Camila Molina Pineda

# PRACTICA 8

## PROTECCION Y CONFIGURCION DE APLICACIÓN DE ACUERDO CON LAS NECESIDADES

ASWE

Informática 404

Conalep 027

***NOTA: No todos los pasos tienen imágenes porque al hacer clic se anulaba la grabación de pasos

# Introducción

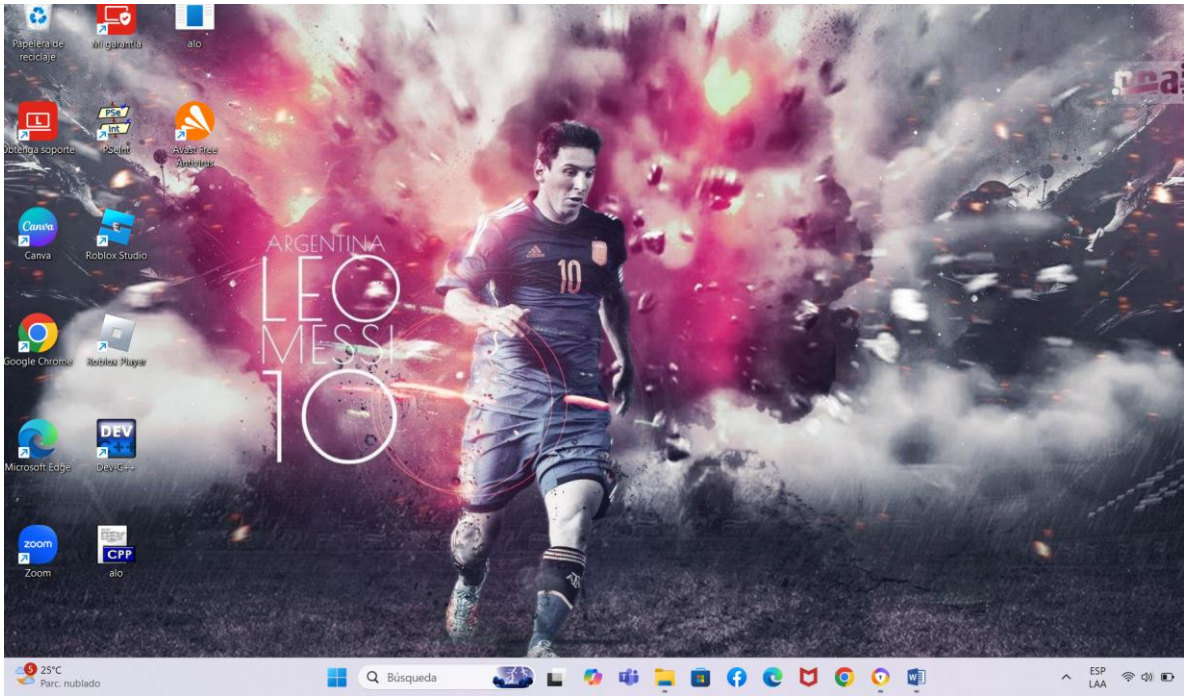
La protección y configuración de las aplicaciones web son componentes clave para garantizar su funcionamiento seguro y eficiente. Cada aplicación tiene necesidades específicas en términos de seguridad, rendimiento y accesibilidad, lo que requiere una configuración adaptada a esos requisitos. A medida que las amenazas en línea se vuelven más sofisticadas, es fundamental establecer medidas de protección robustas que salvaguarden tanto los datos sensibles como el acceso no autorizado a los sistemas. En esta práctica, aprenderemos a configurar y proteger las aplicaciones web según las necesidades particulares de cada entorno, utilizando estrategias como la autenticación, el control de acceso y la encriptación para fortalecer la seguridad, al mismo tiempo que se optimiza el rendimiento y la fiabilidad de las aplicaciones.

***NOTA: No todos los pasos tienen imágenes porque al hacer clic se anulaba la grabación de pasos

# PRACTICA 8: PROTECCION Y CONFIGURCION DE APLICACIÓN DE ACUERDO CON LAS NECESIDADES

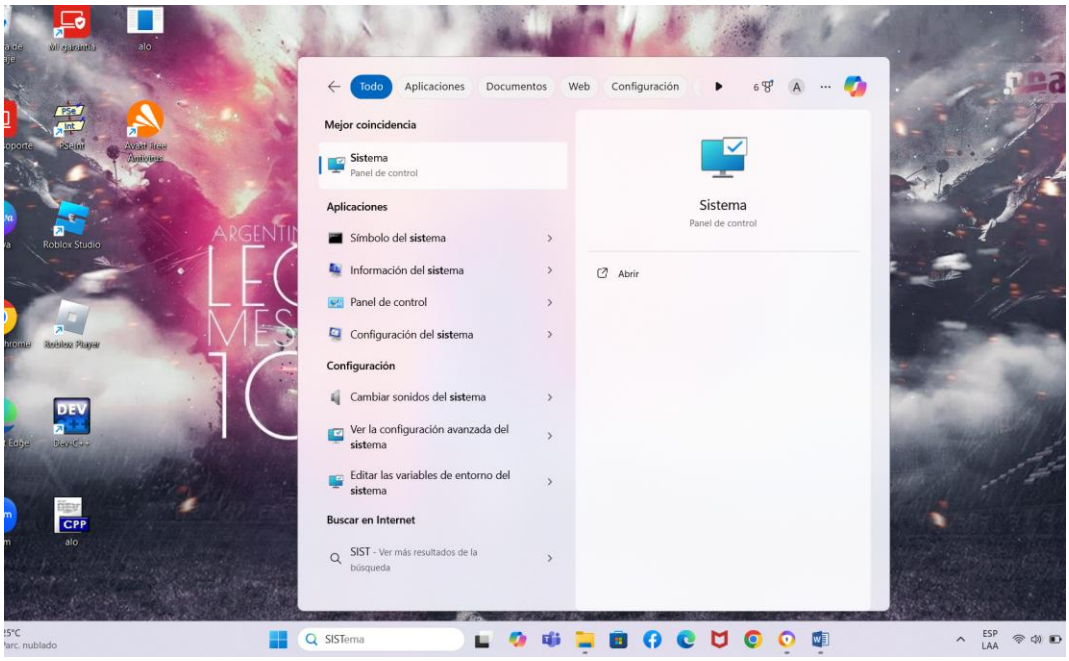
## Configuración del Grado de Protección y Extensiones de Archivos en IIS

1. Encender el equipo de cómputo y asegurarse de que esté conectado a la red en caso de necesitar actualizaciones o asistencia remota.



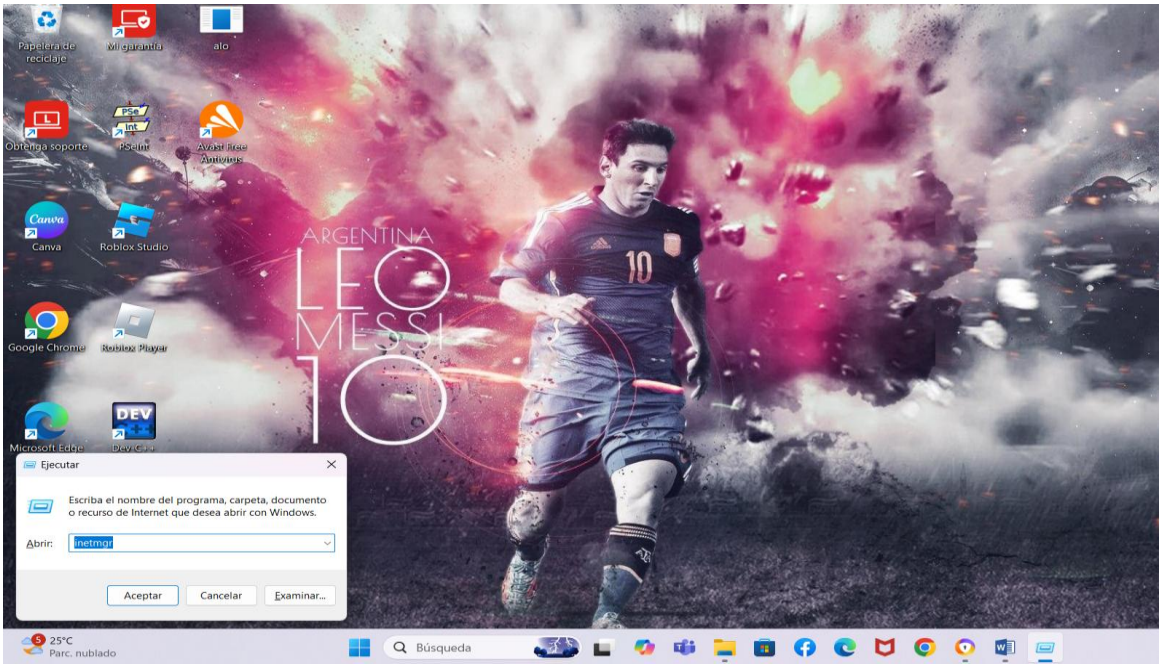

***NOTA: No todos los pasos tienen imágenes porque al hacer clic se anulaba la grabación de pasos

2. Iniciar sesión en el sistema operativo con una cuenta que tenga privilegios de administrador.



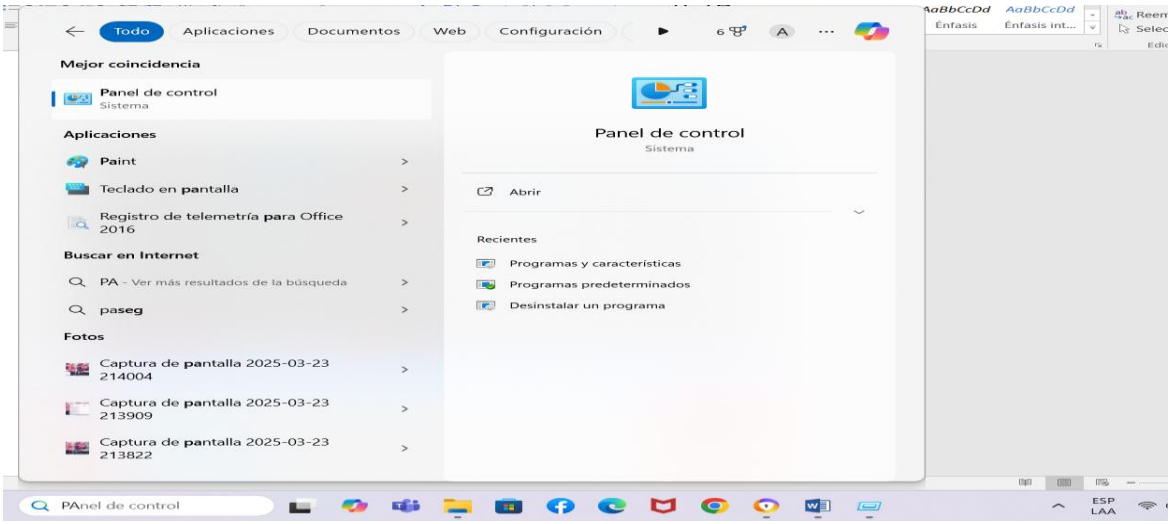

3. Abrir el Administrador de Servicios de Internet (IIS):

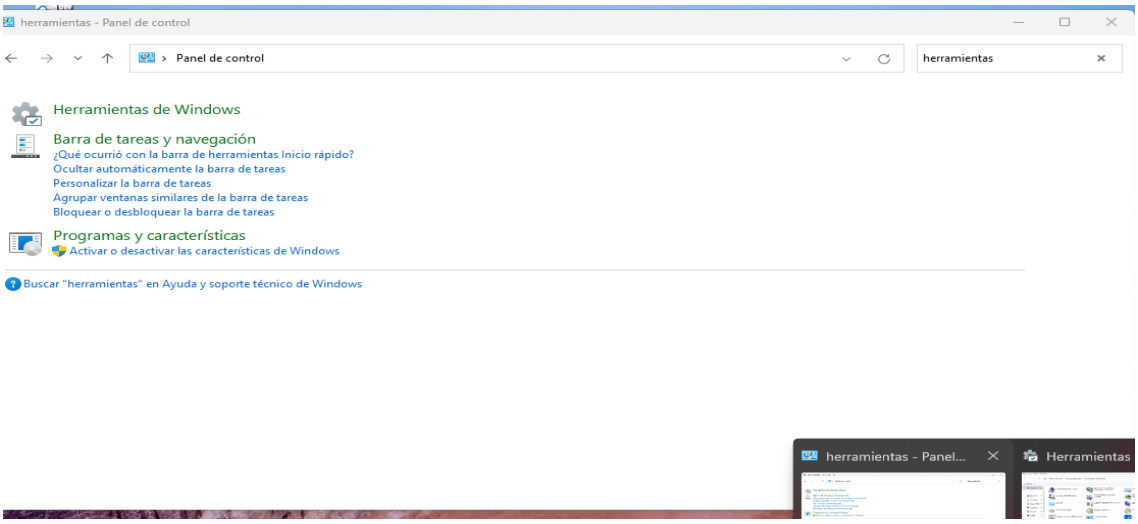
Presionar Win + R, escribir inetmgr y presionar Enter, o

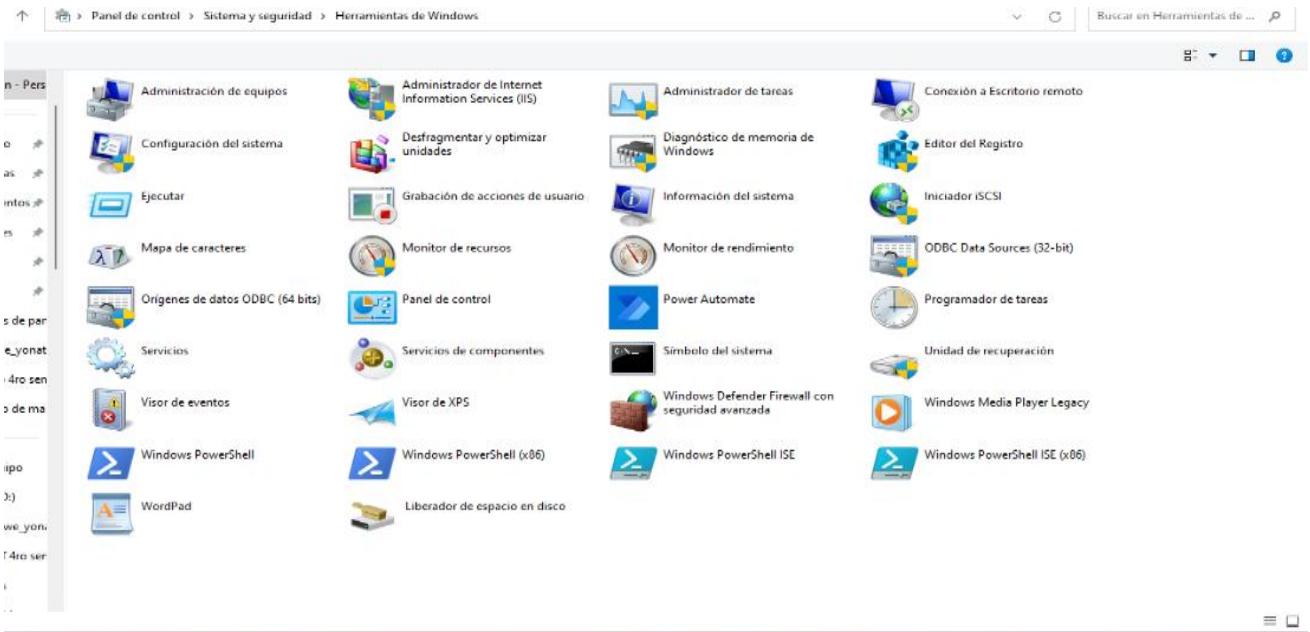



***NOTA: No todos los pasos tienen imágenes porque al hacer clic se anulaba la grabación de pasos

Ir a Panel de Control → Herramientas Administrativas → Internet Information Services (IIS) Manager.

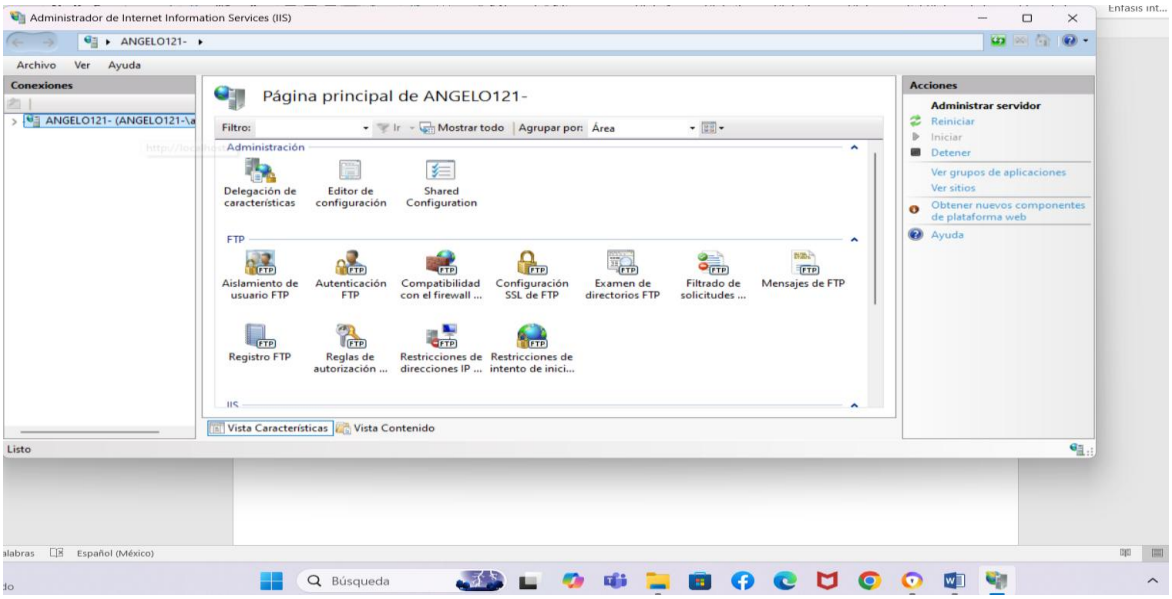


2. Configuración del Grado de Protección en IIS

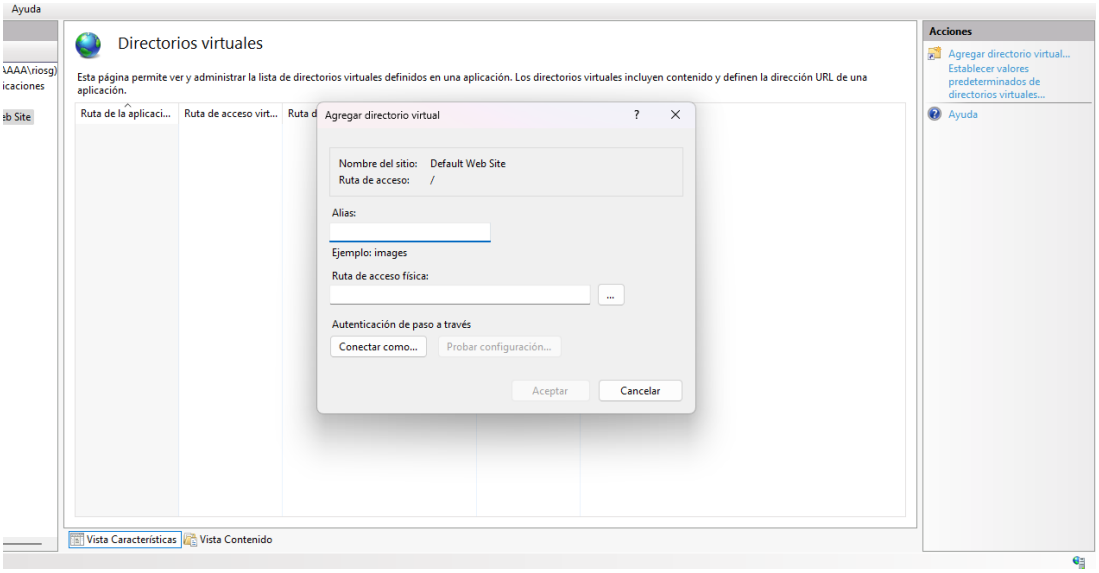
El grado de protección en IIS determina el nivel de aislamiento de una aplicación en el servidor, lo que influye en su seguridad y estabilidad.



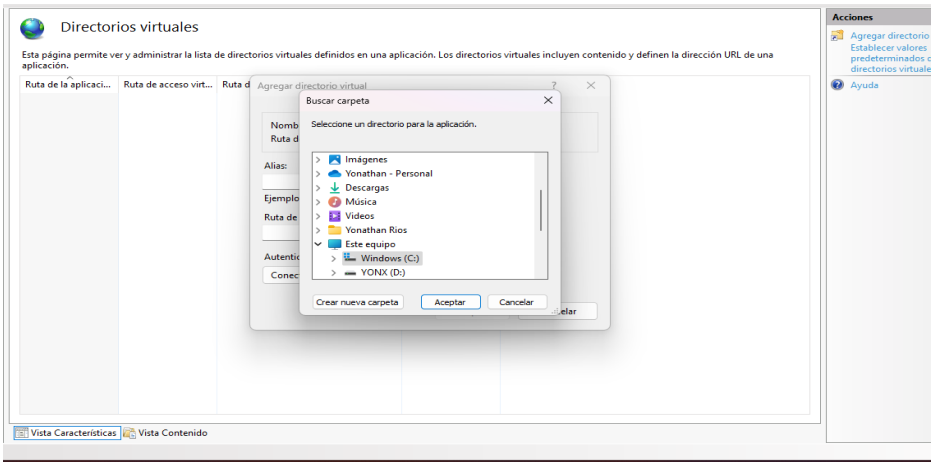

4. Dentro del Administrador de IIS, ingresar a la sección "Directorio" de la aplicación que se desea configurar.


***NOTA: No todos los pasos tienen imágenes porque al hacer clic se anulaba la grabación de pasos

5. Establecer el grado de protección de la aplicación en "Medio (agrupado)", lo que permite que varias aplicaciones compartan un mismo proceso de trabajo, reduciendo el consumo de memoria y mejorando la eficiencia sin comprometer demasiado la seguridad.




6. Realizar pruebas empleando otros grados de protección para analizar su impacto en el rendimiento y seguridad del sistema:

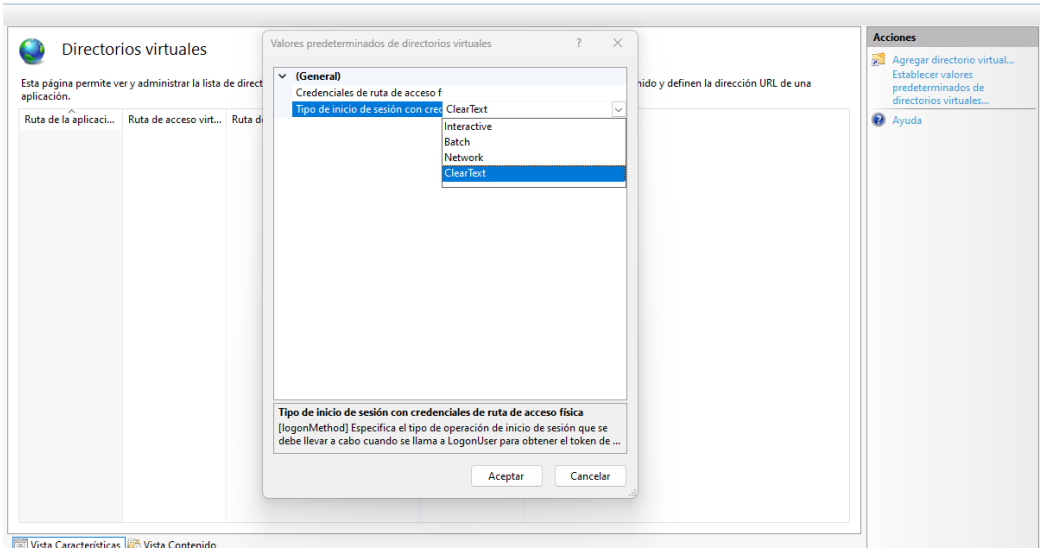



Bajo (Sin aislamiento): Todas las aplicaciones se ejecutan en el mismo proceso, lo que mejora el rendimiento, pero puede generar problemas si una aplicación falla.

Medio (Agrupado): Varias aplicaciones comparten un mismo proceso de trabajo, lo que mejora la estabilidad sin consumir demasiada memoria.

Alto (Aislado): Cada aplicación se ejecuta en su propio proceso, lo que brinda mayor seguridad, pero aumenta el consumo de recursos.

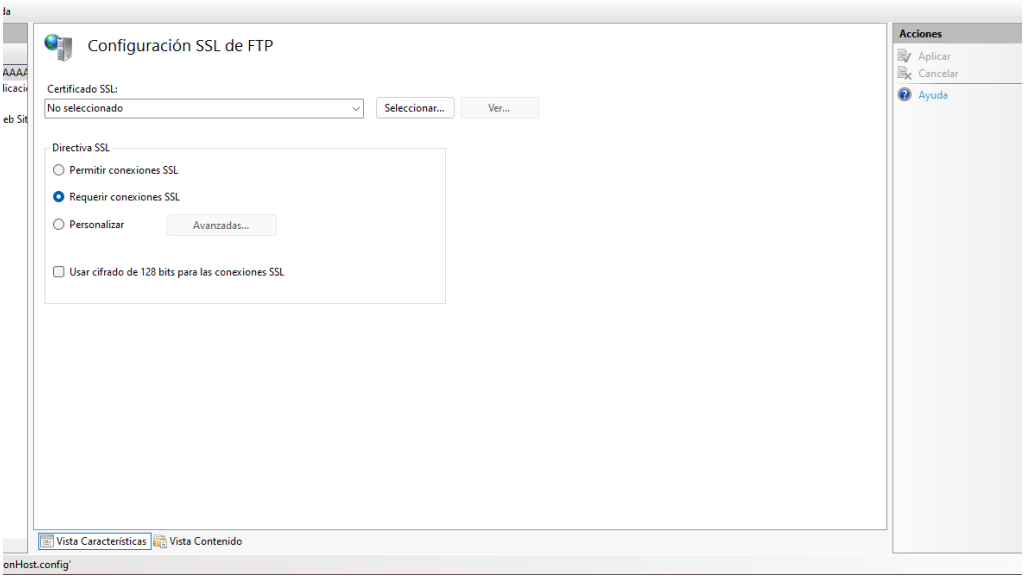
***NOTA: No todos los pasos tienen imágenes porque al hacer clic se anulaba la grabación de pasos




3. Configuración de la Aplicación y Extensiones de Archivo

Para permitir la ejecución de scripts CGI escritos en PERL, es necesario configurar correctamente las extensiones de archivo en IIS.

7. Ingresar a la opción "Configurar" dentro de las propiedades de la aplicación en IIS.



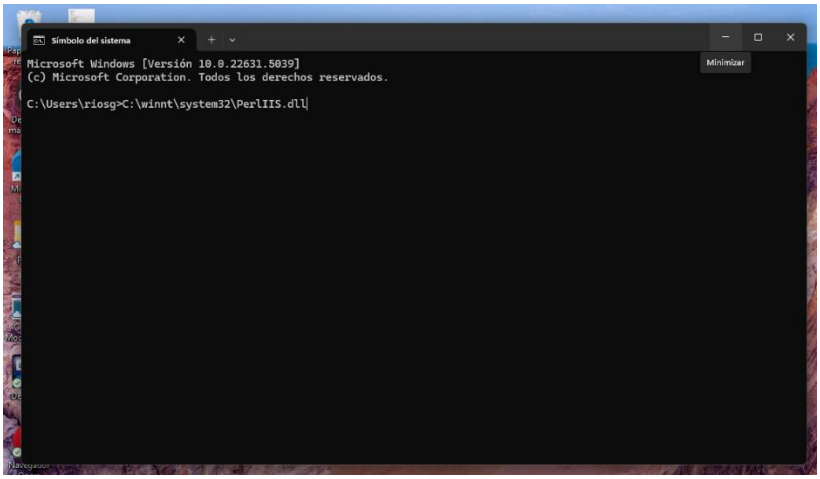

***NOTA: No todos los pasos tienen imágenes porque al hacer clic se anulaba la grabación de pasos

8. Agregar los siguientes parámetros para permitir la ejecución de scripts CGI:

Ejecutable: C:\winnt\system32\PerlIIS.dll

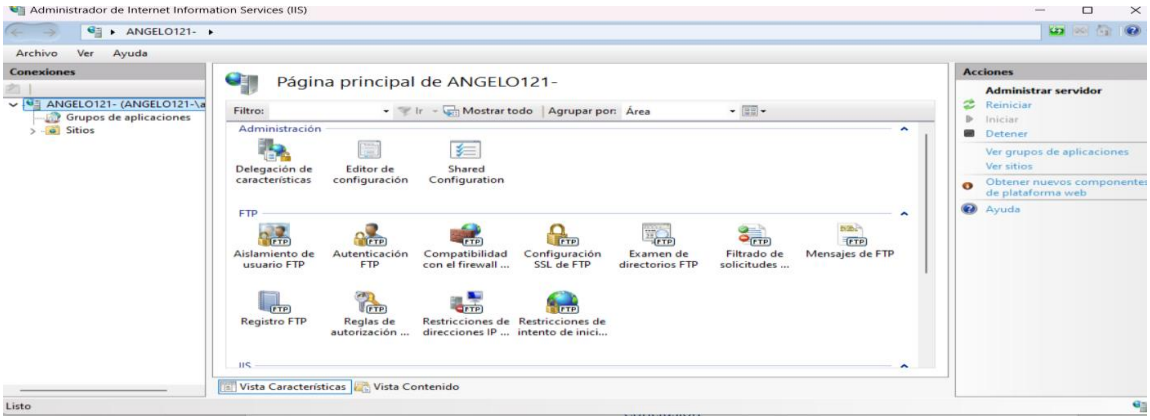
Extensión: .cgi

Verbos permitidos: GET, HEAD, POST, TRACE (Estos métodos HTTP determinan qué tipo de solicitudes puede manejar el script).




9. Habilitar la verificación del Motor de Secuencia de Comandos, lo que garantiza que los scripts CGI sean procesados correctamente antes de ejecutarse.

10. Habilitar la comprobación de archivo existente, evitando la ejecución de scripts si el archivo no está disponible o es inválido, lo que mejora la seguridad del servidor.




***NOTA: No todos los pasos tienen imágenes porque al hacer clic se anulaba la grabación de pasos

# Conclusión

En conclusión, la protección y configuración de aplicaciones de acuerdo con sus necesidades específicas es esencial para garantizar que funcionen de manera segura y eficiente. A medida que cada aplicación tiene características y requisitos únicos, la configuración adecuada permite mitigar riesgos de seguridad y optimizar su rendimiento, brindando una experiencia confiable a los usuarios. A través de esta práctica, hemos aprendido cómo adaptar las configuraciones de seguridad y funcionamiento a las necesidades específicas de cada aplicación, fortaleciendo así la infraestructura web y asegurando que las aplicaciones cumplan con los más altos estándares de protección y eficiencia.

***NOTA: No todos los pasos tienen imágenes porque al hacer clic se anulaba la grabación de pasos