Lista de Chequeo: Seguridad de las Comunicaciones. Tabla 9

- Utilizar durante la transmisión de información delicada o sensible el protocolo TLS.
- Utilizar para todo tipo de información transmitida, algoritmos y cifradores bastante poderosos.

Descripción	Nivel		
	1	**2**	**3**
Verificar que puede construirse la cadena de confianza desde una ***CA (Autoridad de Certificación)*** para cada certificado de seguridad de capa de transporte **(TLS, Transport Layer Security)** del servidor y que cada certificado del servidor sea válido.	X	X	X
Verificar que se utiliza **TLS** para todas las conexiones (incluyendo conexiones back-end y externas) autenticadas o que involucran funciones o información sensible, y no recaigan en protocolos inseguros o sin cifrado. Asegúrese de que la alternativa más fuerte es el algoritmo preferido.	X	X	X
Verificar que se registran los fallos de conexiones TLS en el backend.			X
Verificar que se construyen las cadenas de confianza para todos los certificados de clientes mediante anclajes de confianza e información de revocación de certificados.			X
Verificar que todas las conexiones a sistemas externos que involucran acciones o información sensible sean autenticadas.		X	X
Verificar que haya una sola implementación estándar de TLS utilizada por la aplicación la cual esté configurada para operar en un modo aprobado de operación.			X
Verificar que el certificado de clave pública se encuentre fijado (***Certificate Pinning***) con la clave de producción y la clave pública de respaldo.			X
Verificar que los encabezados ***HTTP Strict Transport Security*** sean incluidos en todas las peticiones y para todos los subdominios, como: ***Strict-Transport-Security: max-age =15724800; includeSubdomains***	X	X	X
Verificar que la URL del sitio web de producción haya sido enviada a una lista precargada de dominios de ***Strict Transport Security (STS)*** mantenidos por proveedores de navegadores web.			X
Asegurar que ***foward secrecy*** se esté utilizando para mitigar qué atacantes pasivos puedan grabar el tráfico.	X	X	X
Verificar que una adecuada revocación de certificados, tal como el protocolo de estatus de certificado en línea (**OSCP**), está habilitado y configurado para determinar el estado de vigencia del certificado.	X	X	X
Verificar que se utilicen únicamente algoritmos, cifradores y protocolos fuertes, a través de toda la cadena de confianza, incluyendo certificados raíz y certificados intermediarios de la autoridad certificadora seleccionada.	X	X	X

Verificar que la configuración de **TLS** esté en línea con las mejores prácticas actuales, particularmente debido a que configuraciones comunes se convierten en inseguras a medida que transcurre el tiempo.	X	X	X