



Consejo Nacional de Ciencia y Tecnología
"CONACyT"
Fondo de Cooperación Internacional en Ciencia y Tecnología
"FONCICYT"

Unión Europea Programa Horizonte 2020
Comisión Europea
Dirección General para las Redes de Comunicación, Contenido y Tecnología
e-Infraestructura



Magic

Middleware for collaborative Applications
and Global virtual Communities

Entregable WP2-7

Informe Curso en línea de Federación de Identidad para Instituciones de Educación e Investigación Plataforma Virtual - CUDI

Reporte de Progreso

Entregable MAGIC:MAGIC_D2.3_On_line_Training_Material_on_AAI_develop_for_Staff_training)

Nombre completo del Documento	Curso en línea de Federación de Identidad para Instituciones de Educación e Investigación Plataforma Virtual – CUDI
Fecha	09-01-2017
Actividad	Curso en Línea
Responsable del WP	Fernando Aranda Escobar
Estatus del Documento	Final
Atributos	Público

Resumen: Dentro del marco de trabajo del Proyecto MAGIC y como parte de las actividades del WP2 se ha llevado a cabo un curso en línea sobre entornos federados en instituciones de educación e investigación, el cual tiene como objetivo principal capacitar al personal del área de Tecnologías de la Información de las instituciones que participan en el proyecto MAGIC.

El curso está compuesto de tres módulos, que integran los conceptos teóricos sobre federación de identidades y los refuerza con una serie de prácticas que llevan al participante a realizar la instalación de un Proveedor de Identidad, un Proveedor de Servicio y a federar un servicio básico.

Obteniendo con esto los conocimientos suficientes para identificar cuáles son los procesos necesarios para implementar servicios federados en su institución, y poder agregar estos a la Federación Nacional de Identidades Mexicana.

AVISO DE COPYRIGHT:

Copyright © Miembros del Convenio FONCICYT-CUDI, Proyecto Apoyado por el FONCICYT, Agosto 2015.

MAGIC (Middleware for collaborative Applications and Global vIrtual Communities – Proyecto número: 654225) es un proyecto co-financiado por la Comisión Europea, dentro del Programa Horizonte 2020 (H2020), Dirección General para Redes de Comunicación, Contenidos y Tecnología – e-Infraestructura. MAGIC inició el 1° de Mayo 2015 y tiene una duración de 24 meses.

La Corporación Universitaria para el Desarrollo de Internet, A. C. participa como socio en el proyecto MAGIC, financiado por el Fondo de Cooperación Internacional en Ciencia y Tecnología (FONCICYT), a través del Consejo Nacional de Ciencia y Tecnología (CONACYT) – Proyecto número 245557.

Para mayor información acerca del Proyecto MAGIC, sus socios y contribuciones accede a: <http://www.magic-project.eu>.

Está permitida la copia y distribución, copias literales de este documento que contiene este aviso de copyright con fines no lucrativos. Esto incluye el derecho a copiar este documento en su totalidad o en parte en otros documentos, pero sin modificaciones, adjuntando la siguiente referencia a los elementos copiados: "Copyright © Miembros del Convenio FONCICYT-CUDI, Proyecto apoyado por el FONCICYT, Agosto 2015.

El uso de este documento, en la forma y/o para fines no previstos en el párrafo anterior, requiere la previa autorización escrita de los titulares del copyright.

La información contenida en éste documento representa la opinión de los titulares de los derechos a partir de la fecha en que se publicaron esas opiniones.

LA INFORMACIÓN CONTENIDA EN ESTE DOCUMENTO ES PROPORCIONADA POR LOS PROPIETARIOS DEL COPYRIGHT "TAL COMO ESTÁ" Y TODA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, PERO NO LIMITADO A, LAS GARANTÍAS DE COMERCIALIZACIÓN Y ACONDICIONADAS PARA UN PROPÓSITO PARTICULAR SON RECHAZADAS. EN NINGÚN CASO, LOS MIEMBROS DEL CONVENIO FONCICYT-CUDI, INCLUIDOS LOS PROPIETARIOS DEL COPYRIGHT, O FONCICYT O CUDI, SE HACEN RESPONSABLES POR NINGÚN DAÑO DIRECTO, INDIRECTO, INCIDENTAL, ESPECIAL, EJEMPLAR O CONSECUENTE (INCLUYENDO, PERO NO LIMITADO A LA SUSTITUCIÓN DE BIENES O SERVICIOS; LA PÉRDIDA DE USO, DE DATOS O BENEFICIOS; O LA INTERRUPCIÓN DEL NEGOCIO) INDEPENDIEMENTE DE SU CAUSA Y DE CUALQUIER TEORÍA DE RESPONSABILIDAD, YA SEA POR CONTRATO, RESPONSABILIDAD ESTRICTA O AGRAVIO (INCLUYENDO NEGLIGENCIA) DERIVADO DE CUALQUIER FORMA DEL USO DE LA INFORMACIÓN CONTENIDA EN ESTE DOCUMENTO, INCLUSO SI SE HA ADVERTIDO DE LA POSIBILIDAD DE TALES DAÑOS.

RUTA DEL ENTREGABLE

	Nombre	Institución / WP-Actividad	Fecha	Responsable
De	Fernando Aranda	CUDI/WP2 Infraestructura de Autenticación y Autorización	Enero 9, 2017	Fernando Aranda
Revisado por				
Aprobado por				

TABLA DE CONTENIDOS

AVISO de COPYRIGHT:	3
Ruta del entregable	4
1. Introducción.....	¡Error! Marcador no definido.
2. Referencias	¡Error! Marcador no definido.
3. Proceso de enmienda de Documento	¡Error! Marcador no definido.
4. Glosario	¡Error! Marcador no definido.
5. Resumen Ejecutivo	¡Error! Marcador no definido.
6. Desarrollo del Documento.....	¡Error! Marcador no definido.
6.1. Datos Generales.....	8
6.2. Objetivo	11
6.3. Desglose de Actividades	11
6.4. Resultados Obtenidos, Beneficios.....	15
7. Próximos Pasos	¡Error! Marcador no definido.
8. Conclusión.....	¡Error! Marcador no definido.

1. INTRODUCCIÓN

El propósito de este documento es dar un informe de las actividades realizadas en el curso en línea sobre los Entornos Federados en Las Instituciones de Educación e Investigación, llevado a cabo en octubre y noviembre de 2016, a través de la plataforma virtual de CUDI.

Este curso permitió al personal del área de Tecnologías de la Información de las instituciones participantes obtener los conocimientos básicos sobre la Federación de Identidades y desarrollar las bases para establecer pilotos que ayuden a federar servicios de una manera ágil y segura.

2. REFERENCIAS

- [R1] Sitio Web MAGIC <http://www.magic-project.eu>
[R2] Sitio Web CUDI <http://www.cudi.edu.mx>
[R3] Sitio Web Fenix <http://www.fenix.org.mx>
[R4] Sitio Web eduGAIN https://www.geant.org/Services/Trust_identity_and_security/eduGAIN

3. PROCESO DE ENMIENDA DE DOCUMENTO

Las solicitudes de enmiendas a este documento se deberán hacer al autor (Fernando Aranda Escobar, WP2 Infraestructura de Autenticación y Autorización (AAI), faranda@cudi.edu.mx), con copia al Administrador del proyecto MAGIC (María del Rocío Cos Murillo, rcos@cudi.edu.mx)

4. GLOSARIO

AAI	Authentication and Authorization Infrastructure (Infraestructura de Autorización y Autenticación)
CICESE	Centro de Investigación Científica y de Educación Superior de Ensenada
CINVESTAV	Centro de Investigación y de Estudios Avanzados del instituto Politécnico Nacional
CONACYT	Consejo Nacional de Ciencia y Tecnología
CUDI	Corporación Universitaria para el Desarrollo de Internet, A.C.
EC	European Commission
EU	European Union
EU-LAC	Europe, Latin America and the Caribbean
FENIX	FEderación Nacional de Identidades meXicana

FONCICYT	Fondo de Cooperación Internacional en Ciencia y Tecnología
IdP	Proveedor de Identidad (IdP por sus siglas en inglés)
ITESM	Instituto Tecnológico y de Estudios Superiores de Monterrey
LDAP	Protocolo Ligero de Acceso a Directorios (LDAP por sus siglas en inglés)
RedCLARA	Colaboración Latinoamericana de Redes Avanzadas
REMERI	Red Mexicana de Repositorios Institucionales
SP	Proveedor de Servicio (SP por sus siglas en inglés)
UADY	Universidad Autónoma de Yucatán
UAM	Universidad Autónoma Metropolitana
UDG	Universidad de Guadalajara
UGTO	Universidad de Guanajuato
UNAM	Universidad Nacional Autónoma de México
UV	Universidad Veracruzana
WP	Paquete de Trabajo (WP por sus siglas en inglés)

5. RESUMEN EJECUTIVO

MAGIC (Middleware for collaborative Applications and Global vrtual Communities) es un proyecto financiado por la Comisión Europea, dentro del Programa Horizonte H2020, y tiene como uno de sus objetivos el facilitar la movilidad y el trabajo colaborativo entre los grupos de investigación y educación de los diferentes países que participan en el proyecto.

El proyecto MAGIC, se ha dividido en 6 paquetes de trabajo (Work Package) en donde cada uno de estos paquetes de trabajo contienen objetivos y actividades específicas para la consecución de todo el proyecto.

Uno de los objetivos del paquete de trabajo 2 (WP 2) es desplegar una Infraestructura de Autenticación y Autorización (AAI) a través de plataformas de servicios federados interconectados nacionalmente a través de una federación e internacionalmente a través de eduGAIN.

A partir de este objetivo se ha creado la Federación Nacional de Identidades Mexicana (FENIX), la cual pretende incorporar, como primera etapa a las instituciones que participan en el proyecto, y posteriormente a todas aquellas que quiera integrarse.

Dentro las actividades necesarias para el desarrollo de esta infraestructura se encuentra la capacitación al personal técnico de las instituciones que participan en el proyecto, que les permita comprender el concepto de los entornos federados, los elementos necesarios para hacer un despliegue adecuado en su institución y los procedimientos necesarios para realizar su incorporación a la federación.

En este documento se describe el curso en línea desarrollado en la Plataforma CUDI, dirigido al personal técnico de las instituciones miembros de CUDI y que participan en el proyecto MAGIC, para proporcionarles los conocimientos necesarios acerca de los Entornos Federados y su integración en una Federación, y aplicarlos en sus instituciones.

6. DESARROLLO DEL DOCUMENTO

Este documento tiene como objeto presentar un informe del trabajo desarrollado durante el curso en línea en la Plataforma Cudi, los objetivos, participantes y resultados obtenidos.

6.1 DATOS GENERALES – FICHA TÉCNICA

Nombre del Taller: Curso en línea de Federación de Identidad para Instituciones de Educación e Investigación

Modalidad: En línea (Plataforma CUDI)

Fecha Inicio: 10 de octubre de 2016

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

Cupo: Abierto a inscripción, sin límite de participantes.

Impartido por: Fernando Aranda Escobar, Juan Gabriel Cruz Pérez, Carlos González.

Curso: Federación de Identidades para Instituciones de Educación e Investigación

Presentación:

Este documento integra los recursos elaborados para capacitar el 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:

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.

Desglose de actividades - temario

Módulo I Introducción a los entornos federados en ambientes educativos (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 Servidor RADIUS LOCAL (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

Módulo III Fuentes de autenticación e intercambio de metadatos (14 Horas)

- 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

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

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.

6.2 RESULTADOS OBTENIDOS, BENEFICIOS

Participantes

En este se contó con la inscripción de 24 participantes pertenecientes a las siguientes instituciones:

- CINVESTAV
- UNAM
- UGTO
- ITESM
- UAM
- UDG
- CUDI
- CICESE
- REMERI

De las instituciones participantes el 70% finalizó con el total de las prácticas de una manera satisfactoria, el 20 % finalizó con prácticas parciales y el 10% finalizó el curso sin realizar ninguna práctica.

Los conocimientos adquiridos, permitirán que los participantes, entiendan cómo funcionan las Federaciones de Identidad en todo el mundo, los beneficios que aportan a la comunidad académica y como pueden realizar una implementación en piloto en su institución.

Este curso sienta las bases para que las instituciones participantes inicien con su incorporación a la Federación Nacional de Identidades Mexicana (FENIX), y puedan beneficiar a su comunidad académica y de investigación de los recursos nacionales e internacionales que estarán disponibles a través de ella.

6.3 PRÓXIMOS PASOS

Se tiene la el compromiso de las instituciones que participaron en este curso para realizar las gestiones administrativas y asignar los recursos técnicos para lograr el despliegue de un piloto de Proveedor de Identidad y Proveedor de Servicio institucional, además de seleccionar algún servicio institucional que pueda ser federado y compartido con los demás miembros de la federación a través de FENIX. Se trabajará de manera individualizada con cada institución para apoyar en estas actividades.

6.4 CONCLUSIÓN

Con este curso se da un primer paso en la disseminación de nuevas tecnologías que apoyen el despliegue de servicios federados interconectados nacionalmente a través de la federación (FENIX) e internacionalmente a través de eduGAIN.

También se fortalece la Federación Nacional de Identidades Mexicana, al incorporar nuevos participantes comprometidos en el desarrollo de Infraestructuras de Autenticación y Autorización Federadas, y que estos participantes puedan hacer despliegue de servicios de una manera rápida, con menor costo y en menor tiempo, en beneficio de sus comunidades académicas.