



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

WP2 Plataformas para la Movilidad

Informe Anual de Trabajo AAI Infraestructura de Autenticación y Autorización Federación de Identidades Etapa 1 Mayo 2015 – Agosto 2016



Proyecto Implementado en
México por CUDI



Proyecto implementado
por RedCLARA

Reporte de Progreso

Entregable MAGIC: D2.5_AAI_Pilot; D2.7 AAI_Implementation

Nombre completo del Documento	Informe de Anual de Trabajo AAI - Infraestructura de Autenticación y Autorización, Federación de Identidades, Etapa 1 (Mayo 2015 a Agosto 2016)
Fecha	Agosto, 2016
Actividad	Informe de actividades del WP2/AAI
Responsable del WP	Fernando Aranda Escobar
Estatus del Documento	Final
Atributos	Público

Resumen: Este documento presenta las actividades realizadas en el primer año del proyecto MAGIC en el paquete de trabajo 2 (WP2), que sienta las bases para el despliegue y consolidación de una Infraestructura de Autorización y Autenticación (Federación de Identidades) en México, en conjunto con las instituciones de educación superior que participan en este proyecto.

En esta primera etapa se ha llevado a cabo los trabajos necesarios para que las instituciones que participan en el proyecto puedan realizar un despliegue en prueba de un Proveedor de Identidad y un Proveedor de Servicio y entiendan como pueden adherir estos a la Federación Nacional de Identidad Mexicana (FENIX).



Proyecto Implementado en México por CUDI



Proyecto implementado por RedCLARA

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) INDEPENDIENTEMENTE 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	Agosto, 2017	Fernando Aranda
Revisado por	María del Rocío Cos Murillo	CUDI/WP1 Administración	Agosto 2017	Fernando Aranda
Revisado por				
Aprobado por	María del Rocío Cos Murillo	CUDI/WP1 Administración	Septiembre 2017	Fernando Aranda

TABLA DE CONTENIDOS

Aviso de Copyright:	4
Ruta del Entregable.....	5
1. Introducción	7
2. Referencias.....	7
3. Proceso de Enmienda de Documento	8
4. Glosario	9
5. Resumen Ejecutivo.....	9
6. Desarrollo del Documento	10
Datos Generales.....	10
Objetivo.....	10
Desglose de Actividades	10
Resultados Obtenidos	22
7. Próximos Pasos.....	22
8. Conclusión	23

1. INTRODUCCIÓN

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.

El Paquete de Trabajo 2 (WP 2) denominado “Plataformas para la Movilidad”, tiene como objetivo, desplegar una Infraestructura de Autenticación y Autorización (AAI) nacional a través de plataformas de servicios federados interconectados nacionalmente a través de una federación e internacionalmente a través de eduGAIN.

El resultado esperado es extender el conocimiento sobre Identidades Federadas y capacitación para su implementación en instituciones académicas que serán capaces de incorporar sus servicios federados al mercado académico global y hacer un uso más eficiente de sus recursos.

El propósito de este documento es describir los trabajos realizados en el primer año de actividades de la creación y despliegue de una Infraestructura de Autenticación y Autorización y la integración de una Federación Nacional de Identidades Mexicana (de mayo 2015 a agosto 2016), como parte del Paquete de Trabajo 2 (WP2) dentro del Proyecto MAGIC.

2. REFERENCIAS

[R1]	Sitio Web MAGIC	http://www.magic-project.eu
[R2]	Sitio Web CUDI	http://www.cudi.edu.mx
[R3]	Sitio Web Capacitación Magic	http://magic-project.eu/index.php/training
[R4]	Sitio Web eduGAIN	https://www.geant.org/Services/Trust_identity_and_security/eduGAIN
[R4]	Sitio Web Plataforma CUDI	http://virtual.cudi.edu.mx

3. PROCESO DE ENMIENDA DE DOCUMENTO

Las solicitudes de enmiendas a este documento se deberán hacer al autor (Fernando Aranda Escobar, WP2, Responsable de la Federación Nacional de Identidades Mexicana (FENIX), faranda@cudi.edu.mx), con copia al Administrador del proyecto MAGIC en CUDI (María del Rocío Cos Murillo, rcos@cudi.edu.mx).

4. GLOSARIO

AAI	Authentication and Authorization Infrastructure (Infraestructura de Autorización y Autenticación)
BUAP	Benemérita Universidad Autónoma de Puebla
CODAES	Comunidades Digitales para el Aprendizaje en Educación Superior
CONACYT	Consejo Nacional de Ciencia y Tecnología
CUDI	Corporación Universitaria para el Desarrollo de Internet, A.C.
EC	European Commission
eduGAIN	Servicio interfederado que conecta federaciones de identidades en todo el mundo, simplificando el acceso a contenidos, servicios y recursos para la comunidad global de investigación y educación. eduGAIN comprende más de 50 federaciones participantes que conectan a 2.672 proveedores de identidad con 1.909 proveedores de servicios.
EU	European Union
EU-LAC	Europe, Latin America and the Caribbean
FENIX	FEderación Nacional de Identidades meXicana
IdP	Proveedor de Identidad (IdP por sus siglas en inglés)
ITESM	Instituto Tecnológico de Estudios Superiores de Monterrey
LDAP	Protocolo Ligero de Acceso a Directorios (LDAP por sus siglas en inglés)
SP	Proveedor de Servicio (SP por sus siglas en inglés)
RedCLARA	Red de la Cooperación Latinoamericana de Redes Avanzadas
REMERI	Red Mexicana de Repositorios Institucionales
UAA	Universidad Autónoma de Aguascalientes
UACJ	Universidad Autónoma de Ciudad Juárez

UADY	Universidad Autónoma de Yucatán
UAEH	Universidad Autónoma del Estado de Hidalgo
UAM	Universidad Autónoma Metropolitana
UANL	Universidad Autónoma de Nuevo León
UASLP	Universidad Autónoma de San Luis Potosí
UCOL	Universidad de Colima
UDG	Universidad de Guadalajara
UGTO	Universidad de Guanajuato
UNAM	Universidad Nacional Autónoma de México
UV	Universidad Veracruzana
WAYF	Where Are You From – Servicio de Descubrimiento
WP	Work Package – Paquete de Trabajo

5. RESUMEN EJECUTIVO

En este documento se describen los trabajos realizados en el primer año de actividades de la creación y despliegue de una Infraestructura de Autenticación y Autorización y la integración de una Federación Nacional de Identidades Mexicana (de mayo 2015 a agosto 2016), como parte del Paquete de Trabajo 2 (WP2) dentro del Proyecto MAGIC.

Durante el primer año se iniciaron los trabajos que sientan las bases para el desarrollo de una Federación Nacional de Identidades Mexicana para que las instituciones que participan en este proyecto adquieran los conocimientos y puedan integrarse a ella a través de la implementación en prueba de un Proveedor de Identidad, también se realizaron los trabajos para el diseño y desarrollo del portal de la Federación que sirva como base de conocimiento y difusión hacia las instituciones de educación e investigación.

En esta primera etapa, participan en el proyecto, 8 instituciones de educación e investigación en México, que son las siguientes: Universidad Nacional Autónoma de México (UNAM), Universidad de Guadalajara (UdG), Universidad de Colima (UCOL), Instituto Tecnológico de Estudios Superiores de Monterrey (ITESM), Centro de

Investigaciones Avanzadas del Instituto Politécnico Nacional (CINVESTAV), CICESE, Universidad Autónoma de México (UAM) y Benemérita Universidad de Puebla (BUAP).

6. DESARROLLO DEL DOCUMENTO

Este documento tiene como objeto presentar un informe del trabajo desarrollado de Mayo de 2015 a agosto de 2016.

DATOS GENERALES

Introducción:

Durante este año de trabajo, se iniciaron los trabajos para iniciar el despliegue de **FENIX**, la **F**ederación **N**acional de Identidades **meX**icana, a través de diversas actividades como el desarrollo de una infraestructura base que soporte las actividades de la Federación, el desarrollo de un portal que contenga la información necesaria que sirva como guía para las instituciones que deseen afiliarse, y el desarrollo del material necesario para impartir un curso de capacitación en línea que permita al personal técnico de las instituciones el despliegue de un Proveedor de Identidad y un Proveedor de Servicio y como adherirlos a FENIX.

OBJETIVO

Sentar las bases para el despliegue de una Infraestructura de Autorización y Autenticación Nacional (AAI por sus siglas en inglés), que comparta servicios federados entre las instituciones de educación superior que estén incorporadas a la federación y con otras instituciones en otras federaciones en el mundo.

DESGLOSE DE ACTIVIDADES

Durante este primer año, las actividades se enfocaron en desarrollar una infraestructura que permita el despliegue de una Infraestructura de Autorización y Autenticación Nacional (AAI por sus siglas en inglés), incluyendo el desarrollo de políticas, el portal web y el material de capacitación para un curso en línea.

Capacitación



- **Asistencia a Taller**

El staff técnico de CUDI asistió al taller “Federated Access and eduroam workshop in the Caribbean” el cual se llevó a cabo los días 7, 8 y 9 de octubre de 2015 en la Universidad de West Indias Campus Mona, en Jamaica, auspiciado por Jamaica Research and Education Network (JREN) y la colaboración de CKLN (Caribbean Knowledge and Learning Network), el taller fue impartido dentro del marco del proyecto MAGIC.

El objetivo general de este taller fue capacitar al personal de las RNIE’s en como desplegar una Infraestructura de Autorización y Autenticación (AAI), para que estas a su vez repliquen esta acción entre sus miembros, extendiendo el conocimiento sobre las identidades federadas y que las instituciones sean capaces de incorporar servicios federados a la federación que pertenecen y también a hacer uso de los servicios de otras federaciones en el mundo.

Dentro de las actividades del taller se llevó a cabo el despliegue de un Proveedor de Identidad (IdP) y un Proveedor de Servicio (SP), como adherirlos a una federación y como trabajar con otras federaciones en el mundo, este fue impartido por Brook Schofield responsable en eduGAIN de la afiliación de las Federaciones de Identidad a nivel mundial.

<http://magic-project.eu/index.php/2015-05-28-22-53-32/news-and-events/192-federated-access-and-eduroam-workshop-in-the-caribbean>

- **Desarrollo de Curso en Línea**

En este año, también se diseñaron y desarrollaron materiales para impartir un curso en línea, estos materiales se desarrollaron con el estándar necesario para poder impartirlos dentro de la Plataforma de Aprendizaje CUDI.

El objetivo de este curso es que los participantes obtendrán el conocimiento sobre los entornos federados, como realizar el despliegue de un Proveedor de Identidad y un Proveedor de Servicio y como adherirlos a la federación.

El curso y sus materiales se encontrarán disponibles en la Plataforma de Aprendizaje CUDI <http://virtual.cudi.edu.mx> (requiere registro).

Infraestructura Federación Nacional de Identidades Mexicana (FENIX)



- **Planeación**

Se realizó la planeación para el despliegue de una Infraestructura de Autorización y Autenticación (AAI) en México, esta planeación incluyó la calendarización de actividades y su asignación a cada uno de los participantes del proyecto.

Como primera etapa se incluyó el diseño, compra, instalación y puesta a punto de a infraestructura en donde estará soportada la federación, sus servicios y el portal.

En esta etapa se decidió utilizar para la federación una plataforma de virtualización open basada en Linux KVM, la cual permitirá el maximizar los recursos de hardware y software con que se contarán, se realiza una evaluación de diferentes marcas y modelos de servidores y se seleccionan servidores de la marca IBM Lenovo con diseño para virtualizar.

- **Despliegue**

Una vez instalados los servidores y la plataforma de virtualización, se genera un servidor virtual para el despliegue de un Proveedor de Identidad para los usuarios de CUDI, un servidor virtual para un Proveedor de Servicio para un servicio de levantamiento de tickets de CUDI, un servidor virtual para el servicio de descubrimiento de la federación (WAYF), y un servidor virtual para el portal web de FENIX.

Se selecciona como sistema operativo para todos los servidores Linux Debian, el cual se instala, configura, se pone a punto y se realizan pruebas de un buen funcionamiento.

Se define como protocolo a usar en la federación SAML 2.0, y como aplicación para el despliegue SimpleSAMLphp, la cual se instala y se realizan las configuraciones necesarias para su funcionamiento.

<https://simplesamlphp.org/>

SimpleSAMLphp

[Home](#)
[Download](#)
[Documentation](#)
[Security](#)
[Modules](#)
[Translation](#)
[Devel](#)

SimpleSAMLphp is an award-winning application written in native PHP that deals with authentication. The project is led by UNINETT, has a large user base, a helpful user community and a large set of external contributors. The main focus of SimpleSAMLphp is providing support for:

- **SAML 2.0 as a Service Provider (SP)**
- **SAML 2.0 as an Identity Provider (IdP)**

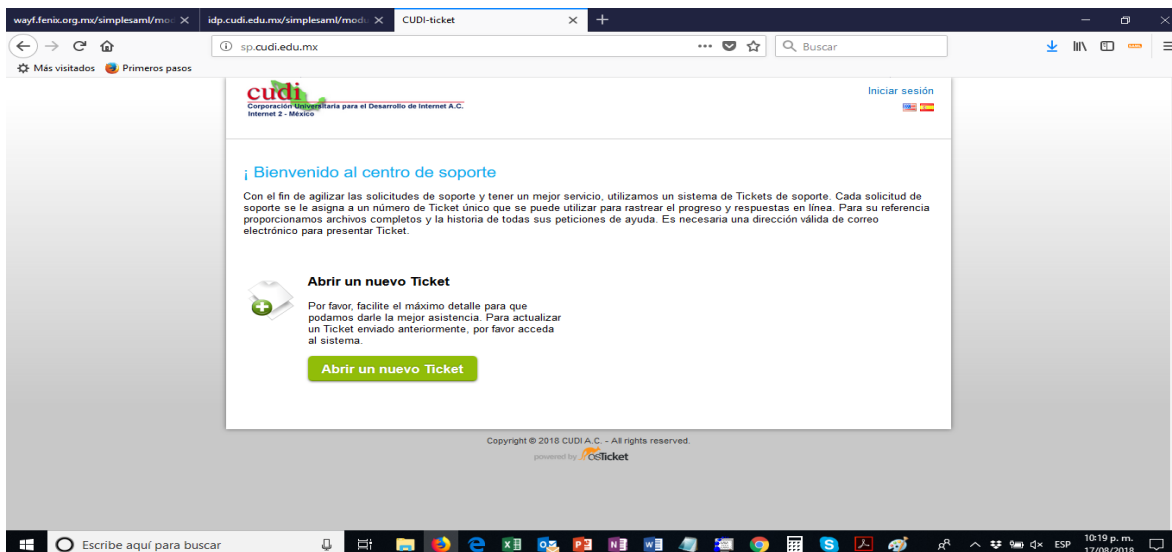
However, it also supports some other identity protocols and frameworks, such as Shibboleth 1.3, A-Select, CAS, OpenID, WS-Federation or OAuth, and is easily extendable, so you can develop your own modules if you like.

With the memcache session handler, **SimpleSAMLphp scales pretty well**. A replication layer is built upon memcache, such that an unlimited number of SimpleSAMLphp web front-ends can work with a back-end matrix of memcache servers with both replication (fail-over) and load-balancing.

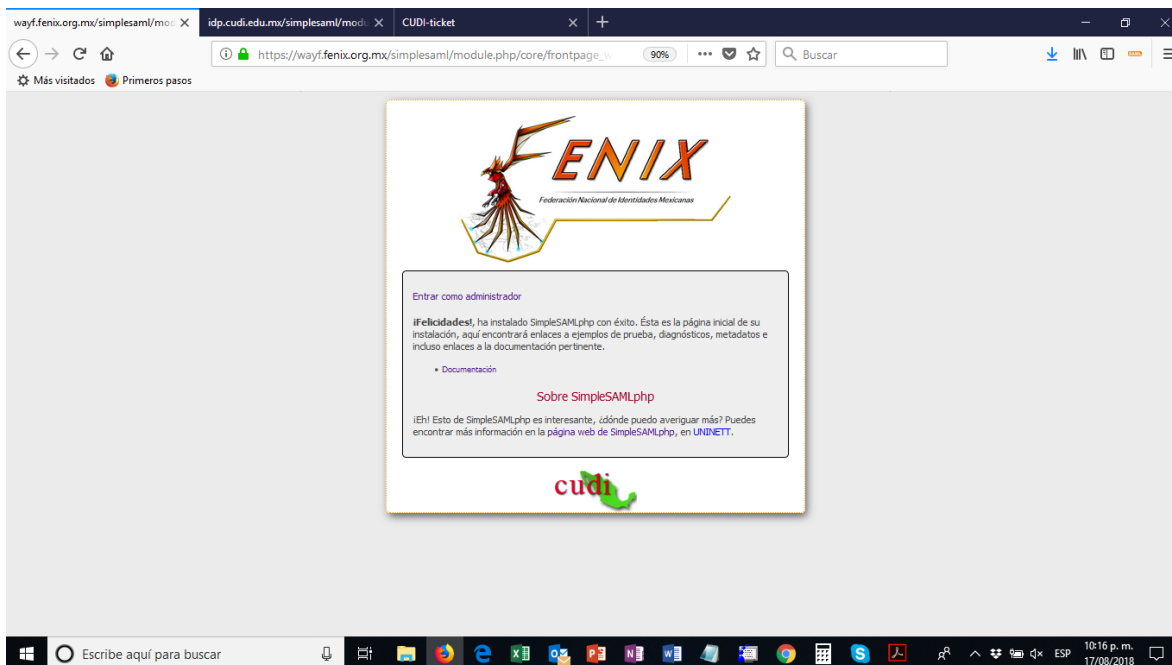
Como siguiente paso se realiza el despliegue de un piloto de Proveedor de Identidad (IdP) que autentifique a los usuarios de CUDI y el despliegue en piloto de un servicio de descubrimiento (WAYF) que será el servicio que centralizará a los Proveedores de Identidad que se vayan agregando a la federación.



Se realiza la adaptación y configuración de una aplicación para que las instituciones que participarán en la federación puedan levantar algún ticket de servicio para reportar fallas de red, la base utilizada para esta aplicación es osTicket.

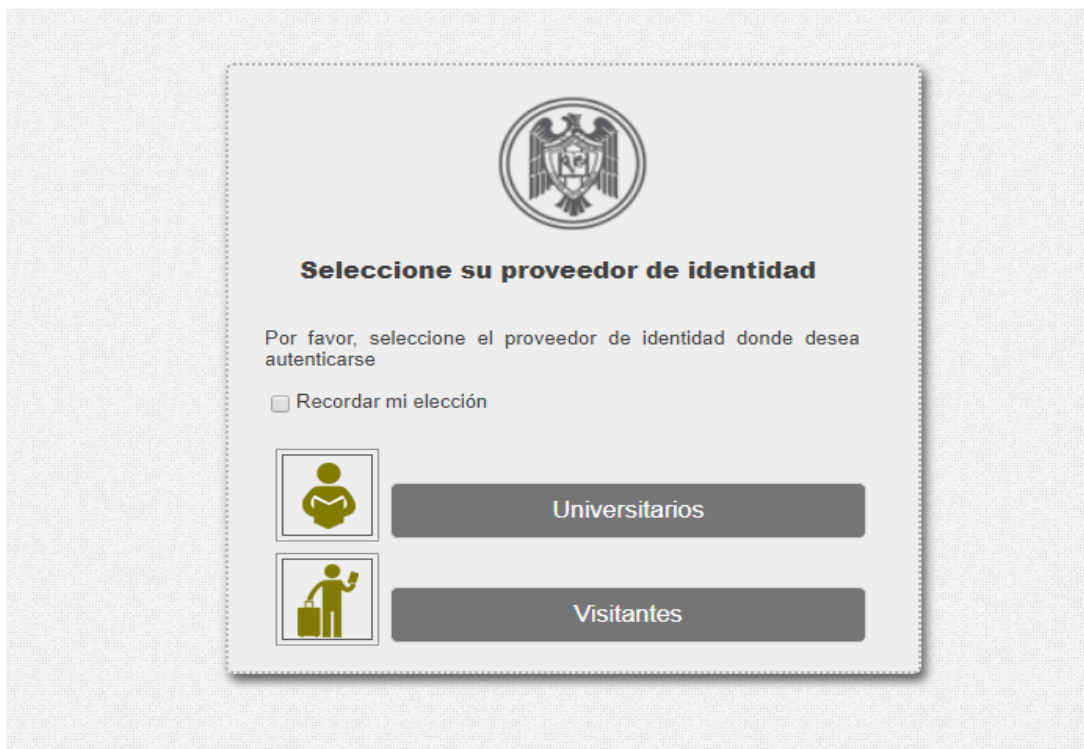


Se instala la aplicación en un servidor virtual y se realiza el despliegue en piloto de un Proveedor de Servicio conectado al servicio de ticket y también al WAYF de la federación, se realizan pruebas de interoperabilidad entre todos los elementos, quedando en funcionamiento para realizar pruebas finales.



UCOL

Una vez desplegados los elementos anteriores se realiza la configuración en el WAYF de FENIX para la interconexión con el Proveedor de Identidad (IdP) de la Universidad de Colima, el cual ya se encuentra en producción, pues la Universidad tiene ya algún tiempo trabajando con servicios federados de manera interna.



- **Desarrollo de Políticas**

En este primer año se elaboró el documento de Políticas de la Federación Nacional de Identidades Mexicana, este documento está basado en el documento modelo para las federaciones que pertenecen a eduGAIN.

Este documento detalla los lineamientos que las instituciones de educación e investigación tienen que seguir al adherirse a FENIX.

El documento desarrollado estará disponible en el portal web de Fenix en el apartado de “Conéctate”, en la siguiente dirección:

<https://www.fenix.org.mx/procedimientos.html>

Se han desarrollados también los documentos de Políticas para los Proveedores de Identidad (IdP) y los Proveedores de Servicio (SP), los cuales contienen los lineamientos para las instituciones de educación e investigación que quieran su IdP o SP a la federación.

Estos documentos estarán disponibles en el portal web de Fenix en el apartado de “Conéctate”, en la siguiente dirección:

<https://www.fenix.org.mx/procedimientos.html>

- **Portal FENIX**

Como parte de las actividades de este primer año, se realizó el diseño y desarrollo en piloto del portal web de la Federación Nacional de Identidades Mexicana.

Se decidió que el portal tuviera cinco secciones, además de la sección de inicio, las cuales son:

- Beneficios: En esta sección se mencionan cuales son los beneficios que tendrán las instituciones al adherirse a la federación, algunos casos de uso y la liga a un video sobre FENIX.
- Como Funciona: En esta sección se describe el funcionamiento de la federación, la interacción entre un Proveedor de Identidad, un Proveedor de Servicio y un Servicio de Descubrimiento, y un diagrama de todo este proceso.
- Conéctate: En esta sección estará disponible el procedimiento para que las instituciones se adhieran a la federación, los documentos que tienen que firmar, las políticas que deberán seguir y los atributos que se tienen que liberar.
- Participantes: en esta sección estarán los Proveedores de Identidad, los Proveedores de Servicio, los Servicios y las instituciones que han agregado a la federación.
- Grupo Técnico: En esta sección estará la información de las instituciones y personas que están en el grupo de coordinación de la Federación.



<https://www.fenix.org.mx/index.html>

RESULTADOS OBTENIDOS, BENEFICIOS

En este primer año de trabajo se ha realizado las actividades necesarias para desarrollar las bases de la Federación Nacional de Identidades Mexicana como parte de una Infraestructura de Autorización y Autenticación Nacional sólida que agrupe a las instituciones de educación superior mexicanas.

Se han implementado un piloto con 2 Proveedores de Identidad, 1 Proveedores de Servicio y 1 Servicio de Descubrimiento para FENIX.

También se ha diseñado y desarrollado un piloto del portal web de FENIX, que contiene la información necesaria sobre como incorporarse, los beneficios de pertenecer, los documentos técnicos, las políticas y toda la información acerca de la Federación.

Se desarrollaron también los documentos que las instituciones utilizarán para afiliarse a FENIX.

PRÓXIMOS PASOS

Para dar continuidad a lo realizado en este año se requiere continuar con los trabajos con las instituciones participantes en el proyecto, para lograr que desplieguen sus Proveedores de Identidad y de Servicio y los adhieran a la federación

También se debe realizar una mayor difusión sobre el tema de Federación de Identidades, sus beneficios y como pueden participar las instituciones académicas y de gobierno en México.

Será importante también, iniciar los procedimientos de adhesión a eduGAIN que es la organización que agrupa a las Federaciones de Identidad en el mundo, y establecer convenios en donde se pueda hacer uso de servicios federados de otras Redes de Educación e Investigación en el mundo.

CONCLUSIÓN

Este primer año de trabajo se han dado avances significativos para la creación de una Infraestructura Nacional de Autenticación y Autorización a través de los trabajos hechos en la Federación Nacional de Identidades Mexicana (FENIX), el despliegue de los pilotos de los Proveedores de Identidad de la Universidad de Colima (UCOL) y de la Corporación Universitaria Para el Desarrollo de Internet (CUDI).

La capacitación que recibió el staff técnico de CUDI permitirá apoyar a las instituciones participantes en el despliegue de sus Proveedores de Identidad y sus Proveedores de Servicio y brindar los servicios de capacitación en beneficio de su comunidad académica.

Es necesario seguir trabajando para continuar con el avance de FENIX y lograr los objetivos planteados, se espera que, en el siguiente año, logremos la incorporación de más instituciones a FENIX y se pueda consolidar la federación.