UNIVERSIDAD DE LAS FUERZAS ARMADAS
ESPE

Sistemas Operativos

Departamento de Ciencias de la Computación

Seguridades en Sistemas Operativos

Estudiantes:

Josué Merino, Adrián Ramos, Paúl Sánchez

Docente:

Ing. Washington Loza Herrera

Índice general

Índice de figuras

Índice de Tablas

1. Objetivos

1.1. Objetivo General

Analizar y comparar los mecanismos de seguridad implementados en los sistemas operativos Windows y Linux, así como en las plataformas móviles Android e iOS, con el fin de evaluar su eficacia en la protección de datos y prevención de vulnerabilidades.

1.2. Objetivos Específicos

- Identificar y describir las principales características de seguridad en Windows y Linux, incluyendo sistemas de autenticación, cifrado y protección contra malware.
- Examinar las medidas de seguridad en Android e iOS, comparando sus modelos de protección de aplicaciones, gestión de permisos y respuesta ante amenazas.
- Evaluar las fortalezas y debilidades de cada sistema operativo en términos de seguridad, considerando ataques comunes y estrategias de mitigación.

2. Windows

La aplicación Seguridad de Windows es una solución de seguridad completa integrada en Windows, está diseñada para proteger el dispositivo y los datos de diversas amenazas. Incluye funciones como antivirus Microsoft Defender, firewall de Windows y control de aplicaciones inteligentes, que funcionan de forma conjunta para proporcionar protección en tiempo real contra virus, malware y otras amenazas de seguridad. La aplicación está integrada en Windows, lo que garantiza que el dispositivo esté protegido desde el momento en que se inicia. [1]

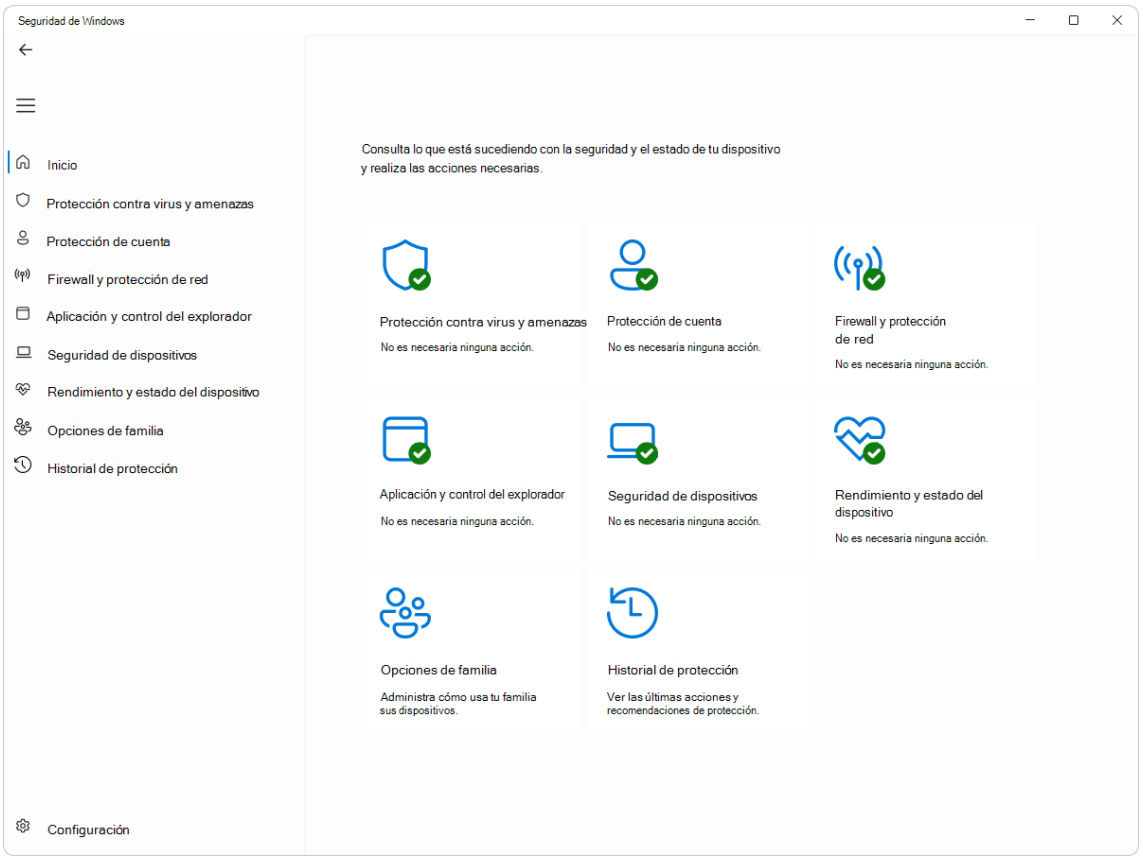

Figura 2.1: Seguridad de Windows

2.1. Servicios

Windows ofrece capas de seguridad para ayudar a mantener alejadas a las personas malintencionadas. [2] Desde protección de datos y malware hasta apps de confianza, credenciales, fotos y archivos están protegidos.

- Antivirus de Microsoft Defender: Una solución de protección antivirus en tiempo real y siempre activa de nueva generación,
- SmartScreen de Microsoft Defender: Si un sitio web, aplicación o descarga fuese potencialmente malintencionado SmartScreen advertirá.
- Firewall de Windows: El tráfico no deseado se bloquea y se impide su entrada a la PC.
- Protección Bluetooth: Ya sea que se use cascos, ratones, teclados u otros accesorios inalámbricos Bluetooth, la conexión es segura.
- Conexión Wifi segura: La característica Wi-Fi de Windows admite métodos estandarizados del sector para autenticación y cifrado que ayudan a proteger independientemente dónde se conecte, incluso en las redes públicas.
- Redes privadas virtuales (VPN): Una VPN, o red privada virtual, es una tunelización segura que conecta la PC a Internet. En la Microsoft Store se ofrece una variedad de apps VPN.

2.2. Seguridad del Dispositivo

La seguridad basada en el hardware y el nivel de confianza que ofrece ayudan a conservar y validar la integridad del sistema y del hardware. Arranque seguro de UEFI sirve para evitar que el malware se incruste en el hardware o se inicie antes que el SO. Arranque seguro ayuda a conservar la integridad del resto del SO. [3] La seguridad basada en virtualización (VBS), impulsada por la tecnología de hipervisor, mueve algunos de los procesos más sensibles de Windows a un entorno de ejecución seguro, con el fin de evitar falsificaciones y cuando ya se ha expuesto al riesgo el kernel de Windows. [3]

2.3. Medidas de Seguridad en Windows

Windows incorpora diversas medidas de seguridad para proteger a los usuarios contra amenazas cibernéticas, pérdida de datos y accesos no autorizados. A continuación, se describen algunas de las principales características de seguridad. [1]

2.3.1. Protección contra Ransomware

Windows Defender incluye la función de acceso controlado a carpetas, la cual evita que aplicaciones no autorizadas realicen cambios en archivos protegidos. Además, la integración con OneDrive permite la recuperación de archivos en caso de ataques de ransomware.

2.3.2. Cifrado y Protección de Datos

Para garantizar la seguridad de la información almacenada en los dispositivos, Windows ofrece las siguientes opciones de cifrado:

- **BitLocker:** Proporciona cifrado de disco completo para proteger los datos en caso de robo o pérdida del dispositivo.
- **Encrypting File System (EFS):** Permite cifrar archivos y carpetas de manera individual en sistemas con formato NTFS, proporcionando una capa adicional de seguridad.

Figura 2.2: BitLocker

2.3.3. Autenticación y Control de Acceso

El sistema operativo Windows implementa diversas tecnologías para mejorar la autenticación y restringir accesos no autorizados:

- **Windows Hello:** Soporta autenticación biométrica mediante reconocimiento facial o huellas dactilares para una mayor seguridad en el inicio de sesión.
- **Control de Cuentas de Usuario (UAC):** Previene cambios no autorizados en el sistema solicitando permisos administrativos cuando es necesario.
- **Windows Credential Guard:** Utiliza virtualización para proteger credenciales y evitar ataques de robo de credenciales como Pass-the-Hash o Pass-the-Ticket.

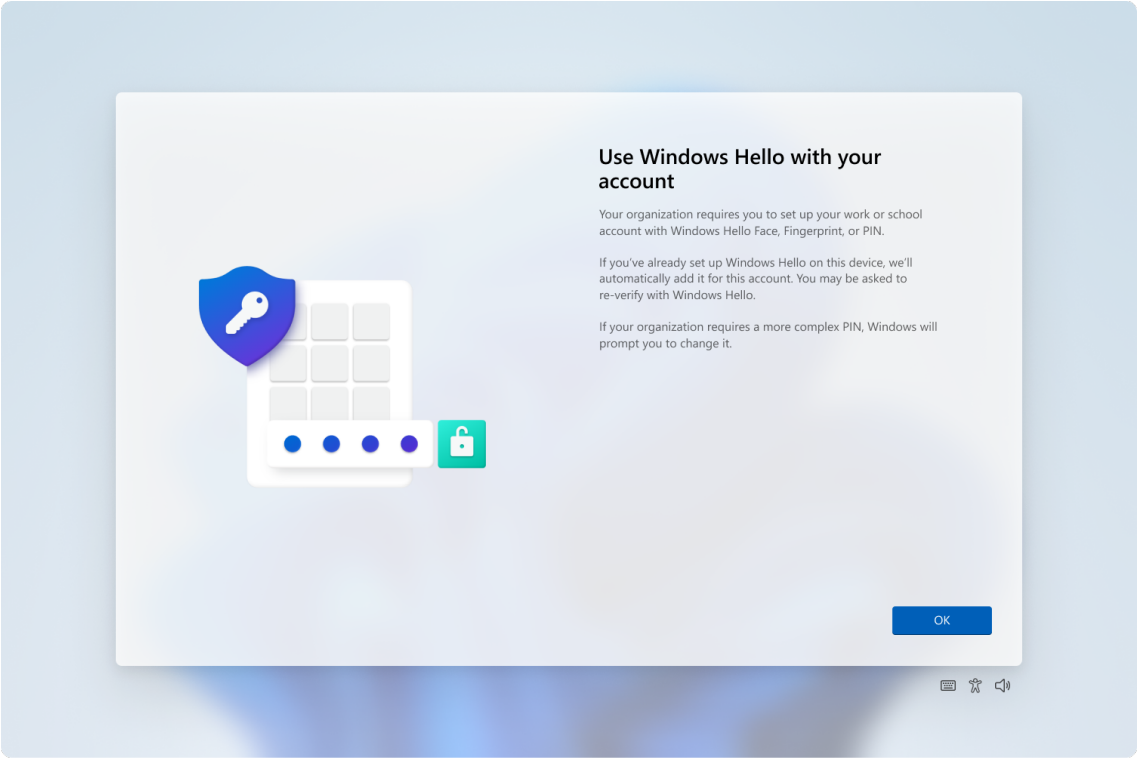

Figura 2.3: Windows Hello

2.3.4. Protección en Navegadores

Microsoft Edge, el navegador de Windows, implementa funciones avanzadas de seguridad para proteger a los usuarios mientras navegan en línea:

- **SmartScreen de Microsoft Defender:** Filtra sitios web maliciosos y protege contra ataques de phishing.
- **Windows Defender Application Guard:** Ejecuta sitios web sospechosos en un entorno virtualizado para prevenir ataques que comprometan el sistema operativo.

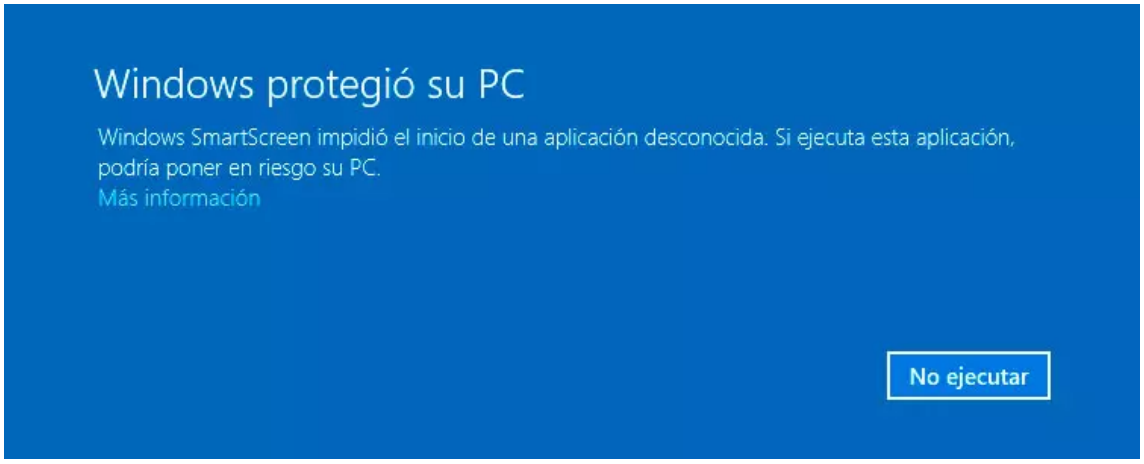

Figura 2.4: Smart Screen

2.3.5. Seguridad en Entornos Empresariales

Para empresas y organizaciones, Windows proporciona herramientas avanzadas de seguridad y gestión de dispositivos:

- **Windows Defender for Endpoint:** Solución avanzada de detección y respuesta ante amenazas (EDR).
- **Microsoft Intune:** Plataforma para la gestión y seguridad de dispositivos en entornos corporativos.
- **Active Directory y Azure AD:** Servicios para la administración de usuarios y políticas de seguridad en redes empresariales.

Figura 2.5: Microsoft Intune

3. Linux

3.1. Vulnerabilidades

3.1.1. Contraseñas débiles o por defecto

El uso de contraseñas débiles – o incluso la ausencia de contraseñas – permite que los ciberdelincuentes obtengan acceso sin restricciones a los sistemas y ambientes. A pesar de los esfuerzos por promover el uso de contraseñas fuertes, las contraseñas débiles o por defecto siguen siendo comunes. Las contraseñas, siendo una pieza crítica de información sensible, deben ser protegidas de la mejor forma posible [9]

3.1.2. Servicios expuestos en el internet

Dejar servicios expuestos al internet cuando deberían ser accesibles solo a redes locales o adyacentes es una de las fallas de configuración más serias, a menudo ignoradas. Es importante destacar que no todos los ataques se manifestarán con ruido.[ev]idente; un atacante podría dejar un backdoor o ejecutar una actividad de bajo cómputo en el sistema comprometido, lo que hace que sea más difícil detectar estos ataques [9]

3.1.3. Compartir archivos abiertamente

Tener archivos accesibles públicamente pone en riesgo mucha información. Compartir servicios como FTP, SMB, NFS, directorios en servidores web, o incluso almacenamiento en la nube (como Amazon S3 o Azure Blob), puede exponer datos a la audiencia equivocada [9]

3.2. ¿Qué tipos de seguridades hay?

3.2.1. Seguridad física

El nivel de seguridad física requerido por un sistema depende de su entorno físico. Un usuario doméstico generalmente no necesitará proteger su equipo más allá de medidas simples, como evitar el acceso no autorizado de niños o protegerlo de condiciones ambientales. En un entorno corporativo, los requisitos de seguridad física pueden ser mucho más estrictos. Linux proporciona las herramientas necesarias para asegurar un sistema operativo a nivel físico: [8]

- Arranque seguro con identificación de usuario a través de login.
- Registro de intentos de acceso (fallidos o no).
- Capacidad de bloquear terminales.
- Salvapantallas.
- Capacidades de un sistema multiusuario.

3.2.2. Seguridad local

Linux permite que múltiples usuarios trabajen al mismo tiempo en un sistema, lo que requiere medidas de seguridad adicionales:

- Control de acceso mediante usuario y clave.
- Cada archivo y directorio debe tener su propietario y permisos asignados.
- Las contraseñas deben ser fáciles de recordar pero difíciles de adivinar.
- Se deben localizar y eliminar los ejecutables SUID/SGID innecesarios.

3.2.3. Seguridad del sistema de archivos

Cada usuario debe tener solo los permisos necesarios para su trabajo sin comprometer la seguridad de otros usuarios. Para ello, es recomendable:

- Distribuir correctamente el espacio de almacenamiento para limitar el riesgo de fallo de particiones.
- Asegurarse de que los ficheros sean accesibles solo por los usuarios necesarios.
- Usar enlaces duros o simbólicos adecuadamente.
- Ejecutar programas como Tripwire para verificar la integridad de los archivos.

3.2.4. Seguridad del root

El administrador debe evitar daños al sistema por errores de confianza. Para ello, debe:

- Evitar usar la cuenta de root por defecto.
- Ejecutar los comandos de manera segura, verificando previamente la acción.
- Utilizar canales seguros (como SSH) para evitar que la clave de root viaje sin cifrar.

3.2.5. Seguridad del host

El administrador de seguridad local debe asegurarse de:

- Elegir contraseñas seguras.
- Asegurar los servicios de red local del host.
- Mantener registros detallados de las cuentas y mejorar los programas con exploits conocidos.

3.3. Herramientas de seguridad

3.3.1. Bastille

Bastille es una herramienta diseñada para aumentar la seguridad a nivel local en entornos Linux. Gestiona medidas para prevenir problemas en caso de que un atacante ingrese al sistema. Bastille automatiza tareas comunes, como la eliminación

de servicios innecesarios, proporcionando una configuración más segura del sistema operativo [8]

3.3.2. Nessus

Nessus es un scanner de vulnerabilidades que permite realizar una exploración exhaustiva de los puertos de un sistema y detectar posibles vulnerabilidades [8]

3.3.3. TCP Wrappers

TCP Wrappers filtra el acceso a servicios de red, controlando las conexiones a sistemas basados en UNIX como Linux o BSD [8]

3.3.4. Tripwire

Tripwire es una herramienta de código abierto que ayuda a verificar la integridad de los archivos, alertando al administrador sobre cambios no autorizados [8].

3.3.5. Netcat

Netcat es una herramienta de red que permite abrir puertos TCP/UDP en un host y asociar una shell a un puerto específico [8]

3.3.6. TCPDump

TCPDump permite monitorizar el tráfico de red, capturar paquetes y detectar posibles problemas como ataques ping [8]

3.4. Bibliografía

Chiesa, M. L. (s.f.). *Seguridad en Linux*. ElHacker. https://elhacker.info/Cursos/(Tutorial)

Trend Micro. (2021, febrero 23). *LINUX: Amenazas, Riesgos y Recomendaciones - Trend Micro Simply Security*. Trend Micro Simply Security. http://blog.la.trendmicro.com/linu amenazas-riesgos-y-recomendaciones/

4. Android

4.1. Introducción

Android es un sistema operativo desarrollado por Google basado en un modelo de código abierto. Esta característica permite una gran personalización y adaptación por parte de fabricantes y desarrolladores, lo que genera un ecosistema muy diverso. Sin embargo, esta flexibilidad también plantea desafíos para lograr una implementación homogénea de las medidas de seguridad en todos los dispositivos [5].

4.2. Estructura del Sistema Operativo

Al ser un sistema de código abierto, Android permite que terceros modifiquen y adapten la plataforma según sus necesidades. Esta capacidad de personalización resulta en variaciones significativas en la implementación de medidas de seguridad, ya que cada fabricante puede introducir sus propios ajustes y parches. Por ello, la seguridad en Android depende en gran medida de la colaboración entre Google, los fabricantes y los operadores móviles [5].

4.3. Actualizaciones de Seguridad

Google publica parches de seguridad de forma mensual para abordar vulnerabilidades conocidas en Android. No obstante, la efectividad de estas actualizaciones depende de la rapidez con que sean distribuidas e instaladas por los fabricantes y operadores. Esta fragmentación en la distribución de actualizaciones representa uno de los principales retos para mantener la seguridad en el ecosistema Android [5].

4.4. Protección contra Software Malicioso

Para combatir el software malicioso, Android cuenta con **Google Play Protect**, un mecanismo que analiza las aplicaciones instaladas y las que se descargan desde la Google Play Store. Este sistema escanea continuamente en busca de comportamientos anómalos y posibles amenazas, protegiendo al usuario de aplicaciones maliciosas [7].

4.5. Gestión de Permisos

Una de las ventajas de Android es su capacidad para gestionar de forma granular los permisos que se otorgan a cada aplicación. Los usuarios pueden controlar qué datos y funciones del dispositivo pueden ser accedidos por las aplicaciones, lo que reduce la posibilidad de que una app comprometida pueda exponer información sensible [7].

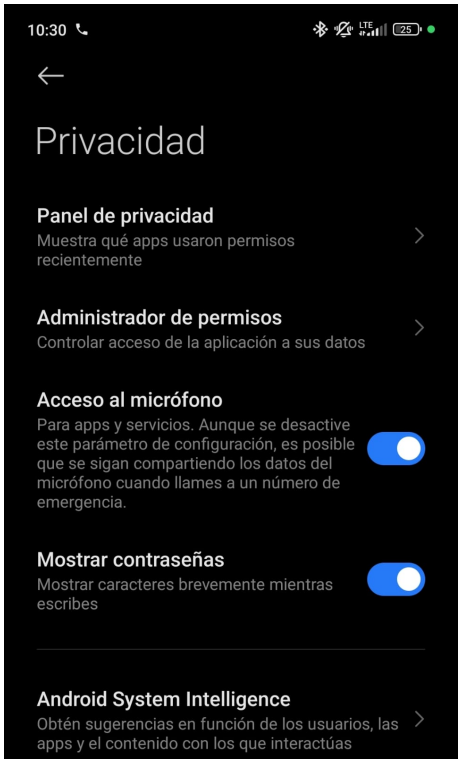

Figura 4.1: Diagrama de las funciones de seguridad en Android

4.6. Funciones Antirrobo

Android incorpora diversas funcionalidades para proteger la información en caso de pérdida o robo del dispositivo:

- **Bloqueo Remoto:** Permite bloquear el dispositivo a distancia para evitar accesos no autorizados.
- **Detección de Robo:** Utiliza algoritmos de inteligencia artificial para identificar comportamientos sospechosos y activar mecanismos de bloqueo.
- **Bloqueo Offline:** Si el dispositivo permanece desconectado por un tiempo prolongado, se activa un bloqueo que protege la información.

Estas funciones son esenciales para garantizar la seguridad de los datos del usuario ante situaciones de extravío [7].

4.7. Protocolos de Seguridad

Para asegurar las comunicaciones y la integridad de los datos, Android implementa diversos protocolos:

- **SSL/TLS:** Se utiliza para cifrar la información que se transmite a través de internet, asegurando la confidencialidad de los datos.
- **IPsec:** Empleado en conexiones VPN, este protocolo garantiza la autenticidad y la integridad de la información durante su transmisión.

La siguiente tabla resume las principales medidas de seguridad implementadas en Android:

Característica	Descripción
Código Abierto	Permite alta personalización, pero puede generar inconsistencias en la implementación de la seguridad.
Actualizaciones	Parcheos mensuales, cuya distribución depende de fabricantes y operadores.
Google Play Protect	Sistema automático que analiza aplicaciones en busca de comportamientos maliciosos.
Gestión de Permisos	Control granular del acceso de las aplicaciones a datos y funcionalidades del dispositivo.
Funciones Antirrobo	Incluyen bloqueo remoto, detección de robo y bloqueo offline para proteger la información.
Protocolos de Seguridad	Uso de SSL/TLS e IPsec para garantizar la confidencialidad e integridad de las comunicaciones.

Cuadro 4.1: Resumen de medidas de seguridad en Android

5. iOS

5.1. Introducción

iOS es el sistema operativo de Apple, diseñado con un enfoque de código cerrado que permite un control riguroso tanto del hardware como del software. Esta integración vertical favorece una experiencia de usuario consistente y la implementación centralizada de políticas de seguridad, lo que reduce significativamente la exposición a vulnerabilidades [4].

5.2. Estructura del Sistema Operativo

El modelo de código cerrado de iOS permite a Apple mantener un control absoluto sobre el ecosistema. Esto posibilita una implementación uniforme de las medidas de seguridad en todos sus dispositivos, eliminando las variaciones que se observan en sistemas abiertos y minimizando el riesgo de modificaciones no autorizadas [4].

5.3. Actualizaciones de Seguridad

Una de las ventajas de iOS es la distribución directa y simultánea de actualizaciones de seguridad. Apple se encarga de enviar los parches a todos los dispositivos compatibles de manera inmediata, lo que garantiza que los usuarios siempre dispongan de la protección más reciente contra vulnerabilidades conocidas [4].

5.4. Protección contra Software Malicioso

El App Store de Apple se caracteriza por su estricto proceso de revisión de aplicaciones, lo que reduce considerablemente el riesgo de que software malicioso llegue a los usuarios. Esta medida, combinada con otros mecanismos de seguridad, crea un entorno más controlado y seguro para la descarga e instalación de aplicaciones [6].

5.5. Gestión de Permisos

iOS proporciona herramientas intuitivas para la gestión de permisos, permitiendo a los usuarios controlar el acceso de las aplicaciones a información y funcionalidades sensibles. Esto es fundamental para proteger la privacidad del usuario y evitar la exposición de datos personales [6].

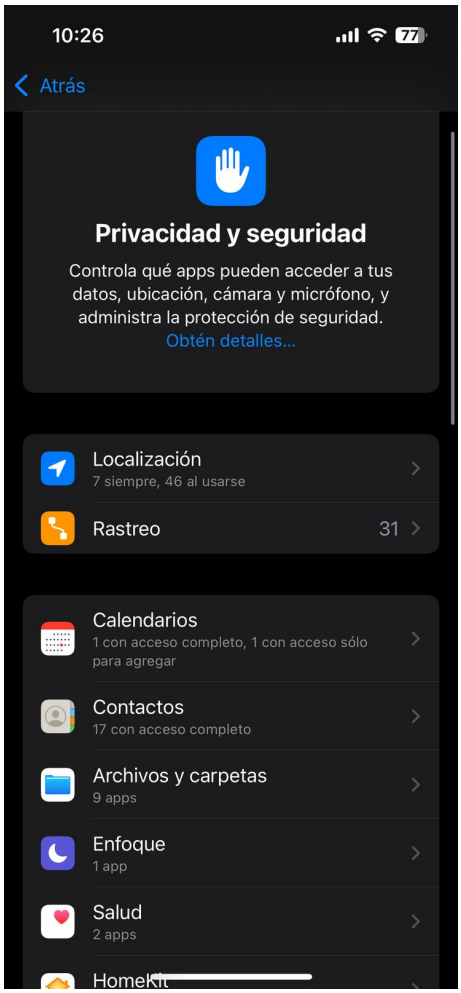

Figura 5.1: Diagrama de las funciones de seguridad en iOS

5.6. Funciones Antirrobo

Una característica destacada de iOS es **Buscar mi iPhone**, que ofrece varias funciones esenciales:

- Permite localizar el dispositivo en caso de pérdida.
- Facilita el bloqueo remoto para prevenir accesos indebidos.
- Posibilita el borrado de la información del dispositivo de manera remota para proteger la privacidad.

Estas medidas garantizan que, incluso en caso de extravío o robo, la información personal del usuario se mantenga segura [4].

5.7. Protocolos de Seguridad

Para proteger los datos y las comunicaciones, iOS implementa protocolos de cifrado robustos:

- **SSL/TLS:** Garantiza el cifrado de la información transmitida, protegiendo la confidencialidad de los datos.
- **IPsec:** Se utiliza en conexiones VPN para asegurar la integridad y privacidad de la información.

La siguiente tabla resume las principales medidas de seguridad implementadas en iOS:

Característica	Descripción
Código Cerrado	Control total de Apple, que permite una implementación uniforme y robusta de la seguridad.
Actualizaciones	Distribución simultánea y directa de parches de seguridad en todos los dispositivos.
App Store Controlada	Proceso de revisión riguroso que minimiza la presencia de aplicaciones maliciosas.
Gestión de Permisos	Herramientas intuitivas para controlar el acceso a datos y funcionalidades críticas.
Funciones Antirrobo	*Buscar mi iPhone* que permite localizar, bloquear y borrar el dispositivo en caso de pérdida.
Protocolos de Seguridad	Implementación de SSL/TLS e IPsec para asegurar la integridad y confidencialidad de las comunicaciones.

Cuadro 5.1: Resumen de medidas de seguridad en iOS

6. Conclusiones

- Los sistemas operativos Windows y Linux presentan enfoques distintos en seguridad: mientras que Windows prioriza la accesibilidad con herramientas integradas como Windows Defender y BitLocker, Linux enfatiza la flexibilidad y control del usuario mediante permisos avanzados y cifrado personalizado.
- En el ámbito móvil, iOS implementa un ecosistema cerrado con estrictas políticas de seguridad, lo que reduce el riesgo de ataques, mientras que Android, al ser más abierto, es más propenso a amenazas, pero permite mayor personalización en la protección.
- Si bien cada sistema operativo tiene mecanismos efectivos para garantizar la seguridad, la actualización constante, el uso de buenas prácticas y la concienciación del usuario siguen siendo elementos fundamentales para minimizar vulnerabilidades en cualquier entorno digital.

Bibliografía

[1] Mantenerse protegido con la aplicación Seguridad de Windows - Soporte técnico de Microsoft. (s.f.). https://support.microsoft.com/es-es/windows/mantente-protegido-con-seguridad-de-windows-2ae0363d-0ada-c064-8b56-6a39afb6a96

[2] Microsoft. (s. f.). Seguridad de Windows: antivirus de Defender, SmartScreen y mucho más — Microsoft Windows. Windows. https://www.microsoft.com/es-es/windows/comprehensive-security?r=1

[3] Características de seguridad: comparación entre Windows 7 y Windows 10. (2021, 25 octubre). Lenovo Tech Today Honduras. https://techtoday.lenovo.com/hn/es/solutions/large-enterprise/caracteristicas-de-seguridad-comparacion-entre-windows-7-y-windows-10

[4] Kaspersky. Android vs iPhone Mobile Security. https://latam.kaspersky.com/resource-center/threats/android-vs-iphone-mobile-security

[5] Android. Seguridad en Android. http://android.com/intl/es_us/safety/security/

[6] AVG. Android vs iOS Security. https://www.avg.com/es/signal/android-vs-ios-security

[7] Prey Project. 20 maneras de proteger tu teléfono. https://preyproject.com/es/blog/seguridad-movil-20-maneras-de-proteger-tu-telefono?utm_source=chatgpt.com

6.1. Bibliografía

[8] Chiesa, M. L. (s.f.). *Seguridad en Linux*. ElHacker. https://elhacker.info/Cursos/(Tutorial)%20Hacking%20Etico%20Avanzado/Sesion%2014%20Linux%20Hacking/documentos/seguridad-en-linux.pdf

[9] Trend Micro. (2021, febrero 23). *LINUX: Amenazas, Riesgos y Recomendaciones - Trend Micro Simply Security*. Trend Micro Simply Security. http://blog.la.trendmicro.com/linux-amenazas-riesgos-y-recomendaciones/