Bloque II

Taller mitigación y pruebas Web con .Net

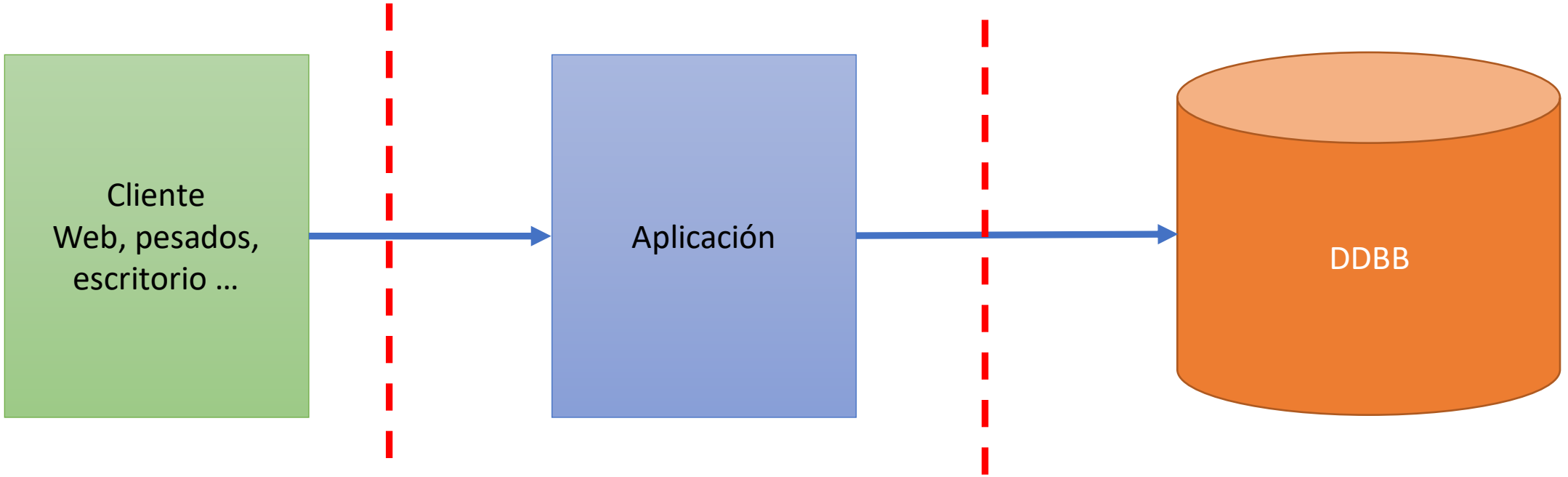
Contenidos

1. Introducción a los modelos de desarrollo MicroSoft: ASP.NET, wcf, WebApi, Razor y Blazor.
2. La evolución de .NET
3. Estándares OWASP y OWASP Testing Guide
4. Verificación de la gestión de sesiones
5. Verificación del control de acceso
6. Verificación de entrada maliciosa
7. Verificación de la criptografía
8. Verificación del logging y manejo de errores
9. Verificación de la protección de datos
10. Verificación de la seguridad en las comunicaciones
11. Verificación de la configuración de seguridad HTTP
12. Verificación de los controles maliciosos
13. Verificación de la lógica de negocio
14. Verificación de los recursos y ficheros

1. Introducción a los modelos de desarrollo MicroSoft:

ASP.NET, wcf, WebApi, Razor, Blazor …

Arquitecturas: Evolución



Tantos modelos

- ASP.NET
- Wcf
- Razor
- Blazor
- Aplicaciones metro
- Entity Framework
- WebApi
- …

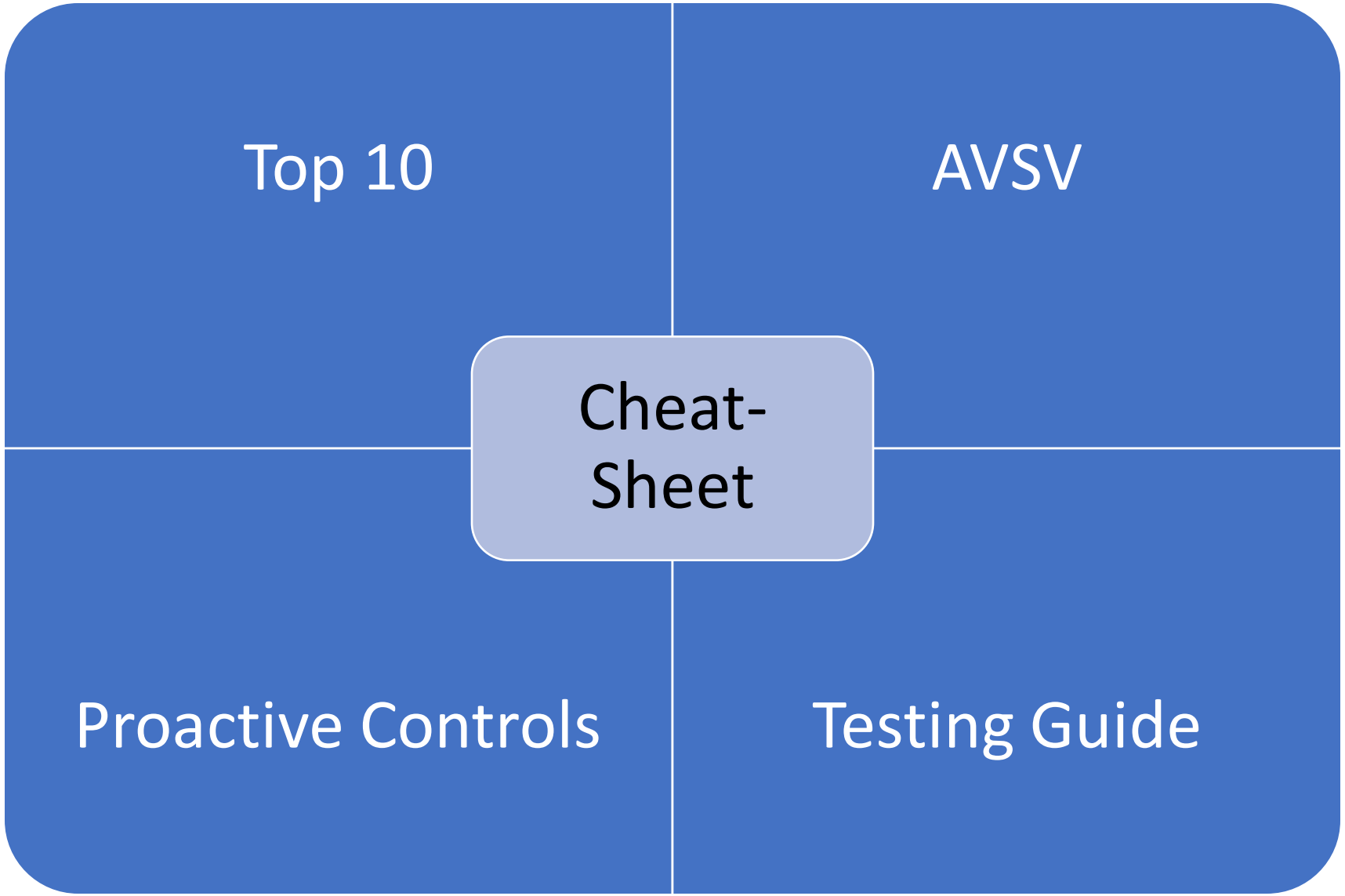
2. La evolución de .NET

Un poco de historia

- Surge en un momento de competición con java: máquinas virtuales
- Evolución relativamente rápida, soporte multilenguaje
- Inicialmente sólo con soporte Windows (excepción: Mono)
- Soporte de múltiples modelos de programación, pero inicialmente centrado en Aplicaciones en IIS
- Se va extendiendo a otros ámbitos: aplicaciones de escritorio
- .Net se mantiene en versiones estables en las 4.x los últimos años
- .Net Core surge como un Branch pero con plan de soporte multiplataforma, modularidad…
- .Net 5 en realidad no es una versión de .Net 4.8, sino de .Net Core 3.1

3. Estándares OWASP y OWASP Testing Guide

INADECO



Pen-Testing

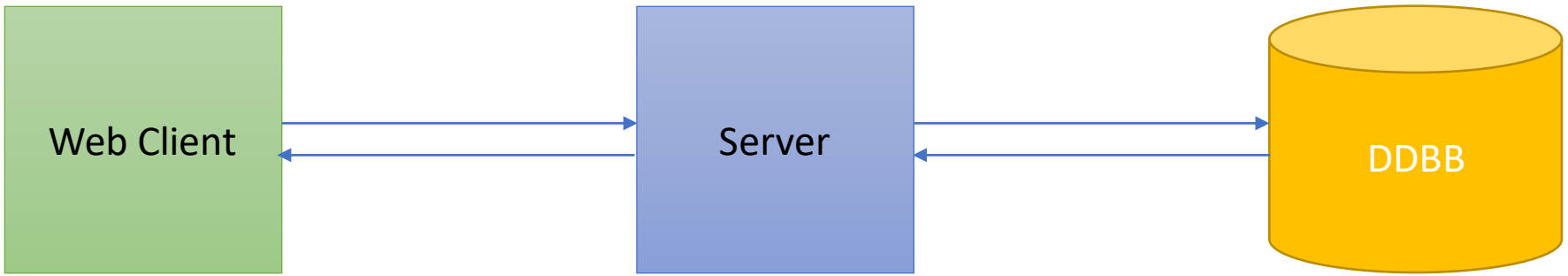
1. Planificación y reconocimiento
2. Escaneo
3. Obteniendo acceso
4. Mantener el acceso
5. Análisis y contramedidas
6. … vuelta al 1

CSRF token operaciones no seguras…¿y REST?

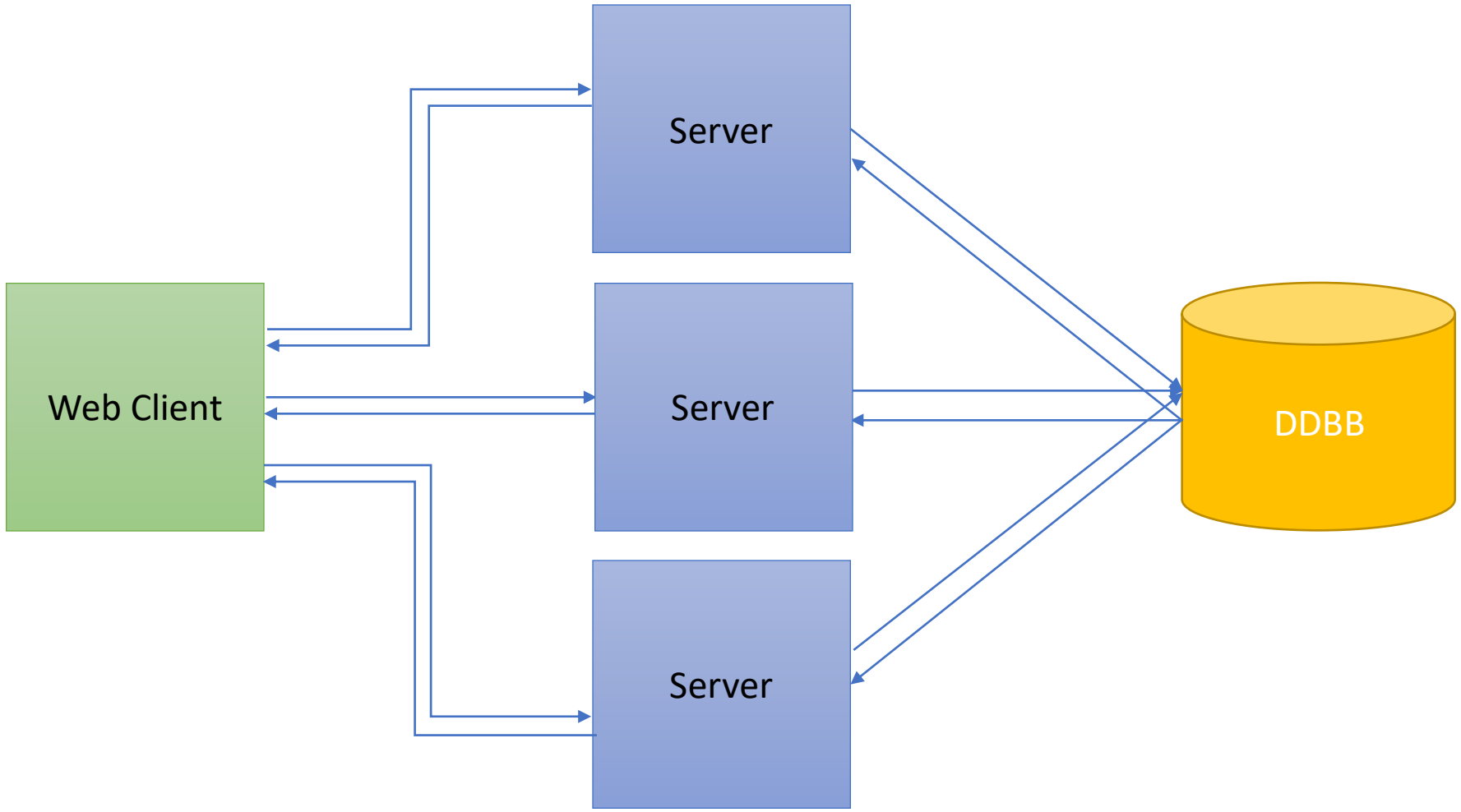
```
…
<form method='POST (PUT o DELETE no soportado en HTML)'>
        <input name='campo1' value='DATO_1'>
        <input name='campo2' value='DATO_2'>
        <input name='x-csrf-token' value='token'>
</form>
…
```

4. Verificación de la gestión de sesiones

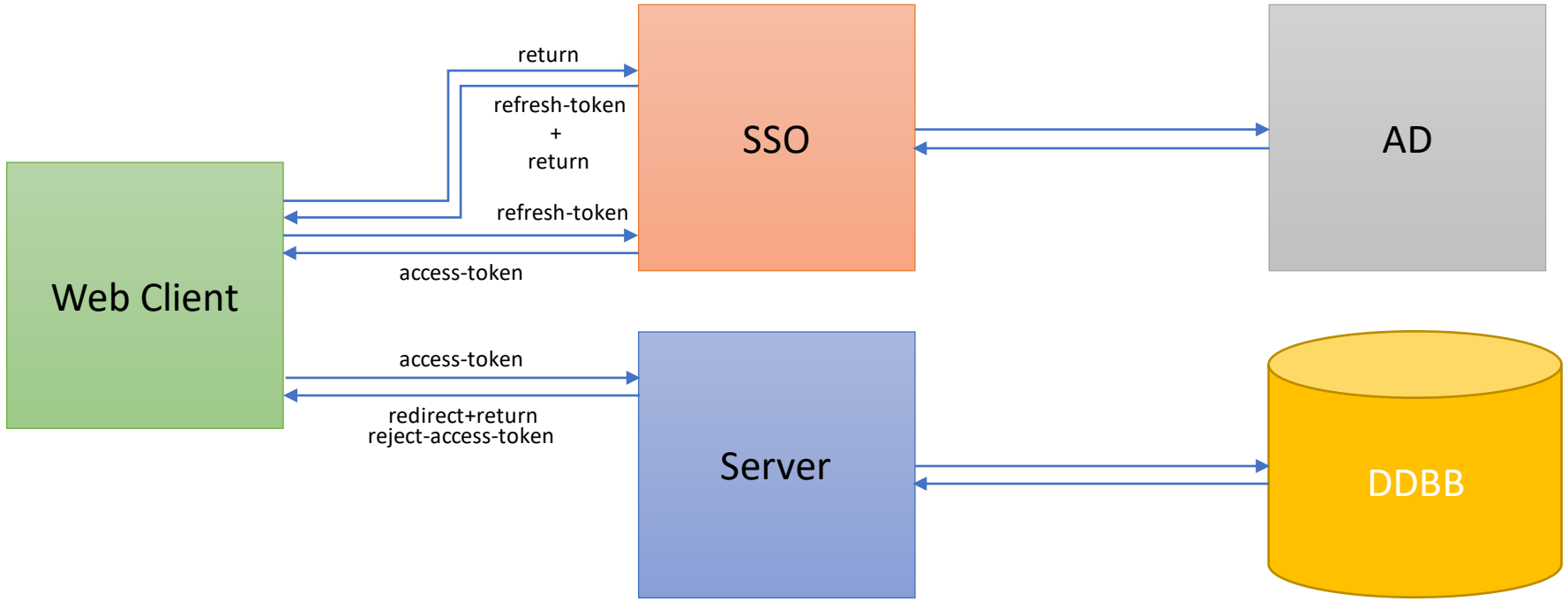
Single Servers: SessionID (stateful)



Multiple Servers: JWT (stateless)



SSO Flow


return
refresh-token
+
return
refresh-token
access-token
SSO
AD
Web Client
access-token
redirect+return
reject-access-token
Server
DDBB

En esta primera sesión

- Threat Model
- Implicaciones
- Conocemos nuestras herramientas:
  - WebGoat
  - Firefox
  - Zap
- Entendiendo los protocolos
- Un ejemplo simple de ataque: 2017 - A2 Broken authentication
- Mejores prácticas:
  - https://docs.microsoft.com/en-us/previous-versions/ms178194(v=vs.140)?redirectedfrom=MSDN
  - https://docs.microsoft.com/en-us/previous-versions/aspnet/zdh19h94(v=vs.100) Antiguo