Parámetros de seguridad

- **Inyección:** son ataques que se realizan a las bases de datos mediante consultas. Para evitar esto tendremos medias se tomarán las siguientes medidas: no se usará los id de trámites en los títulos de estos para evitar que los manipulen, evitar uso de caracteres especiales o usando el escape del intérprete. Con esto se tendrá una API segura,

- **Diseño inseguro:** hay una mala arquitectura del diseño del proyecto lo que crea vulnerabilidades que pueden ser explotadas. Para evitar esto se tendrá un asesoramiento con el área técnica de seguridad para seguir los patrones de diseño e implementar los recursos adecuados para tener un buen diseño. También se generarán pruebas de seguridad mientras se va desarrollando la aplicación.

- **Configuración incorrecta de seguridad:** no está bien configurado, hay muchos puertos abiertos, los sistemas no se actualizan de manera continua. Para evitar esto se debe tener un sistema sin componentes que no son útiles, un proceso automatizado para la efectividad e ir revisando los parches de seguridad y también hay que tener un seguimiento cercano en el ciclo de vida del proyecto.

- **Componentes vulnerables y obsoletos:** el software está desactualizado o es vulnerable. Para prevenirlo hay que tener un inventario de todos los componentes que se usan para tener conocimiento de versiones, borrar componentes desactualizados, usar solamente componentes oficiales y no usar servicios piratas, al momento de usar algún componente se revise previamente la documentación y las versiones que cubre para evitar tener brechas entre las versiones.

- **Pérdida de control de acceso:** se dan permisos a todos los usuarios para que puedan realizar ciertas acciones que solamente deberían poder ejecutar un cierto grupo de usuarios. Tendremos un historial de las operaciones, donde se registrará las acciones de eliminar, actualizar y subir de un trámite; junto con la hora y el nombre del administrador que lo realizó. Solamente las cuentas de administradores tendrán permiso de modificar la información, para los ciudadanos, por defecto, solo podrán leer y buscar trámites.

- **Fallo de integridad de software y datos:** esto ocurre cuando existe dependencia de paquetes o librerías de terceros y no se verifica si existe mal código o violaciones de seguridad dentro de estas librerías. Ocurre con mayor frecuencia si el software se actualiza de manera automática. Para evitar este fallo se utilizará el gestor de dependencias Composer para el backend, ya se utiliza PHP y solo se utilizarán paquetes oficiales de Angular para el frontend. También se revisarán los cambios entre versiones y se tomará una decisión para actualizarlo o no.