

Bloque IV

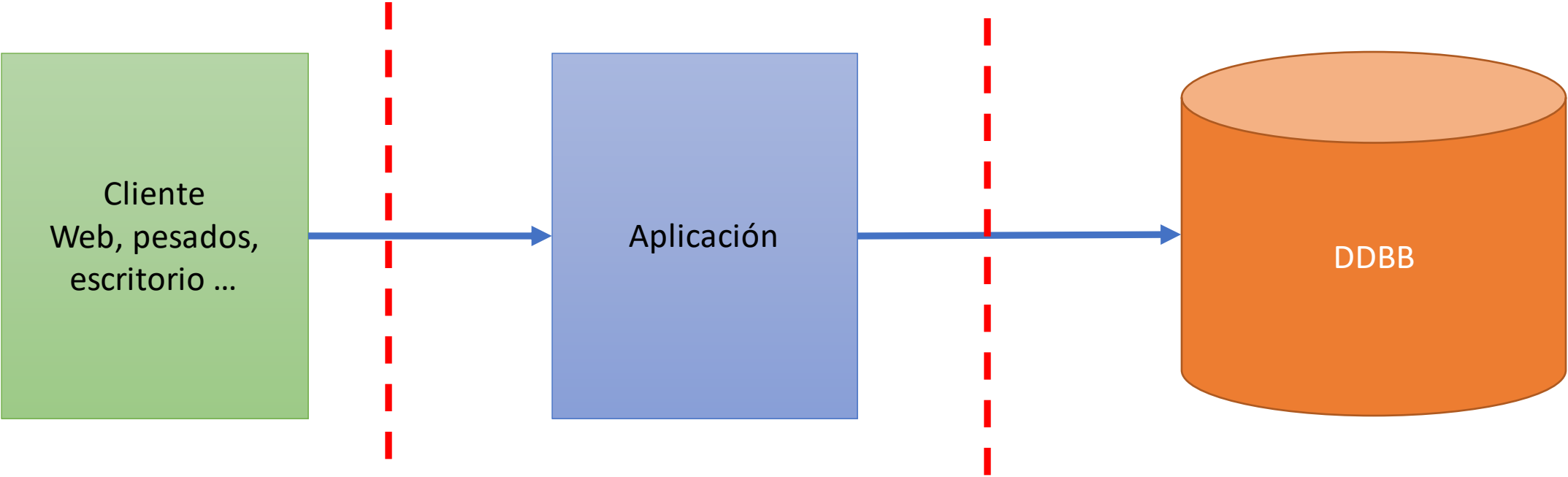
Taller mitigación y testing Cliente / Servidor (cliente pesado) para .Net

Contenidos

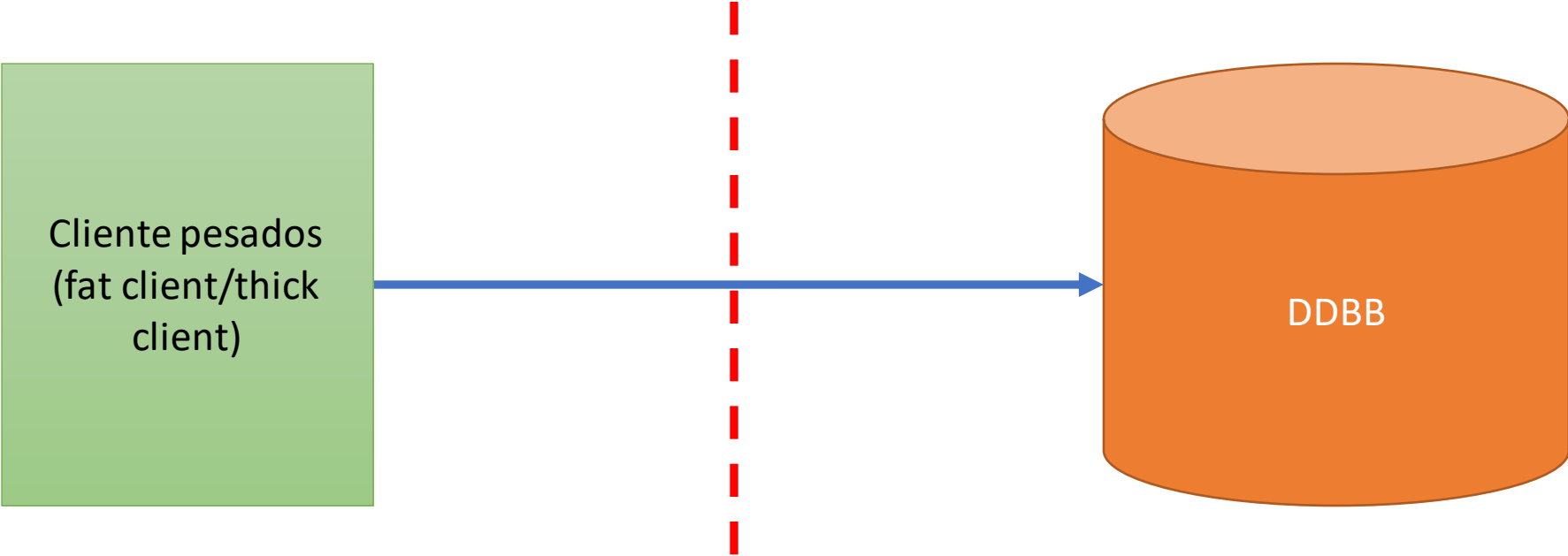
1. Arquitectura: principales variantes e implicaciones
2. Securización de las comunicaciones. Protocolos, Traffic sniffing, Robo de credenciales
3. Securización de Bases de Datos: Ataques de inyección SQL
4. Firewalls y seguridad de red
5. Técnicas de encriptación y hashing
6. Securización de recursos críticos (ficheros de parametrización)
7. Sistemas externos de autenticación, control de acceso y monitorización

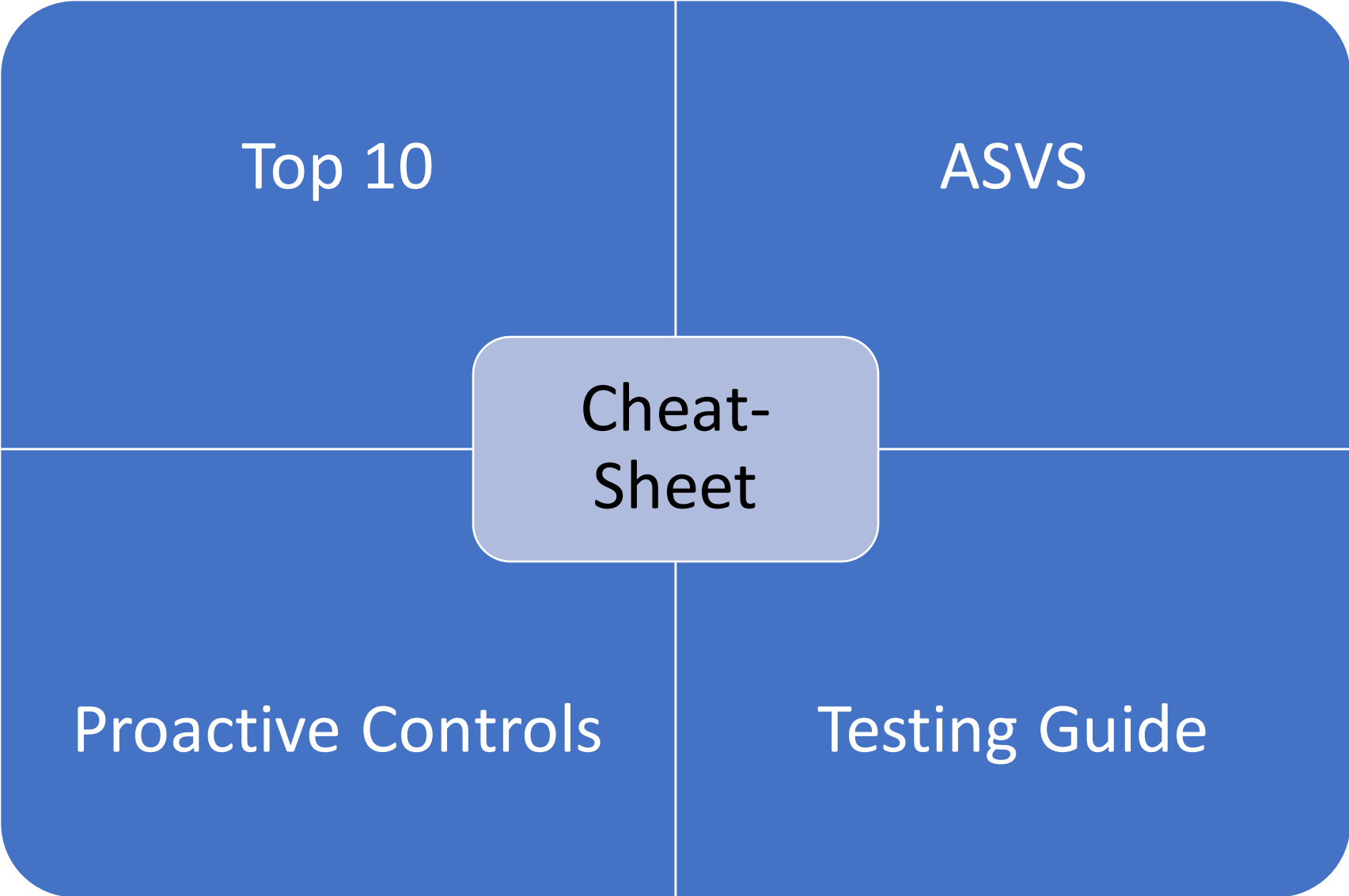
1. Arquitectura: principales variantes e implicaciones

Arquitecturas: Evolución



Cliente pesado: 2 capas





Recursos

Aplicación insegura:

- <https://github.com/NetSPI/BetaFast/>

Entorno:

- <https://developer.microsoft.com/es-es/windows/downloads/virtual-machines/>

Si no está disponible la máquina virtual:

- <https://gitforwindows.org/>
- <https://dotnet.microsoft.com/download/visual-studio-sdks>
- <https://visualstudio.microsoft.com/vs/older-downloads/>
- <https://code.visualstudio.com/>

Pen-Testing

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