UDS
Mi Universidad

Soporte del sistema operativo Windows

Computación l

Actividad de plataforma

Profesor: LUIS ENRIQUE MENESES WONG

Alumna: Katherine Perez Parra

Estructura de Directorios

Estructura y descripción de la jerarquía de directorios

Es una jerarquía que organiza archivos y carpetas en niveles, facilitando la búsqueda y administración de datos en el sistema.Esta jerarquía comienza en la raíz de cada unidad de almacenamiento, que generalmente es representada por letras como C:/ o D:/.

Carpetas más importantes dentro de la jerarquía de Windows 10

- C:\Windows.
- C:\Program Files.
- C:\Users.
- C:\ProgramData.

Navegación básica en el Explorador de archivos

Es la interfaz gráfica principal que utiliza Windows 10 para permitir a los usuarios interactuar con su sistema de archivos. Proporciona una forma visual de explorar, copiar, mover, eliminar y gestionar archivos y carpetas.

Componentes

- Panel de navegación.
- Barra de herramientas de acceso rápido.
- Barra de direcciones.
- Área de contenido.
- Barra de búsqueda.

Atajos de teclado

- Ctrl + C: Copiar un archivo o carpeta.
- Ctrl + X: Cortar un archivo o carpeta.
- Ctrl + V: Pegar el archivo o carpeta copiado o cortado.
- Ctrl + Z: Deshacer la última acción.
- Alt + D: Seleccionar la barra de direcciones para escribir manualmente una ruta.
- Ctrl + E: Resaltar la barra de búsqueda.

Importancia de la organización de archivos

En el ámbito empresarial y de administración, la organización de archivos es vital para mantener la eficiencia y productividad. Una estructura clara de carpetas no solo facilita el acceso a la información, sino que también asegura que todos los miembros de un equipo puedan colaborar de manera eficiente, accediendo rapidamente a los archivos que necesitan

Beneficios

- Acceso rápido a la información.
- Seguridad de los datos.
- Mejora de la colaboración.

Mantenimiento del Sistema y Solución de Problemas

Soluciones para los problemas notificados

Windows 10 ofrece diversas herramientas integradas para la resolución de problemas notificados.

Se encuentran

- Solucionador de problemas de Windows.
- Visor de eventos.
- Administrador de dispositivos.
- Comprobación de archivos del sistema (SFC).
- Diagnóstico de memoria de Windows.

Actualizaciones del sistema operativo

Mantener Windows 10 actualizado es crucial para la seguridad, la eficiencia y la compatibilidad del sistema.

Se divide en varias categorías

- Actualizaciones de seguridad.
- Actualizaciones de características.
- Actualizaciones acumulativas.
- Actualizaciones opcionales.

Solución de problemas: mantenimiento del sistema

El mantenimiento preventivo de Windows 10 es fundamental para asegurar un rendimiento óptimo del sistema a largo plazo.

Principales tareas de mantenimiento

- Liberador de espacio en disco.
- Desfragmentación y optimización de unidades.
- Gestión de programas de inicio
- Verificación de integridad del disco (chkdsk).

Copia de seguridad

Son esenciales para garantizar que los datos críticos estén protegidos frente a desastres como fallos de hardware, ciberataques o errores humanos.

Opciones para realizar copia de seguridad

- Historial de archivos
- Imagen del sistema
- OneDrive

Configuraciones de Seguridad

Firewall de red

Es una herramienta de defensa perimetral que regula el tráfico de datos que entra y sale del sistema. Bloquea accesos no autorizados, permitiendo solo las conexiones seguras y autorizadas por el usuario o el administrador.

Características

- Control de aplicaciones.
- Reglas de entrada y salida.
- Protección adaptada a redes.

Protección antivirus

Es fundamental en cualquier sistema operativo para detectar y neutralizar software malicioso. Windows Defender, el antivirus nativo de Windows 10, ofrece una defensa robusta en tiempo real y se actualiza automáticamente para asegurar la protección frente a las amenazas más recientes.

Protección de acceso a redes

Asegura que solo dispositivos y usuarios autorizados puedan conectarse a la red empresarial, lo que es esencial para mantener la seguridad y confidencialidad en el flujo de datos.

Protección contra spyware y software no deseado

El spyware puede registrar la actividad del usuario, poniendo en riesgo la privacidad y la seguridad de los datos, mientras que el software no deseado puede afectar el rendimiento del sistema.

Características

- Bloqueo de aplicaciones potencialmente no deseadas (PUA).
- Escaneo contra spyware.
- Remediación automática.

Configuración de seguridad de internet

Windows 10 protege contra amenazas en línea, asegurando una navegación segura y reduciendo los riesgos de acceder a sitios maliciosos.

Control de cuentas de usuario

Es una herramienta que protege el sistema al pedir permisos antes de realizar cambios importantes, como instalar software o realizar modificaciones críticas en el sistema operativo.

Características

- Autorización de cambios.
- Protección contra software malicioso.
- Niveles de notificación ajustables.

Protección Avanzada y Auditoría de Seguridad

Herramientas de seguridad avanzadas en Windows 10

Windows 10 ofrece un conjunto de herramientas integradas diseñadas para proteger los datos del sistema y la red.

Herramientas

- Firewall de Windows Defender.
- Windows Defender Antivirus.
- Centro de Seguridad de Windows Defender.
- BitLocker.

Configuración de auditoría de eventos de seguridad

Es un sistema de registro de actividades en el sistema operativo. Estos eventos pueden incluir intentos de acceso, cambios en los permisos de archivos y la ejecución de ciertos programas. La auditoría permite a los administradores monitorear el comportamiento de los usuarios y del sistema para garantizar que las actividades se realicen de acuerdo con las políticas de seguridad.

Tipos

- Eventos de inicio y cierre de sesión.
- Modificación de políticas de seguridad.
- Acceso a objetos.

Importancia de la revisión periódica de los logs de seguridad

Los logs de seguridad, o registros de eventos, contienen información crucial sobre el comportamiento el sistema y de los usuarios. La revisión periódica de estos logs permite detectar patrones inusuales de actividad, como accesos no autorizados o cambios inesperados en la configuración del sistema.

Beneficios

- Detección temprana de amenazas.
- Análisis de incidentes de seguridad.
- Evidencia en auditorías de seguridad.