

En el marco de nuestro proyecto, decidimos implementar Auth0 como nuestro proveedor de Single Sign-On (SSO). Esta decisión se basa en un análisis de las necesidades del sistema y las ventajas que ofrece Auth0 en comparación con otras opciones.

## Por qué es importante un SSO

Actualmente el sistema cuenta con un sistema de inicio de sesión propio. Sin embargo, la implementación de un SSO como Auth0 nos aporta varias ventajas:

**Más seguridad:** Auth0 es una plataforma confiable que se encarga de la autenticación de usuarios, liberando a nuestro sistema de la responsabilidad de gestionar contraseñas y tener posibles vulnerabilidades.

**Mejor experiencia de usuario:** El SSO permite a los usuarios acceder al sistema con sus credenciales de otros proveedores como Google o Microsoft, facilitando el inicio de sesión.

**Acceso centralizado:** Auth0 nos permite gestionar a los usuarios desde una única plataforma, mejorando la administración y el control del acceso al sistema.

## Comparación con otras opciones de SSO

Encontramos otras opciones de SSO similares, como Keycloak, Okta y Firebase Authentication, pero creemos que Auth0 se destaca entre ellas. Principalmente ya que cuenta con una interfaz muy intuitiva y mucha documentación para su implementación y configuración. Además, Auth0 cuenta con herramientas avanzadas como la gestión de roles (algo fundamental para nuestro proyecto).

## Implementación de Auth0 en el proyecto

La implementación de Auth0 en el proyecto se realizaría de la siguiente manera:

**Configuración:** Se configurará una aplicación en Auth0 con las credenciales y permisos necesarios para interactuar con el sistema.


Create Application

Name \*

My App

You can change the application name later in the application settings.


Choose an application type



Native

Mobile, desktop, CLI and smart device apps running natively.


e.g.: iOS, Electron, Apple TV apps



Single Page Web Applications

A JavaScript front-end app that uses an API.


e.g.: Angular, React, Vue



Regular Web Applications

Traditional web app using redirects.

e.g.: Node.js Express, ASP.NET, Java, PHP



Machine to Machine Applications

CLIs, daemons or services running on your backend.

e.g.: Shell script

Cancel

Create

**Integración con el sistema:** Se integrará Auth0 con el sistema mediante la API de Auth0

**Autenticación de usuarios:** Los usuarios podrán autenticarse a través de Auth0 utilizando sus credenciales existentes de otros proveedores de identidad o creando una nueva cuenta.

**Obtención del token:** Auth0 nos emite un token de acceso para cada usuario autenticado.

```
Decoded Token:
{
  "sub": "auth0|67435fd827bf751c6c17a433",
  "email_verified": false,
  "iss": "https://dev-0m2ghq1w4lbd5rhi.us.auth0.com/",
  "picture": "https://s.gravatar.com/avatar/75d23af433e0cea4c0e45a56dba18b30?s\u003d480\u0026r\u003dpg\u0026d\u003dhhttps%3A%2F%2Fcdn.auth0.com%2Favatars%2Fad.png",
  "sid": "fIb66D46z7GH3-_Erq236WVq0Txrarh4",
  "aud": "Yqws7LsFNeyg15evMCPN7SCdv45UDW1A",
  "updated_at": "2024-11-25T23:20:17.820Z",
  "https://heladerAR.com/roles": [
    "ADMIN"
  ],
  "nickname": "admin",
  "name": "admin@gmail.com",
  "exp": 1732612819,
  "iat": 1732576819,
  "email": "admin@gmail.com"
}
```

**Validación del token:** El sistema validará el token de acceso recibido para verificar la identidad del usuario y autorizar el acceso a los recursos correspondientes. Para esto, se debería chequear que el campo “sub” que posee el *subscriber*, coincida con la información creada en nuestra base de datos.

```
"sub": "auth0|67435fd827bf751c6c17a433",
"email_verified": false,
"iss": "https://dev-0m2ghq1w4lbd5rhi.us.au
```

**Gestión de roles:** Se utilizarán los roles definidos en Auth0 para controlar el acceso de los usuarios a las diferentes funcionalidades del sistema.

### Beneficios extras de Auth0

Además de las ventajas mencionadas anteriormente, Auth0 nos ofrece otros beneficios como herramientas de análisis que permiten visualizar estadísticas sobre los inicios de sesión, los usuarios activos y otros datos relevantes.