





# Bloque II

Taller mitigación y pruebas Web con .Net

# Bloques del curso

-  Bloque I - Introducción al Desarrollo Seguro
-  Bloque II - Taller mitigación y pruebas Web con .Net
-  Bloque III - Taller mitigación y pruebas Web con Java
-  Bloque IV - Taller mitigación y testing Cliente / Servidor .Net

Bloque I –

## Horario

- Diario de 8:00 a 11:00
- 5 minutos de descanso: 9:30 a 9:35

	Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo
Febrero		1	2	3	4	5	6
	7	8	9	10	11	12	13
	14	15	16	17	18	19	20
	21	22	23	24	25	26	27
	28						

Introducción al Desarrollo Seguro (4 jornadas x 3horas - 12 horas total)

# Sobre el profesor

- Más de 25 años de experiencia en el sector y todos estos años compaginando la formación con el desarrollo y el I+D+I
- En formación empecé sobre con asignaturas de programación y los últimos años sobre todo BootCamps así como formación a perfiles de desarrollo seniors.
- Actualmente perfil de arquitecto software, aunque he pasado por casi todos los roles.
- Especialidades:
  - SDLC (CI/CD)
  - Computación en la nube
  - Seguridad en el desarrollo, criptografía
  - Data Science
  - Arquitecturas distribuidas e Integración de sistemas

# 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

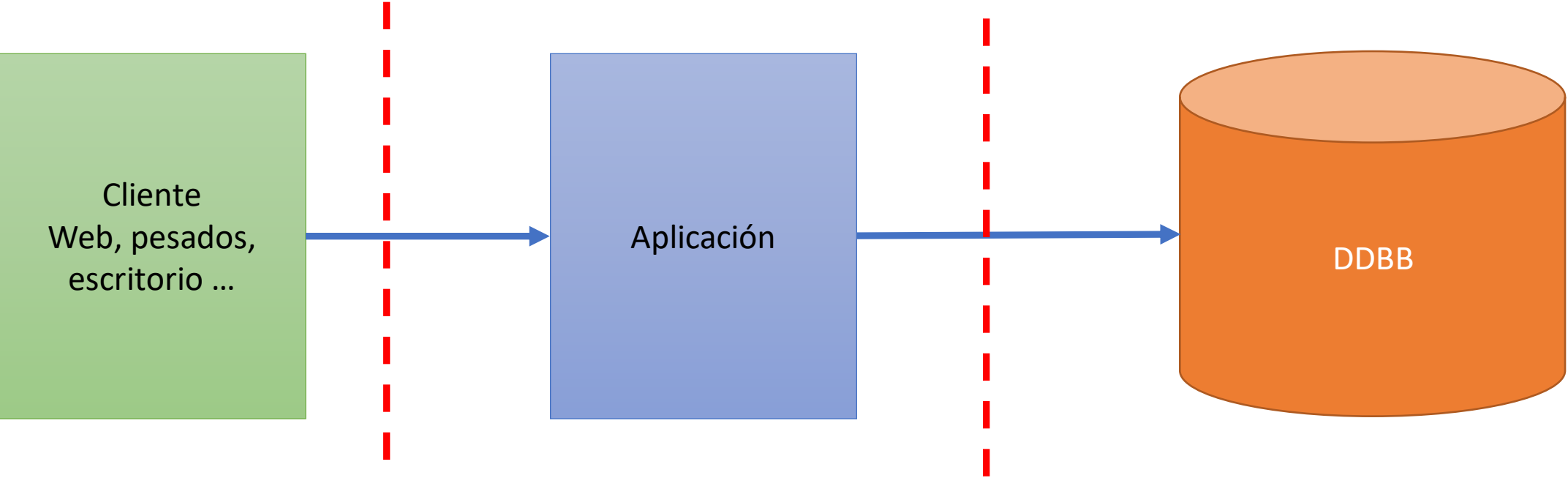
# Repositorio de ficheros

<https://github.com/desarrollo-seguro/web-net-2>

# 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
- ...

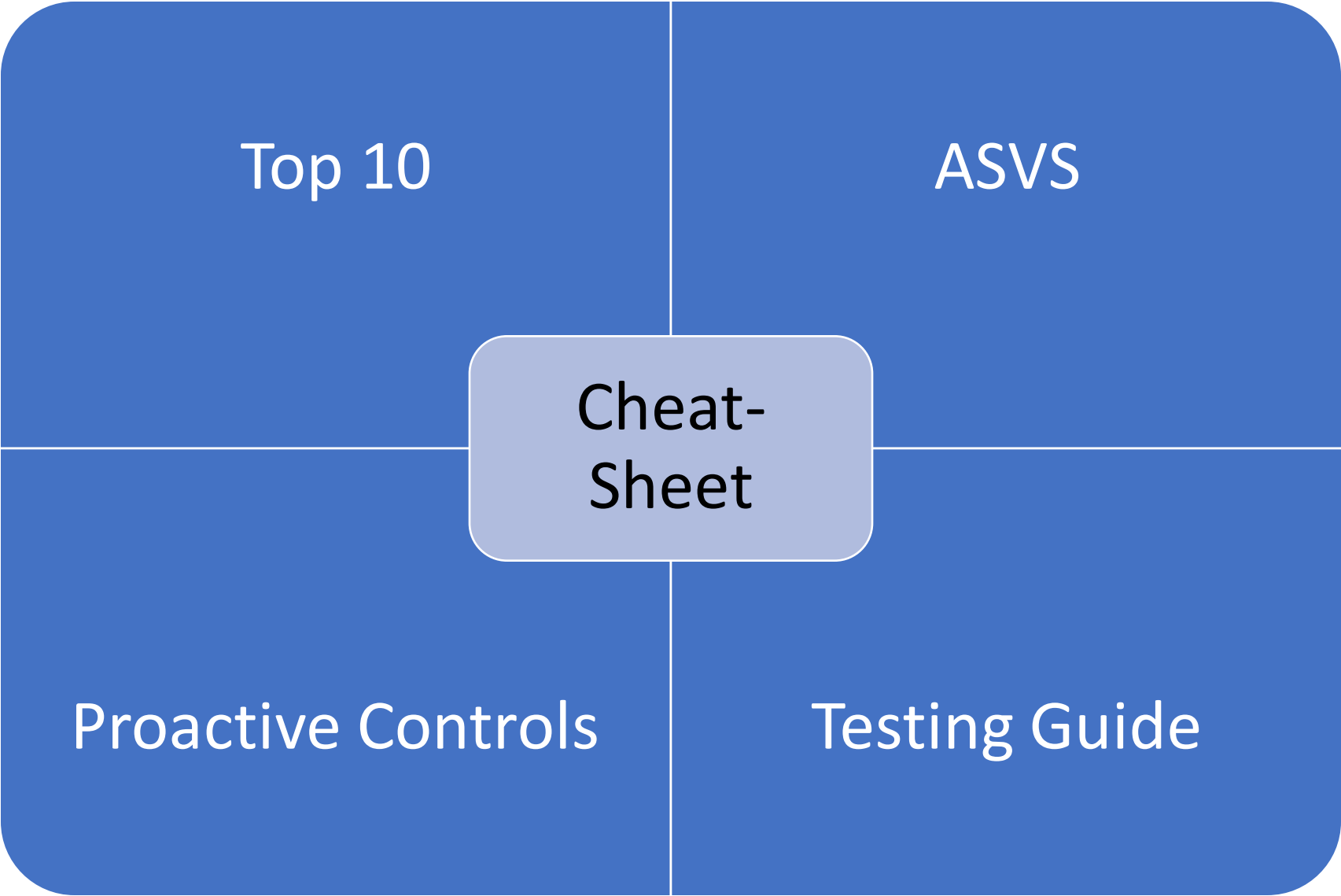


## 2. La evolución de .NET

# 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



Y unimos a estos el Security Knowledge Framework:  
<https://owasp.org/www-project-security-knowledge-framework/>

# 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?

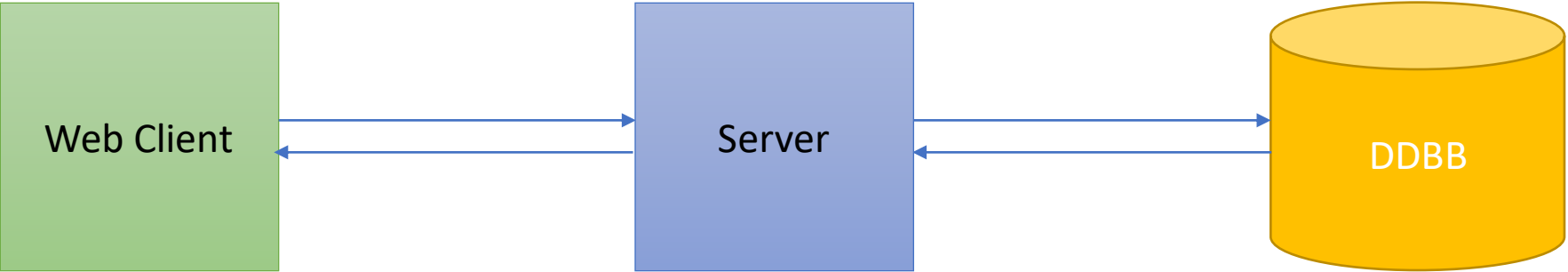
```

...
<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)

