**Metodologías y Tecnologías de la Integración de Sistemas**

Ingeniería Informática

**Arancha Ferrero Ortiz de Zárate**

**72850555X**

*Practica 6*

SSO

**17 de junio del 2018**

# Descripción de la práctica

El objetivo de esta práctica, es implementar un sistema Single Sign On (SSO) y realizar la puesta en marcha empleando la solución SSO de Google.

Finalmente, para poder comprobar visual y fácilmente dichos servicios, crearé un cliente web en PHP empleando el popular framework [Laravel](https://laravel.com/).

# Requisitos del sistema

* PHP 7
* [Composer](https://getcomposer.org/)

# Archivos de la práctica

Junto a esta memoria, adjunto el proyecto de Laravel con el cliente: *mtis-p6*.

# 

# Instalación del software necesario

Para el correcto funcionamiento de la práctica, resulta indiferente el SO empleado.

1. **Descargar e instalar Composer**: En su [web oficial](https://getcomposer.org/download/) nos ofrecen una amplia variedad de formas de instalarlo. Para Windows, sugiero el instalador que nos proporcionan: [Composer-Setup.exe](https://getcomposer.org/Composer-Setup.exe). El cuál, además de instalarnos composer, nos configura la variable de entorno *composer* desde cualquier directorio.
2. **Instalar Laravel:** Una vez instalado Composer, podemos instalar Laravel fácilmente desde una terminal ejecutando:  
    composer global require "laravel/installer"

# Puesta en marcha

## Iniciar servidor Laravel

A la hora de iniciar el servidor en Laravel con el cliente, necesitamos abrir una terminal en la ruta donde se halla el proyecto *cliente-web-laravel* adjuntado en la práctica. En él ejecutamos (sólo la primera vez):

composer update

Y a continuación, iniciamos el servidor con:

php artisan serve

## Abrir URL del cliente en el Navegador

Finalmente, podemos comprobar el funcionamiento de nuestra práctica desde la URL: [127.0.0.1:8000](http://127.0.0.1:8000)

# ¿Qué es SSO?

Single Sign On conocido también como SSO por sus siglas en inglés permite a los usuarios tener acceso a múltiples aplicaciones ingresando solo con una cuenta a los diferentes sistemas y recursos. El SSO es de gran utilidad cuando existen diferentes sistemas a los que es posible acceder mediante una única contraseña y se desea evitar el ingreso repetitivo de estas cada vez que el usuario se desconecte del servicio. Para los usuarios supone una gran comodidad ya que identificándose solo una vez es posible mantener la sesión válida para el resto de las aplicaciones que hacen uso del SSO.

# Ventajas de una arquitectura SSO

Este procedimiento de autenticación facilita las tareas de acceso a las diferentes plataformas, además cuenta con otras importantes características en aspectos de gestión sencilla,seguridad, facilidad de uso y transparencia.

* Gestión sencilla

El uso de SSO realiza la sincronización de contraseñas e información del usuario, lo que proporciona la simplificación del acceso a los diferentes plataformas y recursos.

* Seguridad

Este sistema de autenticación mejora la seguridad de la red y de las aplicaciones. Single Sign On puede identificar inequívocamente a un usuario por lo que cumple con normas más exigentes respecto a la seguridad. La información proporcionada a SSO viaja cifrada por la red.

* Facilidad de uso

Las soluciones SSO mejoran la experiencia del usuario evitando las interrupciones producidas por las solicitudes de contraseñas para acceder a sus herramientas informáticas. El usuario se autentica una vez y el sistema le permite acceder los recursos para los cuales está autorizado.

* Transparencia

El acceso a todas las aplicaciones por parte del usuario se realizan de forma transparente debido a la automatización del inicio de sesión.

# SSO de Google

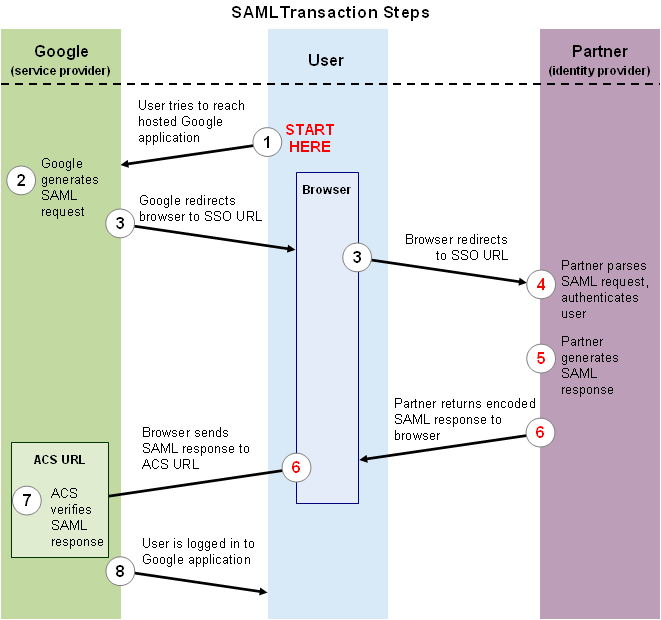
Google ofrece un servicio de inicio de sesión único (SSO) basado en SAML con el que los partners tienen un control completo sobre la autorización y la autenticación de las cuentas de usuario alojadas que pueden acceder a aplicaciones web, como Gmail o Google Calendar. En el modelo SAML, Google actúa como proveedor de servicios y proporciona servicios como Gmail y páginas de inicio. Los partners de Google actúan como proveedores de identidades y controlan los nombres de usuario, las contraseñas y otra información utilizada para identificar, autenticar y autorizar a los usuarios en aplicaciones web alojadas por Google. Existen diversas soluciones de proveedor de identidades de [software libre](https://support.google.com/google-apps/help/open-source#sso) y [comerciales](http://www.google.com/enterprise/marketplace/search?categoryId=2&orderBy=rating) con las que se puede implementar el inicio de sesión único con Google.

En el siguiente proceso se describe cómo inicia sesión un usuario en una aplicación alojada en Google mediante un servicio de inicio de sesión único basado en SAML proporcionado por un partner.

La imagen 1 que se muestra a continuación ilustra el proceso mediante el cual un usuario inicia sesión en una aplicación de Google, por ejemplo Gmail, a través de un servicio SSO basado en SAML. En la lista numerada que sigue a la imagen se explica cada paso con más detalle.

**Nota**: Para que se pueda realizar este proceso, el partner debe facilitar a Google la URL para su servicio de inicio de sesión único, así como la clave pública que Google debería usar para verificar las respuestas SAML.

**Imagen 1: Acceso a Google mediante un servicio de inicio de sesión único (SSO) basado en SAML proporcionado por un partner**



# Pasos seguidos para las elaboración de la práctica

Para elaborar esta práctica he seguido los pasos de la siguiente guía: <https://laraveles.com/como-hacer-inicio-de-sesion-con-google-en-laravel/>

Dicha guía indica de forma muy didáctica cómo integrar el SSO de Google con Laravel en el cliente de forma sencilla.