

Ficha Técnica del Curso

Federación de Identidades Para Instituciones de Educación e Investigación

Entregable: WP2-8.1

Fernando Aranda Escobar



2016

Curso: Federación de Identidades para Instituciones de Educación e Investigación

Presentación:

Este documento integra los recursos elaborados para capacitar al personal técnico de las instituciones que participan en el proyecto MAGIC, acerca de los Entornos Federados y su integración en una Federación.

El curso está estructurado en 3 módulos, que permitirán a los participantes la creación de un Proveedor de Identidad, un Proveedor de Servicio y un Servicio Básico Federado.

Propósito del Taller:

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

Dirigido a:

Al personal técnico de las áreas de TI de las instituciones miembros CUDI que participan en el Proyecto MAGIC y que estarán a cargo de la operación y administración de los servidores y servicios federados.

Objetivo de Aprendizaje:

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

Descripción:

El curso está elaborado y diseñado de manera que al final del mismo, los participantes puedan tener el conocimiento sobre los entornos federados, los conceptos y fundamentos de una Federación de Identidades, comprendiendo las ventajas e importancia que tienen estos entornos para el desarrollo de la educación e investigación colaborativa en las Instituciones de Educación Superior e Investigación.

Los participantes desarrollarán las competencias que les permitan realizar la implementación de un Proveedor de Identidad (IdP) desarrollado a través de SimpleSAMLphp, aplicación que escrita en el lenguaje de programación PHP que se ocupa para la autenticación, la cual tiene una gran base de usuarios instalada en todo el mundo.

El enfoque principal de SimpleSAMLphp es proporcionar soporte para el protocolo SAML 2.0 como Proveedor de Identidad o Proveedor de Servicio, sin embargo también es compatible con otros protocolos de autenticación, como Shibboleth, OpenID, OAuth, etc. SimpleSAMLphp se encuentra instalado en un gran número de Federaciones de Identidad en el mundo.

El Proveedor de Identidad desarrollado en el curso, se conectará a una base de datos en MySQL para la autenticación de usuarios, sin embargo, SimpleSAMLphp permite conectar a diferentes fuentes de autenticación como LDAP, SQLServer, Google, etc., lo que permitirá a los participantes adecuar la instalación a la fuente de autenticación que utilicen en su institución.

Los participantes también adquirirán los conocimientos necesarios para implementar un Proveedor de Servicio con la misma aplicación de SimpleSAMLphp, y comprenderán como se realiza la autorización para utilizar un servicio federado, de acuerdo a los atributos que el Proveedor de Identidad le proporcione.

Así mismo, los participantes desarrollarán una aplicación sencilla en el lenguaje de programación PHP, que se utilizará como ejemplo de un servicio federado, esta aplicación, tendrá las fases de:

Inicio – Cuando la aplicación se encuentra disponible en el catálogo de aplicaciones en una institución.

Autenticación – Cuando un usuario selecciona la aplicación y esta, a través del Proveedor de Servicio, envía la petición de autenticación al Proveedor de Identidad.

Autorización – Cuando el Proveedor de Identidad le responde y envía los atributos del usuario al Proveedor de Servicio y de acuerdo a estos atributos el Proveedor de Servicio decide la autorización (o no) del usuario para hacer uso del servicio que solicitó.

Al terminar el curso, los participantes comprenderán como es que interactúa el Proveedor de Identidad, el Proveedor de Servicio y las aplicaciones en un ambiente federado, así como, cuáles son los requerimientos para interactuar en una Federación de Identidades.

Temario:

Los objetivos específicos a alcanzar en cada unidad temática son:

Módulo I: Introducción a los entornos federados en ambientes educativos.

- El participante se introducirá en el concepto de entorno federado de los ambientes educativos, conocerá que son las federaciones de identidades, verá ejemplos de varias de ellas, así también, entenderá los beneficios que pueden obtener y muestra algunos ejemplos de los servicios que se pueden federar en las instituciones educativas.

Módulo II: Instalación y despliegue de un IdP, SP y Servicio

- El participante instalará y desplegará un proveedor de identidad, un proveedor de servicio y un servicio de prueba, utilizando el protocolo SAML 2.0 mediante la aplicación SimpleSAMLphp

Módulo III: Fuentes de autenticación e intercambio de metadatos

- 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.
- Conocerá como intercambiar metadatos de su proveedor de identidad con la Federación Nacional de Identidades Mexicana (FENIX).

Estructura y Contenidos:

El curso incluye guías de instalación y configuración del servicio, así como algunos gráficos.

Módulo I. Introducción a los entornos federados en ambientes educativos

- I. ¿Qué es una federación?
- II. Elementos de una federación
- III. Interacción entre los elementos de una federación
- IV. Ejemplos de federaciones académicas
- V. FENIX
- VI. Términos en una federación

Unidad II. Servidor RADIUS LOCAL (1 DIA- 6 horas)

- I. Desplegar un Proveedor de Servicio
- II. Desplegar un Proveedor de Identidad
- III. Aplicación de Prueba

Unidad III. Fuentes de autenticación e intercambio de metadatos

- I. Metadatos
- II. Interactuando con otros IdP's

Modalidad:

En línea con soporte en la plataforma de colaboración CUDI (<http://virtual.cudi.edu.mx>)

Los participantes contarán con la participación del asesor en el horario de 09:00-19:00 horas.

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.

Duración:

La duración del curso es de 38 Hrs. para los tres módulos.

El participante deberá cursar un módulo por semana, las actividades de cada módulo tendrán la siguiente duración aproximada:

Módulo I (10 Horas)

Módulo II (14 Horas)

Módulo III (14 Horas)

Pre requisitos y Requerimientos de Equipo:

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

Cupo:

Abierto a inscripción, sin límite de participantes.

Inicio:

10 de Octubre de 2016

Instructores:

Fernando Aranda Escobar – Coordinador de Grupo Técnico de Federación de Identidades CUDI

Juan Gabriel Cruz Pérez – Director del Departamento de Tecnologías de Información de la Universidad de Colima

Carlos González – Responsable Técnico de Red Clara

Evaluación y Reconocimiento:

La evaluación se hará de acuerdo al 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), y se entregará una vez que el curso termine y los participantes tengan el porcentaje de actividades evaluado.