INFORMACIÓN SOBRE COMPONENTES DE SEGURIDAD

Los registros que se realicen por medio de la aplicación web contarán con los estándares de seguridad adecuados para el tipo de información que ésta manejará. Específicamente podemos referirnos a 4 componentes principales dentro del esquema de seguridad:

- **Certificado SSL/TLS[1]:**
  Este certificado permite que haya seguridad en la interacción cliente-servidor (por ejemplo, el sitio web de la aplicación y un navegador web en el computador de un usuario). Es decir, que la información enviada es confidencial y pasa por algoritmos de encriptación o cifrado, impidiendo que los datos puedan ser interceptados, leídos o modificados por un atacante.

- **Implementación encriptación de autenticación:**
  Adicional al cifrado del certificado SSL/TLS asegura aún más las credenciales de acceso para evitar que sean enviados de forma plana.

- **Backup periódico de Base de Datos:**
  Está técnica de respaldo permite generar una copia automática de la base de datos cada cierto tiempo de forma tal que se pueda recuperar la información en caso de que un factor externo afecte la base de datos principal. De esta manera podrá reestablecerse la información a partir del último Backup. Es importante aclarar que este backup no es contemporáneo a la BD, se realiza con un tiempo de retraso.

- **Logs de auditoría:**
  La aplicación prevé que se tenga un registro de todos los eventos y acciones realizadas por un usuario. Esto permite hacer trazabilidad a movimientos indebidos dentro de la aplicación. Se guardará el tipo de acción, fecha/hora y lugar desde donde se haya realizado la acción.

Acciones que se pueden implementar en el corto o mediano plazo:

- **Réplica de Base de Datos:**
  La réplica de una base de datos en tiempo real permite que se tenga un respaldo de la información constantemente. Esta base de respaldo es útil para ser empleada en caso de que la base de datos primaria presente problemas de disponibilidad o accesibilidad.

- **Logs de eventos:**
  Puede implementarse una base de datos (como Redis) que se encargue de almacenar el log de eventos de las transacciones. Con esto puede reconstruirse el histórico de las transacciones realizadas y así, mantener seguro el estado actual del sistema de transacciones. Todo registro fraudulento que aparezca y no haga parte de ese log, puede ser fácilmente identificado.

[1] SSL es el acrónimo de Secure Sockets Layer (capa de sockets seguros) y TLS es para Transport Layer Security (seguridad de la capa de transporte).

- **Tecnologías de Block Chain**
  La plataforma será desarrollada con una arquitectura que permitirá la implementación de Block Chain en el futuro. Con esto se espera brindar una capa adicional de seguridad al persistir las transacciones y generar los registros pertinentes en la comprobación de una transacción.