Tabla 7. Lista de Chequeo: Gestión y registro de errores

- Logs de información que eviten registrar información confidencial si no se requiere.
- El Aseguramiento de que los datos en log se eliminan cumplido un cierto tiempo, definido por la necesidad de la aplicación.

Descripción	Nivel		
	1	2	3
Verificar que la aplicación no emita mensajes de error o rastros de pilas que contengan datos sensibles que podrían ayudar a un atacante, incluyendo el identificador de sesión, versiones de software/entorno y datos personales.	X	X	X
Verificar que la lógica de manejo de errores en controles de seguridad niegue el acceso por defecto.		X	X
Verificar que los controles del registro de seguridad proporcionen la capacidad para registrar los eventos de éxito y sobre todo los eventos de falla que son identificados como relevantes para la seguridad.		X	X
Verificar que cada registro de evento incluya la información necesaria para permitir una eventual investigación y correlación con otros eventos.		X	X
Verificar que todos los eventos que incluyen datos no confiables no se ejecuten como código en el software destinado a la visualización del registro.		X	X
Verificar que los registros de seguridad estén protegidos contra modificación y acceso no autorizado.		X	X
Verificar que la aplicación no registre datos sensibles definidos en las leyes o regulaciones de privacidad local, datos organizacionales sensibles definidos por una evaluación de riesgos, o datos de autenticación sensible que podrían ayudar a un atacante, incluyendo identificadores de sesión del usuario, contraseñas, hashes o tokens de APIs.		X	X
Verificar que todos los símbolos no imprimibles y separadores de campos estén codificados correctamente en las entradas del registro, para evitar la inyección del registro que no permita seguir las pistas de un acto malicioso.			X
Verificar que los campos del registro de fuentes confiables y no confiables sean identificables en las entradas del registro.			X
Verificar que un registro de auditoría o similar permite la no repudiación de transacciones claves.		X	X
Verificar que los registros de seguridad poseen alguna forma de verificación o control de integridad para prevenir modificaciones no autorizadas.			X

Verificar que los registros están almacenados en una partición diferente a donde se ejecuta la aplicación con una rotación de registros adecuada.			X