Lista de Chequeo: Control de Acceso. Tabla 4

- Para acceder a un recurso es necesario que el usuario posea la credenciales y el rol que tiene permisos válidos de ejecución.
- Existe un conjunto de roles y privilegios totalmente definidos para los usuarios del sistema.
- Se protegen de ataques de reutilización y manipulación los metadatos asociados a los roles y permisos.

Descripción	Nivel		
	1	2	3
Verificar que existe el principio de privilegio mínimo - los usuarios sólo deben ser capaces de acceder a las funciones, archivos de datos, URL, controladores, servicios y otros recursos, para los cuales poseen una autorización específica. Esto implica protección contra suplantación de identidad y elevación de privilegios.	X	X	X
Verificar que el acceso a registros sensibles esté protegido, tal que sólo objetos autorizados o datos sean accesibles por cada usuario (por ejemplo, proteger contra la posible manipulación hecha por usuarios sobre un parámetro para ver o modificar la cuenta de otro usuario).	X	X	X
Verificar que la navegación del directorio esté deshabilitada a menos que esto sea deliberadamente deseado. Además, las aplicaciones no deben permitir el descubrimiento o divulgación de metadatos de archivos o directorios, como carpetas que contengan ***Thumbs.db***, ***DS_Store***, o directorios .git o SVN.	X	X	X
Verificar que los controles de acceso fallen de forma segura.	X	X	X
Verificar que las mismas reglas de control de acceso implícitas en la capa de presentación son aplicadas en el servidor.	X	X	X
Verificar que todos los atributos de usuario, datos e información de las políticas utilizadas por los controles de acceso no puedan ser manipulados por usuarios finales a menos que sean específicamente autorizados.		X	X
Verificar que exista un mecanismo centralizado (incluyendo las bibliotecas que requieren servicios de autorización externa) para proteger el acceso a cada tipo de recursos protegidos.			X
Verificar que todas las acciones de control de acceso pueden ser registradas y que todas las acciones fallidas son registradas.		X	X
Verificar que la aplicación o su infraestructura emite ***tokens anti-CSFR*** aleatorios y no existe otro mecanismo de protección de la transacción.	X	X	X
Verificar que el sistema se pueda proteger contra el acceso permanente a funciones aseguradas, recursos o datos. (Por ejemplo, que el sistema utilice un recurso gobernante que limite el número de ediciones por hora o para prevenir que la base de datos sea sobre-utilizada por un único usuario).		X	X
Verificar que la aplicación disponga de autorización adicional (como doble factor de		X	X

autenticación con envío de mensaje de texto o correo electrónico) para sistemas de valores bajos, y/o segregación de funciones para aplicaciones de alto valor para cumplir con los controles anti fraude según el análisis de riesgo de la aplicación y fraudes cometidos en el pasado.			
Verificar que la aplicación aplique correctamente la autorización contextual para no permitir la manipulación de parámetros de la URL.	X	X	X