



Práctica 1: Configuración de un Servidor Web en Windows con IIS y Acceso Remoto

Presentación:

En esta práctica el alumno instalará, configurará y publicará un sitio web básico en un servidor web **IIS** en Windows, además de habilitar el **acceso remoto** desde otra computadora o red. Esta actividad está orientada a comprender cómo se habilita un servicio web accesible tanto local como remotamente, incluyendo la configuración del firewall y del router.

Propósito:

Dotar al alumno de habilidades prácticas para instalar y configurar **Internet Information Services (IIS)**, publicar un sitio web y garantizar que sea accesible desde **otras computadoras de la red local** o incluso desde **Internet**, implementando configuraciones de red y seguridad adecuadas.

Instrucciones Generales:

- La práctica es **individual**.
- El equipo debe contar con **Windows 10 o superior** y permisos de administrador.
- Se debe documentar **cada paso con capturas de pantalla**.
- Si el alumno no puede hacer la prueba externa por restricciones del proveedor de internet o firewall institucional, deberá justificarlo y mostrar evidencia del intento.

Objetivo de la Actividad:

Instalar y configurar el servidor web **IIS**, publicar una página web en el servidor, habilitar el acceso remoto desde otra máquina y realizar ajustes en el firewall y/o router para comprobar que el servidor funciona correctamente desde fuera de la computadora local.

Descripción de la Actividad:

1. **Instalación de IIS:**
 - Activar IIS desde el Panel de Control > Programas > Activar o desactivar características de Windows > Marcar “Internet Information Services”.
 - Verificar instalación accediendo a <http://localhost>.
2. **Publicación de Página Web:**
 - Crear un archivo llamado `index.html` con un mensaje personalizado.
 - Guardar en la carpeta `C:\inetpub\wwwroot`.
 - Verificar que se cargue correctamente en el navegador.
3. **Habilitación del Acceso Remoto:**
 - Obtener la IP local del equipo (`ipconfig`).
 - Desde otro equipo en la misma red, ingresar en el navegador `http://[IP_LOCAL]`.
 - Si no carga, desactivar temporalmente el firewall para comprobar.
4. **Configuración del Firewall de Windows:**
 - Abrir “Seguridad de Windows” > Firewall > Configuración avanzada.
 - Crear una **nueva regla de entrada** para habilitar el puerto **80 (HTTP)**:
 - Tipo: Puerto



- Puerto: 80 (TCP)
- Acci3n: Permitir
- Perfil: Todos
- Nombre: IIS_HTTP_80

5. Configuraci3n del Router (opcional para acceso desde Internet):

- Acceder al router a trav3s de <http://192.168.1.1> o similar.
- Configurar **port forwarding** del puerto **80** hacia la IP local del servidor.
- Obtener la IP p3blica desde <https://www.whatismyip.com>.
- Probar acceso desde un dispositivo en otra red usando IP P3blica.

6. (Opcional) Configurar DNS Dinámico (DDNS):

- Si tu IP p3blica cambia constantemente, puedes configurar un servicio DDNS como **No-IP**.
- Crear un subdominio gratuito, instalar el cliente en tu equipo y configurarlo.

Requisitos de Entrega:

- Documento en Word o PDF con:
 - Portada (nombre, grupo, fecha, materia).
 - Explicaci3n detallada de cada paso realizado.
 - Capturas de pantalla de:
 - Activaci3n de IIS.
 - index.html funcionando en localhost.
 - Prueba desde otra computadora en la red.
 - Configuraci3n del firewall.
 - (Opcional) Configuraci3n del router y prueba desde IP p3blica.
 - Justificaci3n en caso de no poder acceder desde otra red.
- Comprimir y adjuntar la carpeta del sitio (index.html) en .zip o .rar.

R3brica de Evaluaci3n:

Criterio	Puntos
Instalaci3n correcta de IIS	15
Publicaci3n y funcionamiento del sitio web local (localhost)	15
Acceso remoto desde otra PC en red local	15
Configuraci3n correcta del firewall (regla para puerto 80)	15
Configuraci3n de red para acceso desde IP p3blica o intento justificado	15
Evidencias bien organizadas y documentadas	15
Redacci3n y estructura del informe	10
Total	100



Práctica 2: Configuración de un Servidor FTP en Windows con IIS y Acceso Remoto

Presentación:

En esta práctica el alumno instalará y configurará un servidor **FTP** (File Transfer Protocol) utilizando **Internet Information Services (IIS)** sobre Windows. Posteriormente, verificará el funcionamiento del servicio mediante la conexión local y, si es posible, desde otra computadora dentro de la red local o desde el exterior, habilitando el puerto correspondiente y configurando el firewall.

Propósito:

El propósito de esta práctica es que el alumno adquiera habilidades prácticas para implementar un servicio FTP en su máquina local usando IIS, comprender el proceso de configuración de directorios, permisos y conexiones, así como validar el acceso desde clientes remotos.

Objetivo de la Actividad:

Configurar un servidor FTP utilizando IIS en Windows, crear un sitio FTP funcional, establecer permisos de usuarios, y comprobar el acceso desde el mismo equipo y desde otra máquina de la red local (o Internet si es posible).

Descripción de la Actividad:

1. **Activar el servicio FTP en IIS:**
 - Ir a **Panel de control** → **Activar o desactivar características de Windows**.
 - Marcar **Internet Information Services** → **Servicios FTP** → **Servidor FTP y Extensibilidad FTP**.
 - Asegurarse también de marcar **Herramientas de administración web**.
2. **Crear un directorio FTP:**
 - Crear una carpeta en C:\FTP (o en otra ruta) y colocar ahí algunos archivos de prueba.
 - Dar permisos de lectura/escritura a los usuarios que accederán al sitio.
3. **Crear un nuevo sitio FTP en IIS:**
 - Abrir el **Administrador de IIS** (inetmgr).
 - Clic derecho en "Sitios" → **Agregar sitio FTP**.
 - Nombre del sitio: FTPPrueba
 - Ruta física: C:\FTP
 - IP: (Seleccionar la IP local)
 - Puerto: 21 (predeterminado para FTP)
 - Seleccionar la opción de **Inicio automático**
4. **Configuración de autenticación y autorización:**
 - Habilitar **Autenticación básica**.
 - Permitir el acceso a un usuario local (por ejemplo, el mismo con el que se inició sesión).
 - Permitir acceso de **lectura y/o escritura** según el objetivo.



5. **Prueba de acceso desde el navegador o cliente FTP:**
 - En el mismo equipo, acceder al FTP vía navegador:
<ftp://localhost> o vía explorador de archivos: `ftp://127.0.0.1`
 - Ingresar las credenciales del usuario autorizado.
6. **Acceso desde otro equipo en la red local:**
 - Desde otro equipo conectado a la misma red, ingresar:
`ftp://[IP_DEL_SERVIDOR]`
7. **Configurar acceso remoto por Internet:**
 - Redirigir el **puerto 21** en el router al equipo que tiene el servidor FTP.
 - Agregar una **regla de entrada al firewall de Windows** para permitir conexiones entrantes al puerto 21.
 - Acceder desde otro equipo fuera de la red: `ftp://[IP_PÚBLICA]`

Requisitos de Entrega:

- Documento digital PDF que incluya:
 - Portada con nombre, grupo, fecha y práctica.
 - Descripción de los pasos realizados.
 - Capturas de pantalla de:
 - Activación del servicio FTP en Windows.
 - Configuración del sitio FTP en IIS.
 - Conexión local vía navegador o cliente FTP.
 - Conexión remota desde otra PC.
 - Configuración de firewall y/o router.
 - Breve conclusión sobre los resultados obtenidos y posibles problemas encontrados.

Rúbrica de Evaluación:

Criterio	Puntos
Activación e instalación del servicio FTP en IIS	15
Creación y configuración del sitio FTP	20
Acceso exitoso desde el mismo equipo	15
Evidencia de prueba desde otra máquina (opcional)	15
Configuración de firewall y/o router (opcional)	15
Documentación clara y capturas bien presentadas	10
Conclusión reflexiva sobre la práctica	10
Total	100



Práctica 3: Configuración de un Servidor SSH en Windows con Acceso Remoto Seguro

Presentación:

En esta práctica, el alumno instalará y configurará un **servidor SSH (Secure Shell)** en un equipo con Windows, permitiendo el acceso remoto seguro desde otros dispositivos dentro de la red local o desde Internet. El protocolo SSH es ampliamente utilizado para la administración remota de servidores debido a su cifrado y autenticación segura.

Propósito:

Dotar al alumno de habilidades para habilitar un servicio SSH en un entorno Windows, realizar conexiones seguras desde clientes remotos, y comprender el funcionamiento básico de sesiones cifradas dentro del modelo cliente-servidor.

Objetivo de la Actividad:

Instalar el servidor **OpenSSH** en Windows, habilitarlo como servicio, verificar su funcionamiento y permitir conexiones seguras desde otros equipos utilizando un cliente SSH (como PuTTY o el comando ssh en terminales compatibles).

Descripción de la Actividad:

1. Habilitar el servidor OpenSSH en Windows:

- Ir a **Configuración → Aplicaciones → Características opcionales → Agregar una característica.**
- Buscar e instalar:
 - **OpenSSH Server**
 - (Opcional) **OpenSSH Client**
- Esperar a que se complete la instalación.

2. Iniciar y habilitar el servicio SSH:

- Abrir PowerShell o CMD como administrador.
- Ejecutar los siguientes comandos:
net start sshd
Set-Service -Name sshd -StartupType 'Automatic'
- Confirmar que el servicio está corriendo.

3. Permitir el puerto 22 en el Firewall de Windows:

- Abrir el Firewall de Windows > Configuración avanzada > Reglas de entrada.
- Crear una nueva regla para **permitir el puerto TCP 22.**

4. Obtener la IP local del servidor:

- Ejecutar ipconfig y anotar la IP para las pruebas desde otro equipo.

5. Probar conexión desde el mismo equipo:

- Abrir PowerShell o CMD y ejecutar:
ssh [usuario]@localhost
- Iniciar sesión con las credenciales locales del equipo.

6. Probar conexión desde otro equipo en la red:



- Desde una terminal compatible con SSH (Linux, Mac o Windows con OpenSSH), ejecutar:
`ssh [usuario]@[IP_DEL_SERVIDOR]`
- Desde Windows, también se puede usar **PuTTY** como cliente SSH:
 - Host: IP del servidor
 - Puerto: 22
 - Tipo de conexión: SSH
 - Iniciar sesión con el usuario y contraseña del servidor

7. Acceso SSH desde fuera de la red:

- Redirigir el puerto 22 en el router hacia el equipo servidor.
- Conectarse desde otra red usando:
`ssh [usuario]@[IP_PÚBLICA]`
- Verificar que el acceso sea exitoso y seguro.

Requisitos de Entrega:

- Documento en Word o PDF que contenga:
 - Portada con nombre, grupo, práctica y fecha.
 - Explicación paso a paso de todo el proceso realizado.
 - Capturas de pantalla de:
 - Instalación del servidor OpenSSH.
 - Configuración y estado del servicio SSH.
 - Conexión SSH desde localhost.
 - Conexión SSH desde otra PC en la red.
 - Acceso SSH desde otra red (IP pública).
 - Configuración del firewall y/o router.
- Archivo .txt o .docx con los comandos utilizados durante la práctica.
- Justificación en caso de no poder probar conexión externa.

Rúbrica de Evaluación:

Criterio	Puntos
Instalación y activación del servidor SSH	15
Configuración del firewall (puerto 22)	15
Conexión local funcional (ssh localhost)	15
Conexión desde otra máquina en la red	15
(Opcional) Prueba de acceso desde red externa	10
Documentación completa y clara con evidencias	20
Redacción, orden y limpieza del reporte	10
Total	100



Proyecto Final: Simulación Completa de un Entorno Cliente-Servidor

Presentación:

En esta práctica integradora, el alumno simulará una red funcional de tipo **Cliente-Servidor** implementando varios servicios previamente configurados: servidor web, servidor FTP, servidor SSH, servidor de base de datos y servidor de medios (MP3 o streaming). Se realizarán pruebas desde una o más máquinas cliente para demostrar la conectividad, funcionalidad y respuesta del servidor ante diversas peticiones.

Propósito:

Aplicar los conocimientos adquiridos a lo largo del curso para diseñar, configurar y probar un entorno funcional de red Cliente-Servidor, identificando cómo interactúan múltiples servicios dentro de una red y asegurando la conectividad entre dispositivos.

Objetivo de la Actividad:

Diseñar y montar un entorno de red local donde un equipo actúe como servidor central, con múltiples servicios activos y configurados (Web, FTP, SSH, Base de datos y Streaming), y otro equipo o más como clientes que se conecten y prueben el acceso a dichos servicios.

Descripción de la Actividad:

1. Preparación del entorno:

- Asignar un equipo como **servidor** (puede ser una PC o máquina virtual).
- Tener al menos otro equipo o máquina virtual como **cliente**.
- Asegurarse de que ambos equipos estén en la **misma red local** (LAN).

2. Servicios a implementar en el servidor (mínimo 3 de los siguientes):

- **Servidor Web (IIS)**: con una página index.html personalizada.
- **Servidor FTP (IIS o FileZilla Server)**: con archivos disponibles para descarga.
- **Servidor SSH (OpenSSH)**: acceso remoto habilitado.
- **Servidor SQL Server**: base de datos con al menos una tabla y datos.
- **Servidor MP3/Streaming**: Icecast o VLC transmitiendo contenido.

3. Verificación de funcionamiento desde el cliente:

- **Web**: Acceso desde navegador a `http://[IP_SERVIDOR]`.
- **FTP**: Acceso desde navegador, explorador de archivos o cliente FTP.
- **SSH**: Conexión desde terminal con `ssh usuario@[IP_SERVIDOR]`.
- **SQL Server**: Conectarse desde SSMS remoto o cliente SQL y realizar consultas.
- **MP3/Streaming**: Reproducción desde navegador o VLC.

4. (Opcional) Acceso remoto desde fuera de la red:

- Redirección de puertos en el router.
- Comprobación de acceso usando IP pública (si se cuenta con permisos de red).

5. Monitoreo y pruebas de conectividad:

- Realizar pruebas con ping, tracert, telnet, netstat, nmap o **Wireshark** para observar tráfico de red y puertos abiertos.

Requisitos de Entrega:





- Documento Word o PDF con:
 - Portada (nombre, grupo, fecha).
 - Diagrama de red (topología) de la simulaci3n.
 - Explicaci3n detallada de los servicios configurados.
 - Capturas de:
 - Servicios activos en el servidor.
 - Accesos exitosos desde el cliente.
 - Resultados de pruebas de conectividad.
 - Comentarios sobre los problemas enfrentados y soluciones aplicadas.
 - Conclusiones generales.
- Archivos adicionales:
 - Carpeta comprimida .zip o .rar con:
 - Capturas de pantalla.
 - Archivo index.html, archivo SQL y archivos transmitidos (opcional).

Rúbrica de Evaluaci3n:

Criterio	Puntos
Configuraci3n de al menos 3 servicios funcionales en el servidor	30
Accesos exitosos desde el/los clientes a los servicios	20
Diagrama de red claro y representativo	10
Pruebas de conectividad documentadas (ping, telnet, etc.)	10
Evidencias completas con capturas	10
Conclusiones y reflexi3n personal sobre el ejercicio	10
Redacci3n, presentaci3n y estructura del documento final	10
Total	100