Tabla 8. Lista de Chequeo: Protección de Datos

- **Confidencialidad**: nadie sin autorización puede ver los datos almacenados o en transmisión.
- **Integridad**: los datos persistentes no pueden ser alterados o eliminados sin autorización.
- **Disponibilidad**: Los usuarios con un nivel de autorización deberían poder acceder a los datos si los necesitan.

Descripción	Nivel		
	1	2	3
Verificar que todos los formularios que contengan información sensible se les haya desactivado el almacenamiento de caché en el cliente, incluyendo funciones de autocompletar.	X	X	X
Verificar que la lista de datos sensibles procesados por la aplicación se encuentra identificada, y que existe una política explícita de cómo debe controlarse el acceso a estos datos, cifrarse y reforzarse bajo las directivas de protección de datos pertinentes.			X
Verificar que toda información sensible es envíada al servidor en el cuerpo o cabeceras del mensaje HTTP (por ejemplo, los parámetros de la URL nunca se deben utilizar para enviar datos sensibles).	X	X	X
Verificar que la aplicación establece encabezados anti-caché adecuados según el riesgo de la aplicación, tales como las siguientes: ***Expires: Tue, 03 Jul 2001 06:00:00 GMTT*** ***Last-Modified: {now} GMT*** ***Cache-Control: no-store, no-cache, must-revalidate, max-age=0*** ***Cache-Control: post-check = 0, pre-check = 0*** ***Pragma: no-cache***	X	X	X
Verificar que en el servidor todas las copias almacenadas en caché o temporales de datos sensibles estén protegidos de accesos no autorizados o son purgados/invalidados después del acceso por parte del usuario autorizado.		X	X
Verificar que existe un mecanismo para eliminar de la aplicación todo tipo de dato sensible luego de transcurrido el tiempo definido por la política de retención.			X
Verificar que la aplicación reduce al mínimo el número de parámetros en una solicitud, como campos ocultos, variables de Ajax, cookies y valores en encabezados.		X	X

Verificar que la aplicación tenga la capacidad para detectar y alertar sobre un número anormal de solicitudes para la recolección de datos por medio de extracción de pantalla (***screen scrapping***)			X
Verificar que datos almacenados en el cliente (como almacenamiento local de HTML5, almacenamiento de la sesión, IndexedDB, cookies normales o las cookies de Flash) no contengan información sensible o información personal identificable.	X	X	X
Verificar que el acceso a datos sensibles es registrado en bitácora, los datos son registrados acorde a las directivas de protección de datos o cuando el registro de los accesos es requerido.		X	X
Verificar que la información sensible mantenida en memoria es sobre escrita con ceros tan pronto como no es requerida, para mitigar ataques de volcado de memoria.		X	X