UNIVERSIDAD TECNOLÓGICA DE PANAMÁ

FACULTAD DE INGENIERÍA DE SISTEMAS COMPUTACIONALES

LICENCIATURA EN INGENIERÍA DE SISTEMAS DE INFORMACIÓN

Infraestructura Tecnológica

Proyecto Capítulo 12: Sistemas Operativos Linux, Android, Mac OS

Prof. Emilio Dutary

Integrantes:

Cutire, Fernando 8-972-906

Escobar, Jorge 2-747-1772

Gamero, Jonathan 8-982-2008

Grupo: 1IF131

15-06-2021

Índice de contenidos

Introducción

Desde que se hizo la primera llamada desde un teléfono móvil con Martin Cooper, ingeniero de Motorola, los teléfonos móviles han evolucionado en más funciones hasta tener sus propios sistemas operativos.

El trabajo inicia contemplando los sistemas operativos de teléfonos móviles Android e iOS, que son los principales en materia móvil.

Se compararon también funcionalidades entre estos sistemas operativos, como seguridad, control del usuario, duración de la batería y la diferencia entre sistemas de código abierto (Android) y código cerrado (iOS).

Se muestran aplicaciones de mapas, antivirus, servicios en la nube para estos dispositivos también.

Se revisaron los temas de sistemas operativos de escritorio Linux y MacOS. Se observó su relación con Unix, siendo estos , basados en él. Se entró más a fondo a Linux, revisando interfaces , funcionalidades , comandos básicos de terminal y certificaciones linux.

Por último se explora la metodología de desarrollo de problemas para estos sistemas operativos.

Desarrollo

Así como las computadoras, los dispositivos móviles utilizan un sistema operativo para ejecutar software. Antes de analizar o modificar un software es necesario interactuar con su código fuente e cual es una secuencia de instrucciones que se escriben en lenguaje legible para los humanos antes de volverse lenguaje de máquina, el código fuente permite a los usuarios analizar y modificar el código de un software.
Se dice que un software es de código abierto cuando el desarrollador proporciona el código fuente y código cerrado cuando no se publica o comparte dicha información

Pequeña introducción a los principales sistemas operativos para móviles

Android

Es un sistema operativo móvil basado en núcleo Linux y otros software de código abierto. Fue diseñado para dispositivos móviles con pantalla táctil, como teléfonos inteligentes, tabletas, relojes inteligentes (Wear OS), automóviles con otros sistemas a través de Android Auto, al igual que los automóviles con el sistema Android Automotive y televisores Leanback. El código fuente principal de Android se conoce como Android Open Source Project (AOSP), que se licencia principalmente bajo la Licencia Apache.

IOS

iOS es un sistema operativo lanzado y utilizado por Apple. Su nombre proviene de iPhone OS. Es decir, iPhone Operative System o Sistema Operativo de iPhone. Utilizando las siglas, iOS. Se lanzó originalmente para el teléfono de la marca, aunque también se ha utilizado durante años en otros dispositivos de la compañía como en algunos de los reproductores de música iPod o en las tabletas iPad (hasta la llegada de iPadOS)

Se trata de un sistema cerrado que no puedes utilizar salvo en dispositivos de marca Apple.

Sistemas operativos móviles

Android frente a IOS

A menos que haya usado tanto Android como iOS (iOS 10), a menudo se ha preguntado cómo sería usar un dispositivo Android si su dispositivo principal es iOS o un dispositivo iOS si usa principalmente un dispositivo Android.

¿QUÉ DIFERENCIAS PODEMOS ENCONTRAR ENTRE DICHOS SISTEMAS OPERATIVOS MÓVILES?

1. Sistemas abiertos frente a sistemas cerrados

Android es un sistema más abierto en comparación con iOS (iOS 10 incluido). Cualquier aplicación de Android que esté disponible incluso si no está en la tienda de Google Play se puede descargar e instalar en un dispositivo Android. Este no es el caso de iOS. Caso en cuestión: Apple no le permitirá ver videos Flash y jugar juegos Flash en dispositivos iOS por razones que solo ellos conocen.

2. Seguridad

Debido a que Apple mantiene un control tan estricto de las aplicaciones que se pueden permitir en un dispositivo iOS, los dispositivos son más seguros. Por otro lado, la apertura de la plataforma Android significa que existe un mayor riesgo no solo de malware sino de otras amenazas de seguridad. Esto hace que los dispositivos iOS sean una opción más segura para aquellos que desean un dispositivo más seguro

3. Control de usuario

Apple se toma el tiempo para asegurarse de que la interfaz sea agradable y esté bien diseñada. En todos los dispositivos iOS, espera encontrar productos bien diseñados y Apple no defrauda. Pero cuando se trata de poder personalizar cómo aparecerán los widgets, los dispositivos Android te ofrecen un mejor control.

Además, existe una gama tan amplia de dispositivos Android diferentes que para cambiar la interfaz solo se necesita seleccionar un dispositivo Android diferente.

4. Duración de la batería

Por otro lado, los dispositivos Android tienen una duración de batería considerablemente menor, pero nuevamente, hay tantos dispositivos diferentes, lo que significa que puede elegir uno con una mejor duración de batería.

Por lo general, los dispositivos iOS tienen una mejor duración de la batería en comparación con los dispositivos Android. Pero a diferencia de los dispositivos Android, no puede reemplazar la batería usted mismo.

Aplicaciones móviles

Las aplicaciones se escriben y compilan para un sistema operativo móvil específico, como apple IOS, android o windows. Estos traen una variedad de aplicaciones pre instaladas a fin de proporcionar una funcionalidad básica. existen aplicaciones para hacer llamadas telefónicas, enviar y recibir correo, escuchar música, tomar o editar fotografías, entre otros.

las aplicaciones se utilizan en los dispositivos móviles del mismo modo que los programas en las computadoras. En lugar de instalarse desde un disco optico las aplicaciones se descargan desde una fuente de contenido. algunas aplicaciones pueden ser descargadas de manera gratuita, mientras que otras se deben pagar Android tiene la play store y IOS tiene la App Stor

Interfaz Android

Elementos de la pantalla de inicio

De modo similar a las computadoras de escritorio y portátiles, los dispositivos móviles organizan los iconos y widgets en varias pantallas para facilitar su acceso.

Pantalla principal de inicio de Android
Una de las pantallas se designa como pantalla de inicio. Para acceder a las pantallas se debe deslizar la pantalla de inicio hacia la izquierda o derecha. cada pantalla contiene iconos de navegación, el área principal desde donde se accede a los iconos y widgets, e iconos de sistema y de notificación. El indicador de pantalla señala que la pantalla está activa.

Iconos de navegación

El SO android utiliza la barra de sistema para explorar aplicaciones y pantallas. Esta barra siempre se muestra en la parte inferior de cada pantalla

La barra contiene los siguientes botones:
atrás: vuelve a la pantalla anterior. Se muestra el teclado en pantalla, este botón se cierra. Si continúa presionando el botón atrás. se pasa por todas las pantallas anteriores hasta llegar a la pantalla de inicio
Inicio: su función es bastante sencilla y es que como indica su nombre vuelve a la pantalla de inicio
Aplicaciones recientes: permite abrirlas imágenes en miniatura de las aplicaciones utilizadas recientemente. Para abrir una aplicación, toque la imagen en miniatura de esta. Para eliminar una imagen en miniatura de la lista, deslicela hacia arriba.

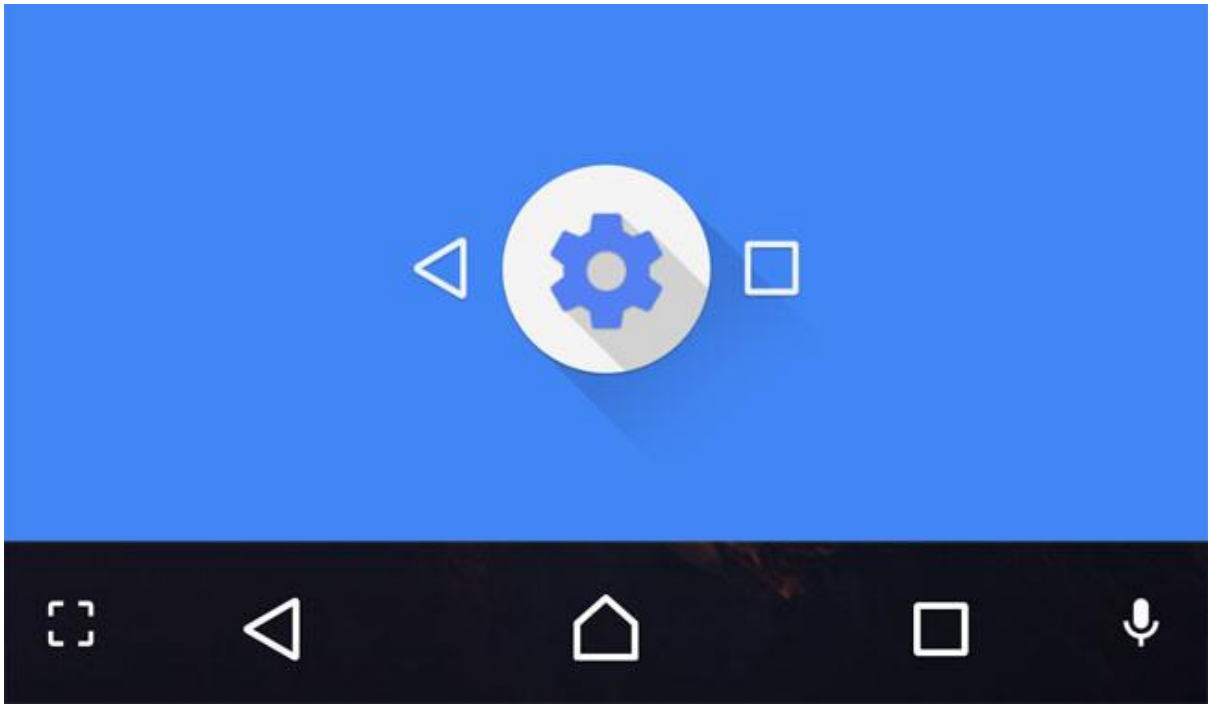

Ilustración 1:iconos barra de navegación android

Iconos de notificación y de sistema

Cada dispositivo android tiene un área con iconos de sistema, como reloj, estado de batería y estado de señales de Wifi y de proveedor. Las aplicaciones como correo electrónico, mensajes de texto y Facebook suelen mostrar iconos 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 estén abiertas

- Responder a una notificación tocandola
- descartar una notificación deslizandola hacia afuera de la pantalla para cualquiera de los lados
- descartar todas las notificaciones

- alternar entre las configuraciones de uso frecuente
- ajustar el brillo de la pantalla
- abrir el menú Configuración con el icono de configuración rápida

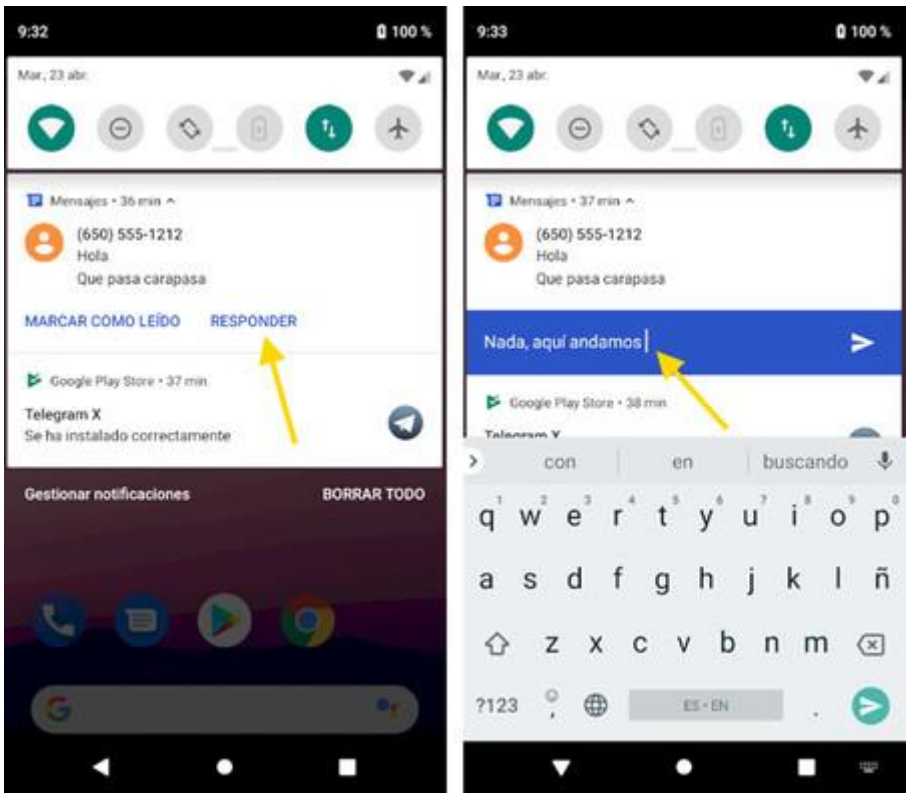

Ilustración 2: Iconos de notificación y de sistema

Interfaz de iOS

la interfaz de iOS funciona de manera similar a la interfaz android. las pantallas de inicio se utilizan para organizar las aplicaciones. las cuales se indican con un toque

- no hay iconos de navegación: en su lugar de tocar iconos de navegación se puede tener que presionar el botón físico
- no hay widgets: solo se pueden instalar aplicaciones.

- 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 iconos de navegación para llevar a cabo las funciones. el botón se encuentra en la parte inferior del dispositivo y puede cumplir muchas funciones:

- Reactivar el dispositivo
- volver a la pantalla de inicio
- Iniciar Siri o el control por voz

Ilustración 3: botón de inicio IOS

Centro de Notificación de IOS

Los dispositivos IOS tiene un centro de notificación que muestra todas las alertas en una ubicación. Para abrir el área de notificación en los dispositivos IOS, toque la parte superior central de la pantalla y deslice el dedo hacia abajo. En el centro de

notificación, puede examinar las notificaciones y alertas, descartarlas, borrarlas y ajustarlas

Ilustración 4: centro de notificaciones IOS

Aspectos a tomar en cuenta al momento de analizar qué sistema operativo se busca

Para iOS:

• Con iOS hay una clara ventaja para las aplicaciones de tableta. Pueden obtener las mismas aplicaciones para teléfonos inteligentes en sus tabletas.

• Las actualizaciones de redes sociales en la plataforma iOS son más fáciles y rápidas debido al hecho de que la integración con Facebook y Twitter es más profunda en comparación con la plataforma Android.

• Ciertas aplicaciones de iOS como FaceTime, Square y pagos móviles están disponibles en iOS y sólo en ciertos dispositivos Android.

• La interfaz en la plataforma iOS está bloqueada. Solo se le permiten opciones de personalización limitadas para las pantallas de inicio y no hay aplicaciones de terceros preinstaladas en el dispositivo. Además, la instalación de la aplicación solo se puede realizar desde la App Store.

• Una de las principales ventajas de iOS es que Apple ofrece actualizaciones de software para todos los dispositivos de forma automática. Esto asegura que los dispositivos se mantengan actualizados, un factor que impulsa el rendimiento.

• Apple también ofrece mejores controles de privacidad, especialmente cuando se trata de permisos de aplicaciones y el tipo de información privada del usuario que las aplicaciones pueden solicitar durante la instalación.

• No podrá instalar aplicaciones que no estén en la tienda de aplicaciones a menos que el dispositivo tenga jailbreak. Esta limitación es un obstáculo para los usuarios de dispositivos iOS que desean probar una aplicación que no está disponible en la tienda de aplicaciones.

Para Android:

• La mayor ventaja de los dispositivos Android es que existe una amplia gama de opciones en términos de hardware. Los dispositivos Android vienen en varios tipos, tamaños de pantalla, diferentes precios, modelos e incluso funciones. Esto significa que puede elegir un dispositivo en función de las funciones que desee tener e incluso un precio que sea más asequible para usted.

• Android también tiene una experiencia de usuario altamente personalizable. Puede personalizar la pantalla de inicio de la forma que desee, no solo con los iconos de la aplicación, sino también con una amplia selección de widgets que le permiten mantenerse informado y conectado.

• La tienda Google Play tiene menos restricciones en lo que respecta a la información del usuario que se puede compartir con las aplicaciones. Esto garantiza que haya una amplia gama de aplicaciones para que los usuarios de dispositivos Android elijan, pero también significa que el dispositivo es menos seguro, más propenso a malware y virus.

• Google también proporciona a los dispositivos Android una amplia red de servicios con los que los usuarios de dispositivos iOS solo pueden soñar.

Características comunes de los dispositivos móviles

- Orientación de la pantalla en los teléfonos móviles

¿Cómo sabe mi celular en qué dirección orientar la pantalla?

Un sensor llamado acelerómetro mide los cambios de velocidad. El software de Android o el de iOS después utiliza los datos del acelerómetro para detectar cómo estás sosteniendo el celular y orientar la pantalla

E**l acelerómetro es un componente mecánico**, un chip en el interior del teléfono de tamaño súper reducido y fabricado en silicio. Esta pieza suele estar compuesta por una parte móvil que se moverá según la velocidad que se le aplique; y por una parte fija que interpreta el voltaje a raíz del movimiento para determinar la velocidad y la orientación.

Se trata de 3 tubos pequeños, tres ejes, que tienen en su interior un muelle y una bola que hace de masa. Esos tres tubos simulan las coordenadas tridimensionales, por lo que, al moverlos, la bola se moverá también y, gracias al movimiento de esa bola, **el terminal sabrá la posición en la que se encuentra el móvil**

para android aparecerá como opción si deslizamos el dedo hacia abajo desde la parte superior de la pantalla, el icono se reconoce como un rectángulo inclinado con dos flechas alrededor que parecen formar un círculo.

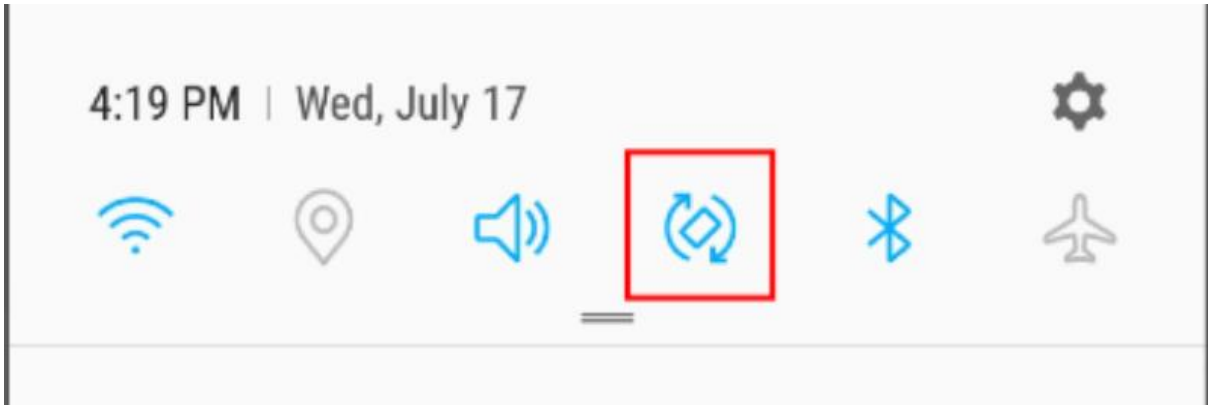

Ilustración 5: Rotación en Android

para iphone, deslizar el dedo hacia arriba y toque el icono de desbloqueo. un candado con una flecha circular alrededor

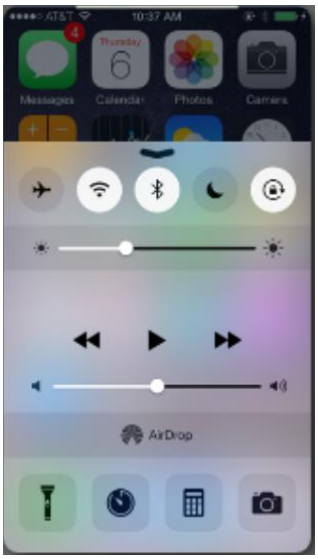

Ilustración 6: Rotación en IOS

Ajustar brillo de la pantalla

La pantalla LCD de la mayoría de dispositivos móviles consumen gran parte de la energía de la batería, por lo que disminuir el brillo del teléfono puede ayudarnos a ahorrar energía. también podemos utilizar la opción de auto ajuste de brillo.

para android deslice el dedo desde arriba hacia abajo, vaya a pantalla, brillo y ajuste hacia el nivel deseado.

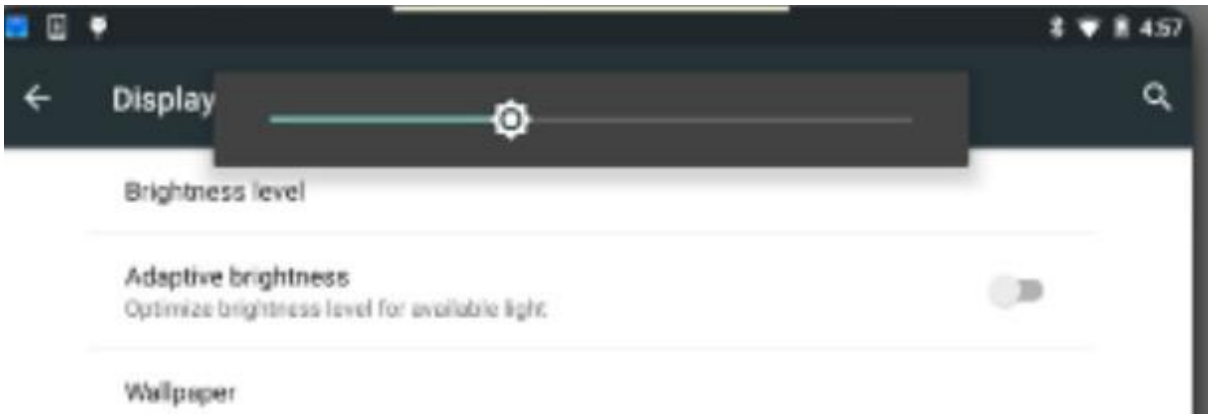

Ilustración7 : Ajustar brillo en Android

Para iphone deslice el dedo hacia arriba, en settings, display and brightness, ajuste el brillo al nivel deseado.

Ilustración 8: Ajustar brillo en IOS

otras características

- Con un teléfono inteligente puedes hacer de todo al mismo tiempo, o lo que es lo mismo, son multitareas.
- Debe contar con algún sistema operativo.
- Poseer memorias externas como micros SD.
- Cámara trasera y delantera
- Poseen agenda digital, administración de contactos
- Permitan leer documentos en distintos formatos, entre ellos los PDFs y archivos de Microsoft Office

Métodos para proteger Dispositivos Móviles

La posibilidad de bloquear el dispositivo móvil es importante porque, en muchos casos, es su primera línea de defensa. Puede que no sea la forma más fuerte de seguridad -de hecho, es sin duda la más débil- pero podría llegar a ser la diferencia en la protección de su organización al mantener el dispositivo bloqueado hasta que las medidas de administración de dispositivos móviles como la limpieza remota se ejecuten.

Bloqueos de pantalla y autenticación biométrica

Aquí cubrimos las diversas opciones de seguridad local y de bloqueo que están disponibles para las diferentes plataformas móviles.

- **Bloqueo Facial:** La mayoría de móviles de hoy en día incorporan reconocimiento facial para desbloquear el teléfono. Desde los ajustes de seguridad podemos acceder a la opción de desbloqueo facial, desde la cual podemos registrar nuestro rostro para que nos identifique y el móvil se desbloquee con solo mirarlo, siendo supuestamente un método más rápido y cómodo que el lector de huellas o la introducción de PIN o patrón.. Puede funcionar bien a través de hardware específico, como la cámara True Depth y los chips neuronales de iPhone, o bien a través del empleo de software, cómo emplean la mayoría de terminales Android. Iphone utiliza una cámara infrarroja que proyecta más de 30.000 puntos en el rostro para crear un mapa del mismo, mientras que android usan la cámara del móvil junto a un software específico para grabar la imagen.

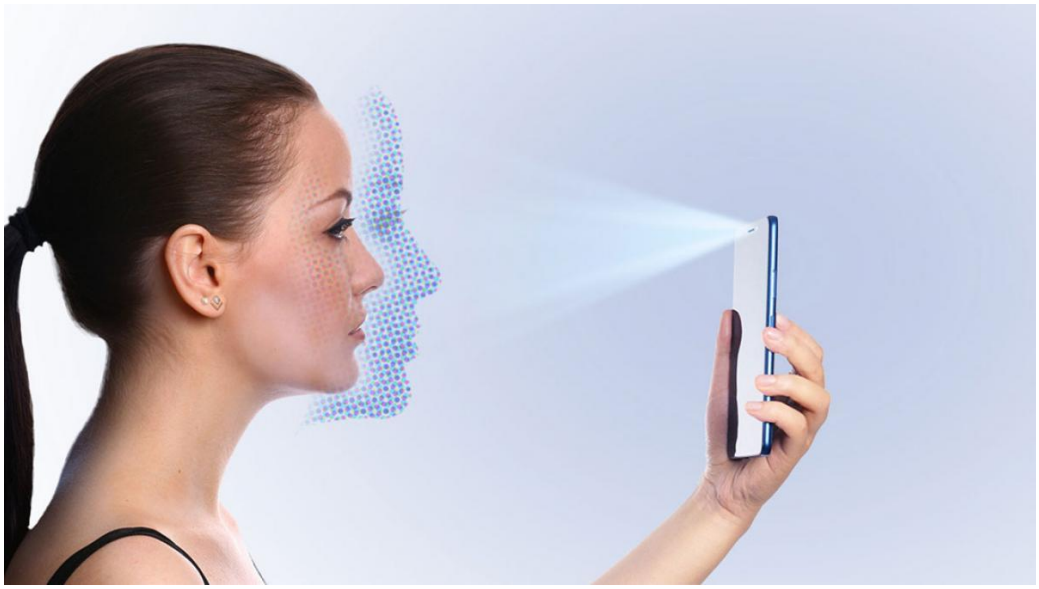

Ilustración 9: Reconocimiento Facial

- **Bloqueo de huella digital:** Este bloqueo de pantalla biométrica permite desbloquear un dispositivo mediante el escaneo de la huella digital del usuario. Funciona en android y IOS, tal que convierte el escaneo de huellas digitales del usuario en un hash exclusivo cuando el usuario toca el sensor de huellas digitales, el dispositivo vuelve a calcular el hash. El dispositivo se desbloquea si los valores del hash coinciden.

Ilustración 10: Reconocimiento Dactilar

- **Clave de bloqueo:** Este es el método más común para bloquear dispositivos móviles. las opciones de contraseña también pueden incluir la configuración de un código numérico o una contraseña alfanumérica. Este bloqueo de pantalla requiere que se ingrese un código numérico de cuatro o seis dígitos para desbloquear el dispositivo móvil.

Ilustración 11: Bloqueo de clave

- **Bloqueo de patrón:** Disponible en muchos dispositivos android. La pantalla se desbloquea dibujando un patrón con el dedo. Este bloqueo de pantalla requiere que el usuario una cuatro o más puntos en un patrón específico para desbloquear el dispositivo.

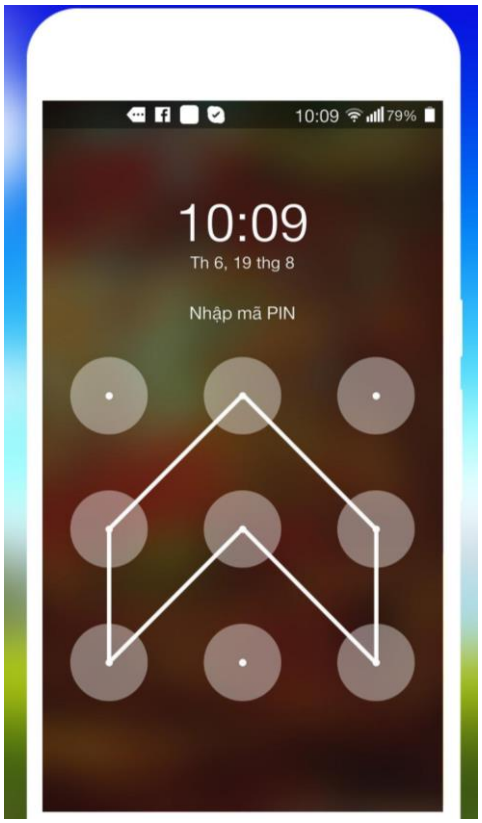

Ilustración 12: Bloqueo de patrón

- **Bloqueo de deslizamiento:** En muchos dispositivos con android también se llama Deslizar para desbloquear. Aunque es conveniente, este método

menos seguro solo se debe utilizar si la seguridad no es importante. Este bloqueo de pantalla requiere que el usuario simplemente deslice el dedo por la pantalla.

Ilustración 13: Bloqueo de deslizamiento

Restricciones tras intentos fallidos de inicio de sesión.

Para desbloquear un dispositivo móvil cuando se implementa una contraseña de manera correcta, es necesario introducir el PIN, la contraseña, el patrón u otro tipo de desbloqueo. 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.

En el caso de los dispositivos Android, la cantidad de intentos fallidos antes del bloqueo depende del dispositivo y la versión del SO Android. Es común que los dispositivos Android se bloquean 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.

Ilustración 14: Restriccion de tiempo para desbloqueo

Eliminación de datos de IOS

En los dispositivos con iOS, se puede activar como se indica la opción de eliminación de datos (Erase Data). 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, si posee copias de respaldo, use la opción de restauración y copia de respaldo (Restore and Backup) en iTunes o la opción de administración de almacenamiento (Manage Storage) en iCloud.

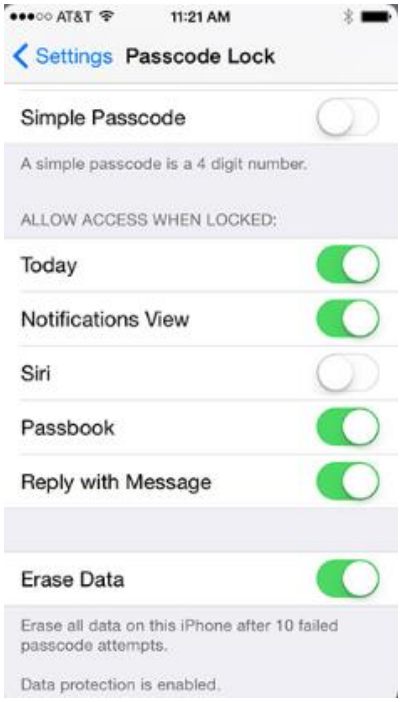

Ilustración 15: Opción de Erase Data en iOS

GUI de iOS

En iOS, para mejorar la seguridad, la contraseña se utiliza como parte de la clave de cifrado para todo el sistema. Debido a que la contraseña no se almacena en ningún lugar, nadie puede acceder a los datos del usuario en los dispositivos iOS, incluidos los dispositivos Apple. El sistema depende del usuario para proporcionar la contraseña antes de que el sistema se pueda desbloquear y descifrar para su uso. Si el usuario olvida la contraseña, no podrá acceder a sus datos y deberá hacer una restauración total con una copia de respaldo guardada en iTunes o iCloud.

Servicios habilitados para la nube para dispositivos móviles

La nube es el espacio virtual al que podemos tener acceso desde nuestros ordenadores y dispositivos móviles, y que podemos utilizar para almacenar todo tipo de archivos.

Ilustración 16: Servicios de nube

Copia de seguridad remota

Los datos de los dispositivos móviles pueden perderse debido a fallas de los dispositivos o la pérdida o el robo de los dispositivos. Se debe realizar una copia de seguridad de los datos periódicamente, para garantizar que se puedan recuperar si es necesario. En los dispositivos móviles, el almacenamiento es a menudo limitado y no extraíble. Para superar estas limitaciones, se pueden realizar copias de seguridad remotas. 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 traen 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 activar la creación automática en la nube de copias de respaldo de datos, aplicaciones y configuraciones. También se puede usar otros proveedores, como Dropbox. También se puede crear una copia de respaldo de los dispositivos móviles en una PC. iOS admite copias de respaldo en la versión de iTunes para PC. Otra opción es configurar software de administración de dispositivos móviles para que cree automáticamente copias de respaldo de los dispositivos del usuario.

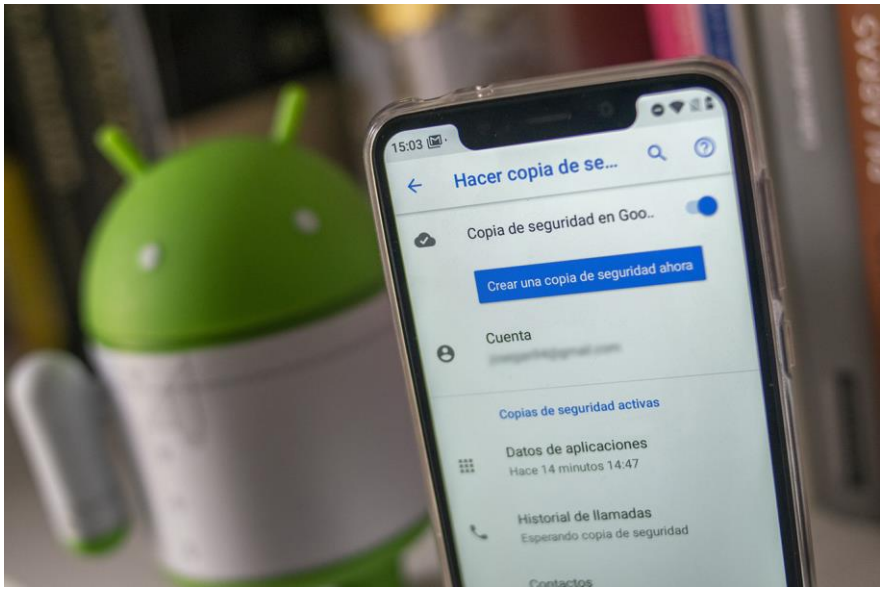

Ilustración 17: Copia de Seguridad en Android

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.

Al igual que Buscar mi iPhone de Apple, Android Device Manager permite al usuario rastrear, hacer sonar o bloquear un dispositivo extraviado, o eliminar sus datos. Para administrar un dispositivo perdido, el usuario debe visitar el tablero del Administrador de dispositivos Android, alojado en https://www.google.com/android/devicemanager, e iniciar sesión con la cuenta de Google utilizada en el dispositivo Android. El Administrador de dispositivos Android se incluye y está habilitado de manera predeterminada en Android 5.x, y se puede encontrar en Configuración > Seguridad > Administración de dispositivos.

Los usuarios de iOS pueden utilizar la aplicación Buscar mi iPhone, como se muestra en la figura. El primer paso es instalar la aplicación, iniciarla y seguir las instrucciones para configurar el software. La aplicación Buscar mi iPhone puede instalarse en otro dispositivo iOS para ubicar el dispositivo perdido.

Es importante saber que si la aplicación no puede localizar el dispositivo perdido, es posible que este se encuentre apagado o desconectado. El dispositivo debe estar conectado a una red inalámbrica o de telefonía móvil para recibir comandos de la aplicación o enviar información sobre su ubicación al usuario.

Una vez que se ubica el dispositivo, es posible realizar acciones adicionales, como enviar un mensaje o reproducir un sonido. Estas opciones son útiles si se perdió el dispositivo. Si este se encuentra cerca, la reproducción de un sonido le indica exactamente dónde está. Si el dispositivo se encuentra en otro lugar, enviar un mensaje para que se visualice en la pantalla permite que quien lo haya encontrado se comunique con usted.

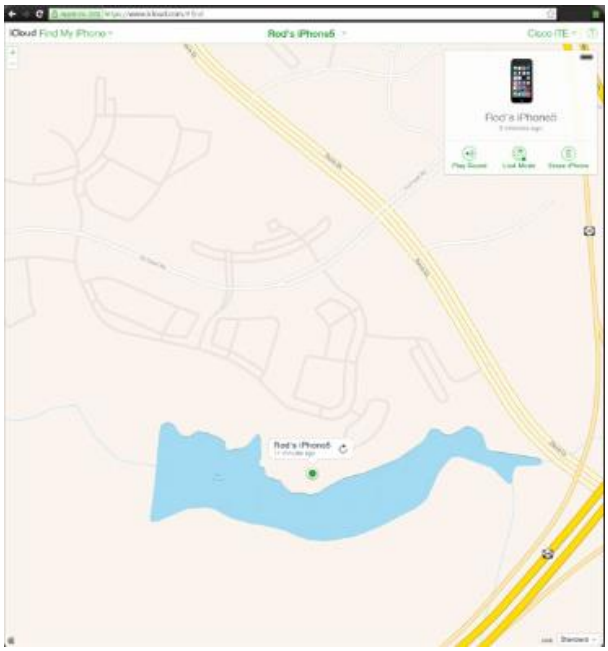

Ilustración 18: Encontrar mi teléfono en iOS

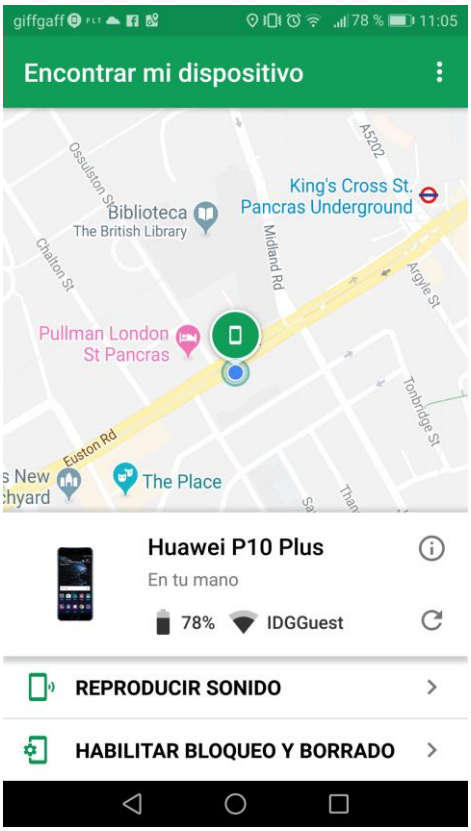

Ilustración 19: Encontrar mi teléfono en Android

Bloqueo y borrado remotos

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 mismas aplicaciones que ofrecen los servicios de encontrar mi dispositivo tienen las funciones de seguridad. Dos de las funciones de seguridad remota más comunes son: Bloqueo remoto (Remote Lock) y Borrado remoto (Remote wipe).

Es importante saber que para que estas medidas de seguridad remotas funcione, el dispositivo debe estar encendido y conectado a una red red WiFi o telefónica.

Ilustración 20: Bloqueo y Borrado Remoto en iOS y Android

- **Bloqueo Remoto:** La función bloqueo remoto de los dispositivos con iOS se denomina Modo Perdido (Lost Mode). El Administrador de dispositivos Android denomina a esta función Bloqueo. Le permite bloquear el dispositivo con una contraseña para que otros no puedan acceder a sus datos. Por ejemplo, el usuario puede mostrar los mensajes personalizados o hacer que el teléfono no suene al recibir llamadas entrantes o mensajes de texto.
- **Borrado Remoto:** La función de borrado remoto de los dispositivos con iOS se denomina Borrar teléfono. El administrador de Android denomina a esta función Borrar. Elimina todo 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.

  La mayoría de los sistemas operativos de dispositivos móviles proporcionan una opción de cifrado completo de dispositivo. El cifrado completo del dispositivo puede impedir que cualquier persona que se haga con el dispositivo eluda los controles de acceso y tenga acceso a los datos sin procesar almacenados en la memoria.

Seguridad de Software

La seguridad de software se utiliza para proteger el software contra ataques maliciosos de hackers y otros riesgos, de forma que nuestro software siga funcionando correctamente con este tipo de riesgos potenciales. Esta seguridad de software es necesaria para proporcionar integridad, autenticación y disponibilidad.

Antivirus

Todos los equipos son vulnerables al software malintencionado. Los smartphones y demás dispositivos móviles son equipos y también son vulnerables. Existen aplicaciones antivirus tanto para Android como para iOS. 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. El archivo debe iniciarse manualmente. iOS no permite análisis automáticos ni programados. Esta es una característica de seguridad que evita que los programas malintencionados utilicen recursos no autorizados o contaminen otras aplicaciones o el OS. Algunas aplicaciones antivirus también proporcionan servicios de localización, y bloqueo o borrado remotos.

Las aplicaciones de los dispositivos móviles se ejecutan en una sandbox. Un 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. En el momento de la instalación, las aplicaciones para Android solicitan permiso para acceder a ciertos recursos. Las aplicaciones malintencionadas tienen acceso a cualquier recurso al que se les haya permitido acceder durante la instalación. Esta es otra razón por la que es importante descargar sólo aplicaciones que provengan de orígenes confiables. Debido a la naturaleza de la sandbox, el software malicioso generalmente no daña los dispositivos móviles; es mucho más probable que un dispositivo móvil transfiera un programa malicioso a otro dispositivo, como un equipo portátil o de escritorio. Por ejemplo, si se descarga un programa malicioso desde el correo electrónico, Internet u otro dispositivo, el programa malicioso podría pasar a un equipo portátil la próxima vez que esta se conecte al dispositivo móvil.

Para impedir que el programa malicioso infecte más dispositivos, se puede usar un firewall. Las aplicaciones de firewall para dispositivos móviles pueden monitorear la actividad de las aplicaciones e impedir las conexiones a puertos o direcciones IP específicas. El firewall, dado que necesita poder controlar otras aplicaciones, funciona lógicamente en un nivel de permisos superior (raíz). Los firewalls que no son de raíz crean una red privada virtual (VPN) y luego controlan el acceso de las aplicaciones a la VPN.

Ilustración 21: Servicios de antivirus

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.

El rooteo y el desbloqueo son dos métodos para eliminar las restricciones y protecciones agregadas a los sistemas operativos móviles. Son un medio para sortear el funcionamiento usual del sistema operativo del dispositivo a fin de obtener permisos de administrador de raíz o superusuario. El rooteo 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. El desbloqueo 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.

Jailbreaking aprovecha las vulnerabilidades de iOS. Cuando se encuentra una vulnerabilidad utilizable, se escribe un programa. Este programa es el software de desbloqueo real y luego se distribuye en Internet. Apple desaconseja usar jailbreaking, y trabaja activamente para eliminar las vulnerabilidades que hacen posible realizar jailbreaking en iOS. Además de las actualizaciones del SO y las correcciones de errores, las nuevas versiones de iOS generalmente incluyen parches para eliminar las vulnerabilidades conocidas que permiten jailbreaking. Cuando se corrigen vulnerabilidades de iOS mediante actualizaciones, esto obliga a los piratas informáticos a empezar de nuevo.

Es importante saber que el proceso de jailbreak es totalmente reversible. Para eliminar el jailbreak y restituir el estado de fábrica del dispositivo, conéctelo a iTunes y ejecute una restauración.

Ilustración 22: Root y Jailbreaking

Revisiones y actualización de los sistemas operativos

Al igual que el OS de los equipos 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.

Debido a la gran cantidad y diversidad de móviles Android, las actualizaciones y las revisiones no se lanzan como un solo paquete para todos los dispositivos. A veces, no se puede instalar una versión nueva de Android en dispositivos más antiguos, debido a que el hardware no cumple con las especificaciones mínimas. En estos dispositivos, se pueden efectuar revisiones para solucionar problemas conocidos, pero no admiten actualizaciones del OS.

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, como se muestra en la figura. Toque la actualización para iniciar el proceso de descarga e instalación.

Las actualizaciones de iOS también utilizan un proceso de entrega automatizado, y también se excluyen los dispositivos que no cumplen con los requisitos de hardware. Para buscar actualizaciones de iOS, conecte el dispositivo a iTunes. Si hay alguna disponible, se abre una notificación de descarga.

Hay otros dos tipos de actualizaciones de firmware de radio de dispositivo móvil que son importantes. Estas se denominan actualizaciones de banda base y consisten en la lista de roaming preferida (PRL) y el ISDN de velocidad primario (PRI). La 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 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.

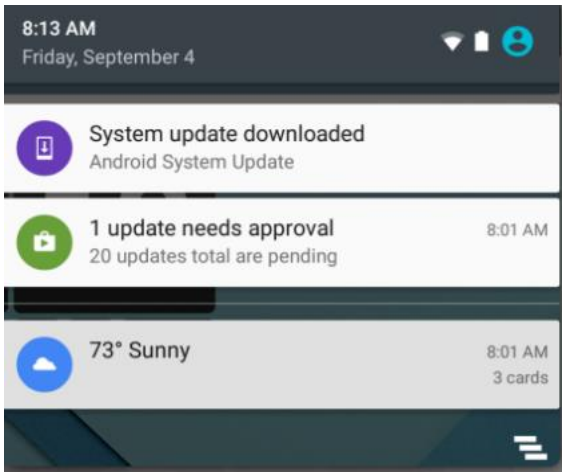

Ilustración 23: Notificación de Actualización de sistema en Android

Sistemas operativos Linux y MacOs

Analizando Linux y macOS, nos encontramos que son sistemas basados en Unix, por lo que creemos que sería excelente que definamos unix, su definición según wikipedia es la siguiente.

Unix es una familia de sistemas operativos de computadora multitarea y multiusuario que se derivan del AT&T Unix original, cuyo desarrollo comenzó en la década de 1970 en el centro de investigación Bell Labs por Ken Thompson, Dennis Ritchie y otros.

Los sistemas Unix se caracterizan por un diseño modular que a veces se denomina "filosofía Unix".

De acuerdo con esta filosofía, el sistema operativo debe proporcionar un conjunto de herramientas simples, cada una de las cuales realiza una función limitada y bien definida.

Un sistema de archivos unificado (el sistema de archivos Unix) y un mecanismo de comunicación entre procesos conocido como "tuberías" sirven como los principales medios de comunicación, y un lenguaje de comandos y secuencias de comandos de shell (el shell de Unix) se utiliza para combinar las herramientas para realizar flujos de trabajo complejos.

Es comprensible la influencia de unix en estos sistemas operativos. Con esto en mente, podemos conocer las virtudes de Linux y las de macOS.

Sobre el término Linux citamos la definición de Karim Yaghmour en el libro Building Embedded Linux Systems:

“Linux se usa indistintamente en referencia al kernel de Linux, un sistema Linux o una distribución de Linux. La amplitud del término juega a favor de la adopción de Linux, en el sentido amplio, cuando se presenta a un público no técnico, pero puede resultar molesto cuando se brindan explicaciones técnicas.” (Yaghmour, 2017)

La confusión del término se debe justamente a que se usa de forma amplia, como es el caso de este ejemplo.

Ilustración 24: Sistema operativo Linux usando la distribución Ubuntu.

Si, por ejemplo, digo: "Linux proporciona redes TCP / IP". ¿Me refiero a la pila de TCP / IP en el kernel o las utilidades de TCP / IP proporcionadas en una distribución de Linux que también son parte de un sistema Linux instalado, o ambos? Esta vaguedad en realidad se convirtió en munición para los defensores del apodo de “GNU / Linux”, quienes señalaron que Linux era el kernel, pero que el sistema estaba construido principalmente sobre software GNU.

Citando wikipedia , MacOS por su lado es un sistema operativo gráfico patentado desarrollado y comercializado por Apple Inc. desde 2001. Es el sistema operativo principal para las computadoras Mac de Apple. (Wikipedia, 2021)

Prácticas recomendadas para Linux y macOS

Comandos básicos de CLI

A continuación presentamos una tabla con comandos sencillos y básicos que puedes emplear en tu sistema operativo Linux y MacOS.

Command	Description
ls	Enumere el sistema de directorio (carpeta).
cd <<dirección>>	Cambiar directorio (carpeta) en el sistema de archivos.
cd ..	Sube un nivel (una carpeta) en el sistema de archivos.
cp	Copie un archivo en otra carpeta.
mv	Mueve un archivo a otra carpeta.
mkdir	Crea un nuevo directorio (carpeta).
rmdir	Eliminar un directorio (carpeta).
clear	Borra la ventana CLI.
exit	Cierra la ventana CLI.
man <<comando>>	Muestra el manual de un comando determinado.

Tabla 1: Tabla de comandos básicos unix.

¿Por qué es importante aprender linux?

Del libro Running Linux, Matthias Kalle Dalheimer, Lar Kaufman, and Matt Welsh nos comentan sus razones.

¿Por qué usar Linux en lugar de un sistema operativo comercial? Podríamos darte mil razones. Sin embargo, uno de los más importantes es que Linux es una excelente opción para la computación personal Unix. Si es un desarrollador de software Unix, ¿por qué usar Windows en casa? Linux le permitirá desarrollar y probar el software Unix en su PC, incluida la base de datos y las aplicaciones X. Si eres estudiante, lo más probable es que el sistema informático de tu universidad

ejecute Unix. Con Linux, puede ejecutar su propio sistema Unix y adaptarlo a sus propias necesidades. Instalar y ejecutar Linux también es una excelente manera de aprender Unix si no tiene acceso a otras máquinas Unix.

Pero no perdamos la perspectiva. Linux no es solo para usuarios personales de Unix. Es lo suficientemente robusto y completo para manejar tareas grandes, así como necesidades de computación distribuida. Muchas empresas se están trasladando a Linux en lugar de otros entornos de estaciones de trabajo basados en Unix. Linux tiene una excelente relación precio-rendimiento, es uno de los sistemas operativos más estables y potentes disponibles y, debido a su naturaleza de código abierto, es completamente personalizable para sus necesidades. Las universidades están descubriendo que Linux es perfecto para impartir cursos de diseño de sistemas operativos. Los proveedores de software comercial más grandes están comenzando a darse cuenta de las oportunidades que puede brindar un sistema operativo gratuito. (Dalheimer et al, 2018)

¿Certificarse en Linux?

Notando las capacidades de linux de influir en diferentes dispositivos y ser motor de tendencias como lo es el internet de las cosas y la computación en la nube. Suena justo que existan certificaciones que permitan a individuos distinguirse como administradores de sistemas operativos. Aquí le presento sobre Linux Professional Institute (LPI) , que es uno de las principales organizaciones que certifica a estos profesionales, tomando el concepto de Adam Haeder, Stephen Addison Schneiter, James Stanger, and Bruno Gomes Pessanha en su libro LPI Linux Certification in a Nutshell, 3rd Edition.

El Linux Professional Institute es una organización sin fines de lucro formada con el único objetivo de proporcionar un estándar para la certificación neutral del proveedor. Este objetivo se logra mediante la certificación de administradores de Linux a través de un proceso de desarrollo de código abierto modificado. LPI busca la opinión del público para sus objetivos y preguntas del examen, y cualquier persona es bienvenida a participar. Cuenta con personal remunerado y voluntario y recibe fondos de algunos de los principales nombres de la industria informática. El resultado es un programa desarrollado públicamente y neutral para el proveedor que se ofrece a un precio razonable.

LPI actualmente organiza su serie de Certificación del Instituto Profesional de Linux (LPIC) más popular en tres niveles. Este libro cubre los exámenes LPIC Nivel 1 101 y 102.

El nivel 1 está dirigido a administradores de Linux de nivel junior a medio con aproximadamente dos años de experiencia práctica en administración de sistemas. El candidato de Nivel 1 debe sentirse cómodo con Linux en la línea de comandos y ser capaz de realizar tareas sencillas, incluida la instalación del sistema y la

resolución de problemas. Se requiere la certificación de nivel 1 antes de obtener el estado de certificación de nivel 2.

Todos los exámenes de LPI se basan en un conjunto publicado de objetivos técnicos. Estos Objetivos técnicos se publican en el sitio web de LPI y, para su conveniencia, están impresos al comienzo de cada capítulo de este libro. A cada Objetivo establecido por LPI se le asigna un peso numérico, que actúa como un indicador de la importancia del Objetivo. Los pesos oscilan entre 1 y 8, y los números más altos indican más importancia. Un objetivo con un peso de 1 puede considerarse relativamente poco importante y no es probable que se cubra con mucha profundidad en el examen. Los objetivos con pesos más grandes seguramente se cubrirán en el examen, por lo que debe estudiarlos de cerca. Los pesos de los objetivos se proporcionan al comienzo de cada capítulo.

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

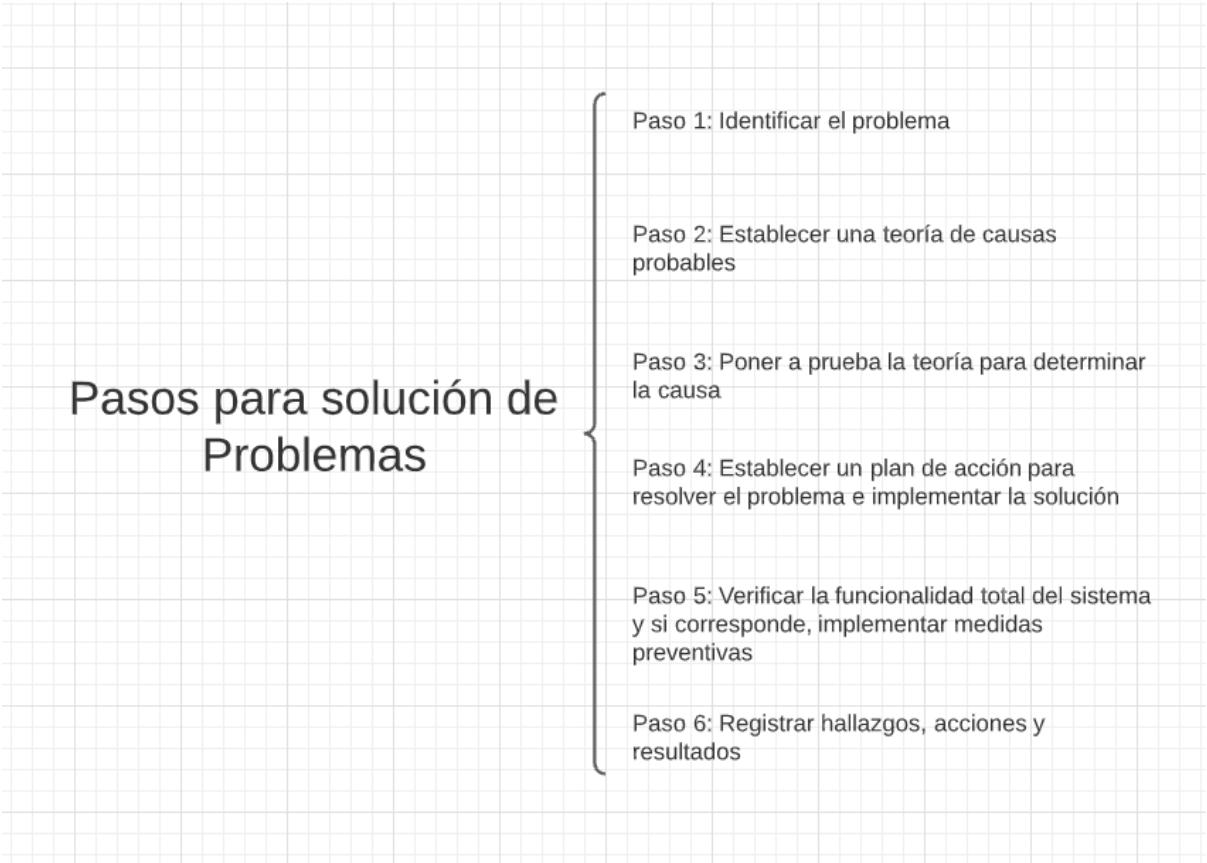

Ilustración 25: Diagrama de llaves con los 6 pasos para solución de problemas

Paso 1: Identificar el problema.

Al ser el primer contacto con el usuario su finalidad es de resolver el problema en cuestión.

Paso 2: Establecer una teoría de causas probables.

Una vez que se habló con el cliente, el profesional empieza a formular una teoría de las causas probables del problema.

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

Con las teorías en mente, es momento de probar las soluciones en mente. Si el problema no se corrige con un procedimiento rápido, quizá sea momento de volver a pasos anteriores y continuar investigando el problema

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

Después de iterar en el paso 3 y ya encontrado la causa exacta del problema, es momento de establecer un plan de acción para resolver el problema e implementar la solución.

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

Una vez que haya corregido el problema, verifique la funcionalidad total y, si corresponde, implemente medidas preventivas.

Paso 6: Registrar hallazgos, acciones y resultados.

El último paso del proceso de solución de problemas consiste en registrar los hallazgos, las acciones y los resultados

Problemas y soluciones comunes de otros sistemas operativos

Dispositivos móviles

- Una aplicación no responde

  Podemos forzar el cierre de la aplicación, reiniciar el dispositivo móvil y/o eliminar la aplicación e instalarla.

- El dispositivo móvil tiene rendimiento lento

Podemos cerrar todas las aplicaciones innecesarias, desactivar el GPS y/o reiniciar el dispositivo

- La pantalla táctil del dispositivo móvil tiene respuesta incorrecta

  Limpiar la pantalla táctil o reemplazar la pantalla táctil si detectamos daños como exposición al agua.

Sistemas operativos Linux y MacOS

- Una aplicación no responde en MacOS

  Podemos forzar el cierre de la aplicación (con Force Quit)

- WI-FI no es accesible a través de Ubuntu

  Instalar el controlador de Linux desde el sitio web del fabricante, si está disponible.

  Instalar el controlador de Linux desde el repositorio Ubuntu , si está disponible.

- El directorio aparece vacío

  Volver a montar el disco mediante el directorio correcto con disk utility.

Conclusiones

1. Si la seguridad y la privacidad son un factor importante para ti, entonces el iPhone será tu mejor opción. Si la vida útil de la batería está en la parte superior de tu lista, y además deseas poder personalizar tu teléfono, opta mejor por Android.
2. la decisión de elegir un tipo de sistema operativo para móviles depende en si de lo que el usuario busque. No podemos decir que un sistema operativo es mejor que el otro ya que cada uno resalta en aspectos diferentes.
3. El sistema operativo android está diseñado para ser utilizado en muchos dispositivos ya que se trata de un sistema operativo abierto mientras que IOS al ser cerrado sucede lo contrario.
4. Si lo que deseas es un dispositivo móvil que cubra tus necesidades más elementales y, además, te permita disponer de las mejores aplicaciones antes que nadie, iOS es tu solución, ya que las nuevas apps suelen aparecer primero en App Store y, más tarde, en Google Play Store.
5. La interfaz de iOS resulta más sencilla e intuitiva que la de Android
6. En un equipo con sistema iOS, las actualizaciones son automáticas mientras que en Android no.
7. Los sistemas operativos Linux y MacOS basados en Unix representan una gran alternativa al sistema Windows.
8. Linux al ser un sistema operativo abierto (de código abierto), es ampliamente utilizado en servidores, internet de las cosas y la nube.
9. MacOS al ser un sistema operativo cerrado, es exclusivo para los productos de la marca App
10. Los dispositivos móviles cuentan con opciones de seguridad como lo son bloqueos de pantalla, la autenticación biométrica, el bloqueo remoto, el borrado remoto, que le brindan una protección en caso de robo o pérdida.
11. Los antivirus juegan un papel importante en la protección de nuestros dispositivos móviles, ya que pueden identificar y borrar cualquier software o archivo malicioso que se encuentre en el móvil e impide que se propague a otros dispositivos gracias a el firewall.
12. El rooting o el jailbreaking pueden ofrecer más libertad en nuestro dispositivo móvil, pero también puede afectar nuestra garantía y poner en peligro nuestro software con virus que fácilmente pueden entrar al no existir una protección del sistema.

Referencias y bibliografía

1. Girao, D. (2020, 6 octubre). *¿Cómo se usan las llamadas Wi-Fi en tu móvil?* MovilZona. https://www.movilzona.es/2020/06/25/activar-llamadas-wifi-marcas/
2. Wikipedia contributors. (2021, 11 junio). *MacOS*. Wikipedia. https://en.wikipedia.org/wiki/MacOS
3. W3Schools. (s. f.). What is CLI. Recuperado 14 de junio de 2021, de https://www.w3schools.com/whatis/whatis_cli.asp
4. Running Linux, Matthias Kalle Dalheimer, Lar Kaufman, and Matt Welsh
5. Ruiz, A. (2020, 30 junio). Medidas de seguridad en telefonía móvil. Tecnología para los negocios.
6. https://ticnegocios.camaravalencia.com/servicios/tendencias/medidas-de-seguridad-en-telefonia-movil/
7. *Android vs iOS*. (s. f.). Diffen. Recuperado 15 de junio de 2021, de https://www.diffen.com/difference/Android_vs_iOS#:%7E:text=Android%20vs.%20iOS.%20Google%27s%20Android%20and%20Apple%27s%20iOS,are%20generally%20more%20customizable%20from%20top%20to%20bottom.
8. *iOS vs Android: The Full Comparison Between Android and iOS*. (s. f.). iSkysoft. Recuperado 15 de junio de 2021, de https://www.iskysoft.com/phone-transfer/ios-vs-android.html
9. colaboradores de Wikipedia. (2021, 12 junio). *Android*. Wikipedia, la enciclopedia libre. https://es.wikipedia.org/wiki/Android
10. Sanmartín, D. (2012, 25 mayo). *Así funciona el acelerómetro en nuestros teléfonos*. Xataka Móvil. https://www.xatakamovil.com/varios/asi-funciona-el-acelerometro-en-nuestros-telefono.

Anexos

Anexo 1 Distribuciones Linux:

Anexo 2 Problemas y soluciones comunes de los sistemas operativos Linux y macOS de Cisco Networking Academy

Networking Academy

Problemas y soluciones comunes de los sistemas operativos Linux y macOS

Identificación del problema	Causas probables	Soluciones posibles
La operación de respaldo automática no se inicia.	Time Machine está desactivado en macOS.	Activar Time Machine en macOS.
La operación de respaldo automática no se inicia.	Déjà Dup está desactivado en Linux.	Activar Déjà Dup en Linux.
El directorio aparece vacío.	El directorio es el punto de montaje para otro disco o partición.	Volver a montar el disco mediante el directorio correcto con Disk Utility (Utilidad de discos) para macOS.
El directorio aparece vacío.	El directorio es el punto de montaje para otro disco o partición.	Volver a montar el disco mediante el directorio correcto con Disks (Discos) para Linux.
El directorio aparece vacío.	Los archivos se eliminaron por accidente.	Restaurar los archivos borrados desde la copia de respaldo a través de Time Machine o Déjà Dup.
El directorio aparece vacío.	Los archivos están ocultos.	Utilizar la opción Mostrar archivos ocultos en el explorador de archivos.
Una aplicación deja de responder en macOS.	La aplicación dejó de funcionar	Aplicar un cierre forzoso de la aplicación (con Force Quit).
Una aplicación deja de responder en macOS.	La aplicación utilizaba un recurso que no está disponible.	Aplicar un cierre forzoso de la aplicación (con Force Quit).
Wifi no es accesible a través de Ubuntu.	El controlador NIC inalámbrico no se instaló correctamente.	Instalar el controlador de Linux desde el sitio web del fabricante, si está disponible.
Wifi no es accesible a través de Ubuntu.	El controlador NIC inalámbrico no se instaló correctamente.	Instalar el controlador de Linux desde el repositorio de Ubuntu, si está disponible.
Wifi no es accesible a través de Ubuntu.	El controlador NIC inalámbrico no se instaló correctamente.	Buscar la tarjeta inalámbrica en la lista de hardware compatible de la distribución de Linux.
macOS no puede leer el disco óptico remoto mediante Remote Disc (Disco remoto).	La Mac ya tiene una unidad óptica instalada.	Colocar los medios en la unidad óptica local.
macOS no puede leer el disco óptico remoto mediante Remote Disc (Disco remoto).	Se ha activado la opción para solicitar permiso para usar la unidad óptica.	Aceptar la solicitud de permiso para usar la unidad.

Identificación del problema	Causas probables	Soluciones posibles
Linux no arranca y recibe un mensaje “Missing GRUB” (GRUB faltante) o “Missing LILO” (LILO faltante).	GRUB o LILO están dañados.	Ejecutar Linux desde los medios de instalación, abrir una terminal e instalar el administrador de arranque con el comando: sudo grub-install o sudo lilo-install.
Linux no arranca y recibe un mensaje “Missing GRUB” (GRUB faltante) o “Missing LILO” (LILO faltante).	GRUB o LILO se eliminaron.	Ejecutar Linux desde los medios de instalación, abrir una terminal e instalar el administrador de arranque con el comando: sudo grub-install o sudo lilo-install.
El sistema operativo Mac o Linux se congela en el inicio y presenta una emergencia de kernel donde hay una pantalla de detención.	Se ha alterado un controlador.	Actualizar todos los controladores del dispositivo desde el sitio web del fabricante.
El sistema operativo Mac o Linux se congela en el inicio y presenta una emergencia de kernel donde hay una pantalla de detención.	El hardware presenta fallas.	Reemplazar cualquier hardware defectuoso.