explicar el propósito y las características de los sistemas operativos móviles.

- Compare los sistemas operativos Android e iOS.
- Describa las características de la interfaz táctil Android.
- Describa las características de la interfaz táctil de iOS.
- Describa las características de la interfaz táctil de Windows.
- Describa las características del sistema operativo que son comunes entre los dispositivos móviles.

▪ 12.2 Métodos para proteger los dispositivos móviles

Explicar los métodos para asegurar los dispositivos móviles.

- Explique cómo configurar diversos tipos de bloqueos de contraseña.
- Describa los servicios habilitados para la nube para dispositivos móviles
- Describa la seguridad del software para dispositivos móviles.

Capítulo 12: Secciones y objetivos (continuación)

▪ 12.3 Sistemas operativos Linux y Mac

Explique la finalidad y las características de los sistemas operativos Linux y Mac.

- Describa las herramientas y características de los sistemas operativos Linux y Mac.
- Describa las prácticas recomendadas para Linux y OS X
- Defina los comandos CLI básicos.

▪ 12.4 Proceso básico de solución de problemas para otros sistemas operativos

Explicar cómo solucionar los problemas de otros sistemas operativos.

- Explique los seis pasos para resolver problemas de otros sistemas operativos.
- Describa problemas y soluciones comunes para otros sistemas operativos

12.1 Sistemas operativos móviles

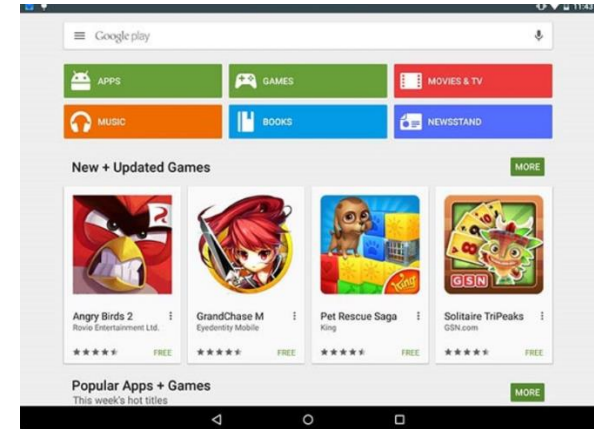
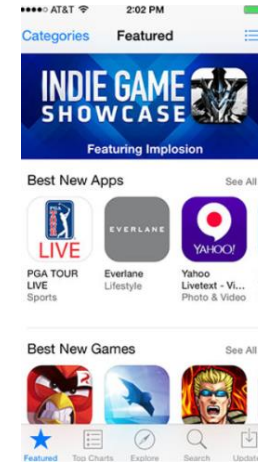
Código abierto frente a código cerrado

- Tal como las computadoras de escritorio y las portátiles, los dispositivos móviles utilizan un sistema operativo (SO) para ejecutar el software.
- Antes de que los usuarios puedan analizar y modificar el software, deben poder ver el código fuente.
 - Cuando el desarrollador elige proporcionar el código fuente, se dice que el software es de código abierto.
 - Si el código fuente del programa no se publica, se dice que el software es de código cerrado.
- Android fue creado por Google e iOS, por Apple.



Fuentes de aplicaciones y contenido

- Las aplicaciones se escriben y compilan para un sistema operativo móvil específico, como Apple iOS, Android o Windows.
- Estos traen una variedad de aplicaciones preinstaladas, a fin de proporcionar una funcionalidad básica.
 - Existen aplicaciones para hacer llamadas telefónicas, enviar y recibir correo electrónico, escuchar música, tomar fotografías, reproducir videos y jugar videojuegos.
- En lugar de instalarse desde un disco óptico, las aplicaciones se descargan desde una fuente de contenido.

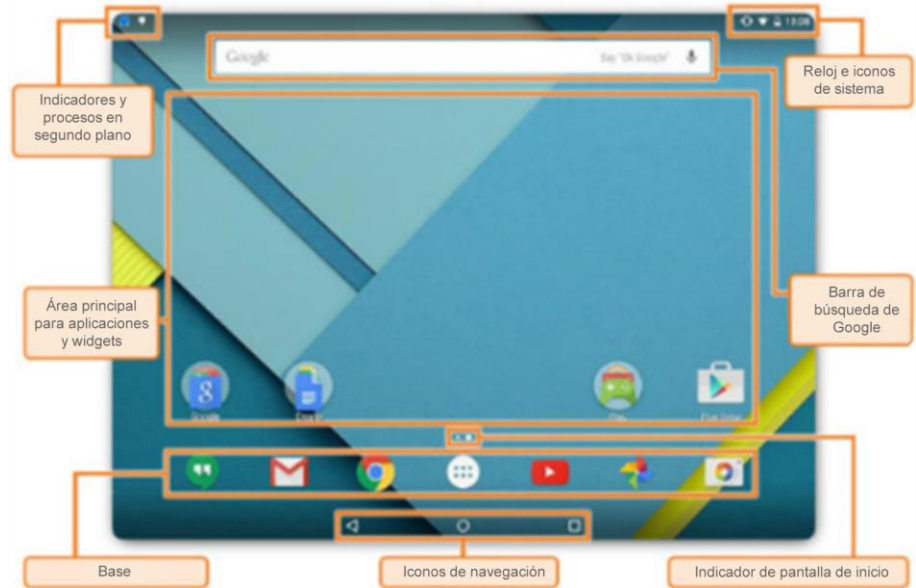


Fuentes de aplicaciones y contenido (cont.)

- Las aplicaciones para dispositivos móviles Apple con iOS se consiguen de forma gratuita o paga en la App Store.
- Apple usa un modelo de jardín de pared para sus aplicaciones, lo que significa que las aplicaciones deben enviarse y estar aprobadas por Apple antes de que se lancen a los usuarios.
 - Esto ayuda a evitar la propagación de malware y código malicioso.
- Las aplicaciones de Android se consiguen en Google Play™ y sitios de terceros, como la App Store de Amazon.
- Las aplicaciones de Android se ejecutan en un sandbox y solo tienen los privilegios habilitados por el usuario.
- Los programas de terceros o personalizados se instalan directamente mediante un archivo de paquete de aplicación de Android (apk).
 - Esto permite a los usuarios instalar aplicaciones directamente sin pasar por la interfaz de la tienda de aplicaciones, y se conoce como Transmisiones.

Elementos de la pantalla de inicio

- Pantalla de inicio principal de Android
 - Una pantalla se designa como pantalla de inicio.
 - Para acceder a las pantallas, se debe deslizar la pantalla de inicio hacia la izquierda o la derecha.
- Íconos de navegación
 - El SO Android® utiliza la barra de sistema para explorar las aplicaciones y pantallas.
 - La barra de sistema contiene los siguientes botones:
 - Atrás
 - Inicio
 - Aplicaciones recientes
 - Menú



Elementos de la pantalla de inicio (cont.)

- Íconos de notificación y de sistema
 - Cada dispositivo Android® tiene un área con íconos de sistema, como el reloj, el estado de la batería y el estado de Wifi y de las redes del proveedor.
 - Las aplicaciones como las de correo electrónico, mensajería de texto y Facebook® suelen mostrar íconos de estado para indicar la actividad de comunicación.
- Para abrir el área de notificación en dispositivos con Android®, deslice hacia abajo desde la parte superior de la pantalla.
 - Puede realizar lo siguiente cuando las notificaciones están abiertas:
 - Responder a una notificación tocándola.
 - Descartar una notificación deslizándola hacia fuera de la pantalla para cualquiera de los lados.
 - Descartar todas las notificaciones con el icono.
 - Alternar entre las configuraciones de uso frecuente.
 - Ajustar el brillo de la pantalla.
 - Abrir el menú Configuración con el icono de configuración rápida.

Práctica de laboratorio: trabajar con Android

En esta práctica de laboratorio, colocará aplicaciones y widgets en la pantalla de inicio y los moverá entre distintas pantallas. También creará carpetas. Por último, instalará y desinstalará aplicaciones del dispositivo Android.

Elementos de la pantalla de inicio

▪ Interfaz de iOS

- La interfaz de iOS® funciona de manera similar a la interfaz de Android®, pero existen diferencias muy importantes.
 - No hay íconos de navegación: en lugar de tocar íconos de navegación, se puede tener que presionar un botón físico.
 - No hay widgets: en las pantallas de los dispositivos iOS®, solo se pueden instalar aplicaciones y demás contenido.
 - No hay accesos directos: Las aplicaciones en la pantalla de inicio no son accesos directos, sino aplicaciones en sí mismas.

▪ Botón de inicio

- A diferencia de Android®, los dispositivos iOS® no utilizan íconos de navegación para llevar a cabo funciones.
- Algunas de las funciones comunes que realiza el botón de inicio son las siguientes:
 - **Active el dispositivo**
 - **Vuelva a la pantalla de inicio.**
 - **Inicie Siri® o el control por voz.**

Elementos de la pantalla de inicio (cont.)

- Centro de notificación de iOS
 - Los dispositivos iOS® tienen un centro de notificación que muestra todas las alertas en una ubicación.
- Configuraciones de uso frecuente
 - Los dispositivos iOS® permiten que el usuario tenga acceso rápidamente a las configuraciones y los switches comunes, aun si están bloqueados.
 - Desde la pantalla de configuración de uso frecuente, un usuario puede:
 - Alternar las configuraciones de uso frecuente, como el modo de avión, Wifi, Bluetooth, el modo de no molestar y el bloqueo de rotación de pantalla
 - Ajustar el brillo de la pantalla
 - Controlar el reproductor de música
 - Acceder a Airdrop
 - Acceder a la linterna, el reloj, el calendario y la cámara
- Spotlight de iOS
 - Spotlight muestra sugerencias de muchas fuentes, por ejemplo, Internet, iTunes®, App Store, horarios de películas y ubicaciones cercanas.

Práctica de laboratorio: trabajar con iOS

En esta práctica de laboratorio, ubicará aplicaciones en la pantalla de inicio y las moverá a distintas pantallas de inicio. También creará carpetas. Por último, instalará una aplicación en el dispositivo iOS y la desinstalará.

Orientación de la pantalla

- Orientación de la pantalla
 - La mayoría de los dispositivos móviles se pueden utilizar en el modo vertical u horizontal.
 - Un sensor interno denominado acelerómetro detecta cómo se está sosteniendo el dispositivo y, con esa información, decide la orientación de la pantalla.
 - Cuando el dispositivo se cambia al modo horizontal, la aplicación de la cámara también adopta ese modo.
 - Algunos dispositivos poseen giroscopios para detectar mejor el movimiento.
 - Los giroscopios permiten que el dispositivo se utilice como mecanismo de control en los juegos de autos en los que el propio dispositivo actúa como volante.
- Configuración de la rotación automática de pantalla de Android
 - Al utilizar un dispositivo Android, para habilitar la rotación automática, vaya a Configuración > Pantalla > Opciones avanzadas > Pantalla de rotación automática.
- Configuración de la rotación automática de pantalla de iOS
 - Al utilizar un dispositivo iOS, para habilitar la rotación automática, deslice el dedo hacia arriba desde la parte inferior de la pantalla y pulse el ícono de candado.

Calibración de la pantalla

- Calibración de la pantalla
 - Cuando la luz solar dificulta la lectura de la pantalla, aumente el brillo.
 - En cambio, si lee un libro en un dispositivo móvil por la noche, le será útil disminuir el brillo.
 - Algunos dispositivos móviles se pueden configurar para que el brillo se ajuste de manera automática según la cantidad de luz del entorno.
 - Para esto, el dispositivo debe contar con un sensor de luz.
- Menú de brillo en Android
 - En los dispositivos con Android, para configurar el brillo de la pantalla, vaya Configuración > Pantalla > Brillo, y ajuste el brillo en el nivel deseado.
- Menú de brillo y pantalla en iOS
 - En los dispositivos con iOS, para configurar el brillo de la pantalla, deslice hacia arriba desde la parte inferior de la pantalla y mueva la barra de brillo hacia arriba o hacia abajo para modificarlo.

GPS

- GPS
 - El Sistema de posicionamiento global (GPS) es un sistema de navegación que determina la hora y la ubicación del dispositivo por medio de mensajes que se envían desde satélites espaciales y de un receptor en la Tierra.
 - El receptor de radio de un GPS utiliza, al menos, cuatro satélites para calcular la posición de este según los mensajes.
 - Los servicios de GPS permiten que los distribuidores de aplicaciones y el sitio web conozcan la ubicación de un dispositivo y ofrezcan servicios específicos para la ubicación, lo que se denomina geotracking.
 - Los sistemas de posicionamiento interior (IPS) pueden determinar la ubicación del dispositivo al triangular su proximidad a otras señales de radio, como puntos de acceso Wi-Fi.
- Servicios de ubicación de Android
 - Para activar el GPS en dispositivos con Android, utilice Configuración > Ubicación > Tocar la opción para activar los servicios de ubicación.
- Servicios de ubicación de iOS
 - Para activar el GPS en dispositivos con iOS, utilice Configuración > Privacidad > Servicios de ubicación > Activar servicios de ubicación.

Práctica de laboratorio: características de los dispositivos móviles

En esta práctica de laboratorio, aprenderá sobre las características de los dispositivos móviles.

Llamada Wifi

▪ Llamada Wifi

- En lugar de utilizar la red de un proveedor de servicios de telefonía móvil, los smartphones modernos pueden utilizar Internet para transportar las llamadas de voz aprovechando una zona de cobertura Wifi local.
- Si no hay una zona de cobertura wifi dentro del alcance, el teléfono utilizará la red de un proveedor de servicios de telefonía móvil para transportar las llamadas de voz.
- La llamada wifi es muy útil en áreas con escasa cobertura de celulares, ya que utiliza una zona de cobertura wifi para cubrir las brechas.
- La zona de cobertura Wifi debe garantizar una velocidad de al menos 1 Mbps para que la calidad de la llamada sea óptima.

▪ Llamadas a través de una red wifi en Android

- Para activar las llamadas Wifi en Android, vaya a **Configuración > Más** (en la sección de conexión inalámbrica y redes) > **Llamadas Wifi** > Toque para activar la opción.

▪ Habilitación de llamadas a través de una red wifi en iOS

- Para habilitar la llamada Wifi en iOS, vaya a **Configuración > Teléfono** y active las llamadas Wifi.

Pago NFC

- Los pagos móviles son los pagos realizados a través de un teléfono móvil.
 - **Pagos transaccionales basados en SMS premium:** los consumidores envían un mensaje SMS al número de teléfono especial de un proveedor que contiene una solicitud de pago, y se informa al vendedor de que se ha recibido el pago y tiene autorización para enviar los productos.
 - **Facturación móvil directa:** Usando una opción móvil de facturación durante el pago, un usuario se identifica (generalmente con una autenticación con dos factores) y permite agregar el cobro en la factura de servicios móviles.
 - **Pagos web móviles:** El consumidor utiliza la red o las aplicaciones dedicadas para completar la transacción.
 - **NFC sin contacto (comunicación de campo cercana):** este método se utiliza principalmente en transacciones de almacenamiento físico en las que un consumidor paga por productos o servicios moviendo el teléfono cerca del sistema de pago.

Características comunes de dispositivos móviles

red privada virtual

- Una red privada virtual (VPN) es una red privada que utiliza una red pública (por lo general, Internet) para conectar sitios o usuarios remotos entre sí.
- Muchas empresas crean sus propias redes privadas virtuales (VPN) para satisfacer las necesidades de los trabajadores remotos y las oficinas lejanas.
 - Cuando se establece una VPN de un cliente a un servidor, el cliente accede a la red detrás del servidor, como si estuviera conectado directamente a esa red.
 - Debido a que los protocolos de VPN también permiten el cifrado de datos, la comunicación entre el cliente y el servidor es segura.
- Configuración de una conexión VPN en Android
 - Para crear una nueva conexión de VPN en Android, vaya a **Configuración > Más** (en la sección de conexión inalámbrica y redes) > **VPN** > Toque el signo + para agregar una conexión de VPN.
- Configuración de una conexión VPN en iOS
 - Para crear una nueva conexión de VPN en iOS, vaya a **Configuración > General > VPN > Agregar configuración VPN**.

Asistentes virtuales

- Un asistente digital, a veces denominado asistente virtual, es un programa que puede comprender el lenguaje conversacional natural y realizar tareas para el usuario final.
 - Estos asistentes digitales dependen de la inteligencia artificial, el aprendizaje automático y tecnología de reconocimiento de voz para comprender los controles por voz de estilo conversacional.
 - Emparejando las solicitudes simples de voz con otros datos, como la ubicación de GPS, estos asistentes pueden realizar varias tareas, entre ellas reproducir una canción específica, ejecutar una búsqueda en Internet, tomar una nota o enviar un correo electrónico.
- Google Now
 - Para acceder a Google Now en un dispositivo con Android, simplemente diga "OK Google" y Google Now se activará y comenzará a escuchar sus órdenes.
- Siri
 - Para acceder a Siri en un dispositivo iOS, mantenga presionado el botón de **Inicio** y Siri se activará y comenzará a escuchar las solicitudes.
 - También se puede configurar Siri para que comience a escuchar al decir "Hola, Siri".

12.2 Métodos para proteger los dispositivos móviles

Práctica de laboratorio: bloqueos de contraseña

En esta práctica de laboratorio, establecerá un bloqueo de contraseña, cambiará una contraseña y producirá un error de autenticación de contraseña. También debe configurar el dispositivo para que use sus huellas digitales si tiene capacidad biométrica. Por último, debe eliminar la contraseña y los bloqueos biométricos

Restricciones por intentos fallidos de inicio de sesión

- Para desbloquear un dispositivo móvil cuando se configuró un código de acceso, es necesario introducir el PIN, la contraseña, el patrón u otro tipo de código de acceso correcto.
 - Teóricamente, una contraseña, como un PIN, podría llegar a adivinarse si se cuenta con el tiempo y la perseverancia suficientes.
- Para evitar que alguien intente adivinar una contraseña, los dispositivos móviles pueden configurarse para llevar a cabo determinadas acciones tras cierta cantidad de intentos fallidos.
 - Es común que los dispositivos Android se bloqueen cuando se introduce una contraseña incorrecta entre 4 y 12 veces.
 - Una vez bloqueado el dispositivo, es posible desbloquearlo introduciendo la información de la cuenta de Gmail que se utilizó para configurar el dispositivo.
- Datos de borrado de iOS
 - Si la contraseña falla 10 veces, la pantalla se va a negro y se eliminan todos los datos del dispositivo.
 - Para restaurar el dispositivo y los datos de iOS, use la opción de restauración y copia de respaldo en iTunes o iCloud.
- GUI de iOS
 - En iOS, para mejorar la seguridad, la contraseña se utiliza como parte de la clave de cifrado para todo el sistema.

Copia de respaldo remota

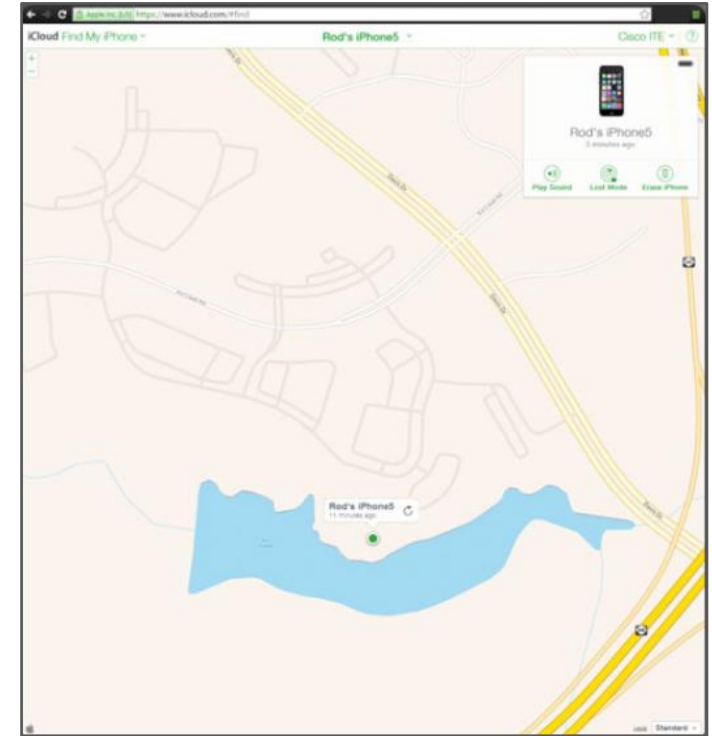
- Una copia de seguridad remota se realiza cuando el dispositivo copia los datos a un almacenamiento de nube por medio de una aplicación de copia de seguridad.
 - Si necesita restaurar datos, ejecute la aplicación de copia de seguridad y acceda a la página web para recuperar los datos.
- La mayoría de los sistemas operativos trae una cuenta de usuario vinculada al servicio en la nube del fabricante, como iCloud para iOS, Google Sync para Android y OneDrive para Microsoft.
 - El usuario puede habilitar copias de seguridad automáticas en la nube para los datos, las aplicaciones y la configuración.
- También hay proveedores de respaldo de terceros, como Dropbox, que se pueden utilizar.
- Otra opción es configurar software de administración de dispositivos móviles para que cree automáticamente copias de respaldo de los dispositivos del usuario.



Servicios habilitados para la nube para dispositivos móviles

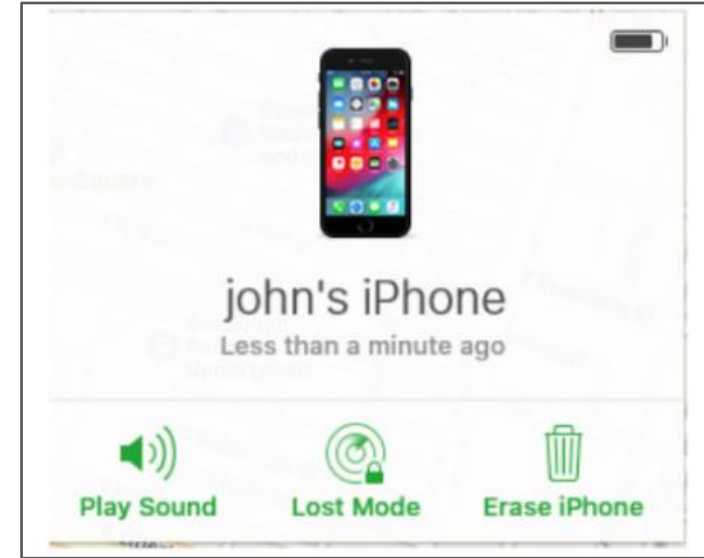
Aplicaciones de localización

- Si un dispositivo móvil se pierde o es robado, es posible encontrarlo por medio de una aplicación de localización.
- Estas aplicaciones se deben instalar y configurar en cada dispositivo móvil, antes de que este se pierda.
- Android y iOS cuentan con aplicaciones para rastrear el dispositivo de forma remota.
 - El Administrador de dispositivos Android permite que un usuario ubique, haga sonar o bloquee un dispositivo Android perdido, o que borre datos del dispositivo.
 - Los usuarios de iOS pueden utilizar la aplicación Buscar mi iPhone.
- Una vez que se ubica el dispositivo, es posible realizar acciones adicionales, como enviar un mensaje o reproducir un sonido.



Bloqueo remoto y Eliminación remota

- Si los intentos de ubicar un dispositivo móvil fallan, existen otras funciones de seguridad disponibles para evitar que los datos del dispositivo se vean comprometidos.
- Las siguientes son dos de las funciones de seguridad remotas más comunes:
- Bloqueo remoto (iOS = modo perdido, Android = bloqueo)
 - Le permite bloquear el dispositivo con un código de acceso para que otros no puedan acceder a sus datos.
- Borrado remoto (iOS = borrar teléfono, Android = Erase)
 - La función de eliminación remota elimina todos los datos del dispositivo y restituye el estado de fábrica del dispositivo.
 - Para restaurar los datos en el dispositivo, los usuarios de Android deben configurarlo por medio de una cuenta de Gmail, y los usuarios de iOS deben sincronizar su dispositivo con iTunes.



Seguridad de software

Antivirus

- Los smartphones y demás dispositivos móviles son vulnerables al software malicioso.
- Según los permisos que se otorguen a las aplicaciones antivirus cuando se las instala en un dispositivo Android, es posible que estas no puedan examinar archivos de manera automática o realizar exámenes de detección programados.
- iOS no permite los exámenes de detección automáticos o programados.
 - Esta es una característica de seguridad que evita que los programas malintencionados utilicen recursos no autorizados o contaminen otras aplicaciones o el OS.
- Las aplicaciones de los dispositivos móviles se ejecutan en una sandbox.
 - Una sandbox es una ubicación del SO que mantiene el código aislado de otros recursos o códigos.
 - Esto dificulta que los programas malintencionados infecten un dispositivo móvil, ya que las aplicaciones se ejecutan dentro de dicho espacio.
 - Para impedir que el programa malicioso infecte más dispositivos, se puede usar un firewall.

Rooting y Jailbreaking

- Los sistemas operativos móviles generalmente están protegidos por varias restricciones de software.
 - Una copia sin modificar de iOS, por ejemplo, ejecuta únicamente código autorizado y permite al usuario un acceso muy limitado al sistema de archivos.
- Rooting y Jailbreaking son dos métodos para eliminar las restricciones y protecciones agregadas a los sistemas operativos móviles.
 - El rooting se usa en los dispositivos con Android para obtener acceso privilegiado o de nivel de raíz, a fin de modificar código o instalar software no diseñado para el dispositivo.
 - Jailbreaking se suele usar en los dispositivos con iOS para eliminar las restricciones del fabricante, a fin de poder ejecutar código de usuario arbitrario y otorgar a los usuarios acceso total al sistema de archivos y a los módulos de kernel.
- Al hacer rooting o jailbreaking de un dispositivo móvil, la GUI se puede personalizar mucho, se puede modificar el SO para ganar velocidad y capacidad de respuesta del dispositivo, y se puede instalar aplicaciones de fuentes secundarias o no admitidas.

Revisiones y actualización de los sistemas operativos

- Al igual que el OS de las computadoras de escritorio o portátiles, es posible actualizar o llevar a cabo revisiones del OS de los dispositivos móviles.
 - Las actualizaciones agregan funcionalidad o aumentan el rendimiento.
 - Las revisiones pueden solucionar problemas de seguridad o cuestiones relacionadas con hardware y software.
- Las actualizaciones y las revisiones de Android utilizan un proceso de entrega automatizado. Cuando el proveedor de servicios de telefonía móvil o el fabricante tienen una actualización para un dispositivo, una notificación en el dispositivo indica que hay una actualización lista.
- Las actualizaciones de iOS también utilizan un proceso automatizado para la entrega y, de manera similar a Android, se abre un aviso para descargar si hay actualizaciones disponibles.
- Hay dos tipos de actualizaciones de firmware de radio de dispositivo móvil.
 - La Lista de roaming preferido (PRL) es la información de configuración que el teléfono celular necesita para comunicarse con otras redes, para poder hacer llamadas fuera de la red de la prestadora telefónica.
 - La ISDN de tasa primaria (PRI) configura las velocidades de transmisión de datos entre el dispositivo y la torre de telefonía móvil. Esto garantiza que el dispositivo pueda comunicarse con la torre a la velocidad correcta.

12.3 Sistemas operativos

Linux y macOS

Introducción a los sistemas operativos Linux y macOS

- Unix
 - Unix es un sistema operativo exclusivo escrito en el lenguaje de programación C.
 - macOS e iOS se basan en la versión de Berkley Standard Distribution (BSD) de Unix.
- Linux
 - Los sistemas operativos Linux se utilizan en sistemas incorporados, dispositivos ponibles, relojes inteligentes, teléfonos móviles, netbooks, computadoras, servidores y supercomputadoras.
 - Existen muchas distribuciones (o distros) de Linux, entre ellas, SUSE®, Red Hat®, CentOS®, Fedora®, Debian®, Ubuntu® y Mint®.
 - Android y muchas distribuciones de SO emplean el núcleo de Linux.
- macOS
 - El sistema operativo para computadoras Macintosh se desarrolla a partir del kernel de UNIX, pero es un sistema operativo de código cerrado.
 - macOS admite la instalación de red remota llamada NetBoot

Descripción general de la GUI de Linux

- Varias distribuciones de Linux se envían con distintos paquetes de software, pero los usuarios deciden cuales permanecen en su sistema instalando o eliminando los paquetes.
- La interfaz gráfica de Linux consta de diversos subsistemas que también se puedan quitar o reemplazar por el usuario.
 - Ubuntu Linux utiliza Unity como la GUI predeterminada.
 - La GUI de Linux tiene la capacidad de poseer múltiples escritorios o espacios de trabajo.
- Canonical tiene un sitio web que simula la IU de Unity y también brinda un recorrido a través de las funciones principales de Unity.
- Para experimentar Unity mediante el sitio web de Canonical visite <http://tour.ubuntu.com/en/>.



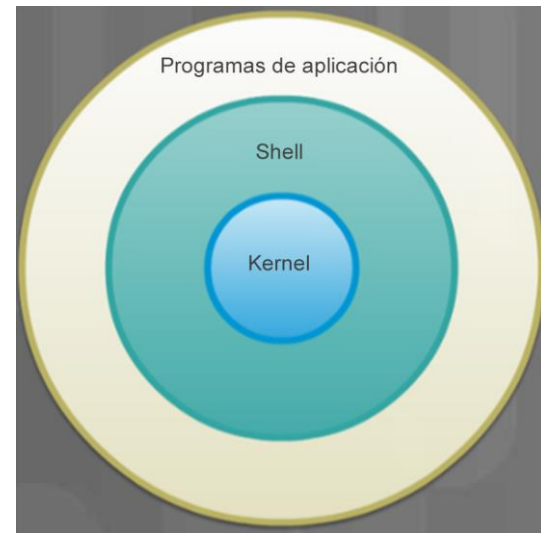
Descripción general de la GUI de macOS

- Dentro de las principales diferencias entre las versiones anteriores de Mac OS y el OS X es la inclusión de la GUI de Aqua.
- Con macOS, el control de misiones es una forma rápida de ver todo lo que se encuentra actualmente abierto en su Mac.
 - El control de misiones le permite organizar sus aplicaciones en varios escritorios.
 - Para navegar en el sistema de archivos, macOS incluye Finder.
 - Finder es muy similar al Explorador de archivos de Windows.
- macOS permite el uso compartido de la pantalla
 - El uso compartido de la pantalla es una característica que permite a otras personas utilizar Macs para ver su pantalla e, inclusive, tomar el control de su computadora.



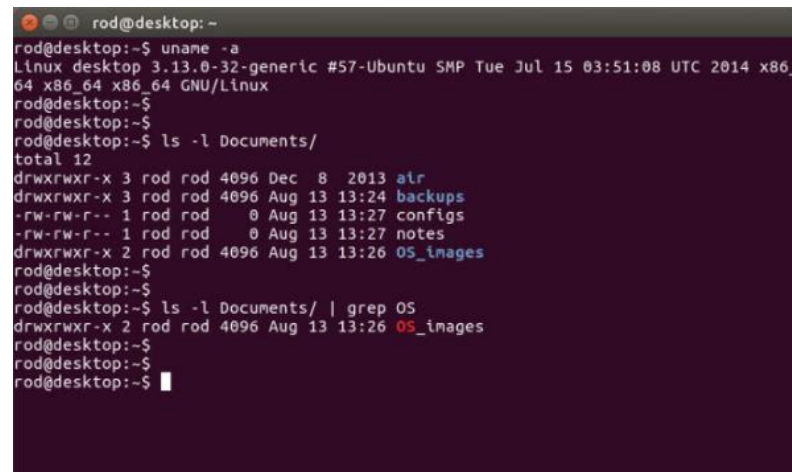
Descripción general de la CLI de Linux y macOS

- En Linux y macOS, el usuario puede comunicarse con el sistema operativo mediante la interfaz de línea de comandos (CLI).
 - Para agregar flexibilidad, los comandos (o las herramientas) que admiten parámetros, opciones y switches, son precedidos generalmente por el carácter de guion (-).
- La mayoría de los sistemas operativos incluye una interfaz gráfica.
 - Aunque una interfaz de línea de comandos aún está presente, el SO arranca a menudo en la GUI de manera predeterminada, escondiendo la interfaz de línea de comandos del usuario.
 - Una forma de acceder a la interfaz de línea de comandos en un sistema operativo basado en GUI es a través de una aplicación del emulador de terminal.
 - Estas aplicaciones proporcionan acceso del usuario a la interfaz de línea de comandos y se denomina generalmente como algunas variaciones de la palabra terminal.



Descripción general de la CLI de Linux y macOS (Cont.)

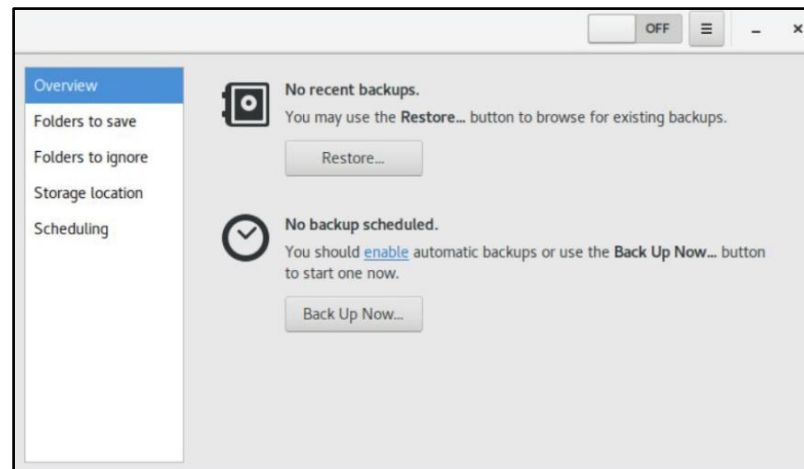
- Un programa llamado shell interpreta los comandos del teclado y los transmite al sistema operativo.
 - Cuando un usuario inicia sesión correctamente en el sistema, el programa de inicio de sesión inicia el shell.
 - Posteriormente, un usuario autorizado puede comenzar a interactuar con el SO a través de los comandos basados en texto.
- Los usuarios interactúan con el kernel a través de un shell.
 - El kernel es responsable de asignar tiempo y memoria de CPU a los procesos.
 - El kernel también administra el sistema de archivos y las comunicaciones en respuesta a las llamadas del sistema.
- Emulador de terminales de macOS
 - macOS incluye un emulador de terminal llamado Terminal pero varios emuladores de terceros están disponibles.



```
rod@desktop: ~  
rod@desktop:~$ uname -a  
Linux desktop 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:08 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux  
rod@desktop:~$  
rod@desktop:~$  
rod@desktop:~$ ls -l Documents/  
total 12  
drwxrwxr-x 3 rod rod 4096 Dec  8 2013 air  
drwxrwxr-x 3 rod rod 4096 Aug 13 13:24 backups  
-rw-rw-r-- 1 rod rod  0 Aug 13 13:27 configs  
-rw-rw-r-- 1 rod rod  0 Aug 13 13:27 notes  
drwxrwxr-x 2 rod rod 4096 Aug 13 13:26 OS_images  
rod@desktop:~$  
rod@desktop:~$  
rod@desktop:~$ ls -l Documents/ | grep OS  
drwxrwxr-x 2 rod rod 4096 Aug 13 13:26 OS_images  
rod@desktop:~$  
rod@desktop:~$  
rod@desktop:~$
```

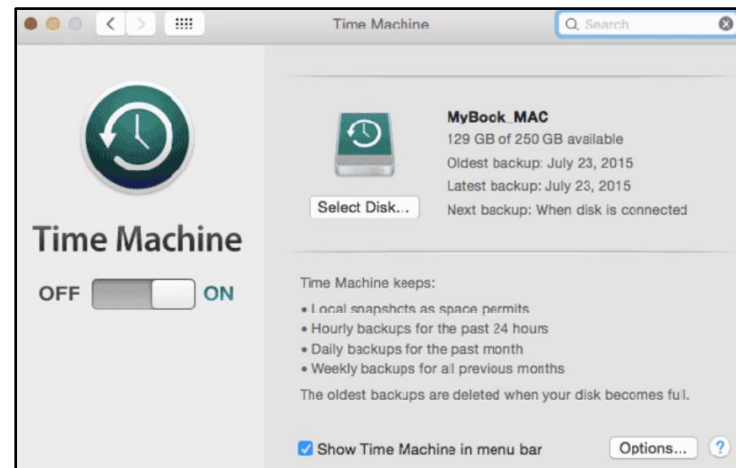
Copia de respaldo y recuperación de Linux

- El proceso de copias de seguridad de los datos se refiere a crear una copia (o varias copias) de datos para guardarla en un lugar seguro.
- Cuando se completa el proceso de copia de seguridad, la copia se denomina copia de seguridad.
- Si bien las copias de seguridad se pueden lograr con un comando de copia simple, muchas herramientas y técnicas existen para hacer el proceso automático y transparente para el usuario.
- Linux no tiene una herramienta de respaldo integrada.
 - Sin embargo, existen muchas soluciones de copia de respaldo comerciales y de código abierto para Linux, como Amanda, Bacula, Fwbackups y Déjà Dup.



Copia de respaldo y recuperación de Linux

- macOS incluye una herramienta de copia de respaldo llamada Time Machine.
- Con Time Machine, los usuarios elijen una unidad externa que se usará como dispositivo de destino de copia de seguridad y la conectan al Mac mediante USB, FireWire o Thunderbolt.
- Time Machine prepara el disco para recibir copias de seguridad y, cuando el disco está listo, realiza copias de seguridad incrementales periódicamente.
- Time Machine almacena algunas copias de respaldo en su Mac, por lo que, si el disco de copia de respaldo de Time Machine no está disponible, puede restaurar una copia de respaldo directamente desde su Mac.



Descripción general de utilidades del disco

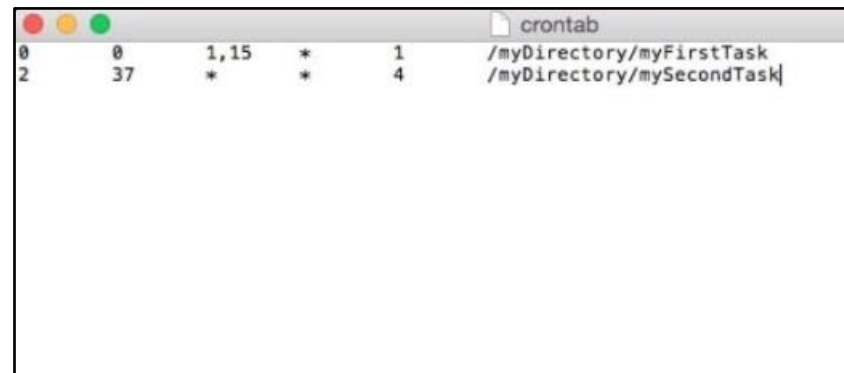
- Para ayudar a diagnosticar y solucionar problemas relacionados, la mayoría de los sistemas operativos modernos incluyen herramientas de utilidad de disco.
- Ubuntu Linux incluye una utilidad de disco llamada Discos.
 - Con los discos, los usuarios pueden realizar las tareas más comunes relacionadas con discos, incluida la administración de la partición, el montaje o el desarmado, formateo de los discos y consulta de Tecnología de análisis e informes (S.M.A.R.T.)
- macOS incluye la utilidad de disco.
 - Además de utilizar las tareas de mantenimiento principales de disco, la utilidad de disco también admite verificar los permisos del disco y los permisos de reparación de disco.
 - El permiso de reparación de disco es un paso común para la resolución de problemas en macOS.
 - La utilidad del disco también se puede utilizar para realizar copias de respaldo de discos a archivos de imágenes y realizar una recuperación de imagen del disco desde los archivos de imagen.

Descripción general de utilidades del disco (Cont.)

- A continuación figuran algunas tareas de mantenimiento comunes que pueden efectuarse mediante el software de utilidad de disco:
 - **Administración de la partición:** al trabajar con discos de la computadora, las particiones se pueden crear, eliminar o modificar de tamaño.
 - **Montar o desmontar particiones de disco:** en sistemas como Unix, el montaje de una partición se relaciona con el proceso de vincular una partición de un disco o un archivo de imagen de disco (generalmente un archivo .iso) con una ubicación de la carpeta.
 - **Formato de disco:** antes de que una partición se pueda utilizar por el usuario o el sistema, se debe formatear.
 - **Verificación de sector defectuoso** Cuando un sector de disco ha sido marcado como defectuoso, se torna inofensivo al SO porque dejará de ser compatible para almacenar datos.
 - Muchos sectores defectuosos podrían ser un indicador de un disco con fallas.
 - **Consultar atributos de S.M.A.R.T.:** S.M.A.R.T. puede detectar e informar atributos sobre el estado de un disco.
 - El objetivo de S.M.A.R.T. es anticipar las fallas de disco, lo que permite al usuario transferir datos a un disco normal antes de que el disco defectuoso se vuelva inaccesible.

Tareas programadas

- Las tareas de mantenimiento se deben programar y realizar con frecuencia para evitar problemas o para detectar los problemas rápidamente.
 - Para evitar perder las tareas de mantenimiento debido a errores humanos, los sistemas de computación pueden programarse para realizar tareas automáticamente.
- Dos tareas que se deben programar y realizar automáticamente son los controles de copias de respaldo y de disco.
- En Linux y en macOS, el servicio cron es responsable de las tareas programadas.
 - Como servicio, cron se ejecuta en segundo plano y ejecuta las tareas en las fechas y horas específicas.
 - Cron utiliza una tabla de planificación denominada Tabla de cron, que puede editarse con el comando crontab.



```
crontab
0      0      1,15  *    1    /myDirectory/myFirstTask
2      37     *    *    4    /myDirectory/mySecondTask
```

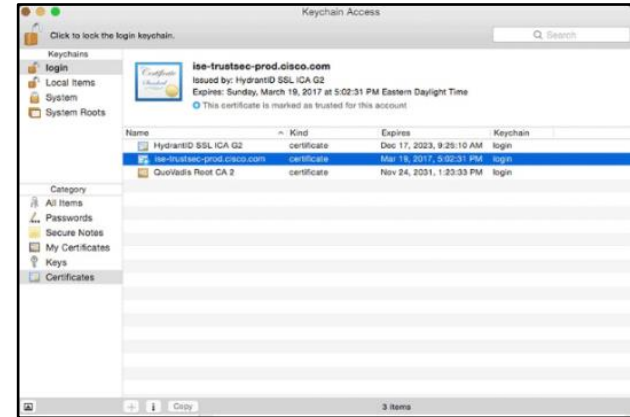
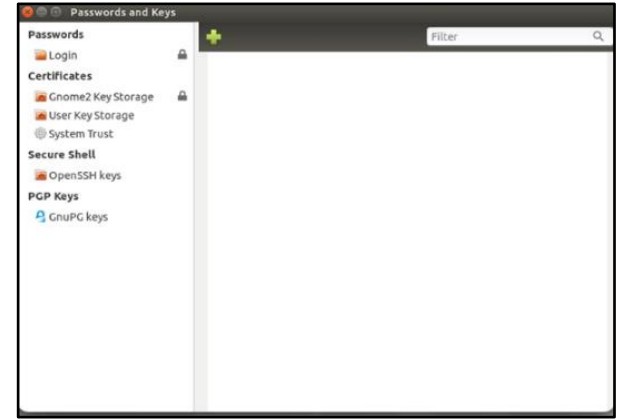
Actualizaciones del sistema operativo

- También conocido como parches, las actualizaciones del SO son lanzadas de forma periódica por las empresas del SO para abordar cualquier vulnerabilidad conocida en sus sistemas operativos.
 - A medida que las empresas tienen programadas las actualizaciones, la versión de las actualizaciones no programadas del SO es común cuando una vulnerabilidad importante se encuentra en el código del SO.
- Actualizaciones de firmware
 - Retenida generalmente en la memoria no volátil, como ROM o flash, el firmware es un tipo de software diseñado para proporcionar la funcionalidad de bajo nivel para un dispositivo.
- Antivirus y Antimalware
 - El antivirus y antimalware dependen de firmas de código para funcionar.
 - Las firmas o archivos de firma son archivos que contienen un ejemplo de código utilizado por virus y malware.
 - El malware nuevo se crea y se reversiona cada día; por lo tanto, los archivos de firma de antivirus y programas antimalware se deben actualizar con frecuencia.

Prácticas recomendadas para Linux y macOS

Seguridad

- Los nombres de usuario, contraseñas, certificados digitales y claves de cifrado son solo algunas credenciales de seguridad asociados a un usuario.
- Debido a la creciente cantidad de credenciales de seguridad necesarias, los sistemas operativos modernos incluyen un servicio para administrarlas.
 - Las aplicaciones y otros servicios pueden pedir y utilizar las credenciales almacenadas por el servicio del administrador de credenciales de seguridad.
- Servicio de credenciales de seguridad en Ubuntu
 - El conjunto de claves Gnome es un administrador de credenciales de seguridad para Ubuntu Linux. Para acceder a Gnome-Keyring en Ubuntu Linux, haga clic en **Guión > Buscar Clave > Hacer clic en Contraseñas y claves**
- Servicio de credenciales de seguridad en macOS
 - La cadena de claves es un administrador de credenciales de seguridad para macOS. Para acceder a las llaves en macOS, vaya a Aplicaciones > Utilidades > Acceso a cadena de claves



Resultado del comando ls -l

rod@machine ~ : \$ ls -l						
-rwxrwx-r--	1	rod	personal	1108485	14 de agosto, 7:34	My_Awesome_File
drwx-----	2	rod	personal	4096	10 de septiembre de 2018	My_Private_Folder
Permiso	Enlace	Usuario	Grupo	Tamaño de archivo	Fecha y hora	Nombre del archivo

- Permiso: define cómo el usuario, el grupo y otros tienen acceso a los archivos y directorios.
- Enlace: la cantidad de enlaces o la cantidad de directorios dentro de este directorio
- Usuario: muestra el nombre de usuario del propietario del archivo o del directorio.
- Grupo: muestra el nombre del grupo que posee el archivo o el directorio.
- Tamaño del archivo: muestra el tamaño del archivo en bytes.
- Fecha y hora: son los datos y la hora de la última modificación.
- Nombre del archivo: muestra el nombre del archivo o directorio.

Permisos básicos de archivos y directorios de Unix

- Para organizar el sistema y reforzar los límites dentro del sistema, Unix utiliza permisos de archivos.
- Cada archivo y directorio en los sistemas Unix trae sus permisos que definen las acciones que el propietario, el grupo y otros pueden hacer con el archivo o directorio.
- El único usuario que puede anular los permisos de archivos en Unix es el usuario raíz.
- El acceso raíz se requiere a menudo antes de realizar el mantenimiento y las tareas administrativas.

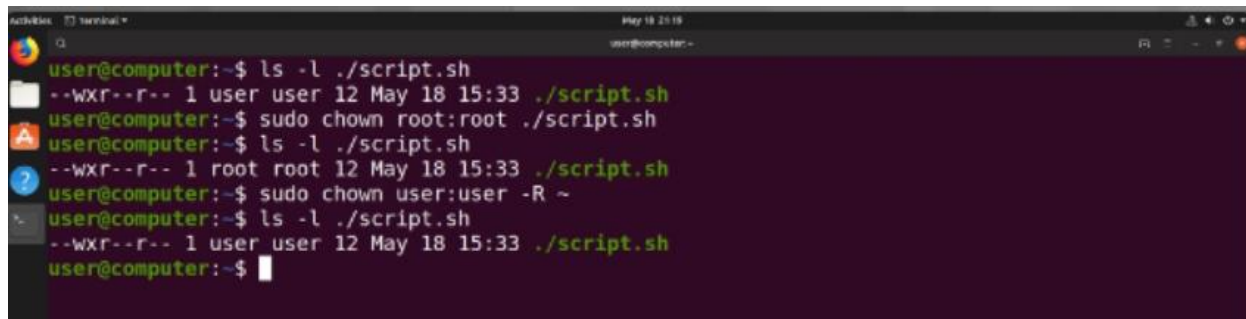


Comandos administrativos de Linux

- Los administradores utilizan el terminal para monitorear y controlar usuarios, procesos, direcciones IP y otras tareas.
 - passwd: permite que los usuarios cambien su propia contraseña en el terminal.
 - ps: permite que los usuarios supervisen sus propios procesos.
 - kill: permite que los usuarios finalicen los procesos que han iniciado.
 - ifconfig: similar al comando ipconfig de Windows; sin embargo, este comando está desaprobadado y se debe utilizar el comando "dirección IP".
 - iwconfig: permite que los usuarios establezcan y vean la configuración inalámbrica.
 - chmod: permite que los usuarios cambien los permisos de los archivos que poseen.

Comandos administrativos de Linux que requieren acceso de raíz

- Los administradores utilizan el terminal para monitorear y controlar usuarios, procesos, direcciones IP y otras tareas.
 - sudo: (Do de superusuarios) otorga acceso de raíz a un usuario sin cambiar su perfil.
 - chown: permite que los usuarios cambien el propietario y el grupo de un archivo o archivos.
 - apt-get: se utiliza para instalar y administrar software en distribuciones de Linux basadas en Debian.
 - shutdown: se utiliza para detener y reiniciar el sistema operativo.
 - DD: (duplicado de disco) se utiliza para copiar archivos y particiones, como también, para crear archivos de intercambio temporales.



```
user@computer:~$ ls -l ./script.sh
--wxr--r-- 1 user user 12 May 18 15:33 ./script.sh
user@computer:~$ sudo chown root:root ./script.sh
user@computer:~$ ls -l ./script.sh
--wxr--r-- 1 root root 12 May 18 15:33 ./script.sh
user@computer:~$ sudo chown user:user -R ~
user@computer:~$ ls -l ./script.sh
--wxr--r-- 1 user user 12 May 18 15:33 ./script.sh
user@computer:~$
```

12.4 Proceso básico de resolución de problemas de los sistemas operativos móviles, Linux y macOS

Los seis pasos del proceso de resolución de problemas

Paso 1. Identificar el problema.

Paso 2. Establecer una teoría de causas probables.

Paso 3. Poner a prueba la teoría para determinar la causa.

Paso 4. Establecer un plan de acción para solucionar el problema e implementar la solución.

Paso 5. Verificar la funcionalidad total del sistema y, si corresponde, implementar medidas preventivas.

Paso 6. Registrar hallazgos, acciones y resultados.

Aplicación del proceso de resolución de problemas a sistemas operativos móviles, Linux y macOS

Identifique el problema

Paso 1: Identificar el problema	
Sistemas operativos de dispositivos móviles	
Preguntas abiertas	• ¿Qué problema tiene? • ¿Cuál es la versión del SO móvil que usa? • ¿Cuál es su proveedor de servicios? • ¿Qué aplicaciones instaló recientemente?
Preguntas cerradas	• ¿Tuvo este problema antes? • ¿Alguien más utilizó el dispositivo móvil? • ¿Está en garantía el dispositivo móvil? • ¿Modificó el sistema operativo del dispositivo móvil? • ¿Instaló alguna aplicación de un origen no autorizado? • ¿El dispositivo móvil puede conectarse a Internet?
Linux o MacOS	
Preguntas abiertas	• ¿Qué problema tiene? • ¿Cuál es la marca y el modelo de la computadora? • ¿Qué versión de Linux o MacOS se está ejecutando? • ¿Qué programas o controladores instaló recientemente? • ¿Qué actualizaciones de SO instaló recientemente? • ¿Qué configuraciones del sistema cambió recientemente?
Preguntas cerradas	• ¿Tuvo este problema antes? • ¿Alguien más utilizó la computadora? • ¿Está en garantía la computadora? • ¿La computadora se conecta a Internet?

Aplicación del proceso de resolución de problemas en sistemas operativos móviles, Linux y macOS

Establecimiento de una teoría de causa probable

Paso 2: Establecer una teoría de causas probables	
Causas comunes de los problemas de los sistemas operativos de dispositivos móviles	• El dispositivo móvil no puede enviar ni recibir correo electrónico. • Una aplicación dejó de funcionar. • Se transmitió una aplicación maliciosa. • El dispositivo móvil ya no responde. • El software o las aplicaciones del dispositivo móvil no están actualizados. • Un usuario olvidó la contraseña.
Causas comunes de los problemas de Linux o macOS	• La computadora no envía ni recibe correo electrónico. • Una aplicación dejó de funcionar. • Se instaló una aplicación maliciosa. • La computadora ya no responde. • El sistema operativo no está actualizado. • Un usuario olvidó las credenciales de inicio de sesión.

Aplicación del proceso de resolución de problemas en sistemas operativos móviles, Linux y macOS

Aplicación de la teoría de determinación de causa

Paso 3: Poner a prueba la teoría para determinar la causa

Pasos comunes para determinar la causa de los problemas de los sistemas operativos de dispositivos móviles

- Forzar el cierre de una aplicación en ejecución.
- Volver a configurar las cuentas de correo electrónico.
- Reiniciar el dispositivo móvil.
- Restaurar el dispositivo móvil desde una copia de respaldo.
- Conectar un dispositivo iOS a iTunes.
- Actualizar el sistema operativo.
- Restablecer los valores predeterminados del dispositivo móvil.

Pasos comunes para determinar la causa de los problemas de Linux o MacOS

- Forzar el cierre de un programa en ejecución.
- Volver a configurar las cuentas de correo electrónico.
- Reiniciar la computadora.
- Restaurar la computadora desde una copia de respaldo.
- Actualizar el sistema operativo de la computadora.

Aplicación del proceso de resolución de problemas en sistemas operativos móviles, Linux y macOS

Establecimiento de un plan de acción para resolver el problema e implementar la solución

Paso 4: Establecer un plan de acción para solucionar el problema e implementar la solución

Si no logró solucionar el problema en el paso anterior, debe realizarse una investigación más exhaustiva para implementar la solución.

- Registros de reparaciones de soporte técnico
- Otros técnicos
- Preguntas frecuentes de fabricantes
- Sitios web técnicos
- Manual del dispositivo
- Foros en línea
- Búsqueda en Internet

Aplicación del proceso de resolución de problemas en los sistemas operativos móviles, Linux y macOS

Verificación de la funcionalidad completa del sistema y, si corresponde, implementación de medidas preventivas

Paso 5: Verificar la funcionalidad total del sistema y, si corresponde, implementar medidas preventivas	
Verificar la solución y la funcionalidad total del sistema para los sistemas operativos de dispositivos móviles.	• Reiniciar el dispositivo móvil. • Navegar en Internet utilizando Wi-Fi. • Navegar por Internet con 4G, 3G u otro tipo de red de la portadora. • Realizar una llamada telefónica. • Enviar un mensaje de texto. • Abrir distintos tipos de aplicaciones.
Verificar la solución y la funcionalidad total del sistema para Linux y MacOS.	• Reiniciar la computadora. • Explorar en Internet utilizando wifi. • Explorar en Internet mediante una conexión cableada. • Enviar un correo electrónico de prueba. • Abrir distintos programas. • Un usuario olvidó las credenciales de inicio de sesión.

Aplicación del proceso de resolución de problemas en sistemas operativos móviles, Linux, y macOS

Registro de hallazgos, acciones y resultados

Paso 6: Registrar hallazgos, acciones y resultados.	
Registrar hallazgos, acciones y resultados.	• Analizar la solución implementada con el cliente. • Solicitarle al cliente que verifique que se haya solucionado el problema. • Proporcionarle todos los documentos pertinentes al cliente. • Registrar los pasos que siguió para resolver el problema en la solicitud de trabajo y en el registro diario del técnico. • Registrar todos los componentes utilizados en la reparación. • Registrar el tiempo que le llevó resolver el problema.

Problemas y soluciones comunes de los sistemas operativos móviles

Identificar del problema

El dispositivo móvil no se conecta a Internet.

Una aplicación no responde.

El dispositivo móvil no responde.

El dispositivo móvil no puede enviar ni recibir correo electrónico.

No se pueden instalar más aplicaciones ni guardar fotos en el dispositivo móvil.

Un dispositivo móvil no se puede conectar o emparejar con un dispositivo Bluetooth.

La pantalla del dispositivo móvil se ve oscura.

El dispositivo móvil no puede transmitir a un monitor externo.

El dispositivo móvil tiene rendimiento lento.

El dispositivo móvil no puede descifrar el correo electrónico.

El sistema operativo del dispositivo móvil se ha estancado.

El dispositivo móvil no tiene ningún sonido proveniente de los altavoces.

La pantalla táctil del dispositivo móvil tiene respuesta incorrecta.

El dispositivo móvil no se conecta a Internet.

Causas probables	Soluciones posibles
La conexión wifi está desactivada.	Activar la conexión wifi.
La configuración de wifi es incorrecta.	Volver a configurar la conexión wifi.
El modo aeroplano está encendido.	Apagar el modo aeroplano.

Ver PDF

Problemas y soluciones comunes de los sistemas operativos móviles

Problemas y soluciones comunes de seguridad del SO móvil

Identificar el problema

Un dispositivo móvil tiene una señal débil o se cayó la señal.

La potencia de un dispositivo móvil se agota más rápido que lo normal.

Un dispositivo móvil tiene poca velocidad de datos.

Un dispositivo móvil se conecta a una red Wi-Fi involuntariamente.

Un dispositivo móvil se empareja con un dispositivo Bluetooth involuntariamente.

Se han fugado archivos y datos personales de un dispositivo móvil.

Personal no autorizado ha accedido a una cuenta de dispositivo móvil.

Una aplicación alcanzó el acceso no autorizado a la raíz.

Se está haciendo el seguimiento de un dispositivo móvil sin permiso.

Se accedió a un micrófono o cámara del dispositivo móvil sin permiso.

Un dispositivo móvil tiene una señal débil o la señal cayó.

Causas probables	Soluciones posibles
No hay suficientes torres celulares en el área.	Moverse a un área más poblada que tenga más torres celulares.
El área se encuentra entre las áreas de cobertura de la portadora.	Moverse a un área dentro del alcance de su portadora.
El edificio donde se encuentra está bloqueando la señal.	Moverse a otra zona del edificio o salir del edificio.
La mano con que sostiene el dispositivo móvil está bloqueando la señal.	Acomodar de otro modo la mano para sostener el dispositivo.

Ver PDF

Problemas y soluciones comunes de los sistemas operativos móviles

Problemas y soluciones comunes de los sistemas operativos Linux y macOS

Identificar el problema

La operación de respaldo automática no se inicia.

El directorio aparece vacío.

Una aplicación deja de responder en MacOS.

Wi-Fi no es accesible a través de Ubuntu.

MacOS no puede leer el disco óptico remoto mediante Remote Disc (Disco remoto).

Linux no arranca y recibe un mensaje "GRUB faltante" o "LILO faltante".

El SO Mac o Linux se congela en el inicio y presenta una emergencia de kernel donde hay una pantalla de detención.

La operación de respaldo automática no se inicia.

Causas probables	Soluciones posibles
Time Machine está desactivado en MacOS.	Activar Time Machine en MacOS.
Déjà Dup está desactivado en Linux.	Activar Déjà Dup en Linux.

Ver PDF

Práctica de laboratorio: Resolución de problemas de dispositivos móviles

En esta práctica de laboratorio, analizará situaciones en las que se presentan problemas comunes de dispositivos móviles e identificará las soluciones.

Se le proporcionó una lista de soluciones de problemas comunes.

Cada solución se puede usar más de una vez.

12.5 Resumen del capítulo

Capítulo 12: Sistemas operativos móviles, Linux y macOS

- Explicar el propósito y las características de los sistemas operativos móviles.
- Explicar los métodos para asegurar los dispositivos móviles.
- Explique la finalidad y las características de los sistemas operativos Linux y Mac.
- Explicar cómo solucionar los problemas de otros sistemas operativos.

