Federación de Identidad para Instituciones de Educación e Investigación

Enregable: WP2-7.2

Curso en línea en la Plataforma CUDI
Material

Fernando Aranda Escobar

Proyecto financiado por FONCICYT

ÍNDICE

1. Bienvenida

¡Bienvenid@s al Curso de Federación de Identidades!

El objetivo de este curso es adquirir los conocimientos sobre los entornos federados en los ambientes educativos y desarrollar las habilidades necesarias para la creación de un proveedor de identidad, de un proveedor de servicio y de un servicio básico federado.

Para iniciar las actividades debes utilizar la herramienta **Guía Didáctica** ubicada en el menú vertical a la izquierda de esta página, ahí encontrarás la ficha técnica del curso y la hoja de ruta del mismo.

Una vez que hayas revisado la Guía Didáctica, selecciona la opción **Módulo I**, donde encontrarás la información del módulo y las actividades que deberás realizar.

2. Guía Didáctica

2.1 Ficha Técnica

Federación de Identidad para

Instituciones de Educación e Investigación

FICHA TÉCNICA	
Nombre:	Federación de identidad para Instituciones de Educación e Investigación
Horas:	38
Modalidad:	A distancia con soporte en la plataforma de colaboración CUDI
Dirigido a:	Personal técnico de las instituciones miembros de CUDI, participantes en el proyecto MAGIC
Instructores y tutoría:	Fernando Aranda Gabriel Cruz Carlos González
Reconocimiento de:	Corporación Universitaria Para el Desarrollo de Internet, A.C. (CUDI)

Objetivo

Que el participante comprenda los entornos federados a través de una infraestructura de autenticación y autorización federada y como puede aplicarla a su institución.

Resultados esperados:

Al finalizar el curso, el participante habrá generado un Proveedor de Identidad (IdP por sus siglas en inglés) y un Proveedor de Servicio (SP por sus siglas en inglés) en SimpleSAMLphp, así mismo federará un servicio de prueba utilizando los servidores generados.

APRENDIZAJES

Módulo I (10 Horas)

- Información General
- Fundamentos
  - ¿Qué es una federación?
  - Elementos de una federación
  - Interacción entre los elementos de una federación
  - Ejemplos de federaciones académicas
  - Términos manejados en una federación
- Preparando el servidor
- Instalación de SimpleSAMLphp en servidor SP
- Probando la instalación

Módulo II (14 Horas)

- Desplegar un Proveedor de Servicio con SimpleSAMLphp
  - Funcionamiento de un SP
  - Estructura de SimpleSAMLphp
  - Principales puntos de configuración
  - Metadatos del SP
  - Probando el SP
- Aplicación de Prueba
  - Instalando la aplicación
  - Configurando la aplicación
- Desplegar un Proveedor de Identidad con SimpleSAMLphp
  - Instalando SimpleSAMLphp en el servidor IdP
  - Funcionamiento de un IdP
  - Principales puntos de configuración
  - Metadatos del IdP
  - Probando el IdP
  - Probando el IdP

Metodología

El curso contempla como medio de soporte la Plataforma de Colaboración de CUDI para todos los procesos que ocurren durante las distintas instancias de formación del curso:

En este espacio de Colaboración el participante encontrará toda la información necesaria para seguir y culminar con éxito su proceso de aprendizaje.

El elemento central es el módulo, que incluye los contenidos alrededor del tema tratado y varias actividades que permitirán al alumno alcanzar los objetivos de aprendizaje determinados.

Además, los participantes recibirán el apoyo de tutoría mediante correo electrónico y participación en el foro, adicionalmente, habrá sesiones semanales por videoconferencia para resolución de dudas.

EVALUACIÓN Y RECONOCIMIENTO

La evaluación se hará en porcentaje de avance de cada módulo.

Cada módulo tiene actividades que se sumarán al final del curso, el participante deberá tener resuelta cuando menos un 60% de las actividades para recibir su reconocimiento.

El reconocimiento será otorgado por la Corporación Universitaria Para el Desarrollo de Internet, A.C. (CUDI), una vez que el curso termine y los participantes tengan el porcentaje de actividades evaluado.

Requisitos de los Participantes

Los participantes en el curso deberán tener los conocimientos:

- **Necesarios:**
  - Sistema Operativo Linux a nivel administrador (servidores)
  - Conocimiento básico de redes
- **Deseables:**
  - Apache
  - Base de datos en MySQL

REQUISITOS TÉCNICOS

Los participantes deberán tener dos servidores (IdP y SP) con las siguientes características:

- Para el Proveedor de Identidad:
  - Servidor virtual o físico
  - 4+GB RAM
  - Disco Duro de 40+ GB
  - Dos núcleos
  - Instalación Estándar de sistema operativo Linux Debian 7 u 8
  - Instalación de PHP
  - Instalación de MySQL
  - Dirección IPv4 Pública
- Para el Proveedor de Servicio y el Servicio Federado:
  - Servidor virtual o físico
  - 4+GB RAM
  - Disco Duro de 40+ GB
  - Dos núcleos
  - Instalación Estándar de sistema operativo Linux Debian 7 u 8
  - Instalación de PHP
  - Dirección IPv4 Pública

2.2 Ruta de Actividades

SEMANA 1

Módulo	Actividades

Módulo I	• Información General
	• Fundamentos
	  ○ ¿Qué es una federación?
	  ○ Elementos de una federación
	  ○ Interacción entre los elementos de una federación
	  ○ Ejemplos de federaciones académicas
	  ○ Términos manejados en una federación
	• Preparando el servidor
	• Instalación de SimpleSAMLphp en servidor SP
	• Probando la instalación

	Evaluación del módulo (30%)

SEMANA 2

Módulo	Actividades

Módulo II	• Desplegar un Proveedor de Servicio con SimpleSAMLphp
	  ○ Funcionamiento de un SP
	  ○ Estructura de SimpleSAMLphp
	  ○ Principales puntos de configuración
	  ○ Metadatos del SP
	  ○ Probando el SP
	• Aplicación de Prueba
	  ○ Instalando la aplicación
	  ○ Configurando la aplicación
	• Desplegar un Proveedor de Identidad con SimpleSAMLphp
	  ○ Instalando SimpleSAMLphp en el servidor IdP
	  ○ Funcionamiento de un IdP
	  ○ Principales puntos de configuración
	  ○ Metadatos del IdP
	  ○ Probando el IdP

	Evaluación del módulo (35%)

SEMANA 3

Módulo	Actividades

Módulo III	• Origen de datos
	  ○ BD de usuarios
	  ○ Agregar el origen de datos
	• Metadatos
	  ○ Preparando los metadatos del IdP
	  ○ Obteniendo los metadatos del IdP
	  ○ Obteniendo los metadatos del SP
	  ○ Intercambiando Metadatos entre el SP y el IdP
	  ○ Probando la aplicación de prueba con el SP y el IdP
	• Interactuando con otros IdP's
	  ○ Agregando los metadatos de otros IdP's
	  ○ Probando la autenticación con otros IdP´s
	• Atributos
	  ○ Liberación de atributos
	  ○ Limitando los atributos
	  ○ Mapeando los atributos
	• Personalizando SimpleSAMLphp
	  ○ Creación de un módulo
	  ○ Activación del módulo
	  ○ Instalación del tema
	  ○ Pruebas del tema

	Evaluación del módulo (35%)

3. Módulo I

3.1 Información General

¡Bienvenid@s al Curso de Federación de Identidades!

El objetivo del curso es adquirir los conocimientos sobre los entornos federados en los ambientes educativos y desarrollar las habilidades necesarias para la creación de un proveedor de identidad, de un proveedor de servicio y de un servicio básico federado.

El curso se ha divido en tres módulos:

El Módulo I, introduce al estudiante en el entorno federado de los ambientes educativos, explica que son las federaciones de identidades, da ejemplos de varias de ellas, así también, menciona los beneficios que pueden obtener y muestra algunos ejemplos de los servicios que se pueden federar en las instituciones educativas.

En el Módulo II, el estudiante instalará y desplegará un proveedor de identidad, un proveedor de servicio y un servicio de prueba, utilizando el protocola SAML 2 mediante la aplicación SimpleSAMLphp.

SimpleSAMLphp es un software publicado bajo licencia libre muy utilizado en las federaciones de identidad basadas en SAML 2.

El Módulo III, permitirá al estudiante utilizar una base de datos de usuarios (MySQL) conectada al proveedor de identidad. Aprenderá a intercambiar metadatos entre los proveedores de identidad y de servicio para conectarlos y probar la aplicación.

Intercambiará metadatos de su proveedor de identidad con la federación de identidad mexicana (FENIX) y se incorporará al WAYF de la federación.

Para iniciar las actividades se debe utilizar la herramienta Guía didáctica ubicada en el menú vertical a la izquierda de la página del curso.

Habrá diferentes espacios de comunicación para la resolución de dudas:

Habrá un foro por cada uno de los módulos del curso.

También podrán enviar sus dudas o comentarios al correo soporte.curso01@fenix.org.mx

Se tendrán sesiones de videoconferencia para resolución de dudas y soporte técnico.

3.2 Fundamentos

3.2.1 ¿Qué es una federación?

Una federación es una red de confianza que permite administrar de mejor manera los acuerdos bilaterales entre los usuarios y los proveedores de servicio. Ofrece a las instituciones la infraestructura de autenticación y autorización necesaria para interconectar personas y compartir recursos y servicios.

La federación utiliza el principio de identidad federada, donde las instituciones implementan diferentes métodos de autenticación, manteniendo la interoperabilidad.

La gran cantidad de servicios que se utilizan en las instituciones, hace que estas deban mantener bases de datos con información de los usuarios que pueden acceder a estos servicios, y definir con qué nivel de privilegio accederán.

Esta demanda de reconocimiento y validación de acceso de los usuarios a los servicios, puede ser sintetizada en dos etapas denominadas autenticación y autorización.

Es importante diferenciar estas dos etapas.

La autenticación es el proceso de verificar la identidad de una persona mientras que la autorización es el proceso de verificación de que una persona ya identificada tenga la autoridad para realizar una cierta operación o para acceder a un cierto servicio o recurso.

Las etapas de autenticación y autorización, son pasos fundamentales para la prestación de un servicio.

La autenticación implica generalmente, la necesidad de mantener bases de datos con registros sobre los posibles usuarios del servicio.

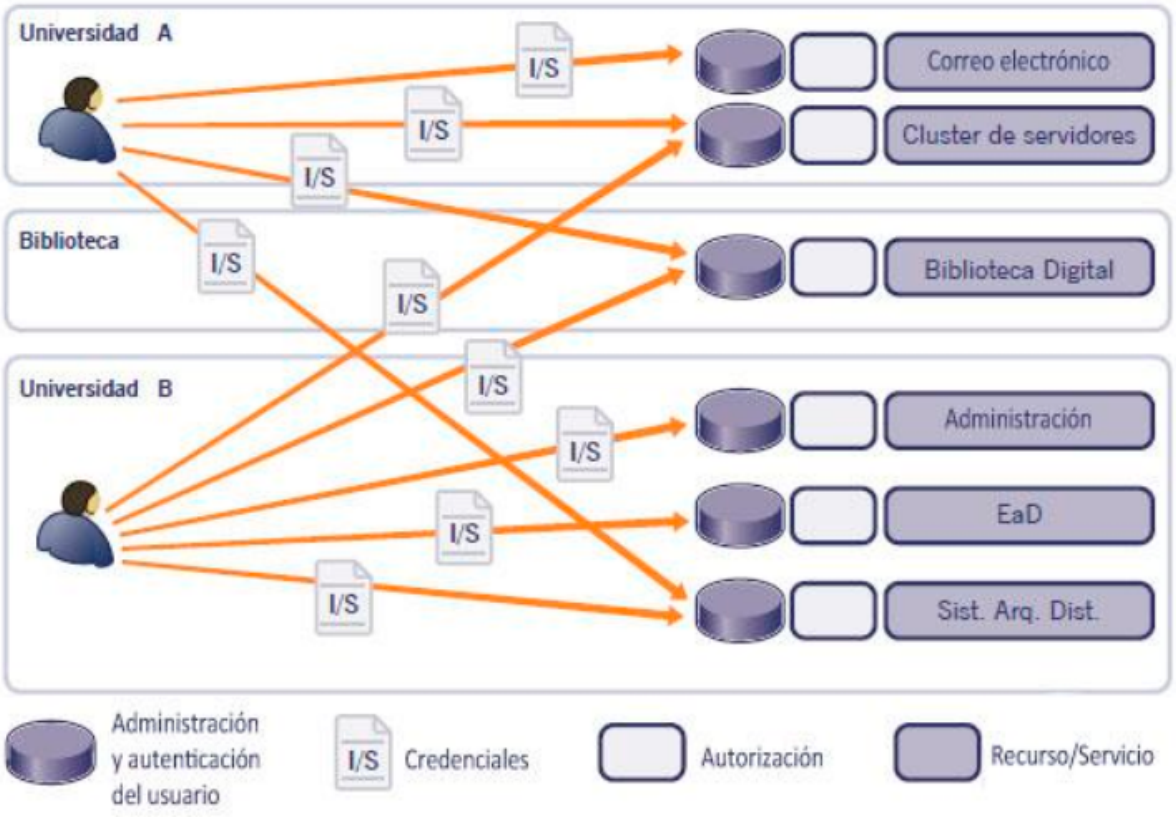
Del lado de quien presta un servicio se tiene la necesidad de crear y mantener sus propias bases de datos de usuarios, y del lado de quien utiliza los distintos servicios disponibles, se tiene la necesidad de crear y mantener cuentas para cada servicio al que desea tener acceso.

El concepto de federación de identidad tiene como objetivo minimizar las demandas de los proveedores y de los usuarios de los servicios prestados por las instituciones, en relación con el mantenimiento de informaciones usadas para la autenticación y autorización de acceso a esos servicios.

La idea básica es la siguiente: la información sobre un usuario es mantenida en una única base, administrada por la institución a la que este usuario está vinculado, y donde cada institución establece su modelo de gestión de identidad, es decir la institución decide que métodos de autenticación utilizará.

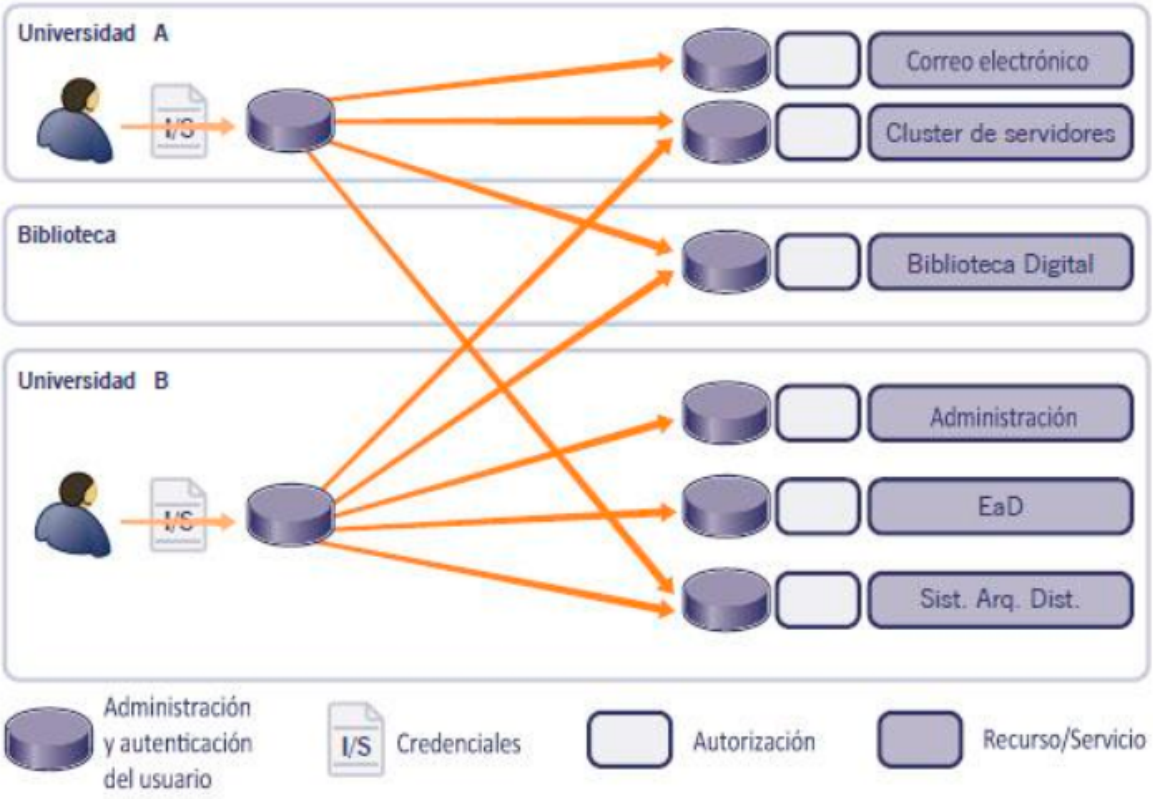
Por otra parte, los proveedores de servicios confían en el modelo de gestión de identidad de las instituciones y disponen sus servicios para los usuarios vinculados a esas instituciones, creando así el principio de identidad federada.

En la siguiente figura se muestra un modelo habitual en el que cada servicio debe mantener la información sobre sus usuarios



En este modelo cuando se implementa un servicio, este debe tener un módulo de registro para los usuarios y entonces cada usuario debe tener un registro (clave y contraseña) para acceder a cada servicio.

En la figura siguiente, la información de los usuarios es generada y administrada en un único lugar.



En este segundo modelo, las informaciones sobre las personas son mantenidas en un único lugar, generalmente la institución con la cual el usuario tiene su vínculo principal, así también, cada usuario solo debe tener un registro (clave y contraseña); en este modelo cuando se implementa un nuevo servicio no se requiere un módulo de registro de usuarios

3.2.2 Elementos de una federación

Una federación incluye dos elementos principales:

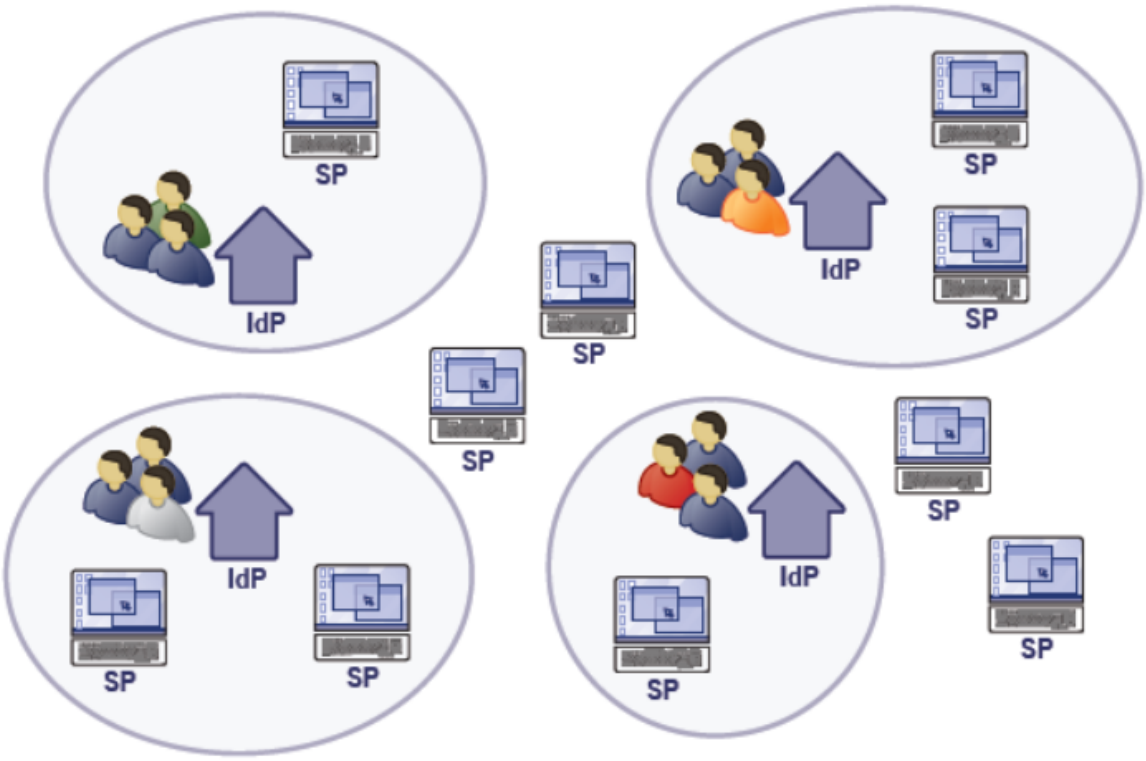
Proveedores de identidad – Es quien almacenan y gestionan las informaciones sobre personas.

Proveedores de servicio – Ofrecen servicios/recursos restringidos a grupos de usuarios.

¿Quienes actúan en una federación?

- ✓ Usuario: es quien desea utilizar un servicio/recurso protegido
- ✓ Proveedor de servicio: es quien tiene el servicio y lo ofrece al usuario, confiando en el proceso de autenticación del proveedor de identidad.

- ✓ Proveedor de identidad: institución del usuario, que tiene un proceso interno de autenticación y envía la confirmación de identidad del usuario que solicitó el servicio/recurso al proveedor de servicio.



La figura anterior nos muestra los principales componentes de una federación y las asociaciones entre ellas.

Como se puede observar, dentro de una federación es posible definir subgrupos con un proveedor de identidad y uno o más proveedores de servicios asociados.

Esto nos sirve para segmentar a los usuarios y permitirles el ingreso a diferentes servicios/recursos como:

Servicios internos de la institución, como la inscripción de alumnos, registro de calificaciones, registro de proyectos, etc.

Servicios externos a la institución, como bibliotecas digitales, educación a distancia, almacenamiento distribuido, etc.

Proveedores de identidad

Los proveedores de identidad implementan la política interna de gestión de identidad de una institución.

- ✓ Definen los atributos de los usuarios:

- ✓ Nombre, fecha del enlace, cargo ocupado, matrícula, etc.
- ✓ Definen el método de autentificación:
- ✓ Login/ contraseña, certificados, etc.
- ✓ Asignan un identificador único para cada persona vinculada a la institución.

Los proveedores de identidad son los responsables de mantener la información sobre los usuarios vinculados a una institución, esta información puede incluir datos personales (nombre, fecha de nacimiento, número de seguro social, sexo, etc.) y datos institucionales (fecha de admisión, cargo, número de matrícula, etc.). El proveedor de identidad establece su método de autenticación y debe garantizar que cada usuario en la institución tenga un identificador único.

Proveedores de Servicio

Tiene servicios que deben estar disponibles para las personas vinculadas a las instituciones.

Los proveedores de servicio requieren:

- ✓ Autenticación: La identificación de los usuarios que quieren acceder al servicio
- ✓ Autorización: Recibir y revisar los atributos adicionales del usuario que garanticen ciertos privilegios de acceso.
- ✓ Tienen el enfoque en la implementación del servicio, y no en el mantenimiento y administración de las bases de datos de los usuarios.

Los proveedores de servicio ofrecen servicios de acceso restringido, y pueden solicitar información adicional del usuario para determinar si este tiene los privilegios necesarios para acceder al servicio, (por ejemplo, que el usuario esté inscrito en determinado curso, que el usuario tenga cierto cargo, etc.).

Cuando se implementa un servicio se define los privilegios de acceso y la información adicional que será solicitada.

El proveedor de servicio no debe mantener esas informaciones, sólo debe solicitarlas a los proveedores de identidad.

Componente adicional de una federación

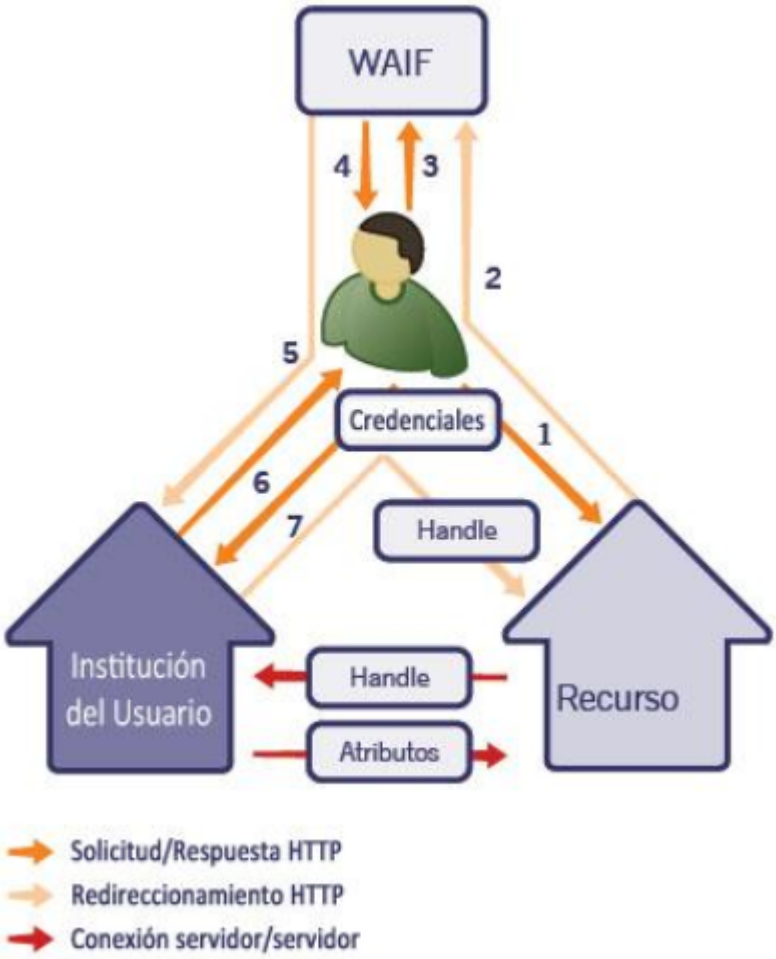
Existe un elemento que centraliza la información de los diferentes proveedores de identidad que tiene la federación, este componente se le conoce como WAYF (Where Are You From) o DS (Discovery Service) y tiene la información de lo proveedores de identidad y sus ubicaciones.

Como los proveedores de servicio en una federación necesitan permitir el acceso de usuarios de diferentes instituciones, el WAYF ayuda a redirigir al usuario a su respectivo proveedor de identidad.

Cuando el usuario selecciona el servicio al que desea acceder, es redirigido al WAYF o DS, y ahí selecciona su institución de origen, y entonces, empieza a interactuar con su proveedor de identidad proporcionando sus credenciales.

3.2.3 Interacción entre elementos de una federación

A continuación, se muestra la interacción entre los elementos de una federación:



1: El usuario accede al proveedor de servicio (SP) y selecciona el servicio al que desea acceder.

2: El servicio redirige al usuario hacia el repositorio centralizado WAYF/DS.

3: El usuario selecciona su institución de origen.

4: El usuario es redirigido hacia su proveedor de identidad (IdP).

5: El IdP autentica al usuario con el método elegido por la institución.

6: El SP recibe la garantía de autenticación del usuario de parte del IdP.

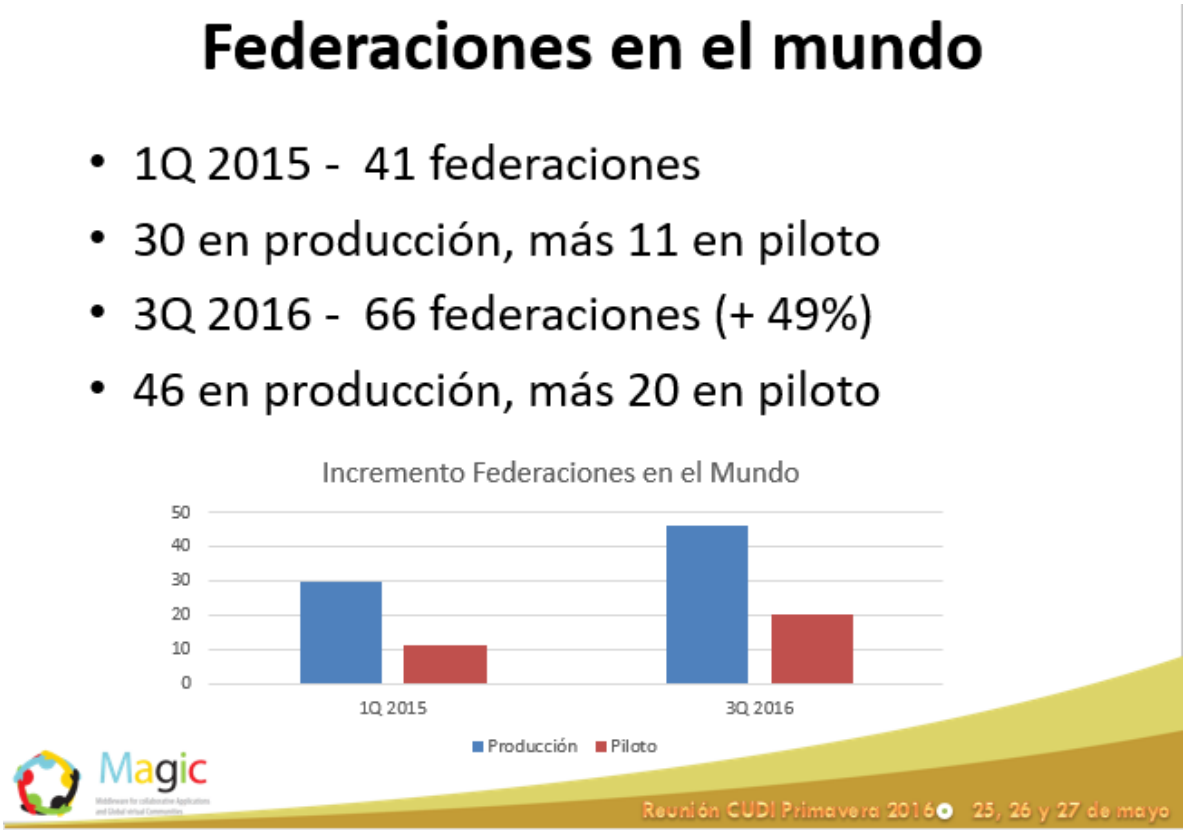
7: Si es necesario, el SP solicita atributos adicionales de ese usuario al IdP; sólo se entregan atributos previamente acordados entre el IdP y el SP.

8: El proveedor de servicio decide sobre las autorizaciones y proporciona el servicio al usuario.

3.2.4 Ejemplos de federaciones académicas

La creación de federaciones de identidad en el mundo se ha incrementado notablemente en el último año, debido al impulso que las RNIE's del mundo le han dado y a los beneficios que estas pueden trasladar a sus instituciones miembros.

En el siguiente gráfico podemos ver el crecimiento de las federaciones en el mundo, en el último año



Algunas de las más importantes son:

- ✓ InCommon - Federación de los EE.UU. con 107 instituciones y con más de dos millones de usuarios
- ✓ Feide - Federación de Noruega
- ✓ Switch - Federación de Suiza
- ✓ SDSS - Federación del Reino Unido
- ✓ CAFe - Federación de Brasil
- ✓ Cofre - Federación de Chile
- ✓ Colfire - Federación de Colombia

- ✓ MATe - Federación de Argentina

En el siguiente gráfico podemos ver algunas de las federaciones en el mundo

Existen actualmente alrededor de 66 federaciones en el mundo (algunas de ellas en piloto), las cuales están son administradas y mantenidas por las RNIE de cada país.

Confederaciones

Una tendencia natural es la unión de federaciones para formar confederaciones, ampliando aún más, el alcance de los servicios disponibles para los usuarios de las instituciones de un país más allá de los límites geográficos de este.

3.2.5 FENIX

FENIX es una Iniciativa de la Corporación Universitaria Para el Desarrollo de Internet, A.C. (CUDI) para crear una Federación de Identidades en México.

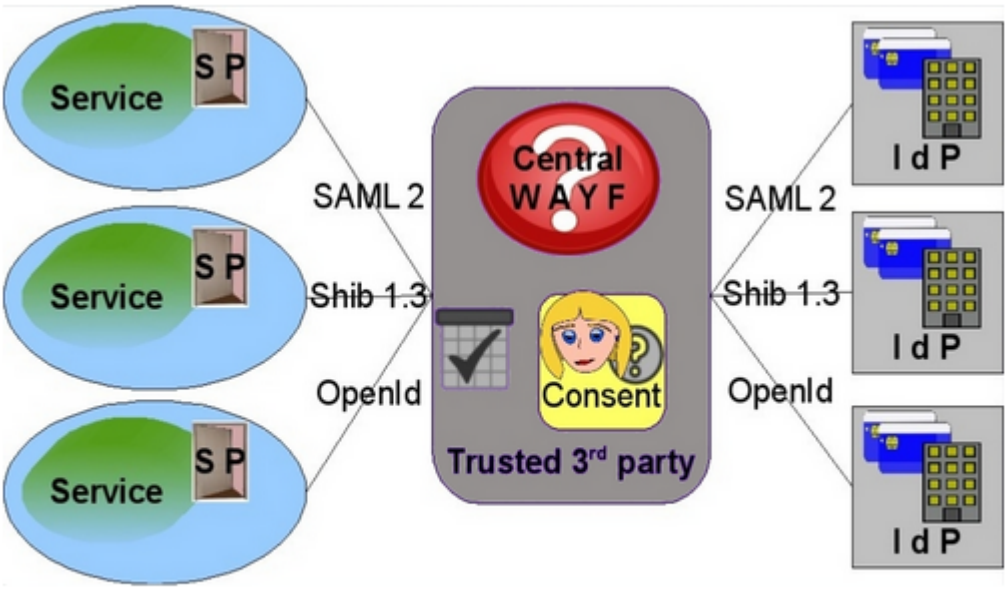
El proyecto inició en 2014 con una federación piloto llamada FIDMEX, estos primeros esfuerzos para construir una federación de identidades dieron lugar a la

creación de FENIX, cuyo objetivo es sumar a todas las universidades e instituciones de investigación mexicanas a la federación de identidad mexicana.

Para la construcción de la federación se utilizaron soluciones de software y estándares ya disponibles y adoptados por otras federaciones.

La creación de FENIX también incluyó el estudio, la propuesta, el análisis y la validación de políticas para el funcionamiento de la federación.

Estas políticas establecen los criterios para la adhesión de proveedores de identidad y de servicio a la federación.



La arquitectura será centralizada, tendrá un WAYF, los proveedores de servicios podrán ser implementados en las propias instituciones que forman la federación, o podrán ser desplegados por proveedores externos que sólo actuarán como proveedores de servicios.

Los proveedores de identidad serán implementados en las instituciones que forman la federación.

3.2.6 Términos en una federación

Los términos generales que se manejan en una federación son:

- ✓ IdP Proveedor de Identidad. Organización que provee la autenticación del usuario y devuelve los datos del usuario que el SP requiere para autorizar su acceso al recurso o servicio.
- ✓ SP Proveedor de Servicio. Cualquier organismo o institución registrado en la federación que provee acceso al usuario final a algún servicio y recurso basandose en una serie de atributos que satisfacen sus requerimientos de autorización.
- ✓ WAYF Cuando un SP está conectado a varios proveedores de identidad surge la necesidad de que el usuario seleccione en que entidad se desea identificar. A este proceso de identificar tu proveedor de identidad se le conoce como WAYF, que viene de las siglas Where Are You From.
- ✓ AA Autoridad de atributos. Sistema que responde consultas sobre atributos.
- ✓ Gestor de metadatos Elemento encargado de gestionar los diferentes metadatos de las entidades que componen la federación (IdPs y SPs). Dichos metadatos deberán de estar actualizados periódicamente. Además opcionalmente puede validar los metadatos, clasificarlos, validar los certificados de los metadatos o gestionar las ARPs.
- ✓ Scoping Indica al IdP el ámbito de la petición. De que SP surgió y con que contexto.
- ✓ Binding Mapeo de una petición SAML o de una aserción de respuesta con un protocolo específico de transporte. (Redirect, POST, Artifact or SOAP)
- ✓ Descubrimiento En términos de federación se hace referencia al descubrimiento como la acción de obtener la lista de proveedores de identidad.
- ✓ Metadatos Conjunto de datos que conforman la información necesaria para que una entidad se comunique con otra entidad de la federación. En el protocolo SAML distinguimos los metadatos de los IdPs y de los SPs.
- ✓ Entity ID Dentro de los metadatos de una entidad se define el entity id como el identificador que unívocamente al SP o IdP. La última tendencia es la de utilizar como entity id la url en la que se publican los metadatos de dicha entidad.
- ✓ ARP Política de liberación de atributos. Política que rige la distribución de los atributos del usuario a los diferentes SPs.
- ✓ Atributo Parte sencilla de los datos de un usuario (como por ejemplo el nombre, apellido, email, etc). Pueden ser generales o personales. Uno o la agrupación de varios atributos identifican unívocamente al usuario.
- ✓ Esquema de atributos Compendio de nombres de atributos estandarizados. Surge de la necesidad de definir un vocablo común que defina un nombre para los diferentes atributos que forman parte de la información del usuario que van a transferirse entre los elementos de la federación de identidades.

- ✓ Identificador opaco Identificador persistente que puede ser usado para conectar cuentas de usuario.
- ✓ Consentimiento En términos de federación se hace referencia al consentimiento como a la acción de que el usuario permita que los atributos que poseía un IdP sobre el se transfieran a un SP (cumpliendo la ARP y de forma segura).
- ✓ XML Encryption Un estandar W3C para cifrar un documento XML. Es usado en SAML para cifrar la Aserción SAML con el fin de dificultar que una entidad o individuo que no pertenezca a la federación pueda obtener los datos del usuario.
- ✓ XML Signature Un estandar W3C para firmar un documento XML. Es usado en SAML para autenticar al organismo que firmo el documento permitiendo establecer una relación de confianza.
- ✓ Profile Reglas que definen como integrar las aserciones SAML y como extraerlas de otros protocolos para poder habilitar el SSO y el SLO. Define también el flujo de peticiones y respuestas SAML que se efectúan en un determinado caso de uso.
- ✓ SSO Single Sign On. Procedimiento de autenticación que habilita al usuario para acceder a varios sistemas con una sola instancia de identificación. En una federación de identidades el SSO habilita al usuario a acceder a cada uno de los SP (previa autorización en el mismo) una vez se haya identificado en un IdP.
- ✓ SLO Single Log Out. Procedimiento por el cual el usuario deja de estar identificado en el conjunto de aplicaciones/elementos en los que estuviera logueado.

3.3 Preparando el servidor

Al finalizar esta actividad el participante contará con un equipo configurado con el sistema operativo Linux Debian, con Servidor Web Apapche e intérprete de PHP y MySQL, así como una Base de Datos para los usuarios que incluirá tres registros.

CONSIDERACIONES

Se utilizará un entorno Linux ya que las practicas considerarán este ambiente.

Todas las actividades están basadas en una distribución de Linux Debian Server, si dispone de otra distribución, deberá utilizar las instrucciones equivalentes cuando se requiera.

El equipo deberá disponer de una dirección IPv4 pública, pues para hacer algunas prácticas deberá ser accesible por el resto de los participantes.

Lo ideal para las prácticas es disponer de un dominio para el IdP y de un dominio para el SP, en donde se mencione “url”, se refiere al nombre de dominio asignado para su servidor (IdP o SP), si no dispone de un dominio asignado, utilice su dirección IP como tal.

En esta actividad se indican las tareas a realizar y no se explican a detalle las mismas ya que no es el objetivo de este curso, sin embargo, se pueden proporcionan referencias para actividades si el usuario lo solicita,

ACTIVIDAD

- Instale Linux Debian en el servidor que utilizará para su Proveedor de Servicio.
- Instale y configure el servidor Web Apache con interprete PHP y MySQL.
    - Asegúrese de que PHP es versión mayor a 5.2 (se recomienda 5.3).
    - Se requiere que estén instaladas las extensiones date, dom, hash, libxml, openssl, pcre, zlib, mcrypt
- Instale el módulo mod_ssl.
- Cree certificados para las aserciones encriptadas (Si ya dispone de certificados seguros para su servidor, puede utilizarlos).
    - **Lo ideal es que cuente con certificados firmados por una autoridad certificadora, si esto no fuera posible, genere certificados auto-firmados.**
    - Procedimiento para generar certificados auto-firmados
        - Vaya a una carpeta que ubique fácilmente y ejecute las siguientes instrucciones en la consola (guarde estos archivos ya que se utilizarán en la siguiente actividad):
        - openssl genrsa -out IP.key 1024
        - openssl req -new -key IP.key -out IP.csr
        - openssl x509 -req -days 1825 -in IP.csr -signkey IP.key -out IP.crt
        - **NOTA**: IP es el dominio de su servidor o la dirección IP.
- Agregue una Base de Datos a MySQL la cual será el origen de los usuarios a autenticar, la base de datos se deberá llamar Usuarios
    - Cree una tabla usuarios, en ella cree al menos los campos id, usuario, clave, nombre, apellidos, correo.
    - Agregue tres registros a su tabla.
- En la carpeta pública del servidor (/var/www/) cree un archivo info.php con el siguiente código:
    - <?php
    - phpinfo();
    - ?>
- Abra la página desde su navegador (http:/url/info.php) y verifique que las extensiones necesarias se encuentran presentes.

Una vez finalizados los pasos anteriores, ya dispondrá de un servidor correctamente configurado y listo para la instalación de **SimpleSAMLphp**.

3.4 Instalación de SimpleSAMLphp

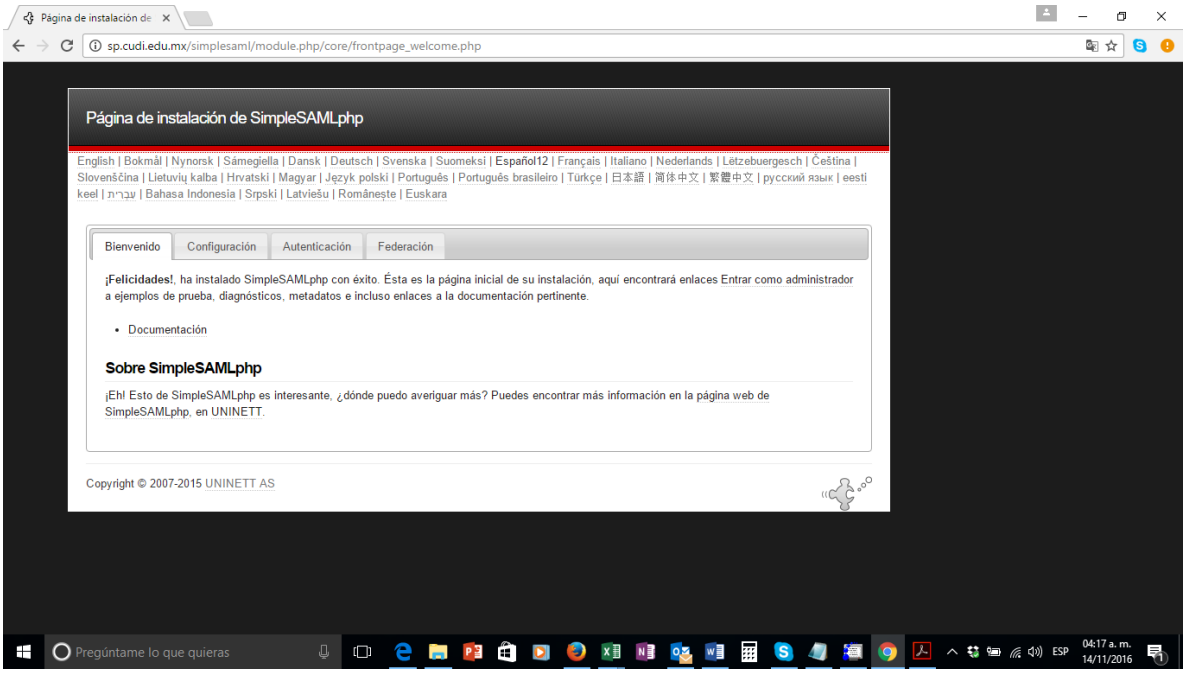
En esta actividad el participante realizará una instalación básica de SimpleSAMLphp en el servidor que utilizará como proveedor de servicio.

Esta actividad se llevará a cabo con la instalación del servidor que se hizo en la actividad anterior “Preparando el Servidor”.

ACTIVIDADES

- Ingrese a la página de SimpleSAMLphp y descargue en una carpeta en el servidor la última versión disponible.
- Una vez que haya descargada la última versión, descomprímala en la carpeta /var/
    - Desde consola:
        - **cd /var**
        - **tar xvzf simplesamlphp-1.x.y.tar.gz**
- Renombre la carpeta que acaba de crearse con la descompresión:
    - **mv simplesamlphp-1.x.y simplesamlphp**
- Configure apache para mostrar la página de SimpleSAMLphp
-
    - Edite el archivo **/etc/apache2/sites-available/default**
        - Agregue la línea " Alias /simplesaml /var/simplesamlphp/www" bajo la línea que dice DocumentRoot como se indica a continuación:
            - <VirtualHost *>
                - #agregar la siguiente línea bajo DocumentRoot (No importa la ubicación, pero facilita la localización y asegura que se coloque en la sección correcta)
                - **Alias /simplesaml /var/simplesamlphp/www**
            - </VirtualHost>
- Reinicie el servidor web apache
    - **service apache2 restart**
- Abra un navegador y teclee:
    - http://url/simplesaml
    - **NOTA:** Recuerde el url se refiere al nombre de dominio o a la dirección IP que tiene su servidor.

El resultado deberá ser parecido al de la siguiente imagen:



De ser así, ya dispone de SimpleSAMLphp instalado en su servidor.

¡Felicidades!

4. Módulo II

4.1 Desplegar un Proveedor de Servicio

4.1.1 Funcionamiento de un Proveedor de Servicio

Proveedor de Servicio (SP).

Un proveedor de servicios es un elemento de la federación que suministra servicios al usuario final.

De manera general, los proveedores de servicios no autentican usuarios, ellos envían la solicitud de autenticación a un proveedor de identidad, al que le delegan la decisión de autenticación.

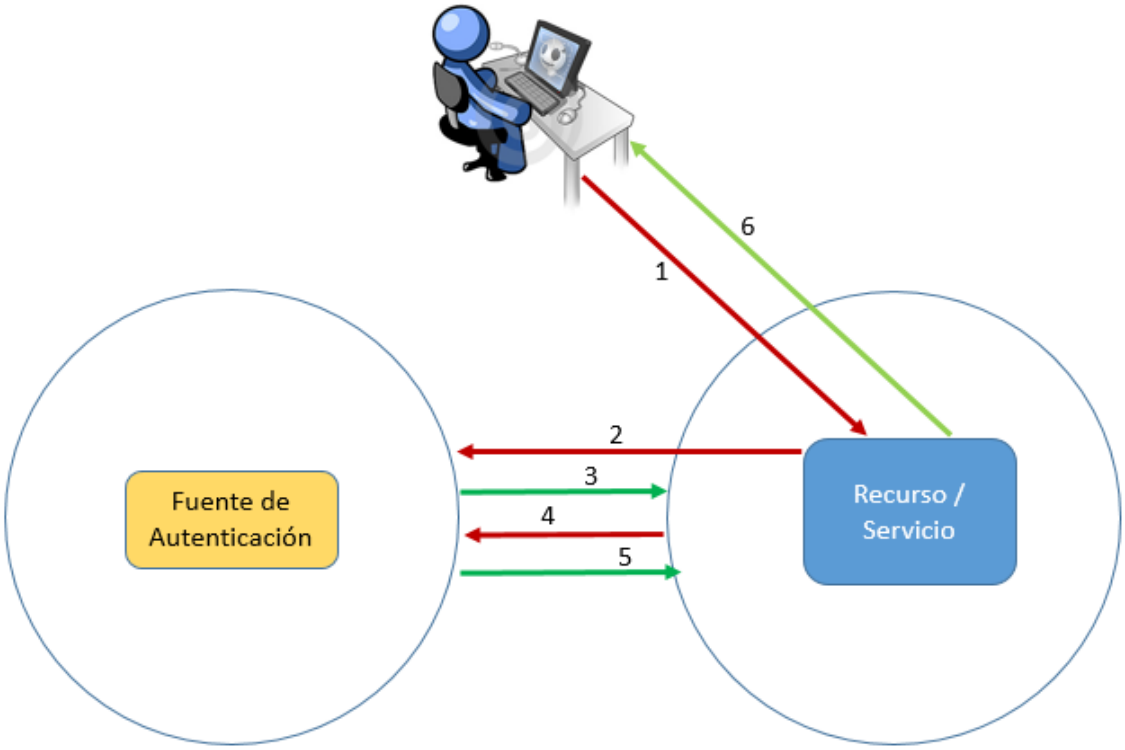
El proveedor de servicio es responsable de hacer la autorización del usuario de acceso al recurso a través de la autenticación y de los atributos que el proveedor de identidad proporcione.

El proceso de autorización y el acceso al recurso se lleva a cabo de la siguiente manera:

- ✓ El usuario solicita el acceso al recurso;

- ✓ El proveedor de servicios solicita que se autentique en el proveedor de identidad de su institución;
- ✓ El proveedor de identidades envía la respuesta testificando la autenticación del usuario;
- ✓ El proveedor de servicio envía una petición al proveedor de identidad solicitando sus atributos;
- ✓ El proveedor de identidades envía los atributos del usuario;
- ✓ Finalmente, el proveedor de servicio procesa la autorización sobre la base de los atributos del usuario y proporciona, el acceso al recurso.

En la siguiente figura se muestra el flujo mencionado anteriormente



4.1.2 Estructura de Carpetas de SimpleSAMLphp

Estructura Principal de SimpleSAMLphp

Una vez que se ha instalado SimpleSAMLphp la estructura principal de los directorios será:

|--cert Directorio donde se alojará el certificado y la clave que serán usados para firmar/cifrar las aserciones.

|--config Directorio donde se encuentran los archivos de configuración de simpleSAMLphp.

|--config-templates Directorio donde se encuentran las plantillas de los archivos de configuración.

|--metadata Directorio donde se guarda el archivo que contiene los metadatos del IdP local y donde se guardan los archivos con los metadatos de los IdP/SPs remotos en los que confiará simpleSAMLphp.

|--metadata-templates Directorio que contiene las plantillas de los archivos de metadatos.

|--modules Directorio con los diferentes módulos de simpleSAMLphp.

|--lib Directorio con las librerías de simpleSAMLphp.

|--www Directorio con la lógica web de simpleSAMLphp.

|--templates Directorio con las plantillas web de simpleSAMLphp.

|--dictionaries Directorio con las traducciones de simpleSAMLphp.

|--docs Directorio con documentación.

|--log Directorio donde alojar los logs de simpleSAMLphp (Requiere configurar el config.php para que se guarden aquí).

|--attributemap Directorio con los archivos con lógica para realizar el mapeo de atributos.

|--schemas Directorio con esquemas xsd.

|--bin Directorio con herramientas de scripts

Los archivos con los que se trabajarán en el Módulo II están en las carpetas: cert, config y metadata.

Además, se deberá dar al usuario de apache, permiso de escritura en las carpetas metadata y log.

4.1.3 Principales Puntos de Configuración y Actividades

Principales puntos de configuración de SimpleSAMLphp

Los archivos de configuración de simpleSAMLphp se localizan dentro de la carpeta config en la ruta donde se haya instalado simpleSAMLphp.

El primer archivo que se debe configurar en una instalación de SimpleSAMLphp es el archivo config.php.

Este archivo es de configuración general y se debe configurar independientemente que SimpleSAMLphp se vaya a utilizar como SP o como IdP.

Las partes básicas que debemos editar son:

- ✓ La contraseña de administrador

- ✓ El atributo “secretsalt”
- ✓ Datos de contacto
- ✓ Zona horaria

Actividad 1

Editar el archivo **config.php** ***(/var/simplesamlphp/config/)***

Establezca un password de administración, necesario para acceder a algunas partes de SimpleSAMLphp

- Busque la línea *'auth.adminpassword' => '12345',* y teclee un password para el administrador de SimpleSAMLphp.

Secretsalt, es una cadena aleatoria, algunas partes de SimpleSAMLphp necesitan esta cadena para generar “hashes” criptográficamente seguros. En el mismo archivo config.php se especifica un comando para generar uno.

- Busque la línea *'secretsalt' => ' '*, y agregue la cadena generada

Establezca la información de contacto técnico, esta se usará en la generación de los metadatos.

- Busque las líneas *'technicalcontact_name' => 'Andreas Åkre Solberg',* y *'technicalcontact_email' => 'andreas.solberg@uninett.no',* y ponga sus datos de contacto.

Especifique su zona horaria

- Busque la línea *'timezone'* (En el archivo config.php se ofrece una url para elegir la adecuada)

Una vez que verifique que los valores establecidos son los correctos, **guarde los cambios en el archivo**.

- Ya que ha establecido la configuración básica, abra un navegador y vaya a http://su.url.ip/simplesaml/.
- Entre como administrador (con la contraseña que colocó en el archivo de configuración), de click en la pestaña **“Configuración”** para confirmar que todas las dependencias necesarias estén cubiertas.

La pantalla debe ser algo similar a:

Verificación de su instalación de PHP

✓	Necesario	PHP Version >= 5.2. You run: 5.3.3
✓	Necesario	Hashing function
✓	Necesario	ZLib
✓	Necesario	OpenSSL
✓	Necesario	SimpleXML
✓	Necesario	XML DOM
✓	Necesario	RegEx support
✓	Necesario	MCrypt
✓	Opcional	MySQL support
✓	Necesario para LDAP	LDAP Extension
✓	Recomendado	technicalcontact_email option set
✓	Necesario	auth.adminpassword option set
✓	Recomendado	Magic Quotes should be turned off

Configuración del SP

SimpleSAMLphp ahora está funcionando, pero aún no le hemos definido cuál va a ser su función.

Para indicarle que funcionará como SP debemos editar el archivo **authsources.php (en la ruta /var/simplesaml/config/)**.

Aquí le indicaremos a SimpleSAMLphp que:

- Es un SP
- Que usará los certificados *mi_certificado.pem y mi_certiicado.key*
- Su identificador interno será *http://su.url.ip/simplesaml/*.
- En este archivo se configuran las fuentes de autenticación cuando SimpleSAMLphp actuará como Proveedor de Identidad, pero en el caso de un Proveedor de Servicio, no necesitará fuentes de autenticación directa.
- **Actividad 2**
- Copie en la carpeta */var/simplesaml/cert* los certificados creados en la actividad **"Preparando el servidor"**.
- Edite el archivo **authsources.php** *(/var/simplesamlphp/config/authsources.php)*
- Elimine el contenido del archivo y en su lugar pegue el siguiente código:
- *<?php*
- *$config = array(*
- *// This is a authentication source which handles admin authentication.*
- *'admin' => array(*
- *// The default is to use core:AdminPassword, but it can be replaced with*
- *// any authentication source.*
- *'core:AdminPassword',*
- *),*
- *// An authentication source which can authenticate against both SAML 2.0*
- *// and Shibboleth 1.3 IdPs.*
- *'default-sp' => array(*

- *'saml:SP',*
- *// The entity ID of this SP.*
- *// Can be NULL/unset, in which case an entity ID is generated based on the metadata URL.*
- *'entityID' => NULL,*
- *// The entity ID of the IdP this should SP should contact.*
- *// Can be NULL/unset, in which case the user will be shown a list of available IdPs.*
- *'idp' => NULL,*
- *// The URL to the discovery service.*
- *// Can be NULL/unset, in which case a builtin discovery service will be used.*
- *'discoURL' => NULL,*
- *),*
- *);*
-
- Asigne un valor al atributo entityID, (ej http://148.202.106.68), esto es solo para darle una identidad única, ya que será el índice de los metadatos a compartir y debe corresponder con la URL de este SP.
- *'entityID' => http://sp.cudi.edu.mx,*
- Agregue el nombre que le dio a su certificado, en las líneas certificate y privatekey (que corresponden a los certificados de su servidor), son las dos partes (pública y privada) del certificado usado en el SP.
- Como se mencionó estos archivos deben estar en el directorio **cert** de la instalación de simpleSAMLphp.
- *'certificate' => 'url.crt',*
- *'privatekey' => url.key',*
- El archivo debe quedar parecido a al siguiente (Se muestra en negrita lo modificado y agregado):
- *$config = array(*
- *// This is a authentication source which handles admin authentication.*
- *'admin' => array(*
- *// The default is to use core:AdminPassword, but it can be replaced with*
- *// any authentication source.*
- *'core:AdminPassword',*
- *),*
-
- *// An authentication source which can authenticate against both SAML 2.0*
- *// and Shibboleth 1.3 IdPs.*
- *'default-sp' => array(*
- *'saml:SP',*
- *// The entity ID of this SP.*
- *// Can be NULL/unset, in which case an entity ID is generated based on the metadata URL.*
- *'entityID' => **'http://sp.cudi.edu.mx'**,*
- *'certificate' => **'148.202.106.68.crt'**,*
- *'privatekey' => **'148.202.106.68.key'**,*
- *// The entity ID of the IdP this should SP should contact.*
- *// Can be NULL/unset, in which case the user will be shown a list of available IdPs.*
- *'idp' => 'NULL',*
- *// The URL to the discovery service.*
- *// Can be NULL/unset, in which case a builtin discovery service will be used.*
- *//'discoURL' => 'http://148.202.106.109/simplesaml',*
- *'discoURL' => NULL,*
- *),*

- *);*
- Una vez terminado, subir la captura de pantalla del archivo **authsource.php**
- _____
- _____

Metadatos del SP

Ahora ya estamos listos para obtener los metadatos de su SP y probar que la configuración de SimpleSAMLphp como Proveedor de Servicio funciona correctamente.
Obtenga los metadatos de su SP

- **Actividad 3**
- Abra el navegador en la dirección local ***http://url/simplesaml/***
- Haga clic en la pestaña **Federación**
- En la sección SAML2.0 SP Metadata haga clic en el enlace Ver Metadatos
- Copie los datos de la segunda sección (la que se indica en la imagen).

Metadatos

en formato xml de metadatos SAML 2.0:

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="http://pruebas.sined.mx">
  <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>MIICFzCCAYACCQCgVVdxMsr9XzANBgkqhkiG9w0BAQUFADBQMQswCQYDVQQGEwJNWDEPMA0GA1UECBMGTUVYSUNPMRAwDgYDV
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:KeyDescriptor use="encryption">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>MIICFzCCAYACCQCgVVdxMsr9XzANBgkqhkiG9w0BAQUFADBQMQswCQYDVQQGEwJNWDEPMA0GA1UECBMGTUVYSUNPMRAwDgYDV
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="http://200.66.101.16/simples
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="http://200.66.101.16/simple
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:1.0:profiles:browser-post" Location="http://200.66.101.16/sim
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" Location="http://200.66.101.16/si
    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:1.0:profiles:artifact-01" Location="http://200.66.101.16/simp
  </md:SPSSODescriptor>
  <md:ContactPerson contactType="technical">
    <md:GivenName>Administrator</md:GivenName>
    <md:EmailAddress>pruebas@sined.mx</md:EmailAddress>
  </md:ContactPerson>
</md:EntityDescriptor>
```

en un fichero de formato simpleSAMLphp - utilice esta opción si está usando una entidad simpleSAMLphp en el otro extremo:

```
$metadata['http://pruebas.sined.mx'] = array (
  'AssertionConsumerService' => 'http://200.66.101.16/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp',
  'SingleLogoutService' => 'http://200.66.101.16/simplesaml/module.php/saml/sp/saml2-logout.php/default-sp',
  'certData' => 'MIICFzCCAYACCQCgVVdxMsr9XzANBgkqhkiG9w0BAQUFADBQMQswCQYDVQQGEwJNWDEPMA0GA1UECBMGTUVYSUNPMRAwDgYDVQQHEwdNRVRFUE
);
```

Los metadatos que obtendrá serán algo como:

$metadata['http://sp.cudi.edu.mx'] = array (

'AssertionConsumerService' => 'http://200.66.101.16/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp',

```
'SingleLogoutService' => 'http://200.66.101.16/simplesaml/module.php/saml/sp/saml2-logout.php/default-sp',

'certData' => 'zCCAYACCQCgVVdxMsr9XzANBgkqhkiG9w0BAQUFADBQMQswCQYDVQQGEwJNWDEPMA0GA1UE',

);
```

4.2 Desplegar un Proveedor de Identidad

4.2.1 Funcionamiento de un Proveedor de Identidad

Proveedor de Identidad (IdP)

Un proveedor de identidad es responsable de proporcionar la autenticación y los atributos de un usuario, para que el proveedor de servicio pueda realizar la autorización de acceso al recurso solicitado.

Un proveedor de identidad no autoriza el acceso a un recurso, sólo confirma que el usuario es quien dice ser y envía los atributos, previamente acordados, con el proveedor de servicio.

El proceso de autenticación y la entrega de atributos se lleva a cabo de la siguiente manera:

El usuario solicita acceso al recurso.

Se le pide seleccionar su Proveedor de Identidad

El usuario selecciona su Proveedor de identidad

Es dirigido hacia su Proveedor de Identidad y se le solicita sus credenciales.

El usuario introduce sus credenciales

El Proveedor de Identidad verifica los datos que el usuario proporcionó.

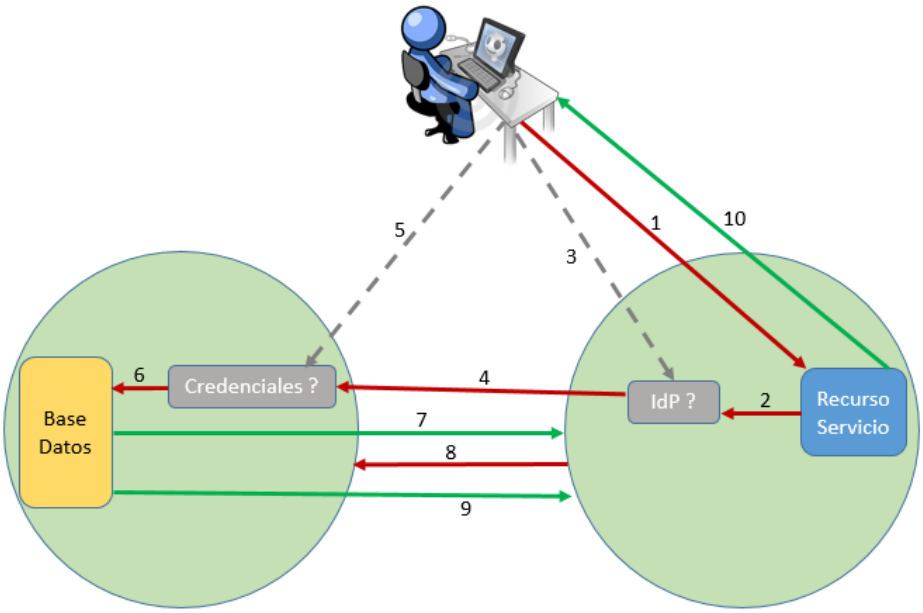
El Proveedor de Identidad envía un identificador del usuario al Proveedor de Servicio certificando que el usuario fue autenticado.

El Proveedor de Servicio utilizando este identificador le solicita el Proveedor de Identidad, la entrega de atributos referentes al usuario.

Finalmente, el Proveedor de Identidad envía estos atributos al proveedor de servicio.

El Proveedor de Servicio autoriza el uso del recurso solicitado.

La figura siguiente, ilustra de forma general el flujo hacia un Proveedor de Identidad



4.2.2 Instalación y Principales Puntos de Configuración de IdP

La instalación básica para un proveedor de identidad es la misma que se realiza para un proveedor de servicio.

Actividad 1 (Instalación y configuración básica)

- Instale SimpleSAMLphp en el servidor para el Proveedor de Identidad, siguiendo las instrucciones del Módulo I en la Actividad *"Instalación de SimpleSAMLphp"*.
- Realice la configuración básica como se hizo en el Módulo II, en la Actividad 1, del tema *"Principales Puntos de Configuración de SimpleSAMLphp"*.
- Asegurarse que esté instalado MySQL, que se haya creado la base de datos y la tabla con los campos necesarios, de acuerdo a las instrucciones descritas en el Módulo I, en la Actividad del tema *"Preparando el servidor"*.

Configuración como IdP

Una vez que SimpleSAMLphp está funcionando y con la configuración básica, debemos decirle que su función será como proveedor de identidad.

Para esto, debemos editar los siguientes archivos:

- ✓ config.php – Indicaremos que SimpleSAMLphp actuará como proveedor de identidad.
- ✓ authsources.php – Indicaremos cual será nuestro origen de datos, de acuerdo a donde se encuentren almacenados los datos de nuestros usuarios, (Ldap, MySQL, Yubikey, Openid, etc..).

- ✓ SimpleSAMLphp puede conectar con diferentes fuentes de datos, existe una plantilla del archivo authsources.php que se encuentra en la carpeta simplesaml/config-templates en donde vienen ejemplos de cómo conectar con diferentes orígenes de datos.

Actividad 2 (Definir el origen de datos)

- Edite el archivo ***config.php*** (simplesaml/config/config.php)
- Busque la línea *"'enable.saml20-idp'"* y cambie el valor a ***true***
- Guarde los cambios

Origen de Datos

En este paso se utilizaremos la base de datos creada anteriormente, y esta será nuestro origen de los usuarios que serán autenticados por este IdP

Agregue el siguiente código dentro del ***array $config*** ya existente

Edite el archivo **authsources.php** (*simplesaml/config/authsources.php*)

Dentro el **array $config** ya existente, agregue lo siguiente:

```
'IdP_Institucion' => array(
    'sqlauth:SQL',
    'dsn' => 'mysql:host=localhost;dbname=Usuarios',
    'usuario' => 'simplesaml',
    'clave' => 'secretpassword',
    'query' => 'SELECT nombre as uNombre, apellidos as uApellidos, correo as uCorreo FROM usuarios WHERE usuario = :usuario AND clave= :password',
),
```

Donde dice **'IdP_Institucion'** sustituya *institución* por las siglas de su institución ej. '**IdP_CUDI**'

Modifique los valores correspondientes al *host, base de datos y la sentencia de consulta* (si los campos de su tabla o el nombre de la tabla es distinto).

Al terminar el archivo ***authsources.php*** deberá verse similar a:

```
<?php
$config = array(
    'IDP' => array(
    'sqlauth:SQL',
    'dsn' => 'mysql:host=localhost;dbname=Usuarios',
    'usuario' => 'simplesaml',
```

```
'clave' => 'secretpassword',

'query' => 'SELECT nombre as uNombre, correo as uCorreo FROM usuarios WHERE correo = :username AND clave = :password',

),

// The entity ID of this SP.

 // Can be NULL/unset, in which case an entity ID is generated based on the metadata URL.

'default-sp' => array(

'saml:SP',

// The entity ID of this SP.

// Can be NULL/unset, in which case an entity ID is generated based on the metadata URL.

'entityID' => NULL,

// The entity ID of the IdP this should SP should contact.

// Can be NULL/unset, in which case the user will be shown a list of available IdPs.

'idp' => NULL,

// The URL to the discovery service.

// Can be NULL/unset, in which case a builtin discovery service will be used.

'discoURL' => NULL,

),

);
```

Una vez terminado lo anterior vaya a la página principal de su SimpleSAMLphp en el servidor de IdP.

http://Su_URL/simplesaml/

Seleccione la pestaña **Autenticación**.

Seleccione "*Probar las fuentes para la autentificación ya configuradas*".

Elija **IdP_Institucion** (Debe aparecer el nombre que puso en el archivo **authsource.php**

Ingrese un usuario y contraseña que exista en la base de datos.

Si los datos son correctos, le mostrará una pantalla con los atributos devueltos por su IdP.

Suba en el Foro del Módulo II la pantalla de captura con los atributos devueltos por su IdP

Nota: Algunos de los errores más comunes suelen ser:

- Comillas mal balanceadas
- Error en la sentencia Sql
- Error en el usuario y contraseña tecleados

4.2.3 Metadatos del IdP

Preparando los metadatos del IdP

Una vez instalado y configurado SimpleSAMLphp como Proveedor de Identidad, debemos configurar los metadatos que se intercambiarán con los Proveedor de Servicios con los que establecerá una relación de confianza..

Los metadatos del servidor, se configuran en el archivo saml20-idp-hosted.php y como regla deberíamos generar este índice en un URL específico.

Actividad 1 (Configurando los metadatos)

- Edite el archivo **saml20-idp-hosted.php** (/var/simplesamlphp/metadata/saml20-idp-hosted.php)
- Busque la línea que dice *"__DYNAMIC:1__"* y cambie el índice de los metadatos a la URL de su servidor.

  Como se mencionó previamente, debería ser distinta del URL de su IdP, para efectos de esta práctica, puede quedar la URL de su servidor + "idp/", ej. http://su_URL/idp/.

- Modifique el parámetro *"host"* por la URL de su servidor (recomendado).
- Agregue los certificados correspondientes en *"privatekey" y "certificate"*
- Agregue el origen de datos que usará el IDP (en este caso, el origen que se configuro lo llamamos "*IdP_Institucion*" por lo que quedaría: *'auth' => 'IdP_Institucion'*)

Al finalizar el archivo deberá ser similar a lo siguiente:

```
<?php
/**
* SAML 2.0 IdP configuration for simpleSAMLphp.
*
*/
    $metadata['http://su_URL/idp/'] = array(
    /*
    * The hostname of the server (VHOST) that will use this SAML entity.
    *
    * Can be '__DEFAULT__', to use this entry by default.
    */
    'host' => '__DEFAULT__',
    /* X.509 key and certificate. Relative to the cert directory. */
    'privatekey' => '200.66.101.16.key',
```

```
'certificate' => '200.66.101.16.crt',
/*
* Authentication source to use. Must be one that is configured in
* 'config/authsources.php'.
 */
'auth' => 'IdP_Institucion',
// Respuestas de inicio y fin de sesión deberán estar firmadas
'redirect.sign' => TRUE,
// Todas las comunicaciones encriptadas
'assertion.encryption' => TRUE,
'saml20.sendartifact' => TRUE,
);
```

Obtener los metadatos de su IDP

Vaya a la página principal de su SimpleSAMLphp

http://su_URL/simplesaml

Seleccione la pestaña **Federación**

Haga clic en *ver metadatos* de la sección *"Metadatos IdP SAML 2.0"*

Al igual que en el **SP**, el texto de la segunda sección es la que debe proporcionar a los servicios para establecer la relación de confianza.

4.3 Aplicación de Prueba

Para esta actividad utilizaremos una aplicación demostrativa, la cual no tiene funcionamiento, pero nos servirá para mostrar los atributos de quien se autentica.

Con esto se pretende demostrar cómo se puede tener acceso a una aplicación autenticando al usuario en la institución de origen.

Los archivos que componen la aplicación y su descripción es:

- ✓ config_saml.php – Contiene las variables y valores globales utilizados por la aplicación.
- ✓ index.php – Es el archivo que se mostrará cuando el usuario ingrese al dominio/ip del SP antes de autenticarse, este archivo estará en la carpeta publica del sitio web, ej. /var/www/
- ✓ login.php – Archivo de inicio de sesión, fuerza al usuario a seleccionar el IdP donde será autenticado.
- ✓ logout.php – Finaliza la sesión

- ✓ aplicación.php – Es el archivo al que se le dirigirá al usuario una vez que se haya autenticado, este archivo estará en una distinta de la carpeta pública ej. /var/www/privada/, sólo se muestra si el usuario está autenticado, si no es así, lo manda al index.php de la carpeta pública.

Actividad 1

- Inicie sesión en la plataforma de colaboración CUDI e ingrese al espacio del curso FENIX
- En la barra de herramientas del lado derecho, de click en Recursos, entre a la carpeta que dice Modulo III y descargue el archivo que se llama aplicación.zip
  - Para descargar:
    - Dar click en el nombre del archivo, o
    - Copie y pegue en su navegador la siguiente dirección *http://virtual.cudi.edu.mx/x/dwuyjK*
- Cargue el archivo en su servidor de SP y descomprímalo en la carpeta /var/www/
- La estructura debe quedar como sigue:

- Edite el archivo **index.php** (*/var/www/index.php*)
- Busque la línea que dice *"echo "<META HTTP-EQUIV=REFRESH CONTENT=0;URL=http://su_URL/privada/aplicacion.php>"*;
- Cambie "**su_URL**" por la **URL/IP** de su servidor SP
- Guarde el archivo

- Edite el archivo **config_saml.php** (*/var/www/index.php*)
- Busque la línea que dice *"$SP_URL = 'http://su_URL'; // url de nuestro servidor*.
- Cambie "**su_URL**" por la **URL/IP** de su servidor SP
- Guarde el archivo

- Abra un navegador y teclee la URL/IP de su servidor ej *http://sp.cudi.edu.mx/*
- Se debe mostrar una pagina que contiene sólo un botón que dice "Ir a la Aplicación"

Para que el botón tenga funcionamiento deberemos realizar el intercambio de metadatos entre el IdP y el SP

5 Conclusiones

En este curso se ha desarrollado los siguientes elementos que constituyen los componentes básicos de los entornos federados.

A través de este trabajo se le proporciona al participante, un panorama general de las Federaciones de Identidades, sus beneficios, y los conocimientos básicos para realizar un despliegue en su institución.