 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-27

ESTUDIO COMPARATIVO DE SEGURIDAD, COMPATIBILIDAD Y RENDIMIENTO DE LOS PROTOCOLOS SAML Y OAUTH COMO MECANISMOS DE AUTENTICACIÓN MEDIANTE SINGLE SIGN ON (SSO) ENTRE LAS PLATAFORMAS JOOMLA Y MOODLE

Jorge Iván Atehortua Alzate

Giovanny Alberto Gómez Yepes

INGENIERIA DE SISTEMAS

Director del trabajo de grado

Javier Mauricio Duran Vásquez

INSTITUTO TECNOLÓGICO METROPOLITANO

Noviembre 8 de 2018

	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

RESUMEN

El presente proyecto permite identificar el método más eficiente de inicio de sesión bajo el sistema Single Sing On (SSO), mediante la comparación de seguridad y rendimiento de los protocolos SAML y OAUTH en las plataformas JOOMLA y MOODLE, aportando conocimientos pertinentes en el tema de seguridad en el área de las Tecnologías de la Información y la Comunicación.

Se inicia a partir del análisis de evidencias científicas por medio de un estado del arte que permite hacer un rastreo en diversas bases de datos como Engineering Village, Dialnet, y la IEEE Xplore Digital Library y enlaces web relacionados con las tecnologías de la información y la comunicación donde se indaga acerca de los antecedentes y desarrollos actuales del Sistema de Autenticación Único Single Sing On (SSO), para ello se retoman diversos artículos e investigaciones tales como, Modelo de Single Sing On para Herramientas de Grupo QUALDEV (2009), Aplicación del mecanismo único de sesión para la Computación Distribuida (2014), Single Sign On en la federación de la nube, usando federación clousing (2015), etc., que permiten validar la pertinencia del proyecto de investigación, encontrando que no existe evidencia acerca de la comparación entre los protocolos SAML Y OAUTH como mecanismos de inicio de sesión en plataformas web.

A partir de la aplicación del modelo experimental lineal secuencial conocido también como modelo de vida básico o de cascada, el cual se desarrolla a través de un enfoque sistemático, se logra identificar cuál de los protocolos a comparar permite tener mayor eficiencia al momento de centralizar las plataformas e implementar un único usuario y clave como inicio de sesión, beneficiando a los usuarios quienes ya no estarán obligados a manejar diversas claves para cada plataforma web existente.

Palabras clave: Single Sing On (SSO), Security Assertion Markup Language (SAML), Open Authorization (OAUTH), JOOMLA, MOODLE, authentication, inicio de sesión

	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

RECONOCIMIENTOS

A Dios Todopoderoso, por darnos la vida y permitirnos la culminación de este proyecto de grado.

A nuestras familias, gracias por su incondicional apoyo especialmente a Mary Luz Mesa Osorio (esposa de Jorge) por brindarnos sus conocimientos y ponerlos a nuestra disposición en la elaboración de este trabajo. A la Institución Universitaria (ITM), por ampararnos en sus aulas y brindarnos las herramientas para poder obtener los conocimientos que nos permitan cumplir nuestras metas. A nuestros Profesores, por transmitirnos sus conocimientos y su gran apoyo para la culminación de nuestros estudios profesionales y para la elaboración de esta tesis; al Profesor Javier Mauricio Duran Vásquez por su apoyo en la orientación para la elaboración de este trabajo. A la empresa CREAME por permitir el uso de sus servidores para la elaboración de este trabajo.

A nuestros compañeros de estudio, quienes nos apoyábamos en clase y a la distancia, nos acompañábamos y dábamos ánimo para seguir adelante. Así mismo, a nuestros compañeros de trabajo, quienes nos apoyaban con sus aportes conocimientos y experiencias.

A todos los que estuvieron a nuestro lado en este camino.

	<p style="text-align: center;">INFORME FINAL DE TRABAJO DE GRADO</p>	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

ACRÓNIMOS

SSO: SINGLE SIGN ON

JOOMLA: GESTOR Y MANEJADOR DE CONTENIDOS WEB DINAMICOS

MOODLE: GESTOR Y MANEJADOR DE CONTENIDOS WEB PARA LE EDUCACION VIRTUAL

OAUTH: OPEN AUTHORIZATION, PROTOCOLO DE AUTORIZACIÓN QUE PERMITE QUE LOS USUARIOS AUTORICEN A TERCEROS A ACCEDER A SU INFORMACIÓN

SAML: SECURITY ASSERTION MARKUP LANGUAGE, ESQUEMA XML PARA EL INTERCAMBIO DE DATOS DE AUTENTICACIÓN Y AUTORIZACIÓN. USUALMENTE LAS PARTES QUE INTERVIENEN EN EL INTERCAMBIO SON UN PROVEEDOR DE IDENTIDAD (ENTIDAD QUE DISPONE DE LA INFRAESTRUCTURA NECESARIA PARA LA AUTENTICACIÓN DE LOS USUARIOS) Y UN PROVEEDOR DE SERVICIO (ENTIDAD QUE CONCEDE A UN USUARIO EL ACCESO O NO A UN RECURSO)

PLUGINS: APLICACIÓN (O PROGRAMA INFORMÁTICO) QUE SE RELACIONA CON OTRA PARA AGREGARLE UNA FUNCIÓN NUEVA Y GENERALMENTE MUY ESPECÍFICA

CPANEL: PANEL DE CONTROL PARA ADMINISTRAR SERVIDORES DE ALOJAMIENTO WEB QUE PROVEEN HERRAMIENTAS DE AUTOMATIZACIÓN Y UNA INTERFAZ GRÁFICA BASADA EN PÁGINAS WEB

HOSTING: ALOJAMIENTO O SERVICIO QUE PROVEE EL ESPACIO EN INTERNET PARA LOS SITIOS WEB.

FTP: PROTOCOLO DE TRANSFERENCIA DE ARCHIVOS

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

Tabla de contenido

Resumen	ii
Reconocimientos	iii
Acrónimos	IV
Tabla de Contenido	V
Lista de Tablas	VI
Lista de Ilustraciones	VII
1. Introducción	1
1.1 Objetivo General.....	2
1.2 Objetivos Específicos.....	2
2. Marco Teórico.....	3
3. Metodología	10
3.1 Cronograma y Fases	12
3.2 Análisis de los requerimientos.....	13
3.3 Implementación	15
3.3.1 Instalación de Plataformas Administradoras de contenido	15
3.3.1.1 Instalación de Joomla para el protocolo Saml.....	16
3.3.1.2 Instalación de Moodle para el protocolo Saml	18
3.3.1.3 Instalación de Joomla para el protocolo Oauth.....	20
3.3.1.4 Instalación de Moodle para el protocolo Oauth.....	22
3.3.2 Instalación de Plugins	24
3.3.2.1 Instalación de Plugins en Joomla para SAML	24
3.3.2.2 Instalación de Plugins en Moodle para Saml.....	25
3.3.2.3 Instalación de Plugins en Joomla para Oauth.....	28
3.3.2.4 Instalación de Plugins en Moodle para Oauth.....	30
3.3.3 Implementación Proveedor de Identidad	31
3.4 Pruebas.....	39
4. Resultados y Discusión.....	45
4.1. Selección de criterios.....	45
4.2. Valoración de criterios.....	45
4.2.1 Seguridad.....	45
4.2.1.1 Confidencialidad.....	46
4.2.1.2 Secuencia básica de Uso de Saml y Oauth.....	48
4.2.2 Compatibilidad	51
4.2.2.1 Respuesta del entorno de Aplicación.....	51
4.2.3 Rendimiento	54
4.2.3.1 Uso de Memoria RAM y CPU	54
5. Conclusiones, Recomendaciones y trabajo Futuro	57
6. Referencias.....	60

	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

Lista de Tablas

Tabla 1 – Cronograma de Actividades.....	12
Tabla 2. Fases de las actividades.....	13
Tabla 3. Características Servidores y Plataformas.....	14
Tabla 4: Claves usadas por las políticas de seguridad	48
Tabla 5: SAML en JOOMLA procesamiento de maquina desde el login hasta su cerrada de sesión.....	54
Tabla 6: SAML en MOODLE procesamiento de maquina desde el login hasta su cerrada de sesión.....	55
Tabla 7: OUTH en JOOMLA procesamiento de maquina desde el login hasta su cerrada de sesión.....	55
Tabla 8: OUTH en MOODLE procesamiento de maquina desde el login hasta su cerrada de sesión.....	55
Tabla 9: Resultados comparativos criterios de valoración.....	57
Tabla 10: cuadro ventajas y desventajas del uso de los protocolos SAML y OAUTH.....	58

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

Lista de ilustraciones

Ilustración 1- Secuencia de autenticación SAML.....	7
Ilustración 2- Secuencia de funcionamiento OAUTH.....	9
Ilustración 3- Archivos de la WEB en JOOMLA.....	16
Ilustración 4 – Listado base de datos.....	17
Ilustración 5: página del administrador de JOOMLA.....	17
Ilustración 6 - Archivos de la WEB en MOODLE.....	18
Ilustración 7 – Base de datos para instalación de MOODLE.....	19
Ilustración 8- Panel de Admon Plataforma MOODLE.....	20
Ilustración 9 – Carpeta para JOOMLA en Protocolo OAUTH.....	21
Ilustración 10 – Base de datos para JOOMLA en protocolo OAUTH.....	21
Ilustración 11 – Panel de Admon JOOMLA para OAUTH.....	22
Ilustración 12 – Carpeta en el Hosting de MOODLE para OAUTH.....	22
Ilustración 13 – Base de datos para MOODLE en OAUTH.....	23
Ilustración 14 – Administrador de MOODLE para OAUTH.....	23
Ilustración 15 – Instalación del componente miniorange-SAML.....	24
Ilustración 16 – Configuración del componente miniorange-SAML.....	25
Ilustración 17: validación de requisitos previos a la instalación.....	26
Ilustración 18: comprobación, instalación del plugin mini Orange SAML.....	26
Ilustración 19: Actualización de la versión del plugin mini Orange SAML.....	27
Ilustración 20: Actualización de la versión del plugin mini Orange SAML.....	27

	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

Ilustración 21: instalación del componente mini Orange OAUTH Client.....	28
Ilustración 22: Configuración del componente mini Orange OAUTH Client.....	29
Ilustración 23: Sincronización de la cuenta con datos de acceso a mini Orange	30
Ilustración 24: Creación del servicio de autenticación.....	31
Ilustración 25: Registro en la plataforma mini Orange como proveedor de Identidad.....	32
Ilustración 26: Creación de app para conexión de JOOMLA con el protocolo SAML.....	33
Ilustración 27: Listado de las 4 aplicaciones para cada gestor de contenido.....	33
Ilustración 28: configuración de la app y datos para configurar los gestores de contenido...	34
Ilustración 29: Creación de una política de seguridad.....	35
Ilustración 30: Listado de políticas para uso de las aplicaciones.....	35
Ilustración 31: creación la app del IDP para JOOMLA en SAML.....	35
Ilustración 32: configuración de la app del IDP para JOOMLA en SAML.....	36
Ilustración 33: parámetros de la app en el IDP para JOOMLA SAML.....	36
Ilustración 34: parámetros finales de la app en el IDP pára MOODLE SAML.....	37
Ilustración 35: configuración en el IDP de la app para MOODLE con SAML.....	38
Ilustración 36: configuración del protocolo OAUTH en la app del IDP para MOODLE.....	38
Ilustración 37: aplicaciones para OAUTH y el enlace a la descarga d los certificados generados.....	39
Ilustración 38: prueba de configuración JOOMLA para SAML.....	40
Ilustración 39: conexión establecida entre JOOMLA y al IDP mini Orange.....	40
Ilustración 40: prueba de configuración de MOODLE con el IDP.....	41
Ilustración 41: test de conexión entre MOODLE y el IDP para el protocolo SAML.....	41
Ilustración 42: Prueba del servicio de autenticación en MOODLE para OAUTH.....	42

	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

Ilustración 43: Home de JOOMLA con los accesos al login de las dos plataformas para el protocolo SAML.....	43
Ilustración 44: login con el usuario del IDP	44
Ilustración 45: acceso a MOODLE usando SSO.....	44
Ilustración 46: Metadatos y certificados de las apps.....	46
Ilustración 47: políticas de seguridad.....	47
Ilustración 48: Secuencia básica de uso de SAML.....	49
Ilustración 49: Secuencia básica de uso de OAUTH.....	50
Ilustración 50: CPANEL como administrador de plataformas.....	51
Ilustración 51: Entorno del proveedor de identidad.....	52
Ilustración 52: Aplicación del protocolo SAML en JOOMLA.....	52
Ilustración 53: Aplicación del protocolo SAML en MOODLE.....	53
Ilustración 54: aplicación del protocolo OAUTH en JOOMLA.....	53
Ilustración 55: Aplicación del protocolo OAUTH en MOODLE.....	54

	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

1. INTRODUCCIÓN

En la actualidad el uso de las TIC se ha masificado, aumentando día a día la implementación de plataformas web que facilitan la interacción, la comunicación y el acceso a la información, sin embargo, también exige a los usuarios utilizar diversos datos como método de autenticación.

En el presente proyecto se plantea la utilización de las plataformas CMS JOOMLA y LMS MOODLE ya que son empleadas masivamente en el mundo, sin desconocer que ambas requieren y recopilan información de datos personales de cada usuario que quiera ingresar a ellas, es decir, que para cada acceso se requiere un usuario y una clave de acuerdo a cada aplicación o plataforma, convirtiendo esto en un trámite repetitivo y engorroso en la medida que el usuario requiere memorizar múltiples y diversas claves, además, cada plataforma expone el total de los datos del usuario ante un posible ataque informático; además según cifras reveladas por diversos estudios citados en el proyecto, comprueban que ambas plataformas son usadas de una forma masiva a nivel mundial tanto en el campo educativo como en el empresarial lo que hace que sea muy significativa la cantidad de información de personas que esta vulnerable y expuesta en la red.

Como solución al problema planteado se propone comparar la seguridad, compatibilidad y el rendimiento de los protocolos SAML y OAUTH como mecanismos de autenticación en las plataformas JOOMLA y MOODLE de los protocolos SAML Y OAUTH implementando un único usuario y clave como inicio de sesión en ambas plataformas.

En la primera parte del texto se exponen diversos referentes teóricos e investigativos que dan sustento a este proyecto, donde se argumenta el uso del SSO como método de autenticación, también se menciona el uso y el impacto reflejado mundialmente del CMS

	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

JOOMLA y el LMS MOODLE; en este apartado también se abordan antecedentes del uso del protocolo SAML y OAUTH como implementación de seguridad.

En la segunda parte del texto se muestra en diferentes campos y plataformas, una visión del uso e impacto en la tecnología web ya que muestran la evolución de la forma de autenticación segura en diferentes plataformas web como son JOOMLA, usada a nivel mundial y catalogada como el segundo CMS más usado en el mundo y MOODLE, por medio de protocolos que permiten simplificar y brindar una mayor seguridad a estas formas de autenticación.

1.1 OBJETIVO GENERAL

Comparar la seguridad, compatibilidad y el rendimiento de los protocolos SAML y OAUTH como mecanismos de autenticación en las plataformas JOOMLA y MOODLE, identificando así el mejor método inicio de sesión bajo la tecnología SINGLE SIGN ON.

1.2 OBJETIVOS ESPECÍFICOS

- Identificar 4 métodos (plugin, módulos o componentes) compatibles para los protocolos SAML y OAUTH que puedan instalarse para un esquema de SINGLE SIGN ON entre las plataformas (CMS) JOOMLA y (LMS) MOODLE
- Seleccionar criterios de valoración que permitan medir la seguridad, compatibilidad y el rendimiento de los protocolos SAML y OAUTH
- Valorar de manera experimental los criterios seleccionados en un esquema de SINGLE SIGN ON entre las plataformas (CMS) JOOMLA y (LMS) MOODLE como entornos de prueba para los protocolos SAML y OAUTH.
- Comparar los resultados de los criterios valorados, determinando las ventajas y desventajas de los protocolos SAML y OAUTH para un esquema de SINGLE SIGN ON entre las plataformas (CMS) JOOMLA y (LMS) MOODLE.

	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

2. MARCO TEÓRICO

Para lograr plena comprensión del presente proyecto de investigación se hace necesario definir algunos conceptos que se consideran fundamentales en el desarrollo de todo el proyecto investigativo, además de enunciar antecedentes referentes a la temática, generando un panorama más amplio para dicho proyecto.

El sistema Single Sing On (SSO), es un procedimiento de autenticación vía web, el cual habilita a un usuario para acceder a varias plataformas usando una sola instancia de identificación. Wikipedia, (2016)

Con este método una persona puede iniciar sesión en uno o varios sistemas sin necesidad de ingresar usuario y contraseña por cada plataforma donde se quiera tener acceso, solo ingresa los datos de acceso en una sola plataforma la cual tendrá los permisos para poder vincularse a las demás instancias que queramos acceder.

En el año 2009, Nelson Barrera Rivera publicó un artículo denominado Modelo de Single Sign-On para Herramientas del Grupo QualDev, en el cual “presentó un modelo para implementar SSO en las principales aplicaciones Web que usa el grupo de desarrollo QualDev. Esta implementación se basa en SAML, un estándar de seguridad propuesto por OASIS para desarrollar el concepto de SSO en aplicaciones distribuidas y sin necesidad de nuevas infraestructuras” (Rivera,2009,p1).

Rivera(2009), de manera general en el artículo ahonda sobre el concepto SSO, sus beneficios y ventajas, además de describir la tecnología SAML y cómo esta ayuda a la fácil implementación del proceso de autenticación del modelo propuesto, sin considerar sistemas y arquitecturas complejas, usando Servicios Web para la comunicación entre entidades. (p.13).

	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

Otro artículo que es necesario retomar fue planteado por Chhatwani and Harkut, denominado Aplicación del mecanismo único de sesión para la computación distribuida, en la Revista Internacional de Ciencias de la Computación y la Informática Móvil en el año 2014, dichos autores argumentan la necesidad de un único inicio de sesión para el acceso a diferentes aplicaciones evitando una sobrecarga de información tanto en la red como para el usuario, en dicho artículo agregan un componente innovador al sistema Single Sign On como lo es el componente biométrico como elemento que permite la autenticación por medio de huella, permitiendo un óptimo nivel de seguridad. (Harkut,2014).

Más adelante Dhole(2015), publicó en la Revista Internacional de la Red de Seguridad Informática un artículo titulado Single Sign-On in Cloud Federation using CloudSim (Single Sign - On en la Federación de la nube, usando Federación CloudSim), en el que se puso en marcha el inicio de sesión único en el escenario Federación usando el kit de herramientas CloudSim, teniendo en cuenta múltiples proveedores de identidad y Cloud Service Proveedores. También consideraron la seguridad como - as- de los datos transferidos entre las diferentes entidades de la federación de nubes durante el mecanismo de SSO. Dicho artículo en los resultados de la simulación muestra que el enfoque de SSO es altamente beneficioso al acceder a múltiples servicios de los CSP en la Federación de la nube, ya que reduce el tiempo de ejecución de la solicitud del usuario para los recursos de la Federación de la nube. En este trabajo, la tramitación de la solicitud de los usuarios de la nube se lleva a cabo de manera secuencial por los CSP de la Federación.

En cuanto a las plataformas MOODLE y JOOMLA respectivamente podemos decir que; MOODLE es considerado como “Un entorno Modular de Aprendizaje Dinámico Orientado a Objetos. Es decir, un programa intuitivo, cooperativo, interactivo, ubicado en el contexto y fácil de usar, donde se potencia el compartir objetos de aprendizaje por varios usuarios, permite incorporar múltiples y variadas actividades como complemento a la docencia presencial” Iglesias, Olmos, Torrecilla, & Juan,(2014,p.156)

	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

Existen diversas referencias acerca de la aplicación o implementación de MOODLE en el mundo, donde se menciona que “MOODLE es hoy el entorno estándar de formación telemática en los centros educativos españoles y en cada vez más empresas. Su facilidad y versatilidad, una atención impecable a la comunidad que lo usa y un original modelo de negocio son las claves de este éxito. Hace dos años, las estadísticas de MOODLE decían que dos millones de personas lo utilizaban en todo el mundo. Hoy son 25 millones y es una cifra a la baja, ya que el registro en la web es voluntario y minoritario. Más de 4.000 escuelas, institutos, academias, universidades y empresas españolas se han registrado (...) MOODLE se usa en más de 7 000 sitios Web alrededor del mundo, está presente en 16 países y se ha traducido a 75 idiomas.” MOLIST,(2008,p.1)

En cuanto a JOOMLA se puede decir que “es un sistema de gestión de contenido (CMS), que permite construir sitios Web y aplicaciones en línea de gran alcance, incluyendo su facilidad de uso y extensibilidad, es un popular software Web. Lo mejor de todo, JOOMLA es una solución de código abierto que está disponible gratuitamente para todo el mundo”. JOOMLA,(2016).

Acerca de esta plataforma también existen muchos estudios que hablan sobre la pertinencia de su implementación, tal es el caso de un estudio realizado por W3Techs donde afirman que “JOOMLA! Es el segundo CMS (Content Management System - Gestor de contenidos web) más usado en la actualidad.

El estudio revela que, a día de hoy, un 22% de las webs existentes utilizan algún tipo de CMS (...) JOOMLA Es el que más aceptación tiene, ya que nada menos que un 10'8% de todas las webs que usan algún CMS, usa JOOMLA, porcentaje muy superior al 6'3% de Drupal, el tercero en este ránking. (W3Techs,2018).

	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

En todos los artículos anteriores se coincide en afirmar la necesidad de un único usuario para inicio de sesión (single sign on) donde se ven diversas formas y entornos de aplicación, sin embargo, cada investigación se enfoca en un uso y aplicación específica, pero ninguno analiza la eficiencia, seguridad y rendimiento de los protocolos SAML y OAUTH y tampoco realizan una comparación entre los dos protocolos en las plataformas web JOOMLA y MOODLE. El planteamiento anterior permite deducir que el presente proyecto de investigación es viable y pertinente en el área de las comunicaciones vía web.

Hablando de confidencialidad podemos argumentar que al tener sus propios sistemas de cifrado para las claves de sus usuarios usando metadatos y certificados de seguridad y teniendo un sistema de encriptación, los dos protocolos son considerados confiables, como vulnerabilidad cabe resaltar que para el protocolo OAUTH el uso inadecuado del parámetro *“redirec_uri”* en su configuración puede ser causa de pérdidas de información, caso que ya se ha evidenciado en enunciados de empresas de seguridad que han documentado la experiencia según un informe publicado en junio de 2017 por la TCS Cyber Security Community <https://securitycommunity.tcs.com/infosecsoapbox/articles/2017/06/07/covert-redirect-vulnerability>

Para total comprensión del proyecto se hace necesario también incorporar la definición de los protocolos SAML y OAUTH; según la revista online CIOPerú(2009), el protocolo Security Assertion Markup Language (SAML), fue desarrollado por el comité Security Services Technical Committee of the Organization for the Advancement of Structured Information Estándar (OASIS) y especifica un esquema basado en XML para intercambiar información sobre autenticación y autorización de sujetos (Subjects) entre diferentes dominios seguros, específicamente entre un proveedor de identidad quien es quien produce la información de autenticación y un proveedor de servicios quien es quien consume dicha información (...) El Lenguaje de marcado para confirmaciones de seguridad (SAML, por sus siglas en inglés)

	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

es un estándar abierto que permite que las credenciales de seguridad sean compartidas por múltiples computadoras a través de una red. Describe un marco que permite que una computadora realice algunas funciones de seguridad en nombre de otra o más computadoras:

- Autenticación: Determinar que los usuarios son quienes dicen ser
- Autorización: Determinar si los usuarios tienen derecho a acceder a ciertos sistemas o contenidos.

En sentido estricto, SAML se refiere al lenguaje variante de XML utilizado para codificar toda esta información, pero el término también puede abarcar varios mensajes y perfiles de protocolo que forman parte del estándar. (párr.1)

Respecto al funcionamiento de SAML en la siguiente “imagen de alto nivel se muestra cómo se lleva a cabo un transacción de autenticación SAML, en la cual el agente usuario sería un navegador WEB (CIO,2017,párr. 6).

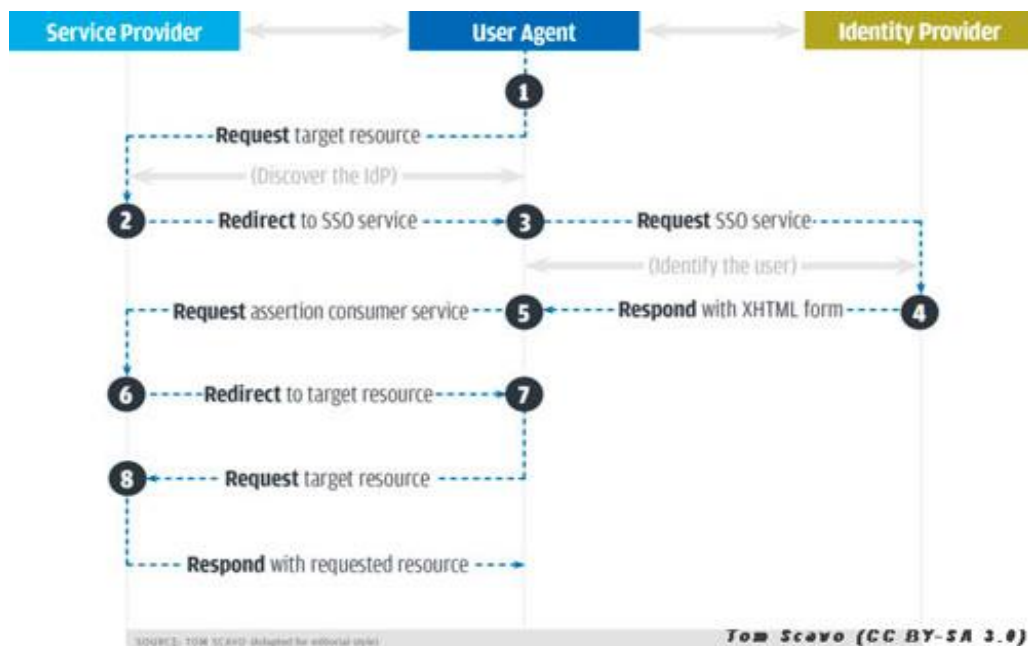


Ilustración 1. Secuencia de autenticación SAML

	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

Acerca del protocolo OAUTH, se retoma lo planteado por Grimes(2017), quien menciona que OAUTH es un marco de trabajo o protocolo de autorización de estándar abierto que describe cómo los servicios y servidores no relacionados pueden permitir un acceso autenticado de manera segura a sus activos, sin compartir la credencial inicial única de registro. En el lenguaje de la autenticación, esto se conoce como delegación autorizada externa de usuario-agente (...) su funcionamiento casi siempre implica a dos servicios o sitios web que intentan lograr algo en representación de los usuarios o su software. Los tres tienen que trabajar juntos, involucrando muchas aprobaciones para la transacción completada para conseguir autorización.

También es útil recordar que OAUTH se trata de autorización en particular, y no de autenticación directamente. La autenticación es un proceso donde un usuario/sujeto está demostrando que es dueño de una identidad presentada proporcionando una contraseña u otro factor presentado o de propiedad individual. La autorización es el proceso de permitir que un sujeto acceda a recursos después de una autenticación exitosa, muchas veces en otro lugar. Muchas personas piensan que OAUTH significa autenticación abierta, pero es más útil entender a OAUTH pensando en esta como una AUTHorization abierta. (párr.2)

“Un implementador temprano describe a OAUTH como la llave (...) permite al usuario -a través de un proveedor de autenticación con el que previamente se han autenticado exitosamente- conceder a otra página web/servicio un *token* de autenticación de acceso para la autorización hacia recursos adicionales”. (Grimes,2017,párr.9).

El protocolo básicamente funciona así: a. El usuario dispone de una serie de recursos propios en un servidor (el “proveedor”). b. Un servidor externo (el “consumidor”) desea acceder a un subconjunto de esos recursos. c. El consumidor redirige al usuario hacia el proveedor. d. El usuario se autentica en el proveedor (si no lo estaba previamente). El proveedor pregunta al usuario si autoriza al consumidor a que utilice esos determinados

recursos. f. El usuario autoriza al consumidor a utilizar esos recursos. g. El servidor externo (consumidor) consigue acceso a esos recursos. En la siguiente imagen se ilustra el funcionamiento descrito del protocolo OAUTH:

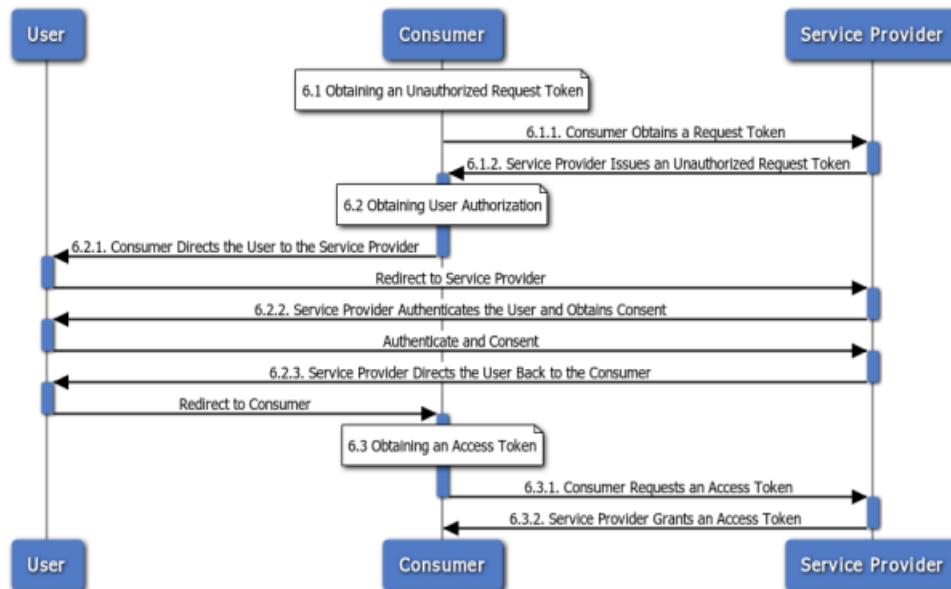


Ilustración 2. Secuencia de funcionamiento OAUTH.

	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

3. METODOLOGÍA

Para el desarrollo del presente proyecto el primer proceso llevado a cabo es la documentación, en donde se tienen en cuenta diversas fuentes científicas como investigaciones, artículos de revista, entre otras fuentes, como base para dar validez al trabajo; además de aportar conocimientos sobre los desarrollos actuales que se han implementado en el tema Single Sign On.

Todo proyecto de ingeniería tiene unos fines ligados a la obtención de un producto, proceso o servicio que es necesario generar a través de diversas actividades. Algunas de estas actividades pueden agruparse en fases porque globalmente contribuyen a obtener un producto intermedio, necesario para continuar hacia el producto final y facilitar la gestión del proyecto. Al conjunto de las fases empleadas se le denomina “ciclo de vida”. Tomado de http://www.spw.cl/proyectos/apuntes2/cap_6.htm (Agosto 26 de 2018).

Es por ello que el desarrollo de este proyecto se lleva a cabo a partir de un modelo experimental que permite comparar la seguridad y el rendimiento de los protocolos SAML y OAUTH; para ello se implementa el modelo lineal secuencial conocido también como modelo de vida básico o de cascada, el cual se desarrolla a través de un enfoque sistemático o secuencial que abarcará los siguientes pasos: Documentación, análisis, implementación, pruebas y finalmente la validación de resultados.

El análisis de los resultados se realiza bajo criterios tanto cualitativos como cuantitativos; los aspectos cuantificables son medidos por medio de la representación gráfica de barras, que según la Universidad Autónoma de México (2016) es entendida como la representación visual de datos, utilizando rectángulos horizontales o verticales, cuyas longitudes son proporcionales a las cantidades que representan (...) éstas son utilizadas para datos cualitativos o categóricos o para describir variables cuantitativas discretas que toman pocos

	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

valores. En dichas gráficas se comparan criterios tales como: seguridad, compatibilidad y rendimiento. La observación cualitativa se realiza mediante la descripción de la experiencia en el trabajo realizado teniendo en cuenta el comportamiento de los sistemas hardware-software y su configuración.

Como criterios a valorar de los protocolos SAML y OAUTH se seleccionaron los siguientes: en la Seguridad, la Confidencialidad y la Secuencia básica de uso; teniendo en cuenta lo que plantea la investigación Information Technology Security Evaluation Criteria (ITSEC) – a Contribution to Vulnerability? (1992), donde se establecen diversos criterios de seguridad dentro de los cuales se encuentran los criterios objeto de análisis.

Para la Compatibilidad, entendiéndose según el Diccionario Enciclopédico Vox.1 (2009) como un concepto básico en el área de la informática que determina la capacidad de dos o más ordenadores para ejecutar idénticos programas o conectarse a los mismos periféricos, por tanto en dicho aspecto se determina como criterio de valoración la respuesta del entorno de instalación (servidor con todos sus aplicativos); es decir, el comportamiento del servidor y los recursos de la máquina en cuanto a la instalación de las diferentes aplicaciones.

Finalmente para el Rendimiento, el cual de acuerdo con Alegsa (2016) se entiende como la medida o cuantificación de la velocidad/resultado con que se realiza una tarea o proceso. En una computadora, su rendimiento no depende sólo del microprocesador como suele pensarse, sino de la suma de sus componentes como la memoria, el bus, los diversos dispositivos, etc. y sus softwares; se establece como criterio de valoración el Uso de memoria RAM y el uso de la CPU.

A continuación se especifican cada uno de los pasos mencionados que se desarrollan en el proyecto.

	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

3.1 Cronograma y Fases

CRONOGRAMA DE ACTIVIDADES			
FASE	NOMBRE	ACTIVIDADES	TIEMPO
1	Documentación	1. Documentación sobre JOOMLA, MOODLE, protocolos SAML, OAUTH y sistema single sign on	2 semanas
2	Análisis	2. Análisis de especificaciones y requerimientos de servidor y plataformas	3 semanas
3	Implementación	3. Instalación de plataformas JOOMLA y MOODLE con sus plugins, módulos o componentes 4. Implementación del proveedor de identidad en las plataformas JOOMLA y MOODLE 5. Configuración de los protocolos SAML y OAUTH en las anteriores plataformas	4 semanas
4	Pruebas	6. Ejercicios de autenticación con un solo usuario para probar eficiencia entre los protocolos a comparar (SAML y OAUTH)	1 semana
5	Validación de resultados	7. Documento final con los resultados hallados en las pruebas de comparación y conclusión sobre el protocolo más eficiente.	3 semanas

Tabla 1 – Cronograma de Actividades

	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

También se vincula el Diagrama de Gantt como herramienta que permite graficar la distribución de las fases que se llevarán a cabo en la ejecución del modelo experimental; como lo menciona OBS Bussines School (2018) “el diagrama de Gantt es una herramienta para planificar y programar tareas a lo largo de un período determinado. Gracias a una fácil y cómoda visualización de las acciones previstas, permite realizar el seguimiento y control del progreso de cada una de las etapas de un proyecto y, además, reproduce gráficamente las tareas, su duración y secuencia, además del calendario general del proyecto”.

DIAGRAMA DE GANTT: Fases de las actividades														
FASE	ACTIVIDAD	SEMANA												
		1	2	3	4	5	6	7	8	9	10	1 1	1 2	1 3
Documentación	1	x	x											
Análisis	2			x	x	x								
Implementación	3						x							
	4							x						
	5								x	x				
Pruebas	6										x			
Validación de resultados	7											x	x	x

Tabla 2. Fases de las actividades

3.2 Análisis de los Requerimientos

Para el desarrollo de este trabajo se vinculan opciones tecnológicas (servidores) ubicados en La empresa CREAME, Incubadora de empresas dedicada al apoyo en la creación de empresas y en la cual el estudiante Jorge Iván Atehortua hace parte como Coordinador del Área de Sistemas; al realizar el análisis de especificaciones y requerimientos de servidor y

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

plataformas utilizadas por Créame, se encuentra que la empresa cuenta con un servidor dedicado bajo el sistema operativo centos, 8gb de Ram, 2 procesadores Intel(R) Core(TM)2 Duo CPU E4600 @ 2.40GHz, 2 discos duros en Raid de 500Gb, cuenta con APACHE, WHM, CPANEL y todo lo necesario para ser compatible con las plataformas JOOMLA y MOODLE; también en el Instituto Tecnológico Metropolitano – ITM en sus salas de sistemas y a través de máquinas virtuales. Como recurso humano se vincula también el acompañamiento y asesoría del MSc Javier Mauricio Durán Vásquez Docente de la facultad de ingeniería del mencionado Instituto y el trabajo directo de los ingenieros en formación Jorge Iván Atehortua y Giovanni Alberto Gómez Yepes; contando así con la capacidad de implementar lo necesario y poder comparar la eficiencia de los protocolos SAML y OAUTH.

A continuación se reflejan las características del servidor y plataformas como el sistema operativo y los aplicativos utilizados en la empresa CREAME:

Sistema operativo:	Empresa Linux - • CENTOS 6.10 standard [server] • v74.0.6 , Incluye Whm (Web Host Mamanager) and CPANEL
Processor Information	Processor #1 Vendor GenuineIntel Name Intel(R) Core(TM)2 Duo CPU E4600 @ 2.40GHz Speed 2400.312 MHz Cache 2048 KB Processor #2 Vendor GenuineIntel Name Intel(R) Core(TM)2 Duo CPU E4600 @ 2.40GHz Speed 2400.312 MHz Cache 2048 KB
Memory Information	Memory: 8020512k/9437184k available (5396k kernel code, 1059472k absent, 357200k reserved, 7012k data, 1296k init)

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

Physical Disks	<pre> sd 0:0:0:0: [sda] 976773168 512-byte logical blocks: (500 GB/465 GiB) sd 0:0:0:0: [sda] 4096-byte physical blocks sd 0:0:0:0: [sda] Write Protect is off sd 0:0:0:0: [sda] Mode Sense: 00 3a 00 00 sd 0:0:0:0: [sda] Write cache: enabled, read cache: enabled, doesn't support DPO or FUA sd 1:0:0:0: [sdb] 976773168 512-byte logical blocks: (500 GB/465 GiB) sd 1:0:0:0: [sdb] 4096-byte physical blocks sd 1:0:0:0: [sdb] Write Protect is off sd 1:0:0:0: [sdb] Mode Sense: 00 3a 00 00 sd 1:0:0:0: [sdb] Write cache: enabled, read cache: enabled, doesn't support DPO or FUA sd 1:0:0:0: [sdb] Attached SCSI disk sd 0:0:0:0: [sda] Attached SCSI disk sd 0:0:0:0: Attached scsi generic sg0 type 0 sd 1:0:0:0: Attached scsi generic sg1 type 0 </pre>
-----------------------	--

Tabla 3. Características Servidores y Plataformas

3.3 Implementación

A continuación se detalla el procedimiento de instalación de las plataformas Joomla y Moodle y los métodos (plugin, módulos o componentes) buscando identificar aquellos compatibles apropiados para la implementación de los protocolos SAML y OAUTH, en el siguiente apartado se desarrolla con detalle del proceso de configuración

3.3.1 Instalación de Plataformas Administradoras de Contenido

El primer paso para la implementación es la instalación de las respectivas plataformas JOOMLA y MOODLE, para ello se procede a la descarga de paquetes de los sitios oficiales disponibles en los siguientes enlaces: <https://www.JOOMLA.org/> y <https://MOODLE.org>

	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

3.3.1.1 Instalación de JOOMLA para el protocolo SAML

El procedimiento para instalar la plataforma JOOMLA para el protocolo SAML requiere que los paquetes descargados en el paso anterior sean subidos al servidor hosting a través de CPANEL o en este caso la página queda instalada en la siguiente ruta a través del servicio FTP: Ruta: <http://67.205.67.219/~sso2017/JOOMLA>

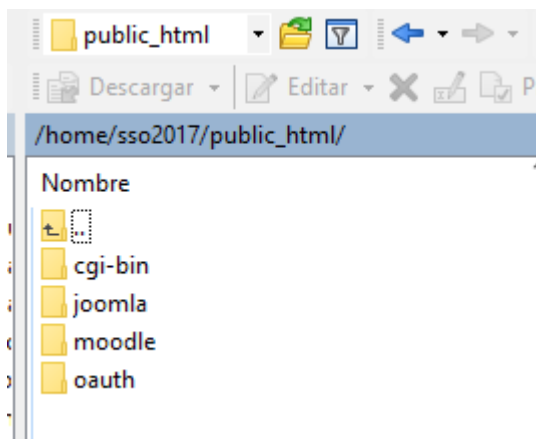


Ilustración 3- Archivos de la WEB en JOOMLA

Para continuar con el proceso se ingresa al CPANEL del servidor y se crea la base de datos y se procede a ejecutar el instalador vía web desde la Ruta: <http://67.205.67.219/~sso2017/JOOMLA>, apareciendo como se muestra a continuación

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

Bases de datos actuales



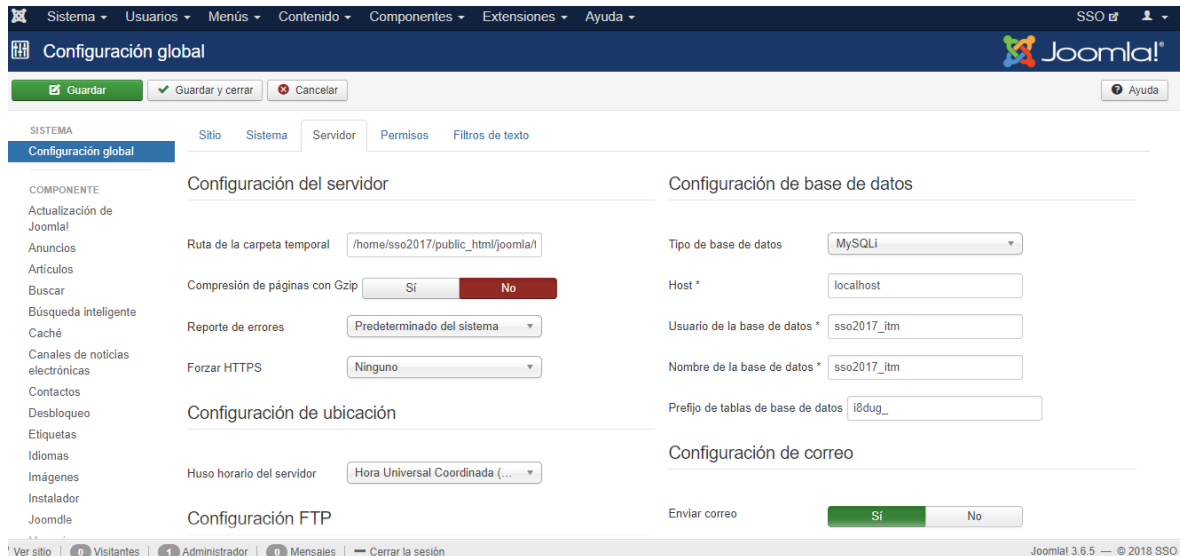
Base de datos	Tamaño	Usuarios con privilegio
sso2017_itm	3.77 MB	sso2017_itm 
sso2017_moodle	16.58 MB	sso2017_moodle 
sso2017_oauthjoomla	3.81 MB	sso2017_oauthjoo 
sso2017_oauthmoodle	9.55 MB	sso2017_oauthmoo 

Ilustración 4 – Listado base de datos

Después de la ejecución del instalador y la creación de la base de datos, se continúa indicando usuario y contraseña que será el administrador de la página, posteriormente el instalador lleva a la página de administración a través de la siguiente ruta: <http://67.205.67.219/~sso2017/JOOMLA/administrator>



The screenshot shows the Joomla! administrator interface for 'Configuración global'. The 'Servidor' tab is active, displaying server configuration options. The 'Configuración de base de datos' section is highlighted, showing the following settings:

- Tipo de base de datos: MySQL
- Host *: localhost
- Usuario de la base de datos *: sso2017_itm
- Nombre de la base de datos *: sso2017_itm
- Prefijo de tablas de base de datos: i8dug_

Other visible settings include: Ruta de la carpeta temporal (/home/sso2017/public_html/joomla/), Compresión de páginas con Gzip (No), Reporte de errores (Predeterminado del sistema), Forzar HTTPS (Ninguno), Huso horario del servidor (Hora Universal Coordinada), and Configuración de correo (Enviar correo: Si).

Ilustración 5: pagina del administrador de JOOMLA

	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

3.3.1.2 Instalación de MOODLE para el protocolo SAML

Para instalar la plataforma MOODLE, luego de la descarga de los paquetes de la página oficial <https://MOODLE.org> se procede a subir los datos en este caso por ftp al hosting empleado, tal como se presenta en la siguiente imagen:

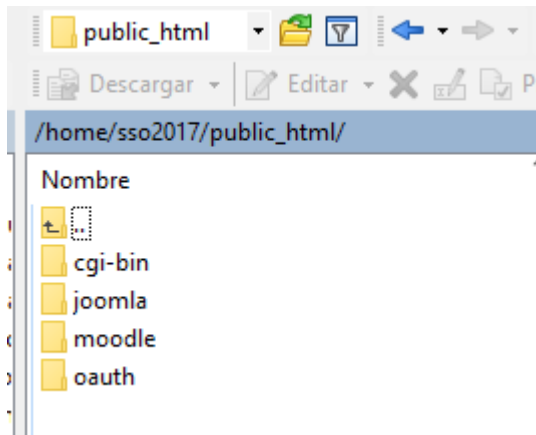


Ilustración 6 - Archivos de la WEB en MOODLE

Para dar continuidad al procedimiento se ingresa al panel de administración del hosting, se crea la base de datos y se procede a ejecutar el instalador de MOODLE vía web desde la Ruta: <http://67.205.67.219/~sso2017/MOODLE/>

	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

Bases de datos actuales

Base de datos	Tamaño
sso2017_itm	3.77 MB
sso2017_moodle	16.58 MB
sso2017_oauthjoomla	3.81 MB
sso2017_oauthmoodle	9.55 MB

Ilustración 7 – Base de datos para instalación de MOODLE

Siguiendo con el procedimiento el asistente de administración guía el proceso donde nos solicita los datos de la base de datos y el usuario y clave para ingresar al panel de administración de MOODLE, así:

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

SSO Español - Internacional (es) ▾

SSO

[Página Principal](#) ▶
[Administración del sitio](#) ▶
[Usuarios](#) ▶
[Cuentas](#) ▶
[Examinar lista de usuarios](#)

NAVEGACIÓN ☰ ☱

[Página Principal](#)

- [Área personal](#)
- ▶ [Páginas del sitio](#)
- ▶ [Mi perfil](#)
- ▶ [Cursos](#)

ADMINISTRACIÓN ☰ ☱

▶ [My profile settings](#)

▾ [Administración del sitio](#)

- ⚙ [Notificaciones](#)
- ⚙ [Registro](#)
- ⚙ [Características avanzadas](#)
- ▾ [Usuarios](#)
 - ▾ [Cuentas](#)
 - ⚙ [Examinar lista de usuarios](#)
 - ⚙ [Acciones de usuario masivas](#)

4 Usuarios

▾ Nuevo filtro

Nombre completo del usuario ▾

Añadir filtro

[Ver más...](#)

Nombre / Apellido(s)	Dirección de correo
giova1038@gmail.com	giova1038@gmail.com
Joomla Connector	joomla@donotdeletemeplease.com
JORGE ATEHORTUA	JORGYATE@GMAIL.COM
jorgyate@hotmail.com	jorgyate@hotmail.com

Agregar un usuario

Ilustración 8- Panel de Admon Plataforma MOODLE

3.3.1.3 Instalación de JOOMLA para el protocolo OAUTH

Para la implementación del protocolo OAUTH se procede con instalación de otra web en JOOMLA en otra carpeta del mismo servidor, quedando en la siguiente ruta:

<http://67.205.67.219/~sso2017/OAUTH/JOOMLA/>

Como paso a seguir se suben los datos por ftp al hosting anteriormente mencionado para proceder con su instalación, lo que se refleja en la siguiente ilustración:

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

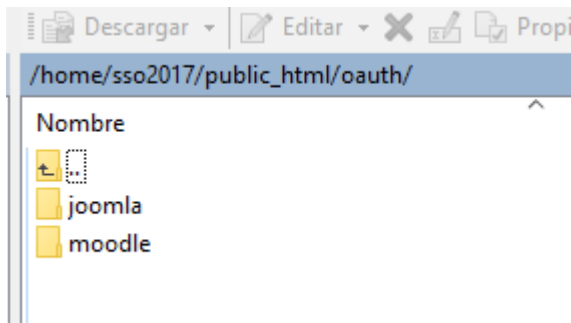


Ilustración 9 – Carpeta para Joomla en Protocolo OAUTH

Seguidamente se ingresa al panel de administración del hosting, se crea la base de datos y se procede a ejecutar el instalador vía web desde la Ruta:

<http://67.205.67.219/~sso2017/OAUTH/JOOMLA/>

Bases de datos actuales


Base de datos	Tamaño	Usuarios con privilegio
sso2017_itm	3.77 MB	sso2017_itm 
sso2017_moodle	16.58 MB	sso2017_moodle 
sso2017_oauthjoomla	3.81 MB	sso2017_oauthjoo 
sso2017_oauthmoodle	9.55 MB	sso2017_oauthmoo 

Ilustración 10 – Base de datos para JOOMLA en protocolo OAUTH

Como paso seguido el instalador hace de guía y pide los datos como nombre de la base de datos, usuario y contraseña para posteriormente ingresar al panel de administración en la siguiente ruta: <http://67.205.67.219/~sso2017/OAUTH/JOOMLA/administrator>

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

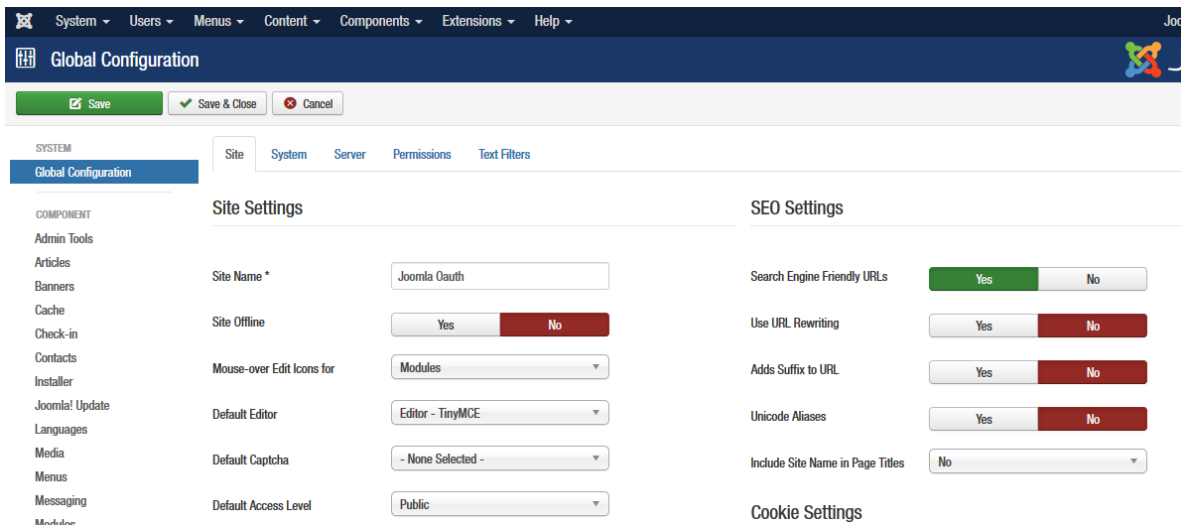


Ilustración 11 – Panel de Admon JOOMLA para OAUTH

3.3.1.4 Instalación de MOODLE para el protocolo OAUTH

En el procedimiento de la instalación de MOODLE para el protocolo OAUTH, se suben los los datos por ftp al hosting quedando con las indicaciones del asistente de instalación

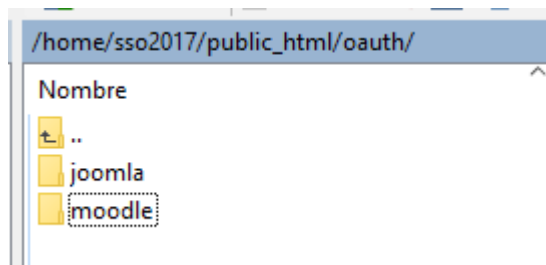


Ilustración 12 – Carpeta en el Hosting de MOODLE para OAUTH

De manera seguida se ingresa al panel de administración del hosting, se crea la base de datos y se procede a ejecutar el instalador vía web desde la Ruta: <http://67.205.67.219/~sso2017/OAUTH/MOODLE>

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

Bases de datos actuales

Buscar

Base de datos	Tamaño	Usuarios con privilegio
sso2017_itm	3.77 MB	sso2017_itm 
sso2017_moodle	16.58 MB	sso2017_moodle 
sso2017_oauthjoomla	3.81 MB	sso2017_oauthjoo 
sso2017_oauthmoodle	9.55 MB	sso2017_oauthmoo 

Ilustración 13 – Base de datos para MOODLE en OAUTH

Continuando, se ejecuta el instalador el cual pide información como nombre de la base de datos, usuario y contraseña para posteriormente ingresar al panel de administración en la siguiente ruta:
<http://67.205.67.219/~sso2017/OAUTH/MOODLE>



Ilustración 14 – Administrador de MOODLE para OAUTH

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

3.3.2 Instalación de Plugins

En el proceso de selección de los plugins, módulos y componentes se instalaron para pruebas un total de 9 aplicativos así: para JOOMLA – OAUTH, 3 plugins y 1 componente; JOOMLA – SAML, 2 plugins y 1 componente, en MOODLE - OAUTH, 1 modulo y para MOODLE SAML, 1 modulo. Luego de las instalaciones se lograron determinar 4 aplicativos configurables para la realización del trabajo siendo descartados los demás.

3.3.2.1 Instalación de Plugins en JOOMLA para SAML

Luego de instalar el gestor de contenidos JOOMLA se ingresa al área de administración antes mencionada, se procede a entrar por el menú extensiones y allí se realiza la instalación del componente miniorange-SAML-sso-for-JOOMLA, este paquete se puede descargar desde la siguiente ruta: <https://extensions.JOOMLA.org/extension/miniorange-sso-for-JOOMLA/>

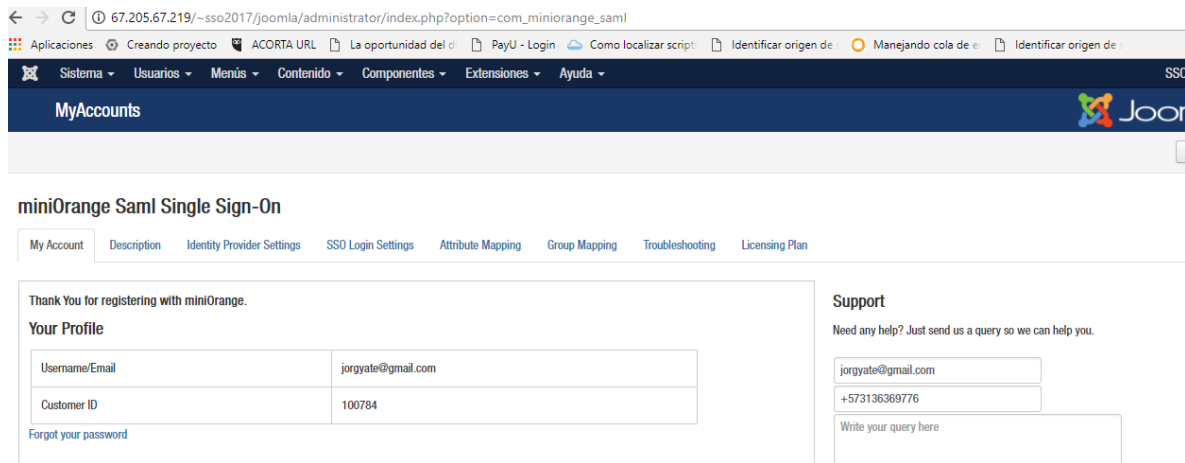
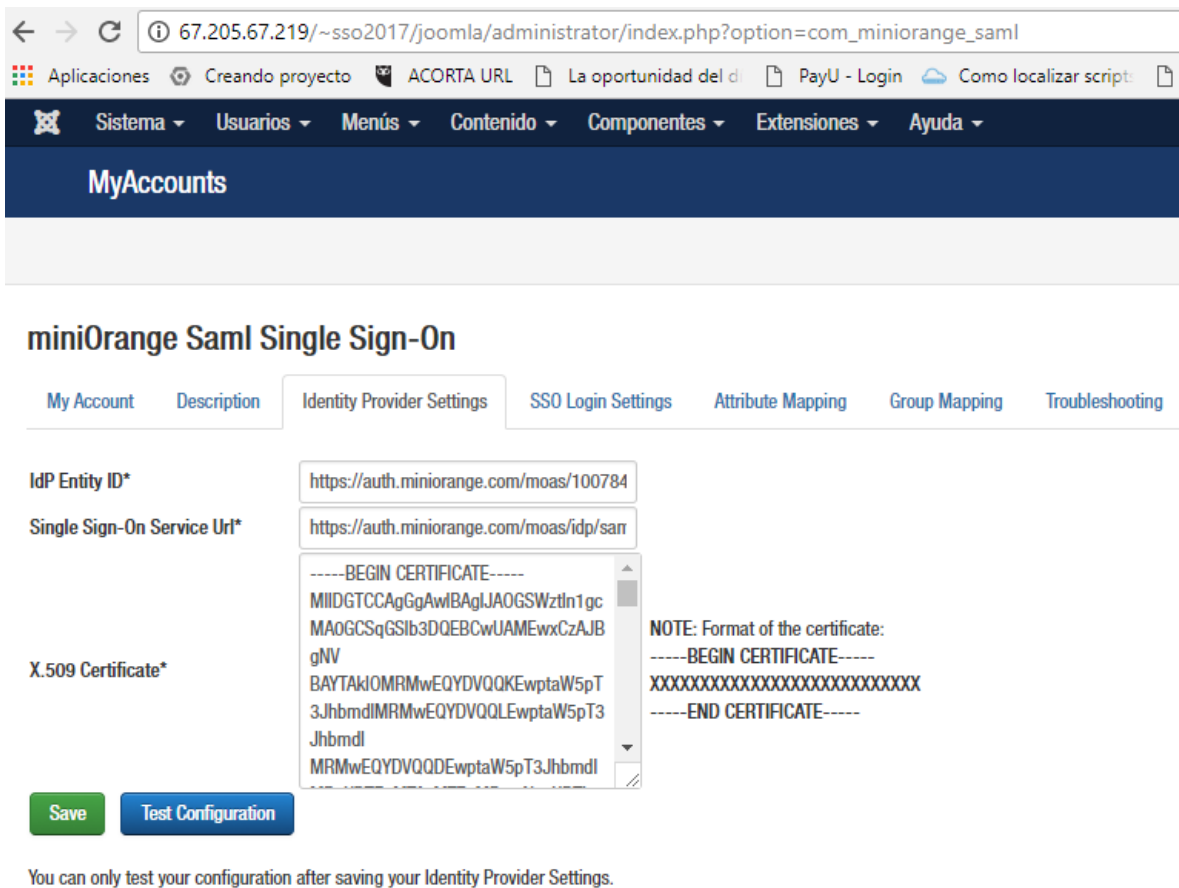


Ilustración 15 – Instalación del componente miniorange-SAML

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22



miniOrange SAML Single Sign-On

My Account Description Identity Provider Settings SSO Login Settings Attribute Mapping Group Mapping Troubleshooting

IdP Entity ID*

Single Sign-On Service Url*

X.509 Certificate*

```
-----BEGIN CERTIFICATE-----
MIIDGTCCAqGgAwIBAgIJAOGSWztIn1gc
MAOGCSqGSIb3DQEBCwUAMEwxCzAJB
gNV
BAYTAKlOMRMwEQYDVQQKEwptaW5pT
3JhbmdlMRMwEQYDVQQLwptaW5pT3J
hbmdl
MRMwEQYDVQQLwptaW5pT3Jhbmdl
```


NOTE: Format of the certificate:
-----BEGIN CERTIFICATE-----
XXXXXXXXXXXXXXXXXXXXXXXXXXXX
-----END CERTIFICATE-----

You can only test your configuration after saving your Identity Provider Settings.

Ilustración 16 – Configuración del componente miniorange-SAML

3.3.2.2 Instalación del plugin en MOODLE para SAML

Después de instalar el gestor de contenidos MOODLE se procede a ingresar a su área de administración seguido de la opción extensiones, instalación de módulos externos para continuar con la instalación del módulo Auth Mod SAML, este paquete se puede descargar desde la siguiente ruta: https://MOODLE.org/plugins/auth_SAML

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

67.205.67.219/.../moodle/admin/tool/installaddon/validate.php?sesskey=1JAeGYE6qm&jobid=cb43d67f5022e98e1fc079d526ec898d&zip=mo_saml.zip&type=auth&rootdir

Factura Actual Creando proyecto ACORTA URL La oportunidad del cl PayU - Login Como localizar script Identificar origen de Manejando cola de Identificar origen de

Español - Internacional (es) JORGE ATEHORTUA

Principal > Administración del sitio > Extensiones > Instalar módulos externos Activar la edición de bloques

Validación del paquete de módulo externo

¡Requisitos válidos!

Estado	Mensaje	Info
OK	Nombre del módulo externo que se debe instalar	mo_saml
OK	Versión del módulo externo	2017013101
OK	Versión de Moodle requerida	2014111000
OK	Nombre completo del componente	auth_mo_saml

Ilustración 17: validación de requisitos previos a la instalación

Comprobación de 'plugins'

Esta página muestra las extensiones (plugins) que pueden requerir su atención durante la actualización. Los elementos resaltados incluyen nuevas extensiones (plugins) que están a punto de ser instalados, los que van a ser actualizados y las extensiones anteriores que ahora faltan. Los módulos externos (add-ons) también se destacan. Se recomienda que compruebe si hay versiones más recientes de los módulos externos disponibles y actualice su código fuente antes de continuar con esta actualización de Moodle.

[Compruebe actualizaciones disponibles](#)

Número de extensiones (plugins) que requieren atención durante esta actualización: 1

[Mostrar la lista completa de extensiones \(plugins\) instalados](#)

Nombre de la extensión	Directorio	Origen	Versión actual	Nueva versión	Requiere	Estado
Extensiones de identificación						
miniOrange SAML 2.0 SSO	/auth/mo_saml	Adicional		2017013101	Moodle 2014111000	Para instalarse

[Recargar](#)

[Actualizar base de datos Moodle ahora](#)

Ilustración 18: comprobación, instalación del plugin mini Orange SAML

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

Actualizando la versión

auth_mo_saml

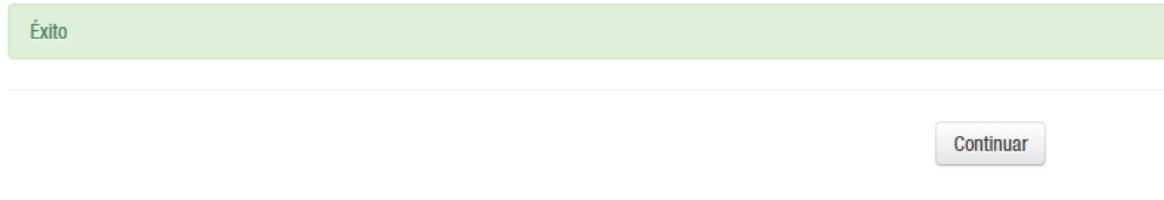
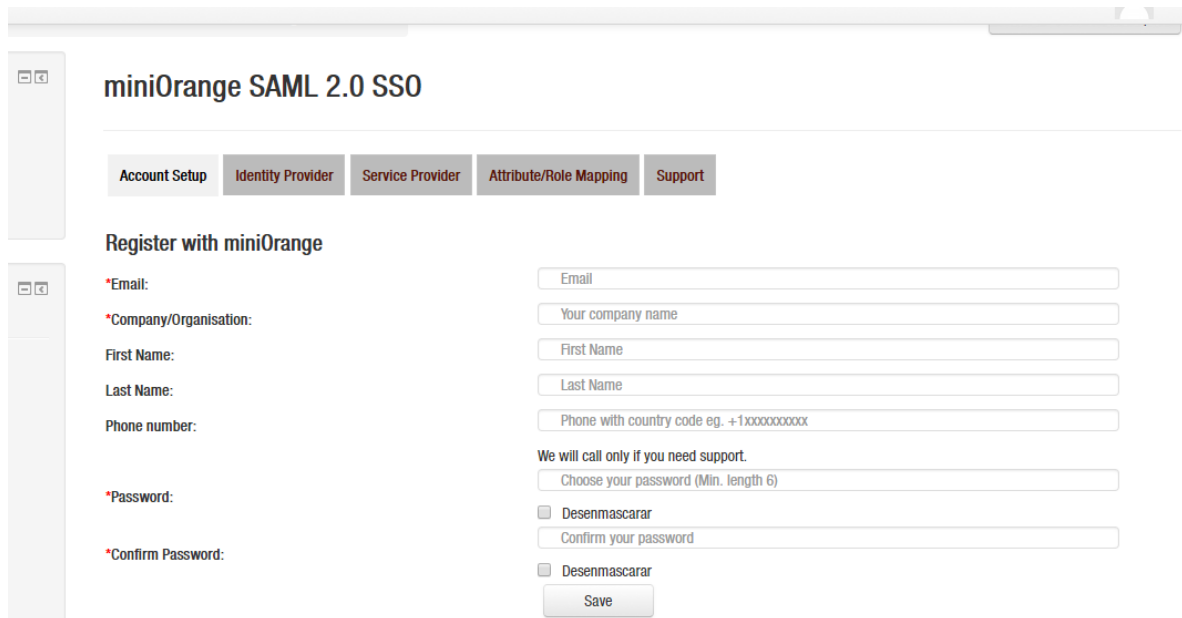


Ilustración 19: Actualización de la versión del plugin mini Orange SAML

Se continua con la configuración del plugin con los parámetros del IDP (proveedor de identidad) mini Orange.



miniOrange SAML 2.0 SSO

Account Setup | **Identity Provider** | Service Provider | Attribute/Role Mapping | Support

Register with miniOrange

*Email:

*Company/Organisation:

First Name:

Last Name:

Phone number:

We will call only if you need support.

Choose your password (Min. length 6)

Desenmascarar

Confirm your password

Desenmascarar

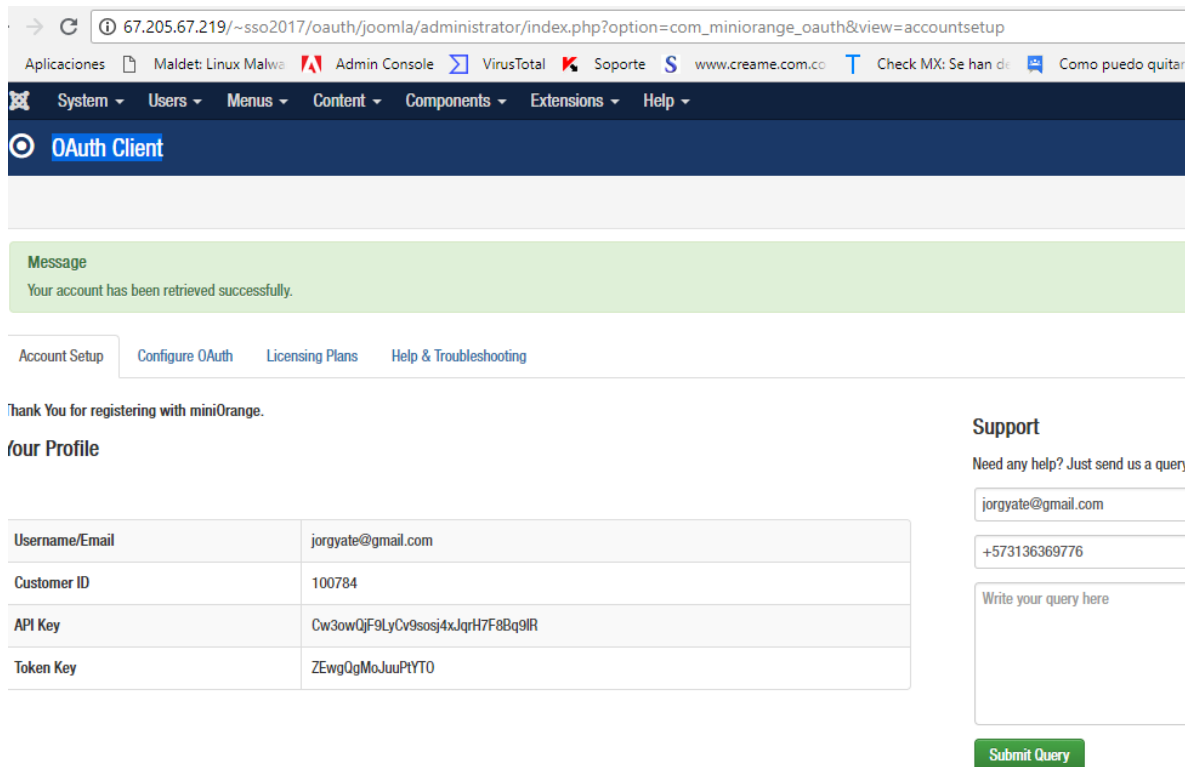
Ilustración 20: Actualización de la versión del plugin mini Orange SAML

	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

3.3.2.3 Instalación de Plugins en JOOMLA para OAUTH

Luego de la instalación del gestor de contenidos JOOMLA se ingresa a su área de administración, se procede por el menú superior extensiones y allí se realiza la instalación del componente OAUTH Client, este paquete se puede descargar desde la siguiente ruta:

<https://extensions.JOOMLA.org/extension/miniorange-OAUTH-client/>



Message
Your account has been retrieved successfully.

Account Setup | Configure OAuth | Licensing Plans | Help & Troubleshooting

Thank You for registering with miniOrange.

Your Profile

Username/Email	jorgyate@gmail.com
Customer ID	100784
API Key	Cw3owQjF9LyCv9sosj4xJqrH7F8Bq9lR
Token Key	ZEwgUgMoJuuPYT0

Support
Need any help? Just send us a query

jorgyate@gmail.com

+573136369776

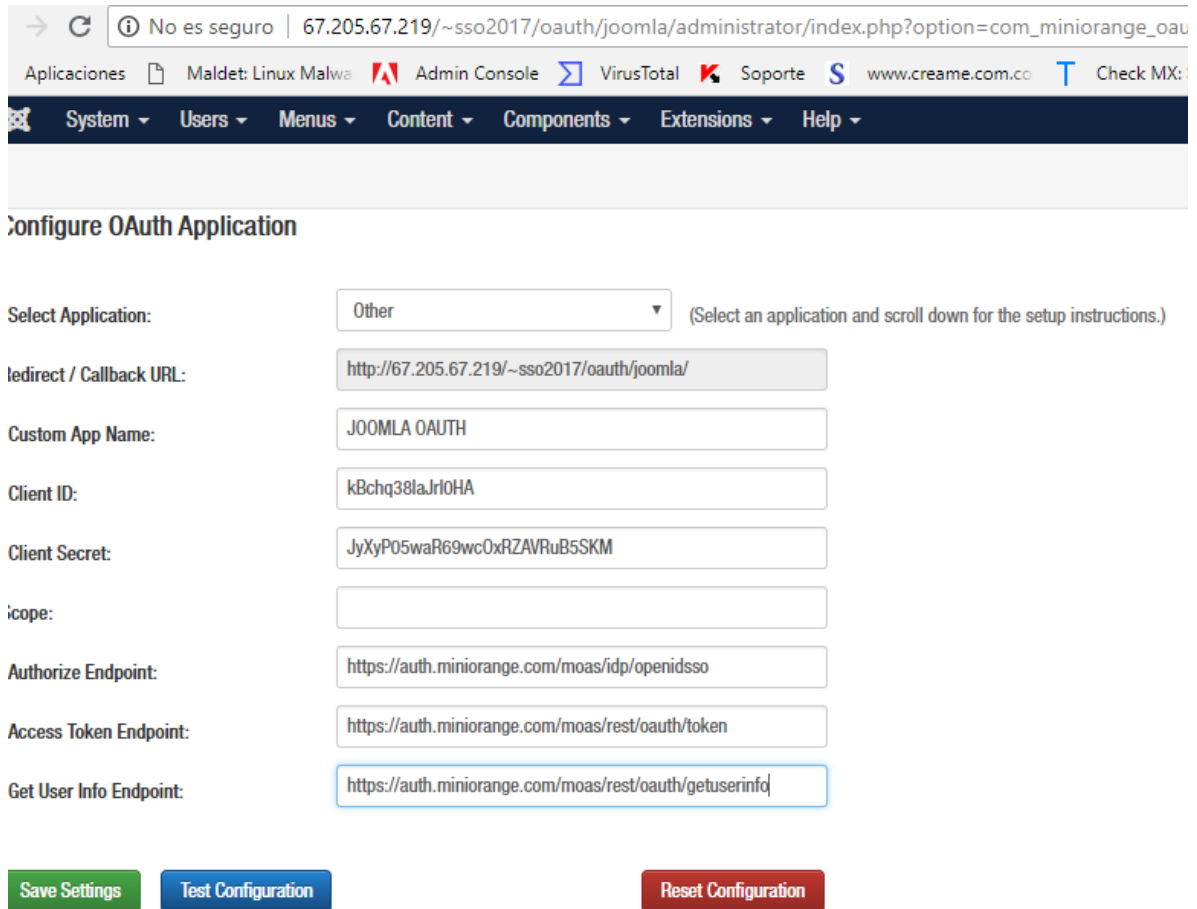
Write your query here

Submit Query

Ilustración 21: instalación del componente mini Orange OAUTH Client

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

Paso seguido se procede con la configuración del componente de acuerdo con los parámetros del IDP mini Orange que permiten las conexiones necesarias.



Configure OAuth Application

Select Application: (Select an application and scroll down for the setup instructions.)

Redirect / Callback URL:

Custom App Name:

Client ID:

Client Secret:

Scope:

Authorize Endpoint:

Access Token Endpoint:

Get User Info Endpoint:

Ilustración 22: Configuración del componente mini Orange OAUTH Client

Si siguiendo con el proceso se continúa con el registro del plugin con los datos generados por el IDP

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

Message

Attribute Mapping saved successfully.

[Account Setup](#)

[Configure OAuth](#)

[Licensing Plans](#)

[Help & Troubleshooting](#)

Thank You for registering with miniOrange.

Your Profile

Username/Email	jorgyate@gmail.com
Customer ID	100784
API Key	Cw3owQjF9LyCv9sosj4xJqrH7F8Bq9lR
Token Key	ZEwgQgMoJuuPtYTO

Ilustración 23: Sincronización de la cuenta con datos de acceso a mini Orange

3.3.2.4 Instalación de Plugins en MOODLE para OAUTH

Luego de la instalación del gestor de contenidos MOODLE, se procede con la instalación del módulo para el protocolo OAUTH en MOODLE, para ello se ingresa por el área de administración en la opción Servidor- Servicios de OAUTH2 y se procede a instalar y configurar el servicio de autenticación OAUTH

	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

Servicios OAuth 2

[Área personal](#) / [Administración del sitio](#) / [Servidor](#) / [Servicios OAuth 2](#) / Edit identity issuer: jorge

Edit identity issuer: jorge

i Instrucciones detalladas sobre la configuración de los servicios comunes de OAuth 2

Name	! ?	jorge
Client ID	! ?	8Zft57HvDN9IASc
Client secret	! ?	P8umD-4hj3rOA5zoW_M
Scopes included in a login request.	! ?	jorgyate@gmail.com
Scopes included in a login request for offline access.	! ?	jorgyate@gmail.com

Ilustración 24: Creación del servicio de autenticación

3.3.3 Implementación Proveedor de Identidad

El proveedor de identidad utilizado para este trabajo proviene de la empresa MINIORANGE quien permitió utilizar su tecnología como IDP.

Se procede a realizar el registro de los usuarios que utilizarán en la implementación del presente trabajo en la página web <https://www.miniorange.com/>

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

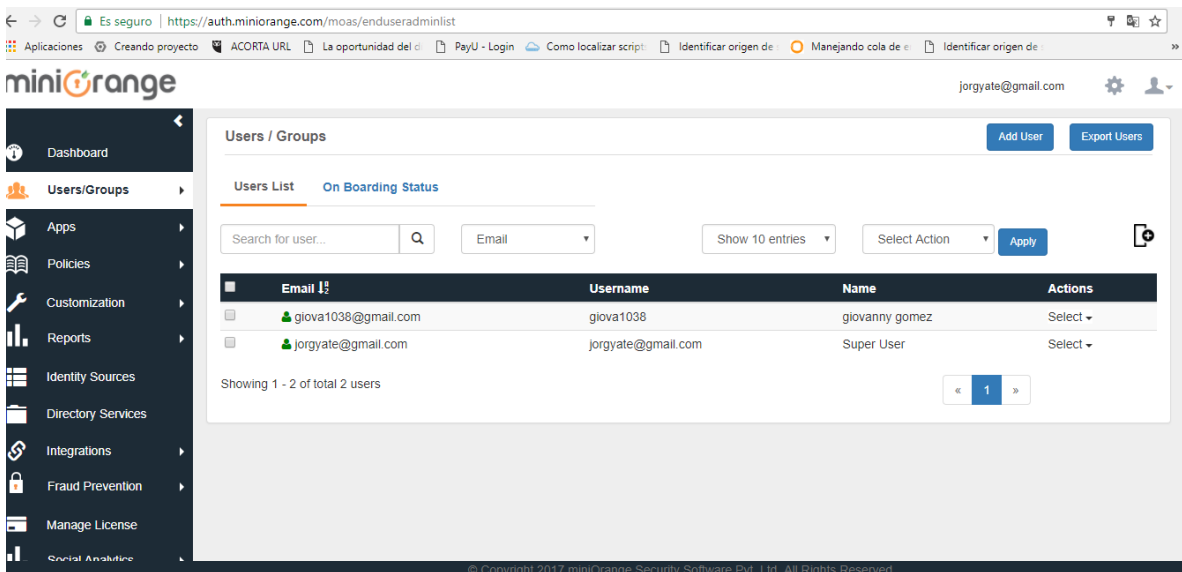


Ilustración 25: Registro en la plataforma mini Orange como proveedor de Identidad

En el menú izquierdo apps – en la opción manage apps se crean las aplicaciones por cada gestor instalado, (en total son 4 apps), se crea un enlace por cada protocolo y cada plataforma web a utilizar; en la siguiente ilustración se ejemplifica el Protocolo SAML para JOOMLA

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22


APPS / ADD APPLICATION Back to M


[SAML](#)
[OAuth/OIDC](#)
[External/JWT/PwdLess](#)
[WS-Fed](#)
[Radius](#)
[Browser Add-On/Form Post](#)
[Social Login](#)

[ALL](#)
[0-9](#)
[A](#)
[B](#)
[C](#)
[D](#)
[E](#)
[F](#)
[G](#)
[H](#)
[I](#)
[J](#)
[K](#)
[L](#)
[M](#)
[N](#)
[O](#)
[P](#)
[Q](#)
[R](#)
[S](#)
[T](#)
[U](#)
[V](#)

[W](#)
[X](#)
[Y](#)
[Z](#)

Add App


 Jira (SAML)


 Jitbit



 Joomla (SAML)

Ilustración 26: Creación de app para conexión de JOOMLA con el protocolo SAML

miniOrange Settings jorgyate@gmail.com

- Dashboard
- Configure
- Identity Providers
- User Stores
- Apps
- Policies
- Customization
- 2-Factor Authentication
- Adaptive Authentication
- Manage
- Users
- Groups
- Reports

VIEW APPS Configure Apps

[ALL](#)
[0-9](#)
[A](#)
[B](#)
[C](#)
[D](#)
[E](#)
[F](#)
[G](#)
[H](#)
[I](#)
[J](#)
[K](#)
[L](#)
[M](#)
[N](#)
[O](#)
[P](#)
[Q](#)
[R](#)
[S](#)
[T](#)
[U](#)
[V](#)
[W](#)
[X](#)

[Y](#)
[Z](#)

Show All entries Search Apps

Application	Provider Name	Group Name	App Type	Account Type	Id	Action
Default API App	api	N/A	API	Individual Account	87430	Edit Delete
joomla	joomla_saml	N/A	SAML	Individual Account	87683	Edit Metadata Delete Link
JOOMLA OAUTH	OpenId Connect	N/A	OpenID	Individual Account	130371	Edit Certificate Delete
moodle	moodle_saml	N/A	SAML	Individual Account	89820	Edit Metadata Delete Link
moodle oauth	OpenId Connect	N/A	OpenID	Individual Account	129284	Edit Certificate Delete

Showing 1 to 5 of 5 entries First Previous **1** Next Last

Ilustración 27: Listado de las 4 aplicaciones para cada gestor de contenido

	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

Se toma nota de la información generada por el IDP en cada aplicación para poder llevar los datos a los componentes directamente en los gestores de contenido JOOMLA Y MOODLE

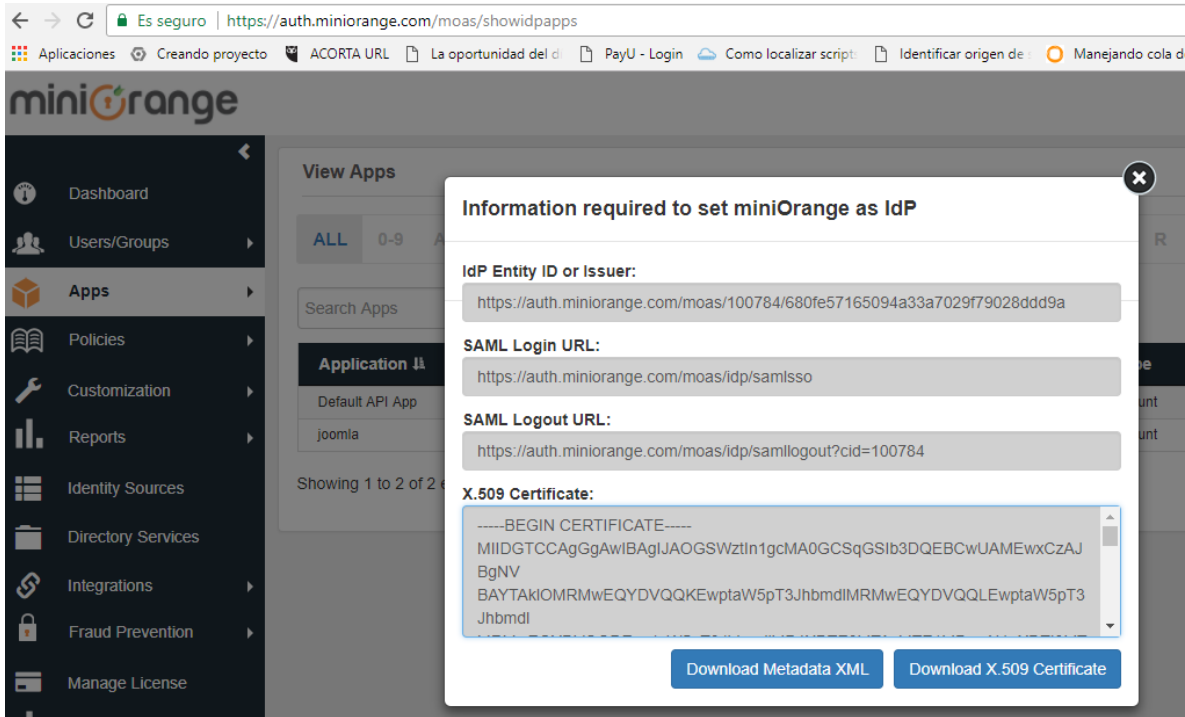


Ilustración 28: configuración de la app y datos para configurar los gestores de contenido

Se procede a realizar una política de seguridad requerida para el control de la autenticación y para generar el enlace confiable entre aplicativos. La política se crea a través del menú izquierdo Políticas - add policy.

Por cada protocolo en cada gestor de contenido se crea una política, para un total de 4 políticas.

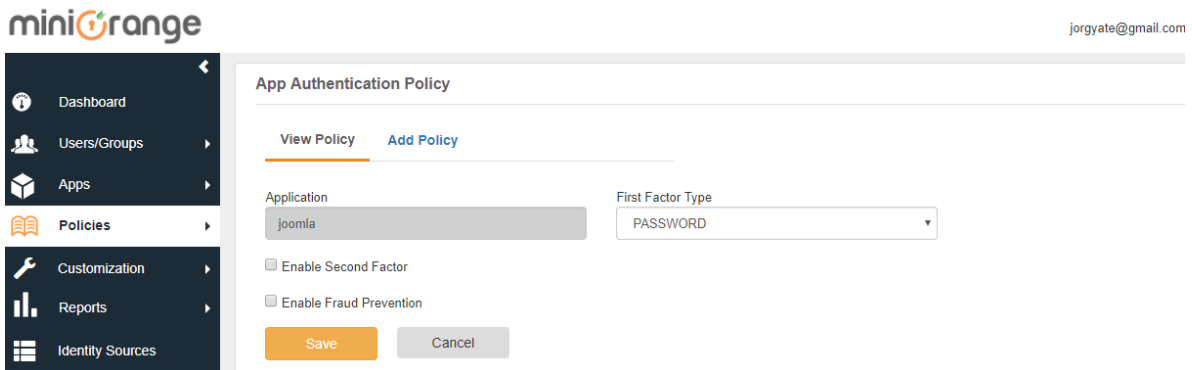


Ilustración 29: Creación de una política de seguridad

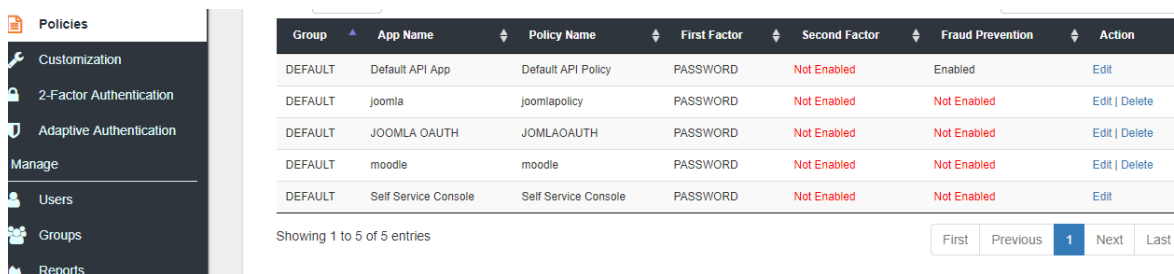


Ilustración 30: Listado de políticas para uso de las aplicaciones

A continuación se muestra como quedan las configuraciones en general por parte del IDP y los gestores de contenidos, como ejemplo se toma la configuración del IDP para JOOMLA en protocolo SAML

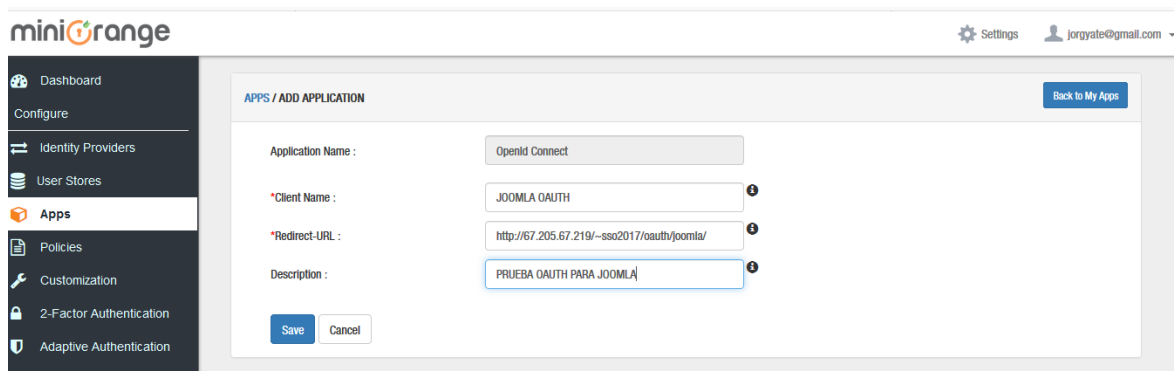
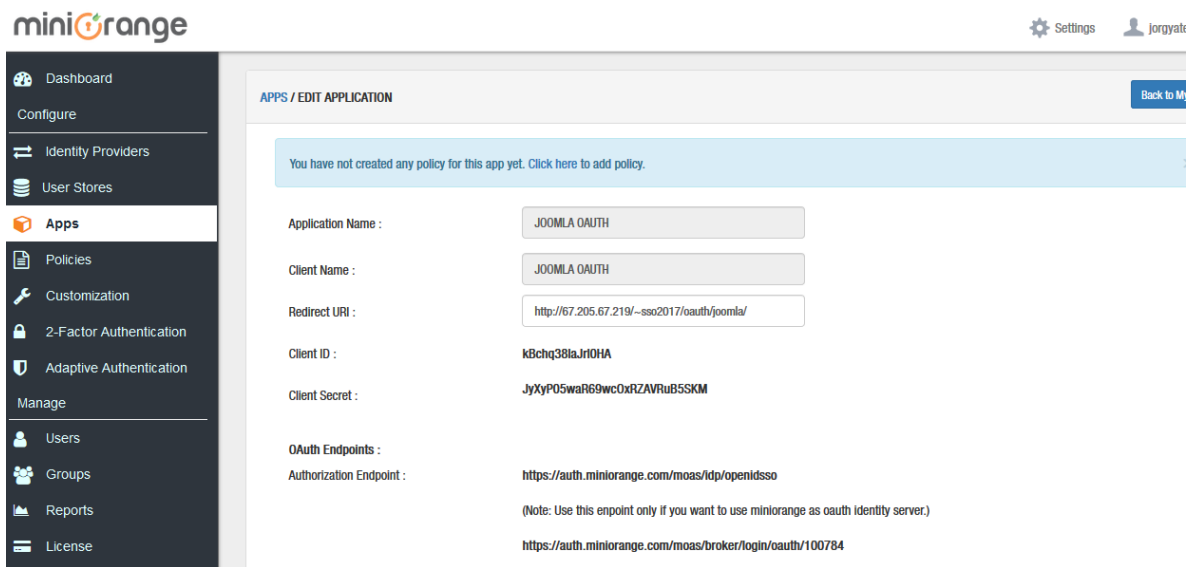


Ilustración 31: creación la app del IDP para JOOMLA en SAML

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22



miniOrange Settings jorgyate

APPS / EDIT APPLICATION [Back to M](#)

You have not created any policy for this app yet. [Click here to add policy.](#)

Application Name : JOOMLA OAUTH

Client Name : JOOMLA OAUTH

Redirect URI : http://67.205.67.219/~sso2017/oauth/joomla/

Client ID : kBChq38laJr10HA

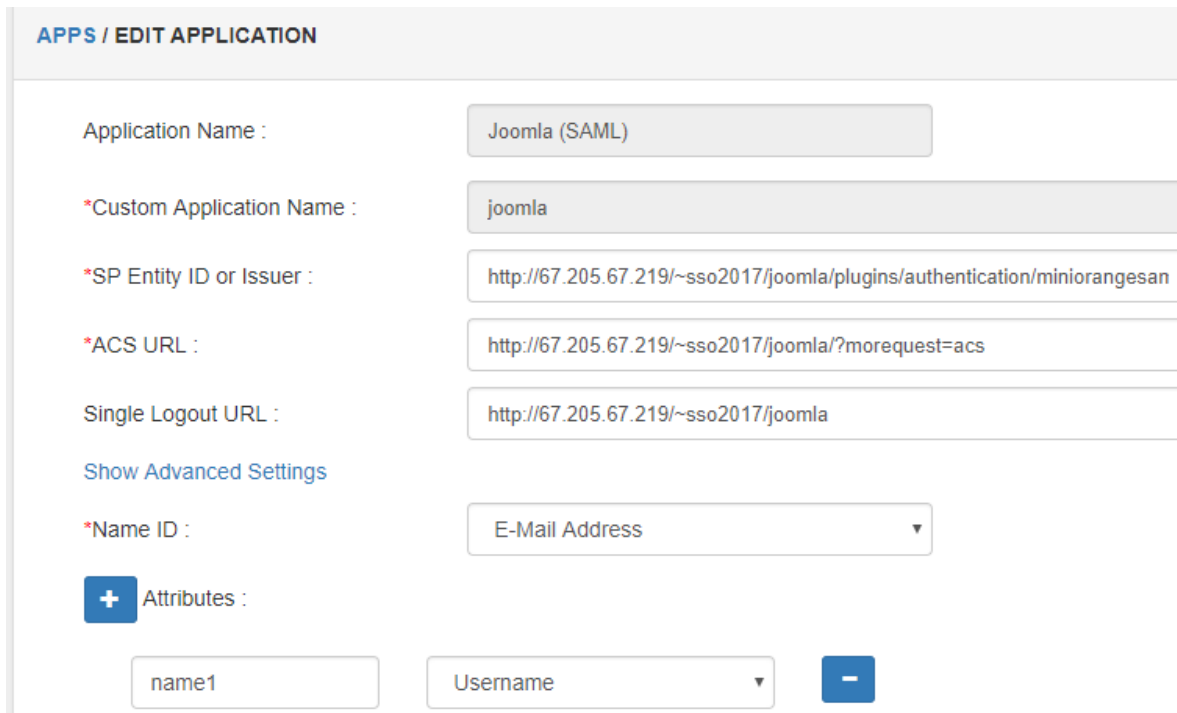
Client Secret : JyXyP05waR69wcOxrZAVRuB5SKM

OAuth Endpoints :

Authorization Endpoint : https://auth.miniorange.com/moas/ldp/openidssso
(Note: Use this endpoint only if you want to use miniorange as oauth identity server.)
https://auth.miniorange.com/moas/broker/login/oauth/100784

Ilustración 32: configuración de la app del IDP para JOOMLA en SAML

LA siguiente ilustración se evidencian los parámetros finales para la conexión de JOOMLA con el IDP en el protocolo SAML



APPS / EDIT APPLICATION

Application Name : Joomla (SAML)

*Custom Application Name : joomla

*SP Entity ID or Issuer : http://67.205.67.219/~sso2017/joomla/plugins/authentication/miniorangesan

*ACS URL : http://67.205.67.219/~sso2017/joomla/?morequest=acs

Single Logout URL : http://67.205.67.219/~sso2017/joomla

[Show Advanced Settings](#)

*Name ID : E-Mail Address

+ Attributes :

name1 Username -

Ilustración 33: parámetros de la app en el IDP para JOOMLA SAML

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

También se puede observar los parámetros de la app en el IDP para el protocolo SAML en la plataforma MOODLE

APPS / EDIT APPLICATION

Application Name :

*Custom Application Name :

*SP Entity ID or Issuer :

*ACS URL :

Single Logout URL :

[Show Advanced Settings](#)

*Name ID :

+ Attributes :

-

Ilustración 34: parámetros finales de la app en el IDP pára MOODLE SAML

Se procede a observar la configuración final de la app en el IDP para el protocolo OAUTH en la plataforma JOOMLA

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

APPS / EDIT APPLICATION

Application Name : JOOMLA OAUTH

Client Name : JOOMLA OAUTH

Redirect URI : <http://67.205.67.219/~sso2017/oauth/joomla/>

Client ID : **kBchq38laJrI0HA**

Client Secret : **JyXyP05waR69wcOxRZAVRuB5SKM**

OAuth Endpoints :

Authorization Endpoint : **<https://auth.miniorange.com/moas/idp/openidsso>**

(Note: Use this endpoint only if you want to use miniorange as oauth identity server.)

<https://auth.miniorange.com/moas/broker/login/oauth/100784>

(Note: Use this endpoint only if you are configuring any Identity Provider in Identity Provider miniorange as IDP.)

Ilustración 35: configuración en el IDP de la app para MOODLE con SAML

Luego se pasa a registrar la configuración en el IDP para el protocolo OAUTH en la plataforma MOODLE.

APPS / EDIT APPLICATION

Application Name : moodle oauth

Client Name : moodle oauth

Redirect URI : <http://67.205.67.219/~sso2017/oauth/moodle>

Client ID : **8Zft57HvDN9IA Sc**

Client Secret : **P8umD-4hj3rOA5zoW_M9Hnk4fDE**

OAuth Endpoints :

Authorization Endpoint : **<https://auth.miniorange.com/moas/idp/openidsso>**

(Note: Use this endpoint only if you want to use miniorange as oauth identity server.)

<https://auth.miniorange.com/moas/broker/login/oauth/100784>

Ilustración 36: configuración del protocolo OAUTH en la app del IDP para MOODLE

	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

Para el protocolo OAUTH en los dos aplicativos webs utilizados, la app genera un certificado de encriptación el cual debe ser vinculado tanto en JOOMLA como en MOODLE

JOOMLA OAUTH	OpenId Connect	N/A	OpenID	Individual Account	130371	Edit Certificate Delete
moodle	moodle_saml	N/A	SAML	Individual Account	89820	Edit Metadata Delete Link
moodle oauth	OpenId Connect	N/A	OpenID	Individual Account	129284	Edit Certificate Delete

Ilustración 37: aplicaciones para OAUTH y el enlace a la descarga d los certificados generados

3.4 Pruebas

Con los aplicativos ya instalados en los entornos JOOMLA y MOODLE se procede a realizar pruebas experimentales de conexión, autenticación con usuarios específicos y pruebas de acceso a las aplicaciones en los protocolos SAML y OAUTH, logrando determinar resultados para cada uno de los criterios establecidos en párrafos anteriores para la seguridad, la compatibilidad y el rendimiento; finalmente se realizan comparaciones de los resultados, logrando establecer un análisis con ventajas y desventajas de los protocolos SAML y OAUTH para un esquema de SINGLE SIGN ON entre las plataformas (CMS) JOOMLA y (LMS) MOODLE.

En este caso se utiliza el único usuario de acceso Jorgyate@gmail.com quien por medio del IDP otorga ingreso a las plataformas JOOMLA y MOODLE bajo las dos opciones de protocolo planteadas SAML y OAUT.

Realizando la prueba de configuración y conexión en JOOMLA para el protocolo SAML se encuentran resultados positivos, puesto que se realiza la conexión de manera exitosa

miniOrange SAML Single Sign-On

[My Account](#) | [Description](#) | [Identity Provider Settings](#) | [SSO Login Settings](#) | [Attribute Mapping](#) | [Group](#)

IdP Entity ID*
 Single Sign-On Service Url*
 X.509 Certificate*

```
-----BEGIN CERTIFICATE-----
MIIDGTCCAgGgAwIBAgIJAOGS
Wztln1gcMA0GCSqGSIb3DQEB
CwUAMEwxCzAJBgNV
BAYTakiOMRMwEQYDVQQKE
wptaW5pT3JhbmdlMRMwEQYD
VQQLewptaW5pT3Jhbmdl
MRMwEQYDVQQDEwptaW5pT
```


NOTE: Format of the certificate:
 -----BEGIN CERTIFICATE-----
 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
 -----END CERTIFICATE-----

You can only test your configuration after saving your Identity Provider Settings.

Ilustración 38: prueba de configuración JOOMLA para SAML

© 67.205.67.219/~sso2017/joomla/?morequest=acs

TEST SUCCESSFUL




Hello, jorgyate@gmail.com

ATTRIBUTES RECEIVED:

ATTRIBUTE NAME	ATTRIBUTE VALUE
name1	jorgyate@gmail.com
ASSERTION_NAME_ID	jorgyate@gmail.com

Ilustración 39: conexión establecida entre JOOMLA y al IDP mini Orange

Se procede con la prueba del protocolo SAML y su conexión entre MOODLE y el IDP, también con resultados satisfactorios

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

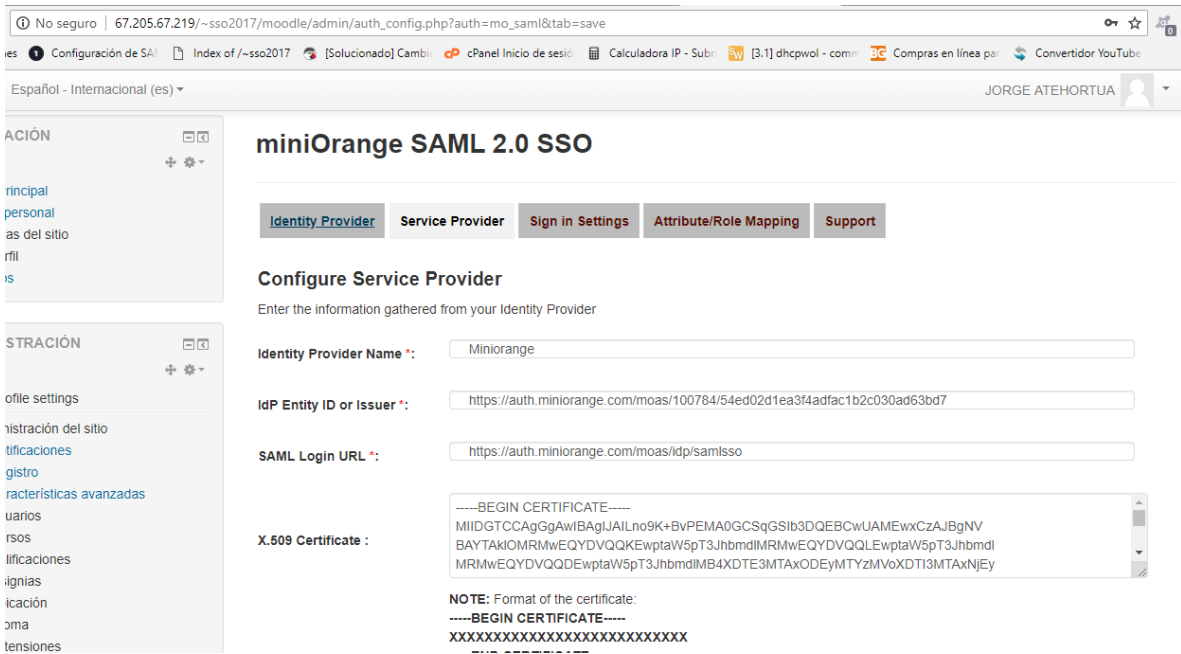
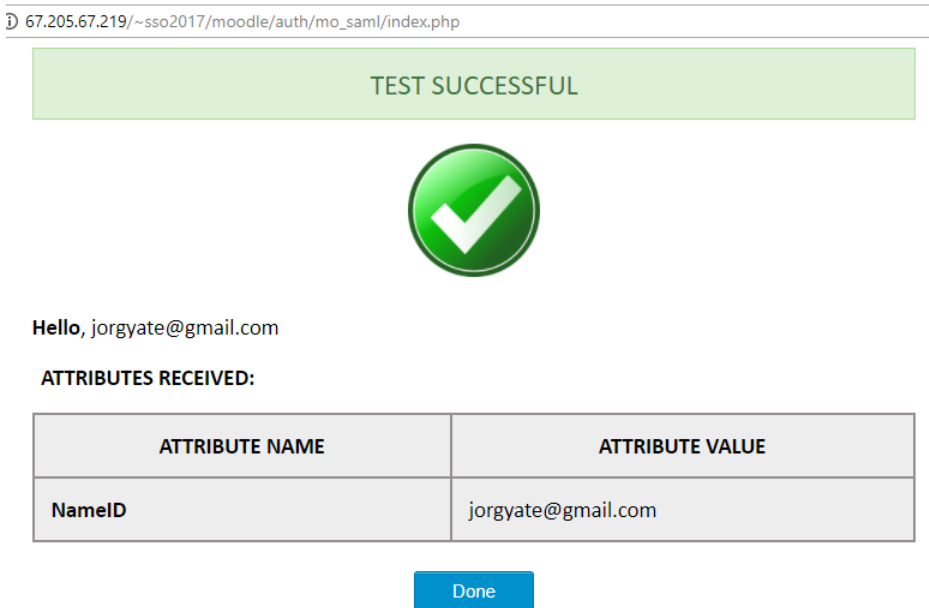



Ilustración 40: prueba de configuración de MOODLE con el IDP



67.205.67.219/~sso2017/moodle/auth/mo_saml/index.php

TEST SUCCESSFUL



Hello, jorgyate@gmail.com

ATTRIBUTES RECEIVED:

ATTRIBUTE NAME	ATTRIBUTE VALUE
NameID	jorgyate@gmail.com

[Done](#)

Ilustración 41: test de conexión entre MOODLE y el IDP para el protocolo SAML

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22







Se procede con las pruebas esta vez para el protocolo OAUTH y el gestor MOODLE con el IDP, evidenciándose una correcta conexión

Servicios OAuth 2

[Área personal](#) / [Administración del sitio](#) / [Servidor](#) / [Servicios OAuth 2](#)

Servicios OAuth 2

i [Service provider setup instructions.](#)

Nombre	Configured	Allow login	Discovery	System account connected	Editar
jorge	✓	✓	-	✓ 	    

Create new Google service

Create new Microsoft service

Create new Facebook service

Create new custom service

Ilustración 42: Prueba del servicio de autenticación en MOODLE para OAUTH

Se procede con el ingreso al sitio JOOMLA desde el enlace <http://67.205.67.219/~sso2017/JOOMLA/> y se continua con el logeo desde los botones en el lado derecho; con el usuario establecido en el IDP, posteriormente permite el ingreso tanto a JOOMLA como a MOODLE con los mismos datos de autenticación o llave única.

	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

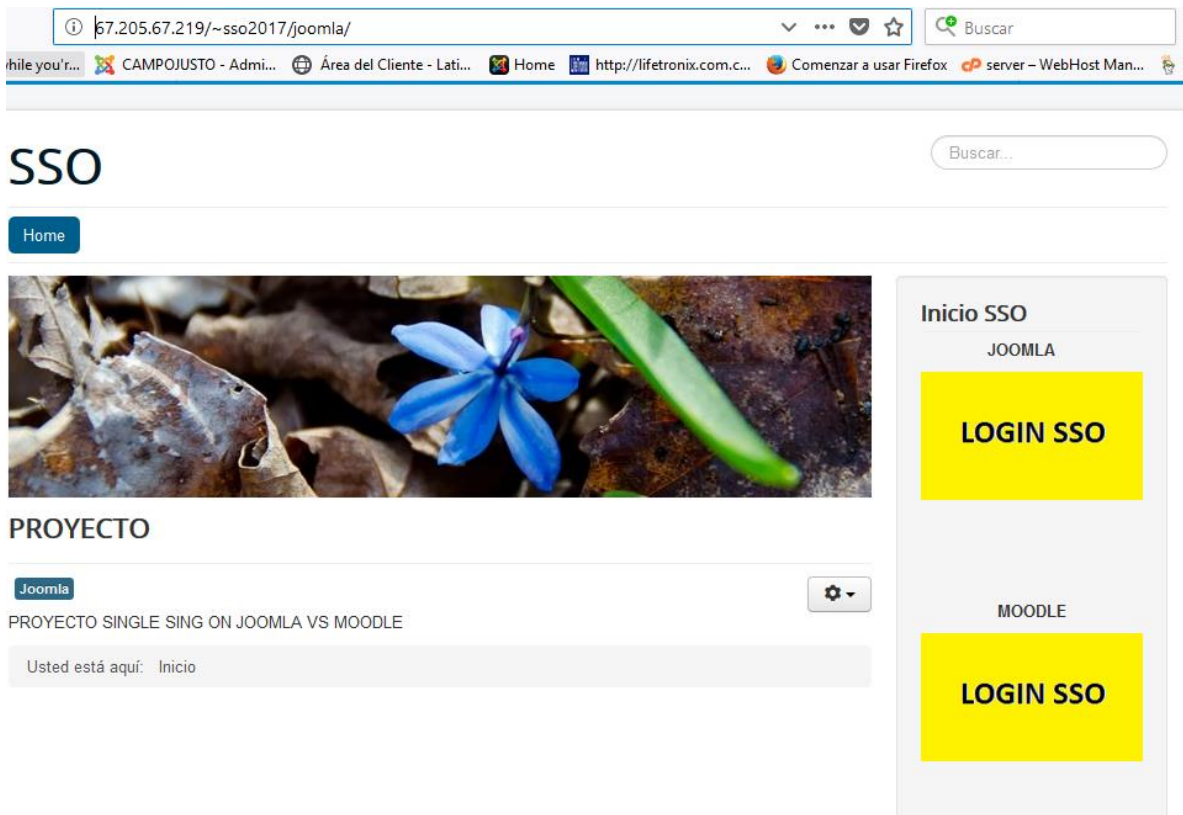


Ilustración 43: Home de JOOMLA con los accesos al login de las dos plataformas para el protocolo SAML

Se prosigue dando click para el login donde solicita el usuario registrado en el IDP que es el que tendrá acceso cifrado y seguro

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

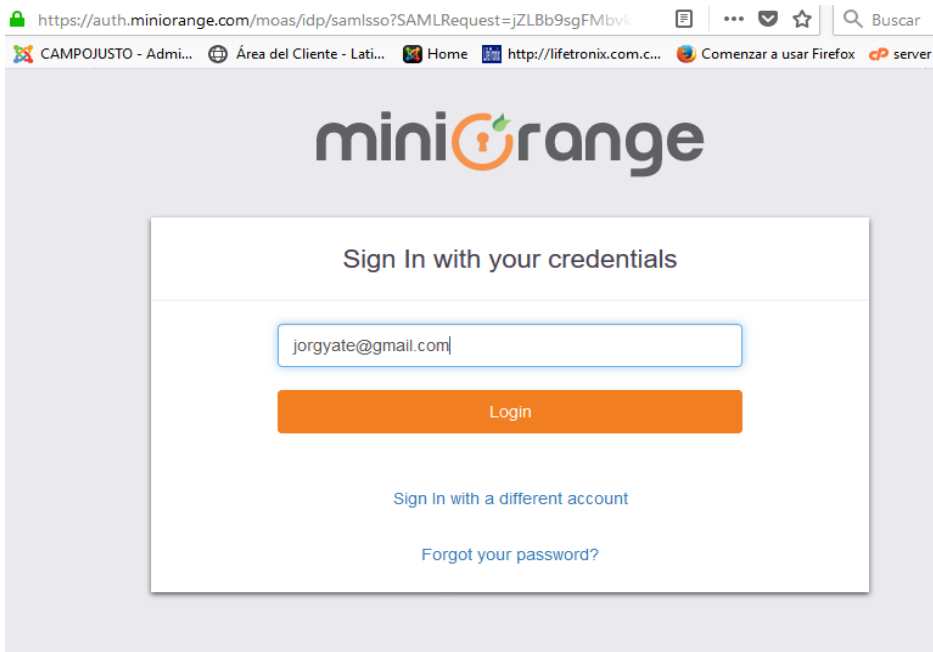


Ilustración 44: login con el usuario del IDP

Luego de ingresar los datos de usuario del IDP se concede acceso tanto a JOOMLA como a MOODLE sin tener que loguearse nuevamente en la segunda plataforma en este caso el MOODLE

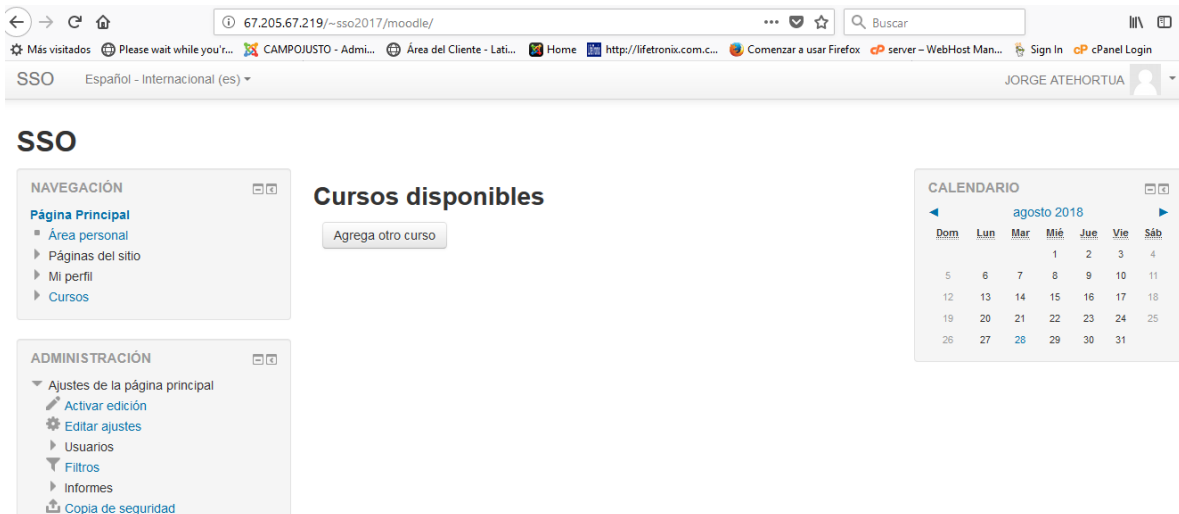


Ilustración 45: acceso a MOODLE usando SSO

	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

4. RESULTADOS Y DISCUSIÓN

4.1 SELECCIÓN DE CRITERIOS

Los resultados que se presentan a continuación responden a un análisis y descripción de los siguientes criterios: confidencialidad, secuencia básica de uso, respuesta del entorno de instalación, uso de la memoria RAM y de la CPU, los cuales se establecen como elementos de valoración para comparar la Seguridad, la Compatibilidad y el Rendimiento de los protocolos SAML Y OAUTH en las plataformas JOOMLA y MOODLE dando cumplimiento al primer objetivo específico.

Antes de describir al detalle la valoración de dichos criterios, es importante mencionar que en la dinámica de elección de los métodos para los protocolos fueron identificados 4 entre plugins, módulos o componentes totalmente compatibles con SAML y OAUTH lo que hizo posible la instalación para el esquema SINGLE SIGN ON entre las plataformas (CMS) JOOMLA y (LMS) MOODLE, que era otro de los objetivos fijados.

Para responder a los dos últimos objetivos específicos se procede a continuación a realizar el análisis de los resultados obtenidos a través de la vinculación de gráficas, tablas e ilustraciones del procedimiento ejecutado, algunas en paralelo como herramienta visual que favorece la comprensión de los hallazgos, su valoración, comparación y determinación de las ventajas y desventajas de los protocolos SAML y OAUTH en el esquema SINGLE SIGN ON.

4.2 VALORACIÓN DE CRITERIOS

4.2.1 SEGURIDAD

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

Los resultados encontrados respecto a este atributo, permiten reflejar que ambos protocolos se pueden considerar seguros, debido a que utilizan un método de autenticación con sus respectivos cifrado, en SAML utilizando metadata y el OAUTH certificados de seguridad, sin embargo es importante detallar que en el OAUTH se ha evidenciado una vulnerabilidad relacionada con la configuración inadecuada del parámetro redirec-uri, permitiendo realizar re direccionamientos de páginas lo que puede ocasionar que se filtre información de los usuarios; dichos hallazgos resultan de las evidencias encontradas en los siguientes criterios:

4.2.1.1 Confidencialidad

Cada protocolo tiene su forma única de identificar sus conexiones y la forma de enlazar las aplicaciones con su sistema IDP, generando mayor confidencialidad en cuanto al acceso de la información, en este caso el IDP utiliza tanto metadatos como certificados según el caso y los cuales se evidencian en la siguiente tabla.

Application	Provider Name	Group Name	App Type	Account Type	Id	Action
Default API App	api	N/A	API	Individual Account	87430	Edit Delete
joomla	joomla_saml	N/A	SAML	Individual Account	87683	Edit Metadata Delete Link
JOOMLA OAUTH	OpenId Connect	N/A	OpenID	Individual Account	130371	Edit Certificate Delete
moodle	moodle_saml	N/A	SAML	Individual Account	89820	Edit Metadata Delete Link
moodle oauth	OpenId Connect	N/A	OpenID	Individual Account	129284	Edit Certificate Delete

Ilustración 46: Metadatos y certificados de las apps

Adicionalmente se complementa con la clave usada por las políticas de seguridad como primer factor de autenticación.


 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

Show All entries

Group	App Name	Policy Name	First Factor
DEFAULT	Default API App	Default API Policy	PASSWORD
DEFAULT	joomla	joomlapolicy	PASSWORD
DEFAULT	JOOMLA OAUTH	JOMLAOAUTH	PASSWORD
DEFAULT	moodle	moodle	PASSWORD
DEFAULT	Self Service Console	Self Service Console	PASSWORD

Ilustración 47: políticas de seguridad

	JOOMLA	MOODLE
SAML	<p>La llave única que se utiliza es la metadata como método de encriptación de las conexiones</p> <p>Information required to set miniOrange as IdP</p> <p>IdP Entity ID or Issuer: https://auth.miniorange.com/moas/100784/680fe57165094a33a</p> <p>SAML Login URL: https://auth.miniorange.com/moas/ldap/samlso/ede7cd02-1d26-11e8-bc54-0ac99f9</p> <p>SAML Logout URL: https://auth.miniorange.com/moas/ldap/samllogout/ede7cd02-1d26-11e8-bc54-0ac99f9</p> <p>Broker Service Login URL: https://auth.miniorange.com/moas/broker/login/saml_login/100784/edd3f2be-1d26-11e8-bc54-0ac99f9</p> <p>Broker Service Logout URL: https://auth.miniorange.com/moas/broker/login/saml_logout/100784/edd3f2be-1d26-11e8-bc54-0ac99f9</p> <p>X.509 Certificate:</p> <pre>-----BEGIN CERTIFICATE----- MIIDGTCCAqGgAwIBAgIJAOGSWztl1gcMA0GCSqGSIb3DQI BgNV BAYTAKIOMRMwEQYDVQQKEwptaW5pT3JhbmdlMRMwEQYI Jhbmdl</pre>	<p>La llave única que se utiliza es la metadata como método de encriptación de las conexiones</p> <p>Information required to set miniOrange as IdP</p> <p>IdP Entity ID or Issuer: https://auth.miniorange.com/moas/100784/54ed02d1ea3f4adfac1b2c030ad63bd7</p> <p>SAML Login URL: https://auth.miniorange.com/moas/ldap/samlso/edd3f2be-1d26-11e8-bc54-0ac99f9</p> <p>SAML Logout URL: https://auth.miniorange.com/moas/ldap/samllogout/edd3f2be-1d26-11e8-bc54-0ac99f9</p> <p>Broker Service Login URL: https://auth.miniorange.com/moas/broker/login/saml_login/100784/edd3f2be-1d26-11e8-bc54-0ac99f9</p> <p>Broker Service Logout URL: https://auth.miniorange.com/moas/broker/login/saml_logout/100784/edd3f2be-1d26-11e8-bc54-0ac99f9</p> <p>X.509 Certificate:</p> <pre>-----BEGIN CERTIFICATE----- MIIDGTCCAqGgAwIBAgIJAILno9K+BvPEMA0GCSqGSIb3DQEB BgNV BAYTAKIOMRMwEQYDVQQKEwptaW5pT3JhbmdlMRMwEQYI Jhbmdl</pre>

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

OAUTH	<p>La llave única que se utiliza es el certificado como método de encriptación de las conexiones</p> <pre> MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzIKQ+V528e3nGaOL72 XA avmL2HAXwdG5+ 0Cg2X+ezPfsn2U+DxbYOKFyHXfdCj4oogF1MRk1ECUDhM126vs1 m7ZPuq9Nus6cYeBxSFdKXaC+vI0hpgkhGwAl7a6YT4HAbZ3qs+T7My5gaeuXI1 j+ 8KBOXR8VRDorxzQ1I0Q+qbfqUSMCNEMsknxFWfgxvVXSBqEOV2Yq0hbp+JSrsB 18 9DefmvNmxUKLDQ65MnIn27HqfE+ocWt6H0ba9zISGgjSEs4m0fy6fr99EhuQ9v KX GcxQfvu2qAOHz0te4yQ67xoUGWzMcMzG3TUTfYz+kFVCSJSrmSnTzppffio7o oA owIDAQAB </pre>	<p>La llave única que se utiliza es el certificado como método de encriptación de las conexiones</p> <pre> MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzIKQ+V528e3nGaOL72 XA avmL2HAXwdG5+ 0Cg2X+ezPfsn2U+DxbYOKFyHXfdCj4oogF1MRk1ECUDhM126vs1 m7ZPuq9Nus6cYeBxSFdKXaC+vI0hpgkhGwAl7a6YT4HAbZ3qs+T7My5gaeuXI1 j+ 8KBOXR8VRDorxzQ1I0Q+qbfqUSMCNEMsknxFWfgxvVXSBqEOV2Yq0hbp+JSrsB 18 9DefmvNmxUKLDQ65MnIn27HqfE+ocWt6H0ba9zISGgjSEs4m0fy6fr99EhuQ9v KX GcxQfvu2qAOHz0te4yQ67xoUGWzMcMzG3TUTfYz+kFVCSJSrmSnTzppffio7o oA owIDAQAB </pre>
--------------	---	---

Tabla 4: Claves usadas por las políticas de seguridad

4.2.1.2 Secuencia básica de uso SAML y OAUTH

Para analizar este criterio se retoma la publicación realizada por Ubisecure (2018), donde se especifican en detalle las secuencias de uso de ambas plataformas así:

Secuencia básica de uso de SAML

1. Un usuario final hace clic en el botón "Iniciar sesión" en un servicio para compartir archivos en example.com . El servicio de intercambio de archivos en example.com es el proveedor de servicios, y el usuario final es el cliente.
2. Para autenticar al usuario, example.com construye una Solicitud de Autenticación SAML, firma y opcionalmente la encripta, y la envía directamente al IDP.
3. El Proveedor de servicios redirige el navegador del Cliente al IDP para su autenticación.
4. El IDP verifica la Solicitud de Autenticación SAML recibida y si es válida, presenta un formulario de inicio de sesión para que el usuario final ingrese su nombre de usuario y contraseña.
5. Una vez que el Cliente ha iniciado sesión correctamente, el IDP genera una Aserción SAML (también conocida como Token SAML), que incluye la identidad del usuario

	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

(como el nombre de usuario ingresado anteriormente) y la envía directamente al Proveedor de Servicios.

6. El IDP redirecciona al cliente de nuevo al proveedor de servicios
7. El proveedor de servicios verifica la aserción de SAML, extrae la identidad del usuario de ella, asigna los permisos correctos para el cliente y luego lo registra en el servicio

SAML 2.0 Flow

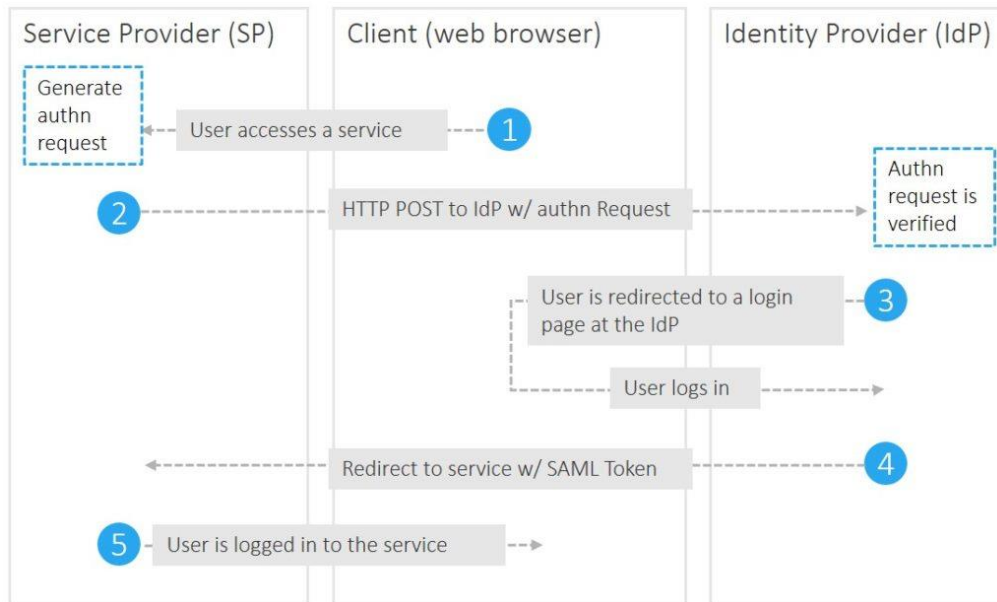


Ilustración 48: Secuencia básica de uso de SAML

Secuencia básica de Uso de OAUTH

OAUTH no supone que el Cliente sea un navegador web.

1. Un usuario final hace clic en el botón "Iniciar sesión" en un servicio para compartir archivos en example.com . El servicio de intercambio de archivos en example.com es el servidor de recursos, y el usuario final es el cliente.

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

2. El servidor de recursos presenta al cliente una concesión de autorización y redirige al cliente al servidor de autorización
3. El cliente solicita un token de acceso del servidor de autorización utilizando el código de concesión de autorización
4. El cliente inicia sesión en el servidor de autorización y, si el código es válido, el cliente obtiene un token de acceso que se puede usar para solicitar un recurso protegido del servidor de recursos.
5. Después de recibir una solicitud de un recurso protegido con un token de acceso adjunto, el servidor de recursos verifica la validez del token directamente con el servidor de autorización.
6. Si el token era válido, el servidor de autorización envía información sobre el cliente al servidor de recursos

OAuth 2.0 Flow

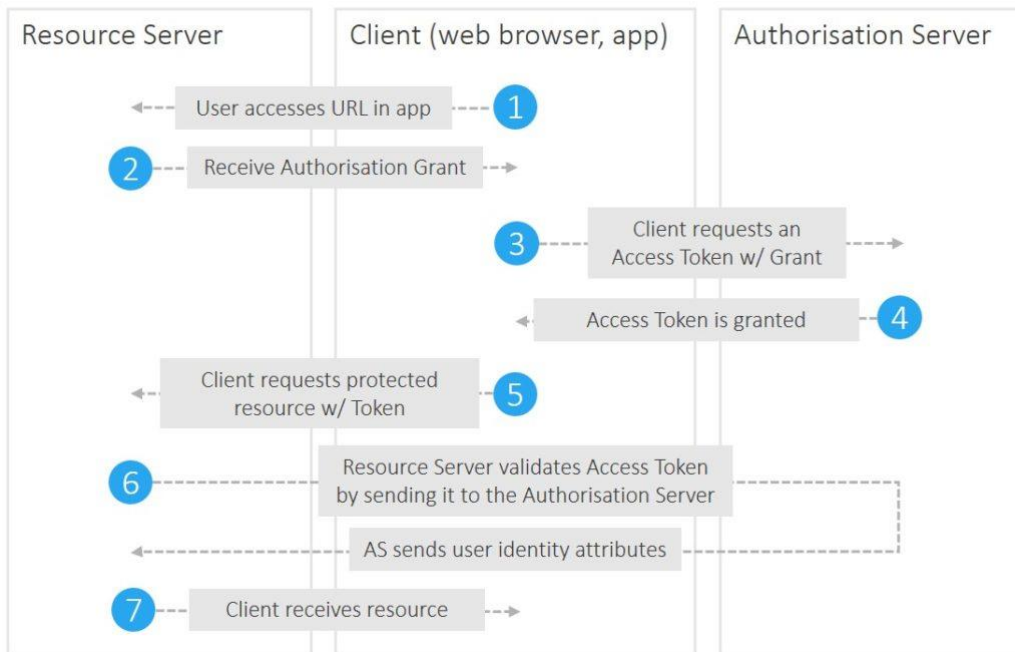


Ilustración 49: Secuencia básica de uso de OAUTH

	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

De acuerdo a los diagramas de ambas secuencias, se puede establecer que la secuencia de trabajo de SAML es más corta debido a que el IDP verifica las credenciales de acceso y si estas son correctas, devuelve el acceso a la plataforma web permitiendo al usuario el login, mientras que OAUTH realiza unos pasos adicionales ya que se deben solicitar el token de acceso al servidor, al obtener el token se debe verificar su validez para tener disponibilidad de los recursos.

4.2.2 COMPATIBILIDAD

La compatibilidad está asociada a la comprensión entre un sistema o arquitectura y una aplicación, mediante hardware y software, en el desarrollo del proyecto se encontró que la interacción entre los componentes del servidor, plataformas web, plugins módulos y componentes, proveedor de identidad para llevar a cabo la conexión de los protocolos SAML y OAUTH son totalmente compatibles, información que se sustenta en los resultados reflejados en la respuesta del entorno de aplicación de los distintos protocolos así:

4.2.2.1 Respuesta del entorno de Aplicación

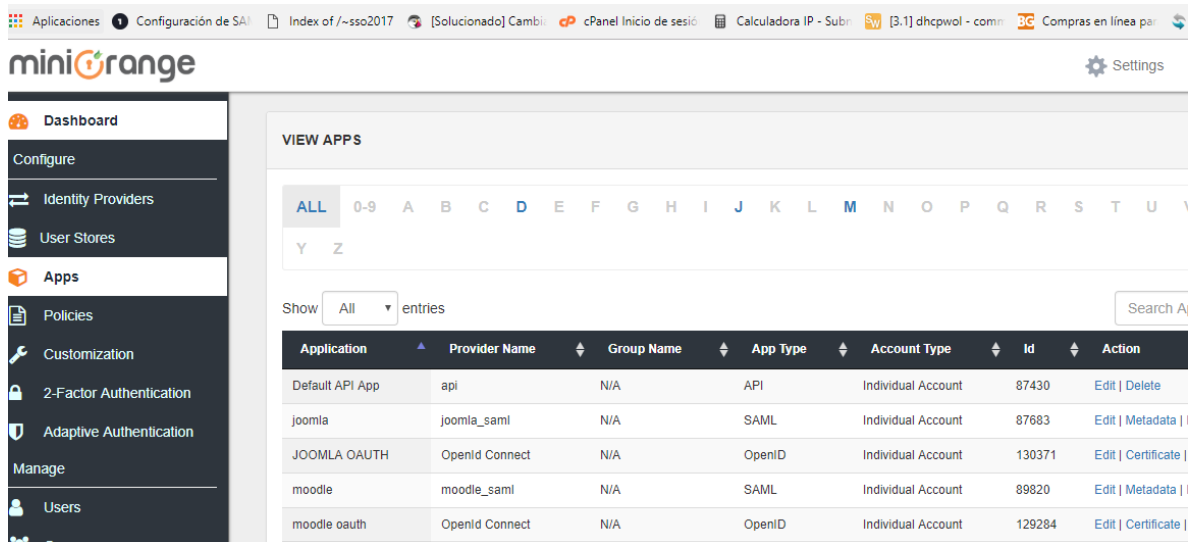
Entorno de aplicación y administración de las plataformas para el uso de los protocolos SAML y OAUTH



Ilustración 50: CPANEL como administrador de plataformas

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

IDP como entorno de aplicación del proveedor de identidad:

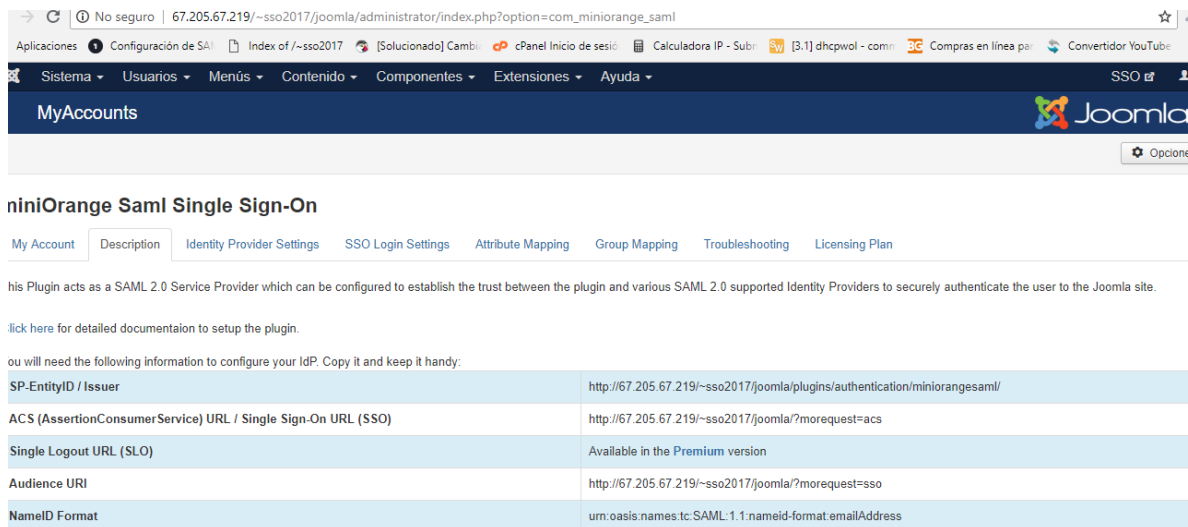


The screenshot shows the MiniOrange SSO configuration interface. The left sidebar contains navigation options: Dashboard, Configure, Identity Providers, User Stores, Apps, Policies, Customization, 2-Factor Authentication, Adaptive Authentication, Manage, and Users. The main content area is titled 'VIEW APPS' and displays a table of configured applications.

Application	Provider Name	Group Name	App Type	Account Type	Id	Action
Default API App	api	N/A	API	Individual Account	87430	Edit Delete
joomla	joomla_saml	N/A	SAML	Individual Account	87683	Edit Metadata
JOOMLA OAUTH	OpenId Connect	N/A	OpenID	Individual Account	130371	Edit Certify
moodle	moodle_saml	N/A	SAML	Individual Account	89820	Edit Metadata
moodle oauth	OpenId Connect	N/A	OpenID	Individual Account	129284	Edit Certify

Ilustración 51: Entorno del proveedor de identidad

Entorno de aplicación del protocolo SAML en JOOMLA



The screenshot shows the Joomla! administrator interface for the 'MiniOrange SAML Single Sign-On' plugin. The page title is 'MiniOrange SAML Single Sign-On' and it includes navigation tabs: My Account, Description, Identity Provider Settings, SSO Login Settings, Attribute Mapping, Group Mapping, Troubleshooting, and Licensing Plan. The main content area provides information about the plugin's role as a SAML 2.0 Service Provider and lists configuration parameters.

his Plugin acts as a SAML 2.0 Service Provider which can be configured to establish the trust between the plugin and various SAML 2.0 supported Identity Providers to securely authenticate the user to the Joomla site.

lick here for detailed documentaion to setup the plugin.

ou will need the following information to configure your IdP. Copy it and keep it handy:

SP-EntityID / Issuer	http://67.205.67.219/~sso2017/joomla/plugins/authentication/miniorangesaml/
ACS (AssertionConsumerService) URL / Single Sign-On URL (SSO)	http://67.205.67.219/~sso2017/joomla/?morequest=acs
Single Logout URL (SLO)	Available in the Premium version
Audience URI	http://67.205.67.219/~sso2017/joomla/?morequest=sso
NameID Format	urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

Ilustración 52: Aplicación del protocolo SAML en JOOMLA

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

Entorno de aplicación del protocolo SAML en MOODLE

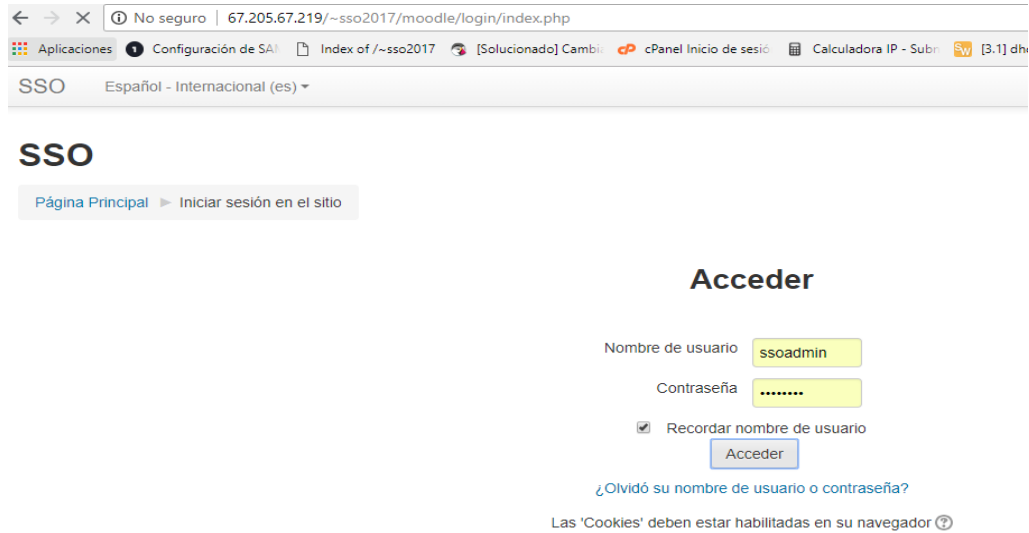


Ilustración 53: Aplicación del protocolo SAML en MOODLE

Entorno de aplicación del protocolo OAUTH en JOOMLA

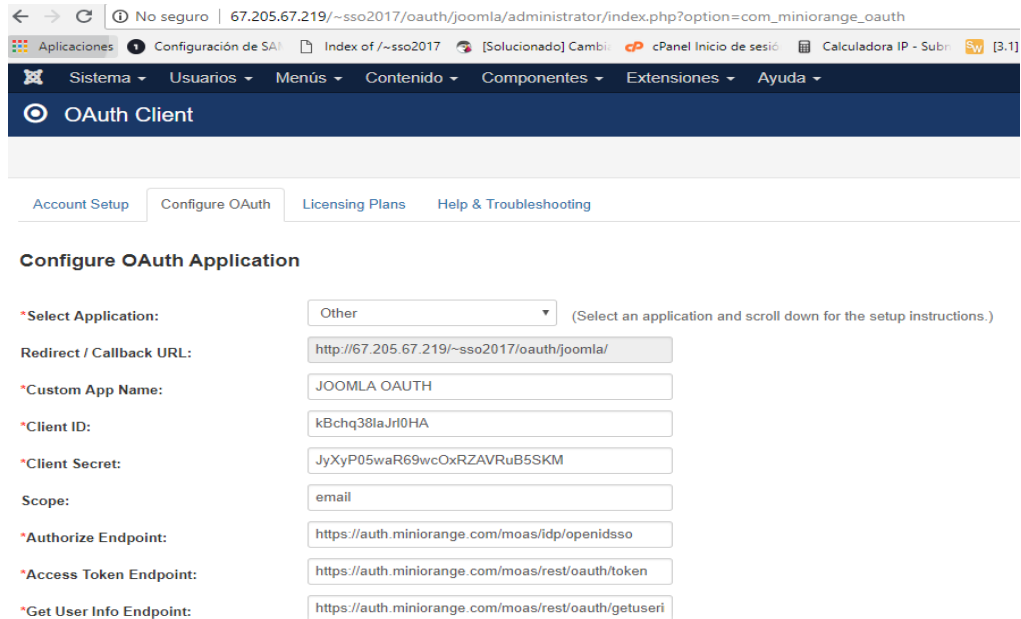


Ilustración 54: aplicación del protocolo OAUTH en JOOMLA

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

Entorno de aplicación del protocolo OAUTH en MOODLE



Ilustración 55: Aplicación del protocolo OAUTH en MOODLE

4.2.3 RENDIMIENTO

Los hallazgos encontrados en este último atributo a comparar, dan cuenta que el servidor consume lo mínimo de recursos para ambas instalaciones. Esta información resulta de la comparación entre uso de la memoria RAM y el uso de la CPU, como se muestra a continuación

4.2.3.1 Uso de memoria RAM y CPU

Artículo del sistema	Detalles	Estado
Carga del servidor	0.378906 (2 CPU)	✓
Memoria que se usó	26.4% (2,125,680 de 8,051,084)	✓
Swap utilizado	1.41% (118,216 de 8,388,600)	✓

Tabla 5: SAML EN JOOMLA procesamiento de maquina desde el login hasta su cerrada de sesión

Artículo del sistema	Detalles	Estado
Carga del servidor	0.379120 (2 CPU)	✓

	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

Artículo del sistema	Detalles	Estado
Memoria que se usó	27.8% (2,231,342 de 8,051,084)	✓
Swap utilizado	1.42% (119,216 de 8,388,600)	✓

Tabla 6: SAML EN MOODLE procesamiento de maquina desde el login hasta su cerrada de sesión

Artículo del sistema	Detalles	Estado
Carga del servidor	0.418906 (2 CPU)	✓
Memoria que se usó	26.9% (2,153,321 de 8,051,084)	✓
Swap utilizado	1.42% (221,267 de 8,388,600)	✓

Tabla 7: OUTH EN JOOMLA procesamiento de maquina desde el login hasta su cerrada de sesión

Artículo del sistema	Detalles	Estado
Carga del servidor	0.416876 (2 CPU)	✓
Memoria que se usó	27.7% (2,194,891 de 8,051,084)	✓
Swap utilizado	1.42% (221,267 de 8,388,600)	✓

Tabla 8: OUTH EN MOODLE procesamiento de maquina desde el login hasta su cerrada de sesión

Para cerrar este apartado de resultados recopilando de manera general lo descrito en los párrafos anteriores se puede decir que, en la sesión de pruebas de nuestro entorno de instalación y configuración, se simuló el uso del single sign on como mecanismo de autenticación en las plataformas JOOMLA y MOODLE usando los protocolos SAML y OAUTH, se puede decir que los resultados que se obtuvieron fueron los esperados ya que los entornos web JOOMLA Y MOODLE pudieron ser instalados sin presentar inconvenientes de compatibilidad de servidor, los plugins, módulos y componentes empleados para poder ejecutar los protocolos SAML y OAUTH también fueron instalados y configurados sin contratiempos y el uso del proveedor de identidad mini orange con sus aplicativos fueron compatibles con las configuraciones presentadas, permitiendo lograr la autenticación de un usuario y poder acceder con un solo inicio de sesión a las dos plataformas, lo cual nos llevó a poder evaluar el comportamiento y definir cuál de los dos protocolos consideramos como el mejor método de autenticación.

	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

Se puede mencionar también que el entorno de instalación empleado ha dado óptimos resultados de compatibilidad, las aplicaciones como los plugins, modulos y componentes para la configuración de los protocolos SAML y OAUTH han respondido de manera adecuada en el servidor, siendo un adecuado sistema de hardware y software. El rendimiento también se ha visto reflejado de manera positiva puesto que los datos de consumo de maquina como memoria RAM, CPU y otros parámetros de servidor se han comportado de manera eficiente permitiendo el flujo de las aplicaciones y los datos que estas transportan.

Al evaluar los comportamientos obtenidos durante la prueba logramos evidenciar que la autenticación se realiza en tiempos óptimos y de manera muy rápida, comparando rendimiento de recursos de servidor, conexión de configuraciones entre las plataformas y el proveedor de identidad, ofreciendo correctamente el servicio de inicio de sesión único (SOO), sin embargo según un informe publicado en junio de 2017 por la TCS Cyber Security Community

- <https://securitycommunity.tcs.com/infosecsoapbox/articles/2017/06/07/covert-redirect-vulnerability> se revela una vulnerabilidad muy posible en cuanto a la utilización del protocolo OAUTH, en conclusión esta comunidad expresa lo siguiente “Cover Redirect es una combinación de una implementación pobre de OAUTH y un redirector abierto. Compuesto por un gran número de empresas involucradas, esta vulnerabilidad podría tener enormes consecuencias si no se resuelve.

El problema principal es que estas vulnerabilidades presentes en aplicaciones de terceros se pueden utilizar para atacar a otras compañías, como Google, eBay, por ejemplo, al eludir sus filtros de redirección abierta (Redirección secreta).

Por lo tanto, este punto final de Redirección abierta debe ser corregido y la lista blanca de URI debe implementarse. Además, el parámetro *'redirect_uri'* debe validarse adecuadamente para que el sistema sea seguro y no se vea comprometido por los

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

atacantes.” Considerando el anterior artículo podemos interpretar que el protocolo más seguro es el SAML puesto que no se ha evidenciado que presente esta posible vulnerabilidad o pueda presentar un riesgo de este tipo de parámetros.

A continuación en la siguiente tabla comparativa se evidencian los resultados expuestos en este apartado acerca de los criterios valorados:

PROTOCOLO	SEGURIDAD		COMPATIBILIDAD	RENDIMIENTO
	Confidencialidad	Secuencia Básica de Uso	Respuesta del entorno de instalación	Uso de la memoria RAM y de la CPU
SAML	✓	✓	✓	✓
OAUTH	? redirec_uri	✓	✓	✓

Tabla 9: Resultados comparativos criterios de valoración

5. CONCLUSIONES, RECOMENDACIONES Y TRABAJO FUTURO

Finalmente, al detallar el logro de cada uno de los hallazgos en los apartados anteriores, se puede dar por logrado el cumplimiento del objetivo general de la propuesta del proyecto, el cual era comparar la seguridad, compatibilidad y el rendimiento de los protocolos SAML y OAUTH como mecanismos de autenticación en las plataformas JOOMLA y MOODLE, identificando así el mejor método de inicio de sesión bajo la tecnología SINGLE SIGN ON, el cual soportado en la información presentada se establece que es SAML.

Esta conclusión emerge luego de haber dado respuesta a cada uno de los objetivos específicos como se especificó en los resultados anteriores, primero con la selección de los criterios para hacer posible la comparación de la seguridad, la compatibilidad y en rendimiento los cuales fueron: confidencialidad, secuencia básica de uso, respuesta del entorno de instalación, uso de la memoria RAM y de la CPU.

	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

Dando respuesta al segundo objetivo específico se concluye que los 4 métodos compatibles para los protocolos fueron miniorange-SAML-sso-for-JOOMLA, Auth Mod SAML, MIniorange OAUTH Client y OAUTH Application.

Con respecto a la valoración de los criterios seleccionados que responde al tercer objetivo específico, se concluye que la confidencialidad se refleja en ambos protocolos por su manera de cifrar las autenticaciones; sin embargo el mal uso en el protocolo OAUTH del parámetro `redirect_uri` puede generar vulnerabilidades; en cuanto a la secuencia básica de uso, vemos que aunque hay parámetros similares SAML emplea un flujo de trabajo más simple y directo que el OAUTH a la hora de realizar los parámetros de conexión; respecto a la respuesta del entorno de instalación se evidencia que las configuraciones, servidor y proveedor de identidad utilizado son compatibles y finalmente para los criterios de rendimiento de memoria RAM y de la CPU se concluye que los dos protocolos en su ejecución no exigen de altos recursos de memoria RAM y CPU teniendo un óptimo desempeño del servidor.

Para terminar las conclusiones del último objetivo específico, es importante comparar las ventajas y desventajas de los protocolos SAML y OAUTH para un esquema de SINGLE SIGN ON entre las plataformas (CMS) JOOMLA y (LMS) MOODLE así:

Ventajas y desventajas de Single Sign On

Ventajas	Desventajas
Simplifica y acelera el acceso de los usuarios a sus aplicaciones	Utilizar una única combinación aumenta las probabilidades de vulnerabilidad de contraseñas
No es necesario memorizar múltiples contraseñas, permitiendo reducir esta carga	Si falla el SSO o el IDP ya no se tendría acceso a los sistemas que intervienen
Su implementación no es complicada a la hora de conectar fuentes de datos nuevas.	Se pueden presentar suplantaciones de identidad en los accesos externos de los usuarios

Tabla 10: cuadro ventajas y desventajas del uso de los protocolos SAML y OAUTH

	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

En el caso de las empresas contar con un sistema de autenticación como Single Sign On significa liberar al usuario de la carga de recordar numerosas contraseñas, además proporciona activos muy importantes relacionados directamente a la eficiencia, de esta manera es posible reducir la llamada al servicio de asistencia técnica o al departamento de informática para dar solución a los problemas originados por la seguridad de las contraseñas.

Luego de culminar el presente proyecto se pueden identificar diversas limitaciones que surgieron en el mismo como fue la opción de generar 50 usuarios adicionales para realizar estas pruebas simultáneamente, el IDP utilizado ya nos exigía una valoración en costos por la implementación de más usuarios lo cual no nos permitió dicha prueba, otra limitación considerada fue encontrar otro IDP diferente ya que los costos no nos lo permitía y así realizar pruebas experimentales con dos alternativas de proveedor de identidad.

En cuanto a la prospectiva de este trabajo aparecen diversas líneas que podrían ahondarse en trabajos futuros; una de las opciones que se propone se relaciona con la creación o la implementación de una herramienta o aplicativo que nos permita validar el funcionamiento de todo el entorno. También sería bueno y beneficioso para las empresas tener una matriz comparativa de las plataformas de distribución libre que se pueden usar con los protocolos trabajados para Single Sign On que contenga una descripción de cada herramienta y permita la toma de decisiones a las organizaciones que tengan necesidades específicas.

	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

6. REFERENCIAS


- Dhole, A. (2015). Single Sign-On in Cloud Federation using CloudSim. . International Journal of Computer Network and Information Security, 7.
- Diagrama de Gantt (2018, 26 de Agosto). <https://www.obs-edu.com/int/blog-project-management/diagramas-de-gantt/que-es-un-diagrama-de-gantt-y-para-que-sir>
- Education and Society, R. Aiken (ed.), Proc. 12th IFIP World Computer Congress (1992) Information Technology Security Evaluation Criteria (ITSEC) – a Contribution to Vulnerability?
- Flujo de trabajo SAML y OAUTH (28 de Agosto de 2018)<https://www.ubisecure.com/uncategorized/difference-between-SAML-and-OAUTH/>
- Gráfica de Barras (2018, 26 de Agosto). Recuperado de <http://asesorias.cuautitlan2.unam.mx/Laboratoriovirtualdeestadistica/DOCUMENTOS/TEMA%201/6.%20GRAFICA%20DE%20BARRAS.pdf>
- Harkut, M. R. (2014). Implementation of Single Sign-On Mechanism for Distributed Computing. International Journal of Computer Science and Mobile Computing, 623-632.
- <http://www.webactualizable.com>. (30 de 08 de 2016). Obtenido de <http://www.webactualizable.com/blog-joomla/167-joomla-el-segundo-cms-mas-usado-del-mundo>
- ICONTEC (1997). Baldosas con superficie de grano -Terrazo- (Vol. NTC 2849). Bogotá: ICONTEC.
- Iglesias, A., Olmos, S., Torrecilla, E., & Juan, M. (2014). EVALUAR PARA OPTIMIZAR EL USO DE LA PLATAFORMA MOODLE (STUDIUM) EN EL DEPARTAMENTO DE DIDÁCTICA, ORGANIZACIÓN Y METODOS DE INVESTIGACIÓN. Tendencias pedagógicas, 155-170.
- Joomla! El segundo CMS más usado del mundo. (2018, 07 de Noviembre). Recuperado de <https://www.webactualizable.com/blog-joomla/167-joomla-el-segundo-cms-mas-usado-del-mundo>
- Joomla. (25 de 09 de 2016). <https://www.joomla.org>. Obtenido de <https://www.joomla.org>: <https://www.joomla.org>
- Modelo de vida basico o de cascada. (2018, 26 de Agosto). http://www.spw.cl/proyectos/apuntes2/cap_6.htm
- MOLIST, M. (04 de 12 de 2008). Moodle llena la geografía educativa española de campus virtuales. Elpais.com, págs. 1-2.
- Roger A. Grimes, CSO (EE.UU.). ¿Qué es OAUTH? Lo que los profesionales de seguridad necesitan saber. (2018, 7 de Noviembre). Recuperado de

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

<https://cioperu.pe/articulo/24429/que-es-oauth-lo-que-los-profesionales-de-seguridad-necesitan-saber/>

- SAML: Qué es, para qué se usa, cómo funciona. (2018, 07 de Noviembre). Recuperado de <https://cioperu.pe/articulo/24726/saml-que-es-para-que-se-usa-como-funciona/>
- Wikipedia. (30 de agosto de 2016). wikipedia.org. Obtenido de https://es.wikipedia.org/wiki/Single_Sign-On

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

 Institución Universitaria	INFORME FINAL DE TRABAJO DE GRADO	Código	FDE 089
		Versión	03
		Fecha	2015-01-22

FIRMA ESTUDIANTES

profs Ivan Alhortua.
GIUANNY GOMEZ VERES

Se aprueba la entrega del trabajo de grado sobre *Simple Sign On* con los ajustes *08/11/18*

FIRMA ASESOR *Javier Mauricio Ruiz V.*

FECHA ENTREGA: _____

FIRMA COMITÉ TRABAJO DE GRADO DE LA FACULTAD _____

RECHAZADO___ ACEPTADO___ ACEPTADO CON MODIFICACIONES___

ACTA NO. _____

FECHA ENTREGA: _____

FIRMA CONSEJO DE FACULTAD _____

ACTA NO. _____

FECHA ENTREGA: _____