

Consideraciones Finales

La implementación de **Acceso Tamaulipas (Fusionauth)** en proyectos Laravel permite centralizar el proceso de autenticación y mantener un esquema institucional uniforme para el acceso a las aplicaciones. Esto facilita la administración de usuarios, reduce la duplicidad de lógica entre sistemas y mejora el mantenimiento general de los proyectos.

Antes de iniciar la integración, se deberá solicitar formalmente la **creación de la aplicación dentro de Acceso Tamaulipas (Fusionauth)**, con la finalidad de que se generen y proporcionen las llaves de acceso necesarias para la conexión del sistema, tales como el `client_id` y `client_secret`.

Dicha solicitud deberá realizarse mediante correo electrónico dirigido a **[nombre del área o dirección correspondiente]**, al correo **[correo@tamaulipas.gob.mx]**, indicando la información general del sistema que se desea integrar, el ambiente correspondiente y la URL donde será publicado el proyecto.

Una vez creada la aplicación en FusionAuth, se deberán configurar las variables de entorno correspondientes en el archivo `.env` del proyecto Laravel, utilizando las llaves de acceso proporcionadas. Es importante conservar correctamente la configuración definida para FusionAuth, especialmente las variables relacionadas con la URL base, el tenant y la URI de callback, ya que estos valores deben coincidir con la configuración registrada en FusionAuth.

Asimismo, se recomienda utilizar migraciones para cualquier modificación en la estructura de la base de datos, ya que esto permite mantener trazabilidad de los cambios y facilita los despliegues en nuevos ambientes. Aunque es posible realizar ajustes mediante SQL directo, esta opción debe considerarse únicamente como alternativa temporal o de emergencia.

El módulo de autenticación debe mantenerse sin modificaciones directas, ya que al ser administrado como una dependencia mediante Composer, cualquier cambio local puede perderse durante actualizaciones o reinstalaciones. En caso de requerir ajustes específicos, se deberán implementar desde el proyecto consumidor o mediante configuraciones externas.

Finalmente, antes de liberar la integración en un ambiente productivo, se deberá validar que el flujo completo funcione correctamente: redirección al login de FusionAuth, autenticación del usuario, retorno mediante callback, registro o actualización del usuario en Laravel, cierre de sesión y validación de acceso al sistema.

Con estas consideraciones, el proyecto quedará preparado para operar con una autenticación centralizada, mantenible y alineada con el estándar institucional.