Lista de Chequeo: Criptografía en el almacenamiento. Tabla 6

- Una gestión correcta de los errores, al realizar una forma segura de fallo para los módulos tipo criptográficos.
- El uso adecuado de un generador aleatorio de números cuando se lo necesite.

- Una forma de acceder a la claves bastante segura y confiable..

Descripción	Nivel		
	1	2	3
Verificar que todos los módulos criptográficos fallen de forma segura y que los errores sean manejados de tal manera que no permitan ataques ***Oracle padding***.	X	X	X
Verificar que todos los números aleatorios, nombres aleatorios de archivo, UID aleatorios y cadenas aleatorias, sean generados usando un módulo criptográfico aprobado del generador de números aleatorios cuando se pretende que estos valores no puedan ser adivinados o predecibles para un atacante.		X	X
Verificar que los algoritmos criptográficos utilizados por la aplicación hayan sido validados contra ***FIPS 140-2*** (***Federal Information Processing Standard***) o un estándar equivalente.	X	X	X
Verificar que los módulos criptográficos operen en su modo aprobado según sus políticas de seguridad publicadas.			X
Verificar que exista una política explícita para el manejo de las claves criptográficas (por ejemplo, generadas, distribuidas, revocadas y vencidas). Verificar que el ciclo de vida de las claves se aplique correctamente.		X	X
Verificar que los consumidores de servicios criptográficos no poseen acceso directo a los datos de la clave. Aislar procesos criptográficos, incluyendo secretos maestros y considerar el uso de un módulo de seguridad de hardware (HSM).			X
La información de identificación personal debe almacenarse de forma cifrada y verificar que la comunicación se lleve a cabo utilizando canales protegidos.		X	X
Verificar que contraseñas y claves criptográficas sean sobrescritas con ceros en memoria tan pronto no sean necesarias, con el fin de mitigar ataques de volcado de memoria.		X	X
Verificar que todas las claves y contraseñas sean reemplazables y sean generadas o reemplazadas durante la instalación.		X	X
Verificar que los números aleatorios sean creados con adecuada entropía, incluso cuando la aplicación se encuentre bajo carga intensa, o que la aplicación se degrade armoniosamente en tales circunstancias.			X