Tabla 10. Lista de Chequeo: Configuración de seguridad HTTP

- Validar la configuración preestablecida del servidor de aplicaciones, buscando mayor protección y blindaje en este punto.
- Para las respuestas de tipo HTTP se debe establecer un conjunto de caracteres bastante seguros.

Descripción	Nivel		
	1	2	3
Verificar que la aplicación acepte solo un conjunto definido de métodos de solicitud HTTP y que son necesarios, como GET y POST, y métodos no utilizados (por ejemplo: TRACE, PUT y DELETE) se encuentran explícitamente bloqueados.	X	X	X
Verificar que cada respuesta HTTP contenga una cabecera content-type en la que se especifique un conjunto utilizando un conjunto de caracteres seguros (Ejemplo: UTF-8, ISO 8859-1).	X	X	X
Verificar que los encabezados HTTP agregados por un proxy confiable o dispositivos SSO, tales como un token de portador (***bearer***), son autenticados por la aplicación.		X	X
Verificar que el cabezal ***X-FRAME-OPTIONS*** se encuentra especificado para los sitios que no deben ser embebidos en X-Frame en sitios de terceros.		X	X
Verificar que los encabezados HTTP o cualquier parte de la respuesta HTTP no expongan información detallada de la versión de los componentes del sistema.	X	X	X
Verificar que todas las respuestas del API contienen opciones: **X-Content-Type: nosniff, Content Disposition: attachment; filename="api.json"**	X	X	X
Verificar que la política de seguridad de contenido (CSPv2) está en uso de tal manera que ayude a mitigar vulnerabilidades de inyección comunes de DOM, XSS, JSON y Javascript.	X	X	X
Verificar que el encabezado "X-XSS-Protection: 1; mode=block" esté presente para habilitar a los navegadores a filtrar XSS reflejados.	X	X	X