# Introducción

Es altamente necesario y recomendable ajustar parámetros del servidor web y del sistema operativo, a fin de lograr mejorar en los aspectos de rendimiento y seguridad.

**Recomendaciones**

Sugiero utilizar los criterios que siguen a continuación:

- **Mínimo Punto de Exposición (MPE)**: Esto significa utilizar lo mínimo de recursos posibles para el servicio en cuestión:
  - asegurarse que sea la última versión del servidor o aquella que no tenga problemas de seguridad
  - solo iniciar el servicio referente a la página web sin nada adicional que limiten el uso de recursos de procesamiento y de memoria.
  - evitar informar la versión del software o agregados (php, cgi, etc.):
    - *ServerSignature Off*
    - *ServerTokens Prod*
  - deshabilitar los módulos del servidor apache que no se utilizan
    - *la opción que permite ver los módulos que son utilizados:* ***httpd -M***
  - desactivar la opción de exploración de directorios:
    - *Options -Indexes*
  - desactivar a nivel de *firewall de borde* el acceso a otros puertos diferentes al utilizado por el servidor web (tcp/80)
  - instalar y configurar el módulo de seguridad del apache (evita ataques del estilo *blind sql injection, cross-site scripting,* entre otros.
    - **mod_security** (http://www.modsecurity.org/)
  - Instalar el módulo de apache **mod_qos** que evita el ataque conocido como “slowloris”, el cual logra que un cliente pueda envenenar el

servidor HTTP mediante conexiones TCP permanentemente abiertas, logrando que el servidor quede sin memoria y sin responder a las peticiones nuevas.

```
LoadModule qos_module modules/mod_qos.so
<IfModule mod_qos.c>
        #Manejo de conexiones hasta 20000 IPs diferentes
        QS_ClientEntries 20000

        # Se permite solamente 100 conexiones por IP
        QS_SrvMaxConnPerIP 100

        # Maximo numero de conexiones TCP activas 156
        MaxClients              512

        # Desactivar la directiva keep-alive cuando el 70%
        # de las conexiones TCP estan ocupadas:
        QS_SrvMaxConnClose      70%
</IfModule>
```

*mod_qos.conf*

- instalar software de protección adicional para el sistema operativo que permita levantar reglas dinámicas de filtrado de paquetes. Este software correctamente configurado puede minimizar los ataques de tipo DoS o DDoS.
  - **csf** (**http://configserver.com/cp/csf.html**)

- **Mínimo Privilegio Posible (MPP):** Evitar en lo posible la escalación de privilegios.
  - La ejecución del servidor web debe realizarse con un rol único
    - User apache
    - Group apache
  - El rol no debe tener acceso a consola, o un shell que no permita la conexión remota
    - SHELL: **/sbin/nologin** o /dev/null

- **Defensa en Profundidad:** Determinar y configurar parámetros que aseguren el buen rendimiento del servidor.
  - Limitar el tiempo de las conexiones para minimizar ataques de tipo DoS
    - *Timeout 50*
  - Limitar tamaño de peticiones: a fin de evitar transferencias innecesarias

    - *LimitRequestBody*
    - *LimitRequestFields*
    - *LimitRequestFieldSize*
    - *LimitRequestLine*
    - *LimitXMLRequestBody*
  - Limitar concurrencia: para evitar la sobrecarga del servidor.
    - *StarServers*
    - *MaxSpareServers*
    - *MaxRequestsPerChild*
    - *ThreadsPerChild*
    - *MaxSpareThreats*
  - Activar los registros de auditoría: con el fin de auditar los accesos
    - *LogLevel*