UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

TEMA:

SISTEMA DE FEDERACIONES DE IDENTIDADES PARA LA FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL USANDO SOFTWARE DE CÓDIGO ABIERTO.

Trabajo de Graduación. Modalidad: Proyecto de Investigación, presentado previo la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos

LÍNEA DE INVESTIGACIÓN:

Sistemas Embebidos

AUTOR:

Alexandra Stefanía Cevallos Teneda

TUTOR:

Ing. David Omar Guevara Aulestia, Mg.

Ambato - Ecuador

Julio, 2016

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Investigación sobre el Tema:

"Sistema de Federaciones de Identidades para la Facultad de Ingeniería en Sistemas, Electrónica e Industrial usando software de código abierto", de la señorita Cevallos Teneda Alexandra Stefanía, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el numeral 7.2 de los Lineamientos Generales para la aplicación de Instructivos de las Modalidades de Titulación de las Facultades de la Universidad Técnica de Ambato

Ambato, Julio de 2016

EL TUTOR

Ing. David Omar Guevara Aulestia, Mg

AUTORÍA

El presente trabajo de investigación titulado: "Sistema de Federaciones de Identidades para la Facultad de Ingeniería en Sistemas, Electrónica e Industrial usando software de código abierto". Es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, Julio de 2016

Alexandra Stefanía Cevallos Teneda

CC: 1804770327

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación.
Cedo los derechos de mi Trabajo de Titulación, con fines de difusión pública, además autorizo su reproducción dentro de las regulaciones de la Universidad.

Ambato, Julio de 2016

Alexandra Stefanía Cevallos Teneda

CC: 1804770327

APROBACIÓN COMISIÓN CALIFICADORES

La Comisión Calificadora del presente trabajo conformada por los señores docentes, Ing Juan Carlos Ruiz e Ing. Félix Fernández, revisó y aprobó el Informe Final del Proyecto de Investigación titulado "Sistema de Federaciones de Identidades para la Facultad de Ingeniería en Sistemas, Electrónica e Industrial usando software de código abierto", presentado por el señorita Alexandra Stefanía Cevallos Teneda de acuerdo al numeral 9.1 de los Lineamientos Generales para la aplicación de Instructivos de las Modalidades de Titulación de las Facultades de la Universidad Técnica de Ambato.

Ing. José Vicente Morales Lozada

PRESIDENTE DEL TRIBUNAL

Ing. Juan Carlos Ruiz	Ing. Félix Fernández
DOCENTE CALIFICADOR	DOCENTE CALIFICADOR

DEDICATORIA

A Dios, que me acompaña en todo momento y me extiende su mano si me tropiezo.

Alexandra Cevallos

AGRADECIMIENTO

A Dios porque con su bendición he culminado una etapa importante de mi vida como lo es la instrucción universitaria, a mis padres que han sido el pilar fundamental de mis estudios y quienes me han impulsado para seguir adelante día con día, a mi hermana y demás familiares porque con su cariño me han apoyado durante mi formación espiritual y académica.

Al Ingeniero David Guevara un especial agradecimiento, por su guía y enseñanza dentro del presente Proyecto de Investigación y durante toda la carrera como docente.

Alexandra Cevallos

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN EJECUTIVO

Las diferentes aplicaciones y sistemas web ofrecen múltiples servicios a los usuarios, por lo tanto los proveedores de estos servicios están forzados a formar colaboraciones temporales o fijas, para brindar dichos beneficios con tan solo un clic.

La gestión de la identidad hace referencia al conjunto de políticas, procesos y tecnologías que permiten establecer cuentas de usuario y reglas relacionadas a la administración de la información y recursos digitales dentro de la organización.

Esto requiere que los participantes de la identidad federada establezcan relaciones de confianza entre sí y por lo tanto permitir el intercambio de servicios o el consumo entre los socios de forma segura y confiable.

Al aprovechar una arquitectura de gestión de identidades se puede establecer, ejecutar, actualizar o disolver las relaciones de confianza que requiere la colaboración institucional, lo que reduce en gran medida los costos de configuración y evita errores en los dominios individuales de la organización.

El presente proyecto de investigación tiene como objetivo brindar a la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, un enfoque orientado a la gestión eficaz de manejo de usuarios en las diferentes plataformas usadas dentro del ámbito académico, para acceder a servicios como cuentas de correo, plataformas educativas, repositorios virtuales, equipos informáticos, entre otros; para esto se ha realizado un análisis previo de las plataformas utilizadas por la Facultad tanto por docentes como estudiantes, además de las diferentes herramientas de código abierto existentes para diseñar una Federación. A continuación se procedió con la instalación y configuración de Shibboleth, una tecnología Open Source, que implementa una solución de autenticación unificado para sistemas web que puede ser utilizada dentro de una organización o a través de diversas instituciones, dicha configuración aplica para Shibboleth como Proveedor de identidad y Proveedor de Servicios. Además se implementó un servidor de autenticación OpenLDAP y Active Directory para futuras conexiones a otros servicios dentro de la comunidad educativa.

ABSTRACT

Different applications and web systems offer multiple services to users , so these services providers are forced to form temporary or permanent partnerships , to provide these benefits with just one click.

The identity management refers to the policies, processes and technologies to establish user accounts and rules related to the information management and digital resources in the organization.

This requires participants federated identity to establish trusting relationships with each other and therefore allow the exchange of services safely and reliably

Taking advantage of an architecture identity management can be established, run or dissolve the trust relationship that require institutional colaboration, which reduces configuration cost in a big measure and avoid errors in the individual domain of the organization.

The present research project aims to provide the School of Systems Engineering, Electronic and Industrial oriented effective management of user management or different platforms used within academic approach to access services such as email accounts, education platforms, virtual repositories, computer equipment, among others; for this it has made a preliminary analysis of the platforms used by the Faculty both teachers and students, in addition to the various open source tools exist to design a federation. Then we proceeded with the installation and configuration of Shibboleth, an open source technology, which implements a solution logging uniffied web systems that can be used within an organization or through various institutions, this configuration applies to Shibboleth as Identity Provider and Service Provider. In addition OpenLDAP authentication server and Active Directory in Windows Server 2012 for future connections to other services within the educational community was implemented.

Glosario de términos y acrónimos

- **IdP:** Proveedor de Identidad. Organización que provee la autenticación del usuario y devuelve los datos del usuario que el Proveedor de Servicios 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 basándose en una serie de atributos que satisfacen sus requerimientos de autorización.
- **WAYF:** Cuando un Proveedor de Servicio 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 su 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.
- **ARP:** Política de liberación de atributos. Política que rige la distribución de los atributos del usuario a los diferentes Proveedores de Servicio.
- **Metadatos:** Conjunto de datos que conforman la información necesaria para que una entidad se comunique con otra entidad de la federación.
- **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.
- **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 Proveedores de Servicio (previa autorización en el mismo) una vez se haya identificado en un Proveedor de Identidad.
- **SLO:** Single Log Out. Procedimiento por el cual el usuario deja de estar identificado en el conjunto de aplicaciones/elementos en los que estuviera logeado.
- **PPP**: Protocolo punto a punto (Point-to-Point Protocol) es un conjunto de protocolos estándar que permiten la interacción de software de acceso remoto de diversos proveedores.

- **LDAP:** (Lightweight Directory Access Protocol ó Protocolo Ligero de Acceso a Directorios) es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar información en un entorno de red. LDAP también es considerado una base de datos a la que pueden realizarse consultas.

- **Shibboleth:** Marco de trabajo Open Source desarrollado en Internet2 que implementa un sistema de Single-Sign-On web con intercambio de atributos basados en estándares abiertos, principalmente SAML. Sistema federado que provee acceso seguro a través de diferentes dominios de seguridad, preservando la privacidad de los datos de sus usuarios, y posibilita la escalabilidad del sistema a través de relaciones de confianza.

- **Autenticación:** Es el proceso por el cual se identifica un cliente (persona) como válida para posteriormente acceder a ciertos recursos definidos.

- **Autorización:** Es el proceso sobre el cual se establecen que tipos de recursos están permitidos o denegados para cierto usuario o grupo de usuarios concreto.

- **PKI:** (Public Key Infrastructure, infraestructura de clave pública) Combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas.

INTRODUCCIÓN

Desde el inicio del desarrollo de las diferentes aplicaciones y plataformas se ha necesitado mantener ciertos niveles de privilegio de acceso a los recursos y servicios que ofrecen estos sistemas. El avance de la tecnología es responsable de la construcción de aplicaciones y del acceso en tiempo real de las mismas por lo cual los administradores deben mantener una base de datos de usuarios con información y roles de acceso lo que provoca que sea una tarea costosa.

La seguridad de la información tiene tres aspectos fundamentales: la disponibilidad, la integridad y la confidencialidad. A través de la disponibilidad los sistemas estarán disponibles cuando se los requiera, garantizando la prestación de las funciones para las cuales han sido diseñados. Mediante la integridad únicamente los usuarios permitidos pueden alterar la información. Por último, la confidencialidad enuncia que nadie, excepto los usuarios permitidos, puede conocer el contenido de la información protegida.

Del lado del cliente, la disponibilidad de diferentes servicios, obliga al usuario a la creación de múltiples identidades para la utilización de los mismos. Por cada servicio, se debe proporcionar información personal, nombre de usuario y contraseña para el acceso. Al crear un nombre de usuario y contraseña para cada servicio se establece un buen nivel de seguridad, sin embargo, administrar esa información para el usuario es una tarea difícil, dada la amplia gama de servicios que se ofrecen hoy en día. La limitación y control de acceso del usuario a los recursos ofrece características de integridad y confidencialidad a la seguridad de la información, con esto se desea evitar que los usuarios no permitidos puedan alterar la información protegida, así como que puedan acceder a su contenido y recuperarla, para lo cual se ha definido diferentes operaciones, entre las cuales se puede encontrar la identificación del usuario, la autenticación y la autorización.

A medida que las distintas aplicaciones se conectaban entre sí para brindar servicios, nació la necesidad del usuario que diferentes dominios de identidad pudiesen acceder a recursos de otros dominios en los que se confiaba; es aquí cuando se desarrolla la federación de identidades, basada en el concepto de integrar y coordinar diferentes dominios de identidad para la gestión y control del acceso.

En el presente proyecto de investigación se analizan las distintas aplicaciones

usadas por los estudiantes y docentes dentro de la Facultad de Ingeniería en Sistemas Electrónica e Industrial, para determinar cual de ellas es apta para la implementación dentro de un Sistema Federado.

CAPÍTULO 1

El problema

1.1. Tema de Investigación

Sistema de Federaciones de Identidades para la Facultad de Ingeniería en Sistemas, Electrónica e Industrial usando software de código abierto

1.2. Planteamiento del problema

El control de acceso a las distintas herramientas y plataformas con las que cuenta la Facultad de Ingeniería en Sistemas Electrónica e Industrial es uno de los mayores desafíos informáticos que se presentan en la actualidad en cuanto a seguridad informática, debido a que estudiantes y docentes poseen varias cuentas de usuario para acceder a servicios que ofrece la institución.

La necesidad y complejidad que tienen los estudiantes y docentes al momento de acceder a las diferentes plataformas internas de la facultad, provoca que el número de cuentas activas que posee, sobrepase la cantidad de datos que puede recordar debido a las obligaciones del diario vivir, lo cual conlleva al olvido de nombres de usuario y contraseña; esta situación afecta directamente al usuario ya que malgasta tiempo y recursos en recuperar su clave y nombre de usuario de la cuenta, debiendo seguir una serie de pasos para confirmar su identidad.

La privacidad del docente y estudiante se ve afectada al momento de acceder a una de las diferentes cuentas que posee, debido a que por facilidad de ingreso, los usuarios acostumbran a ingresar la misma contraseña para el n número de cuentas que posee, lo cual provoca la vulnerabilidad en sus perfiles.

El número de servicios que oferta la Facultad se ve reflejado en las necesidades de la institución y su correcto funcionamiento, sin embargo, existe la preocupación en cuanto a privacidad de los datos, para que estos servicios puedan ser explotados en su totalidad, es necesario proporcionar un adecuado control de acceso a las diferentes aplicaciones. Los aspectos fundamentales de seguridad a considerar son autenticidad, confidencialidad e integridad por lo cual es necesario la implementación de un modelo de gestión segura y fiable.

1.3. Delimitación

- **Área Académica:** Hardware y Redes.
- **Línea de Investigación:** Tecnologías de la Información.
- **Sub líneas de investigación:** Sistemas Embebidos.
- **Delimitación espacial:** Facultad de Ingeniería en Sistemas, Electrónica e Industrial.
- **Delimitación temporal:** La presente investigación se desarrolló en los 6 meses posteriores a la aprobación del proyecto por parte del Honorable Consejo Directivo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

1.4. Justificación

Debido a que en la Facultad de Ingeniería en Sistemas, Electrónica e Industrial no existe un Sistema de Federaciones de Identidad para acceder a las diferentes herramientas y plataformas que posee la Facultad tanto para docentes como para estudiantes, se considera de gran importancia que se desarrolle este proyecto, para así corregir los problemas que se ocasionan al momento de acceder con distintas cuentas de usuario a las aplicaciones con las que cuenta la Facultad.
La realización de este proyecto de investigación es de suma importancia ya que se puede combinar la teoría con la práctica y gracias a esto complementar el desarrollo e implantación de la investigación realizada, además los resultados obtenidos después de un análisis serán de gran ayuda para la elaboración de un Sistema de Federaciones en la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.
Con el desarrollo del presente proyecto se beneficiarán principalmente los estudiantes y docentes de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato a través de la autenticación unificada a las diferentes plataformas con las que cuenta la Universidad. Además, el sistema permitirá usar los servicios de CEDIA y el acceso a todos los servicios de los miembros de la red ecuatoriana como Latinoamérica con un único nombre de usuario. Después de analizar la problemática que se presentaba al momento de acceder a una cuenta de usuario y observando la necesidad de elaborar un sistema de federaciones se indica que el proyecto es totalmente factible de realizar e implementar.

1.5. Objetivos

1.5.1. General

Implementar un Sistema de Federaciones de Identidades para la Facultad de Ingeniería en Sistemas, Electrónica e Industrial usando software de código abierto.

1.5.2. Específicos

- Determinar los Sistemas de identidad federados de código abierto de libre acceso.
- Determinar las aplicaciones y sistemas utilizados dentro de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial que son aptas para la aplicación de federaciones.
- Diseñar el Sistema de federaciones demostrativo para las plataformas utilizadas en la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

CAPÍTULO 2

Marco Teórico

2.1. Antecendentes Investigativos

Tras la revisión y análisis de los distintos repositorios digitales que existen en las Universidades y Politécnicas del país se concluye que no se encontraron temas similares al presente proyecto de investigación, motivo por el cual se procedió a buscar información en las diferentes revistas electrónicas, en las cuales se indica que a través del uso de Sistemas Federados y tarjetas de información dentro de una organización, los usuarios pueden enviar su información a aplicaciones web y así tener un control total sobre la divulgación y difusión de la misma hacia los demás. Además se señala que la asociación de otros factores con la identidad digital, como las huellas digitales de los usuarios y los teléfonos móviles fortalece la credibilidad y la rendición de cuentas de los usuarios, así como la autenticación de los usuarios en el sistema federado. Los usuarios pueden añadir más información a su perfil además de la que se extrae y compartirlo con otros usuarios. Al compartir sus datos personales con los demás, los usuarios pueden construir una agenda personal de direcciones actualizada [1].

La implementación de un sistema federado constituye la solución a la creciente demanda de acceso a servicios a través de la web por parte de los usuarios, ya que en la actualidad los clientes poseen grandes cantidades de información que deben ser organizadas de acuerdo a sus atributos en las distintas plataformas a las que se encuentran asociadas [2].

La implementación de sistemas federados o llamadas aulas colaborativas en las instituciones educativas ofrece una interacción en vivo entre los estudiantes y tutores agrupado varias tecnologías como son conferencias de audio, gestión de aprendizaje, foros, eLearning, entre otros; ya que es posible acceder a recursos distribuidos bajo diferentes dominios administrativos con una política de confianza adecuada [3]. La gestión de Identidad, basada en estándares y tecnologías dentro de la web, ha evolucionado rápidamente en los últimos años, la experiencia del usuario y las necesidades de privacidad han ocasionado que la seguridad de la información se convierta en un tema primordial. Como resultado de estas actividades de Gestión de Identidad, conceptos de Identidad Federada y

Single Sign-On han surgido, en donde un usuario es autenticado una vez provisto de un acceso transparente a múltiples aplicaciones de servicio [2].

2.2. Fundamentación teórica

2.2.1. Identity Management (IdM)

Gestión de Identidad o Identity Management (IdM), es el manejo de diversas identidades y la información relacionada de un usuario en diversos dominios o servicios, garantizando la privacidad y seguridad del cliente, mientras se proveen mecanismos para compartir la información sin tener que recordar cada una de las credenciales o identificarse en cada sitio. Debido a que gran parte de la estructura en la Identidad Federada es orientada a servicios, la idea es unificar gran parte de estos[4].

Requisitos de un sistema de gestión de la identidad.

- **Funcionalidad**: El sistema de gestión de identidad, ayuda al usuario a controlar su identidad. En este sentido, se refiere al mecanismo de revocación de identidad, lo que permitirá al sistema, proporcionar a los usuarios la gestión de la información en sus identidades y revocarla.

- **Usabilidad**: La interfaz de usuario debe permitir interpretar el contexto y elegir la identidad deseada; gestionar la identidad en un mundo digital; y trabajar con diferentes dispositivos como PC (Personal Computer), PDAs (Personal Digital Assistant) y SmartPhones.

- **Seguridad**: Un Sistema de Gestión de Identidad debe ser eficaz contra los ataques a la disponibilidad, integridad y confidencialidad de sus servicios y la información. Esto es necesario debido al gran volumen de información confidencial del usuario existente pudiendo causar intentos de espionaje, manipulación y robo de identidad.

- **Privacidad**: Los usuarios deben tener canales para expresar y hacer cumplir, las preferencias de privacidad de la información personal proporcionada en sus identidades.

- **Anonimato**: Hay que asegurar a los usuarios el derecho de permanecer en el anonimato para que la información proporcionada con su identidad digital no se puede utilizar para buscar datos de sus otras identidades. El uso de seudónimos es una manera de garantizar el anonimato.

- **Fidelidad**: La fidelidad es un requisito previo para todas las transacciones en las que el usuario confía en el proveedor de servicios, incluso en casos en los que el usuario tiene el control total sobre el hardware, software y datos de flujo.
- **Gestión de la confianza**: Las relaciones de confianza entre proveedores de servicios y proveedores de identidad permiten la identidad en dominios diferentes y estos son aceptados entre sí.
- **Interoperabilidad**: Una aplicación de gestión de identidad debe implementar interfaces compatibles con las normas internacionales, y ofrecer compatibilidad e integración con los sistemas existentes. La identidad de los usuarios debe estar representado en un formato común para que puedan ser entendidos y validados en diferentes dominios y seguridad administrativos[5].

2.2.2. Gestión de Identidad Federada

Gestión de Identidad Federada o Federated Identity Management, son aquellos sistemas de IdM que entregan el control a las organizaciones y proveedores, que generalmente comparten intereses económicos o cooperativos, para manejar la información de las identidades del usuario. Estos sistemas se basan en círculos de confianza, generados por un acuerdo entre las partes y cerciorados por una institución externa. A través de este acuerdo se aceptan ciertos protocolos de seguridad y privacidad para compartir información. Cada uno de estos círculos, son llamados federaciones[4].

2.2.2.1. Usuario, identidad y Credenciales

- Un **usuario** puede caracterizarse como un cliente o entidad (host/aplicación) la cual desea obtener algún servicio de un proveedor. El usuario puede ser una persona utilizando un agente interfaz (navegador web) o un sistema informático (servicios web). Un requisito necesario para que el usuario pueda obtener un recurso del proveedor es poseer una identidad que lo represente.
- **Identidad** es una representación de una entidad en un contexto particular. Una identidad posee identificadores y credenciales de los usuarios.
- Una **credencial** es una calificación certificada expedida a un indivıduo por terceros con autoridad y competencia pertinentes para tal acto.[6].

2.2.2.2. Control de acceso (autenticación y autorización)

El proceso de verificar la existencia de una identidad es llamada autenticación. Para que este proceso se inicie es necesario que el usuario proporcione una credencial para validar el método de autenticación utilizado por la entidad de autenticadora. De poseer una credencial valida, la entidad autenticadora podrá verificar en su base de identidades la credencial proporcionada por el usuario. Si la entidad de autenticación encontró datos relacionados con la credencial de entrada, el usuario es autenticado. Con esto se entiende que el usuario ha demostrado ser quien dijo ser.
Una vez realizada la autenticación de usuario, la entidad de autenticación podrá verificar cuál o cuáles son los permisos de acceso al recurso solicitado originalmente. A este proceso de verificar los permisos de acceso a un determinado recurso lo llamamos autorización[7].

2.2.2.3. Modelos de sistemas de gerenciamento de identidades

- **Modelo Silo**

En el Modelo Silo, el proveedor de servicios web tiene la función de proveedor de identidad que emite un ID para el uso de servicios web. El proveedor de servicios especifíca el ID de usuario que únicamente es valida dentro del área de servicio. Cada usuario recibe un ID diferente para cada proveedor de servicio. Este modelo es el más simple y más fácil de implementar. Sin embargo, si el número de servicios en línea aumenta, el número de ID que deben ser gestionados por el usuario también se incrementa[5].

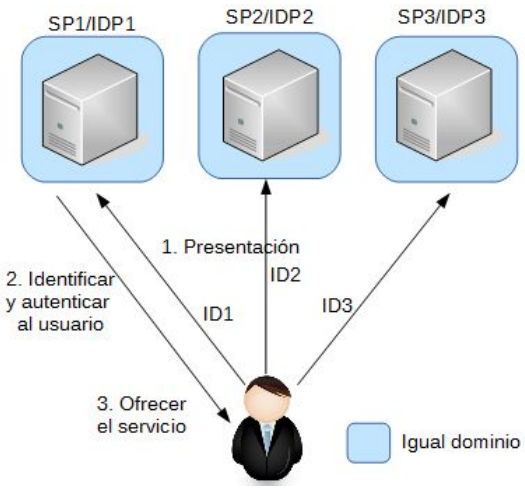

Figura 1: Modelo Silo
Fuente: El Investigador

Este modelo, aunque ampliamente utilizado se considera ineficaz, tanto para los usuarios que tienen que gestionar múltiples cuentas y contraseñas, y para el proveedor de servicios, que pueden tener sus políticas de seguridad y no son respetadas plenamente por los usuarios debido a la cantidad de servicios que disfruta[8].

- **Modelo Centralizado**

El modelo centralizado permite al usuario conectarse a todos los proveedores de servicios dentro del mismo dominio utilizando una identificación emitida por un solo Proveedor de Identidad.
El modelo centralizado se puede implementar de diferentes maneras; el tipo más simple es Single Sign On (SSO). En este modelo, un usuario puede acceder fácilmente y usar diferentes servicios web con una única ID, sin embargo, este modelo tiene algunas vulnerabilidades.
Si el atacante obtiene información de autenticación, puede fácilmente hacerse pasar por el usuario para acceder a todos los servicios en el campo[5].

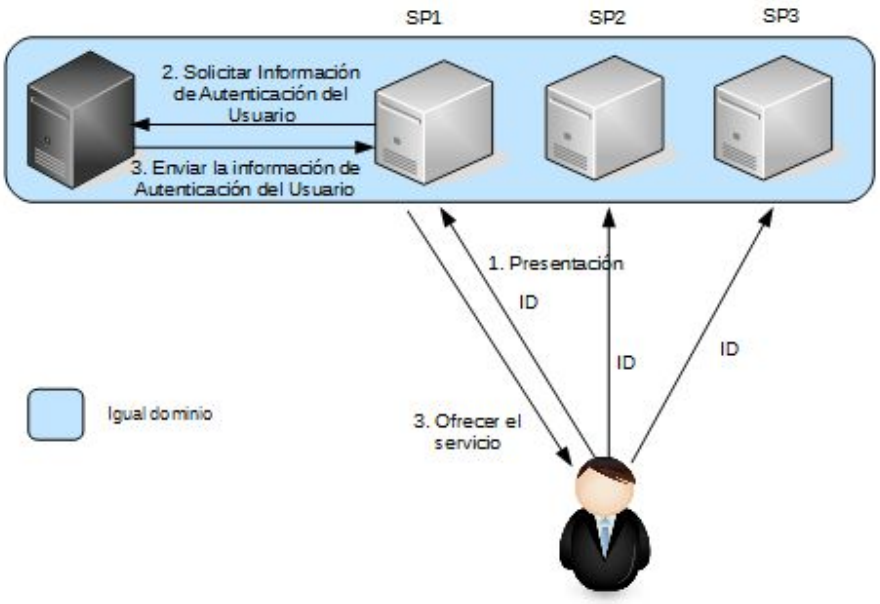

Figura 2: Modelo Centralizado
Fuente: El Investigador

Este modelo es ampliamente criticado por presentar el riesgo de punto único de fallo en el Proveedor de Identidad central, y por lo tanto puede comprometer todo el sistema en caso de fallo de proveedor. Otro de los riesgos asociados a este modelo es el poder informativo concentrado en el Proveedor de Identidad, que sabe todo acerca de los usuarios y se puede utilizar esta información como desee [8].

- **Modelo Federado**

En el modelo federado, el Proveedor de Identidad comparte el ID del usuario entre los proveedores de servicios que pertenecen a un círculo de confianza, el mismo que está constituido por un acuerdo relativo a la seguridad y autentificación entre los Proveedores de Identidad y los proveedores de servicios, y están federados por este acuerdo.
En este modelo se puede proporcionar un servicio de Single Sign On (SSO) en un entorno abierto y puede ser fácilmente compatible con el modelo centralizado, sin embargo, es difícil diferenciar entre un usuario real y un enmascarado como un proveedor de servicio como usuario, además, si los proveedores de servicios son maliciosos, puede investigar el usuario, mapeando varios ID's de usuario, porque parte de la información es compartida entre Proveedor de Identidad (IdP) y Proveedores de Servicio (SP), poniendo en peligro la privacidad de los usuarios.
Por lo tanto, en este modelo se requiere el consentimiento del usuario en relación con el tipo, alcance y propósito del uso de la información presentada durante el mapeo entre el Proveedor de Identidad (IdP) y Proveedores de Servicio (SP)[5].

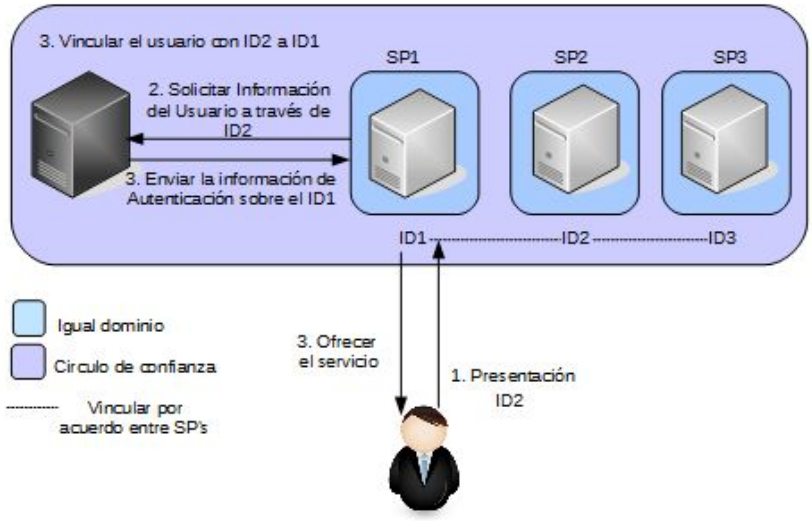

Figura 3: Modelo Federado
Fuente: El investigador

- **Modelo Centrado en el usuario**

En este modelo el usuario controla y gestiona su información y las políticas de uso de identificación. El usuario puede controlar todos los pasos necesarios para crear, utilizar y mantener su Información de Identificación Personal y los ID. En este modelo se requiere el consentimiento del usuario antes de transmitir y compartir su información e ID, así como la información de autenticación[5].

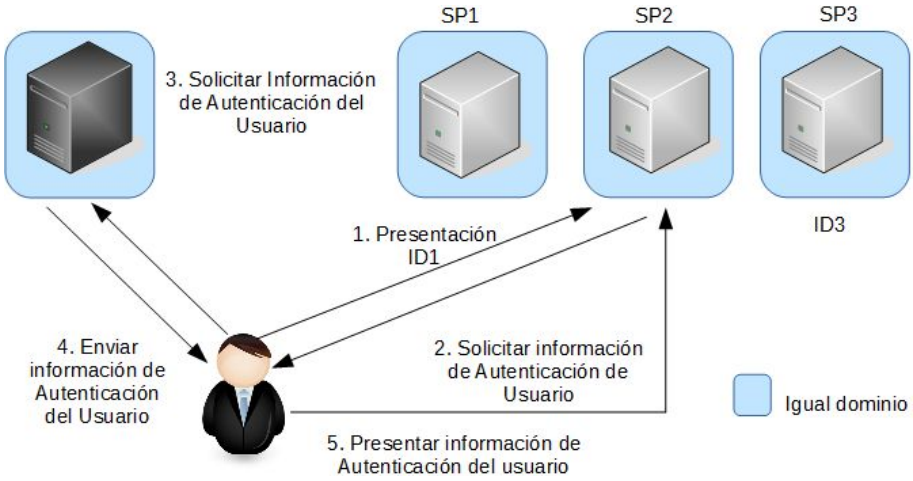

Figura 4: Modelo Centralizado en el Usuario
Fuente: El investigador

MODELO	IDENTIDAD	ID DE USUARIO	CONTRASEÑA	RIESGO
SILO	Administrada por cada servicio del proveedor que también actúa como idp.	Varias para cada servicio	Varias para cada servicio	Múltiples contraseñas mientas aumenta número de servicios, pérdida de información por parte del usuario.
CENTRALIZADO	Único Proveedor de Identidad.	Un solo ID de usuario	Una contraseña	Riesgo de punto único de fallo en el IDP, y por lo tanto pueden comprometer la totalidad del sistema en caso de fallo en el proveedor. El IDP sabe todo acerca de los usuarios y puede utilizar esta información de forma maliciosa. Único dominio.
FEDERADO	ID compartido entre los proveedores de servicios que pertenecen al círculo confianza.	Un solo ID de usuario	Una contraseña	Si el SP es malicioso puede investigar al usuario mapeando varios id's de usuario debido a que la información es compartida entre IDP y SP.
CENTRADO EN EL USUARIO	El usuario tiene control total sobre sus identidades digitales	Un solo ID de usuario	Una contraseña	Los SP no pertenecen a un círculo de confianza y se requiere la autenticación para acceder a los servicios de cada SP.

Tabla 1: Modelos de Sistemas de Gerenciamiento de Identidades

Fuente: El investigador

2.2.3. Federación y SSO (Single Sign -On)

Una federación representa un conjunto de organizaciones que cooperan entre sí de acuerdo con reglas de confianza pre establecidas para la autenticación de usuarios y el intercambio de recursos. Una solución de federaciones es considerada deseable cuando las organizaciones crecen al adquirir nuevos sitios de servicios o recursos, para el mantenimiento de repositorios distribuidos y simplificar la autenticación y autorización de usuarios a los recursos y aplicaciones a través de dominios socios[9].

Mediante una federación los usuarios pueden emplear las mismas credenciales para identificarse en redes de diferentes universidades, empresas o entidades. De este modo las entidades difunden información sin compartir el almacenamiento, seguridad y autenticación de los usuarios. Para su funcionamiento es necesaria la utilización de estándares que definan mecanismos que permiten a las diferentes organizaciones compartir información entre dominios. El modelo es aplicable a un grupo de organizaciones o a una gran organización con numerosas delegaciones y se basa en el círculo de confianza, un usuario es conocido en una comunidad determinada y tiene acceso a servicios específicos[10].
La federación de identidad, describe las tecnologías, estándares y casos de uso los cuales sirven para habilitar la portabilidad de información de identidad entre diferentes dominios de seguridad autónomos. El objetivo final de la federación de identidad es dar acceso seguro a datos, sistemas u otros dominios, a los usuarios de un dominio, y sin necesidad de redundancia de administración de usuarios[11].

Componentes de una Identidad Federada

- **Single Sign On (SSO)** : Un sistema Single Sign On es un sistema que permite simplificar el acceso por parte del usuario, y de las aplicaciones, a diferentes aplicaciones que comparten los mismos usuarios y por tanto el mismo sistema de autenticación. Este sistema nace de la necesidad de autenticar y autorizar al mismo grupo de usuarios, pero en diferentes aplicaciones. Por lo tanto se propone un sistema de autenticación único de tal modo que todas las aplicaciones utilicen este mismo sistema, y mejorando así la experiencia del usuario final ya que siempre introducirá sus credenciales en un sistema homogéneo independientemente de la aplicación, y además la sesión permanece entre diferentes aplicaciones. Por parte de las aplicaciones que utilizan este sistema, evita la necesidad de tratar con la identidad de estos usuarios ya que el sistema de Single Sign On es el que los autentica.

  SSO es un método de control de acceso que permite autenticar al usuario una vez, y conseguir acceso a diferentes recursos en diferentes sistemas. En una infraestructura homogénea, o al menos en una en la que exista un único esquema de autenticación o donde existe una base de datos centralizada de usuarios. En la federación de identidad el Single Sign On no es algo necesario, pero es recomendable. No es un requisito indispensable para montar un sistema de gestión de identidad federada, pero si facilita mucho el acceso por parte del usuario. Por lo tanto en la mayoría de los sistemas

de federación de identidad se hace uso de SSO[12].

- **Proveedor de servicios (SP):** Entidad más cercana al dominio del recurso en cuestión. Es el responsable de verificar y validar los cookies de sesión y de dar los permisos de acceso a los recursos de acuerdo al usuario autenticado.

  El Proveedor de Servicios permite impedir el acceso a las aplicaciones redirigiendo a los usuarios a sus correspondientes Proveedores de Identidad (IdP) para que se autentiquen, y en ese caso permite el acceso comunicándose con el IdP que le proporcionará la información necesaria para la autorización y el correcto funcionamiento de las aplicaciones.

  Un Proveedor de Servicios (SP) está estrechamente relacionado con un servidor web y se comunica con los diferentes Proveedores de Identidad (IdP's) de la federación. Esta es la forma que tiene el sistema de pasar los datos de identidad de una organización a otra de forma segura.

  Cada aplicación web federada deberá estar protegida por un SP, así pues puede haber más de un SP por cada organización[12].

- **Proveedor de Identidad (IdP)**: Un proveedor de identidad es un sistema que gestiona la identidad de los usuarios de una organización y ofrece un servicio de autenticación a otras aplicaciones.

  En la práctica un Proveedor de Identidad es una aplicación web a la cual serán redirigidos todos los usuarios de una organización que quieran acceder a una aplicación federada y donde se autenticarán, y este IdP ofrecerá los datos de autenticación a las diferentes aplicaciones federadas. Es necesario que haya un IdP por cada organización participante en la federación de identidad puesto que es la vía de autenticación de sus usuarios internos. Su función es mantener la base de datos de los usuarios de dominio y validar las credenciales de los usuarios.

  Es aquí donde se hace importante el sistema Single Sign On (SSO) debido a que este, puede enlazar el IdP con el sistema de SSO para ofrecer un sistema de autenticación único para todas las aplicaciones federadas, ya sean internas a la organización o externas, por lo que el usuario final tendrá un acceso homogéneo a todo el sistema federado[12].

- **Proxy proveedor de identidad (IdPproxy) o WAYF (Where Are You From):** Es la entidad encargada de interrogar al usuario sobre su

dominio de origen. Por lo general, la IdPproxy presenta una lista de IdPs al usuario y este selecciona el más adecuado.

El objetivo del servicio "Where are you from"(WAYF) es guiar al usuario a su propio Proveedor de Identidad (IdP). A veces es llamado "Identity Provider Discovery". Básicamente lo que hace es presentar al usuario una lista de Proveedores de Identidad y redirigir al navegador del usuario al IdP seleccionado.

El WAYF es una parte importante en el sistema de la federación puesto que es el elemento que conecta los Proveedores de Servicio (SP) con los Proveedores de Identidad (IdP). Cuando un usuario intenta acceder a una aplicación protegida tras un SP, este será redirigido al WAYF donde el usuario seleccionará cuál es su organización y en consecuencia el sistema WAYF redirigirá al usuario al Proveedor de Identidad pertinente[12].

- **Servicio de directorio (LDAP)**

  Un servicio de directorio (SD) es una aplicación o un conjunto de aplicaciones que almacena y organiza la información sobre los usuarios de una red de ordenadores, sobre recursos de red, y permite a los administradores gestionar el acceso de usuarios a los recursos sobre dicha red. Además, los servicios de directorio actúan como una capa de abstracción entre los usuarios y los recursos compartidos. Realmente no es imprescindible el servicio de directorio para desplegar una arquitectura de identidad federada pero normalmente siempre va ligada a este tipo de aplicaciones. Sin embargo es posible utilizar bases de datos y otros tipos de almacenamiento o gestión de usuarios aunque la configuración sea más compleja y no tan óptima[12].

2.2.4. RADIUS

RADIUS (Remote Authentication Dial In User Server) es un protocolo que nos permite gestionar la “autenticación, autorización y registro” de usuarios remotos sobre un determinado recurso. La tupla “autenticación, autorización y registro” es más conocida como AAA, al ser éste su acrónimo de su denominación original inglesa “Authentication, Authorization, and Accounting”[13].
RADIUS surgió inicialmente como una solución para la administración en el control de acceso para usuarios que soportaban su conexión mediante enlaces seriales y módems, facilitando el control y supervisión de la seguridad, la autorización, la auditoria, verificación de nombres de usuarios y contraseñas, así

como una detallada información de configuración sobre el tipo de servicio que se pretendía entregar al usuario.
Los elementos característicos que posee RADIUS le han permitido guardar un alto grado de compatibilidad con la arquitectura dispuesta por las redes inalámbricas IEEE 802.11, una razón primordial por la cual es éste el servidor recomendado, según la norma, para prestar los servicios de autenticación en redes inalámbricas.
El protocolo RADIUS sigue un modelo cliente/servidor, donde el papel de servidor es desempeñado por RADIUS que contiene información de los usuarios, almacenando sus contraseñas y sus perfiles, y un elemento de red designado como NAS (Network Access Server), toma la función de cliente de RADIUS; el NAS tiene la responsabilidad de servir como puente o mediador entre los mensajes entrantes y salientes desde y hacia el servidor, es decir, se encarga de retransmitir las solicitudes de conexión, autenticación de usuarios y en general toda la información necesaria para el usuario.
Las transacciones realizadas entre el cliente y el servidor RADIUS son autenticadas mediante la utilización de un secreto compartido, que nunca viajará por la red, además del intercambio entre estos dos puntos de una serie de contraseñas de usuarios, con el fin de minimizar la captura de la contraseña verdadera por la parte de algún intruso en la red [14].

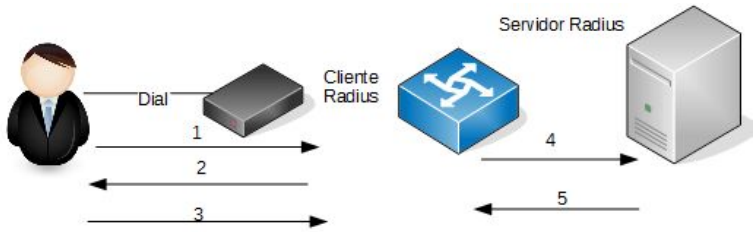

Figura 5: Interacción entre un usuario de marcación de entrada y el servidor y cliente RADIUS
Fuente:El Investigador

1. El usuario inicia la autenticación Point to Point Protocol (PPP) al Network Access Server o Servidor de Acceso a la Red (NAS).

2. El Servidor de Acceso a la Red le pedirá que ingrese el nombre de usuario y la contraseña (en caso de Protocolo de autenticación de contraseña [PAP]) o la integración (en caso de Protocolo de confirmación de aceptación de la contraseña [CHAP]).

3. Contestaciones del usuario.

4. El cliente RADIUS envía el nombre de usuario y la contraseña encriptada al servidor de RADIUS.

5. El servidor RADIUS responde con Aceptar, Rechazar o Impugnar.

6. El cliente RADIUS actúa dependiendo de los servicios y de los parámetros de servicios agrupados con Aceptar o Rechaza[15].

Elementos del servidor RADIUS

- **Protocolo**: Usa 1812 como el puerto de autenticación y 1813 como el puerto de auditoria.

- **Servidor**: El servidor RADIUS se ejecuta en el ordenador o estación de trabajo en el centro, y mantiene la información para la autenticación de usuarios y servicio de de acceso red.

- **Cliente**: El cliente RADIUS se ejecuta en el NASS situado en toda la red[14].

Funciones del Radius

- **Autenticación:** Proceso por el cual se determina si un usuario tiene permiso para acceder a un determinado servicio de red del que quiere hacer uso. El proceso de autenticación se realiza mediante la presentación de una identidad y unos credenciales por parte del usuario que demanda acceso.

- **Autorización**: Se refiere a conceder servicios específicos a un determinado usuario, basándose para ellos en su propia autenticación, los servicios que está solicitando, y el estado actual del sistema. Es posible configurar restricciones a la autorización de determinados servicios en función de aspectos como, por ejemplo, la hora del día, la localización del usuario, o incluso la posibilidad o imposibilidad de realizar múltiples "logins" de un mismo usuario. El proceso de autorización determina la naturaleza del servicio que se concede al usuario, como son: la dirección IP que se le asigna, el tipo de calidad de servicio que va a recibir, el uso de encriptación, o la utilización obligatoria de túneles para determinadas conexiones.

- **Registro**: Registro del consumo de recursos que realizan los usuarios. El registro suele incluir aspectos como la identidad del usuario, la naturaleza del servicio prestado, y cuándo empezó y terminó el uso de dicho servicio[13].

2.2.5. X.500/DAP

X.500 organiza las entradas en el directorio de manera jerárquica, capaz de almacenar gran cantidad de datos, con grandes capacidades de búsqueda y fácilmente escalable. X.500 especifica que la comunicación entre el cliente y el servidor de directorio debe emplear el Directory Access Protocol (DAP). Pero DAP es un protocolo a nivel de aplicación, por lo que, tanto el cliente como el servidor debían implementar completamente la torre de protocolos OSI[16].
En X.500 el agente de sistema de directorio (DSA) es la base de datos donde se almacena información de directorio. Esta base de datos es jerárquica en formulario, diseñado para proporcionar recuperación y búsqueda rápida y eficiente. El agente de usuario de directorio (DUA) proporciona funcionalidad que puede implementarse en todo tipo de interfaces de usuario a través de clientes DUA dedicados, puertas de enlace de servidor de Web o aplicaciones de correo electrónico.
El protocolo de acceso a directorio (DAP) es un protocolo que se utiliza en servicios de directorio X.500 para controlar las comunicaciones entre los agentes DUA y DSA. Los agentes representan el usuario o el programa y el directorio, respectivamente[17].
DAP es un protocolo que resultó ser extremadamente pesado, operaba sobre un modelo OSI (Open System Interconnection) y requería una cantidad significativa de recursos computacionales; por lo que LDAP nació como respuesta para simplificar el acceso al directorio X.500[18].

2.2.6. LDAP

Ligthweight Directory Access Protocol es un protocolo de aplicación sobre TCP/IP que permite el acceso a un servicio de directorio. Los directorios con los que trabaja LDAP son de propósito general si bien es utilizado comúnmente para almacenar la información referente a organizaciones, elementos en redes de computadores, usuarios o documentos [19].
LDAP surge como una alternativa a DAP. Las claves del éxito de LDAP en comparación con DAP de X.500 son:

- LDAP utiliza TCP/IP en lugar de los protocolos del modelo OSI. TCP/IP requiere menos recursos y está más disponible, especialmente en ordenadores de sobremesa.

- El modelo funcional de LDAP es más simple y ha eliminado opciones raramente utilizadas en X.500. LDAP es más fácil de comprender e

implementar.

- LDAP representa la información mediante cadenas de caracteres en lugar de complicadas estructuras ASN.1

El esquema de interacción entre el cliente y el servidor LDAP sigue el siguiente esquema:

1. El cliente indica el servidor y el puerto en el que el servidor LDAP está escuchando. El cliente establece una sesión con el servidor LDAP. El cliente puede proporcionar información de autenticación o establecer una sesión anónima con los accesos por defecto.

2. El cliente efectúa las operaciones sobre los datos. LDAP proporciona capacidades de búsqueda, lectura y actualización.

3. Una vez finalizadas las operaciones, el cliente cierra la sesión.

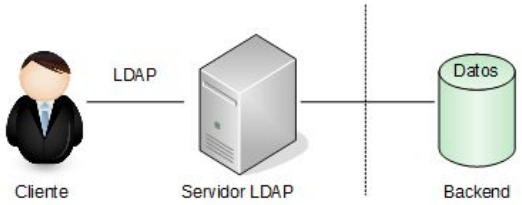

Figura 6: Estructura LDAP
Fuente: El Investigador

Arquitectura Cliente-Servidor del servicio de Directorio.

Los servicios de directorio suelen implementarse siguiendo el modelo cliente-servidor, de modo que una aplicación que desea acceder al directorio no accede directamente a la base de datos, sino que llama a una función de la API (Application Programming Interface), que envía un mensaje a un proceso en el servidor. Dicho proceso accede al directorio y devuelve el resultado de la operación. Algunas veces, el servidor puede convertirse en el cliente de otro servidor para conseguir la información necesaria para procesar la petición que se le ha realizado.

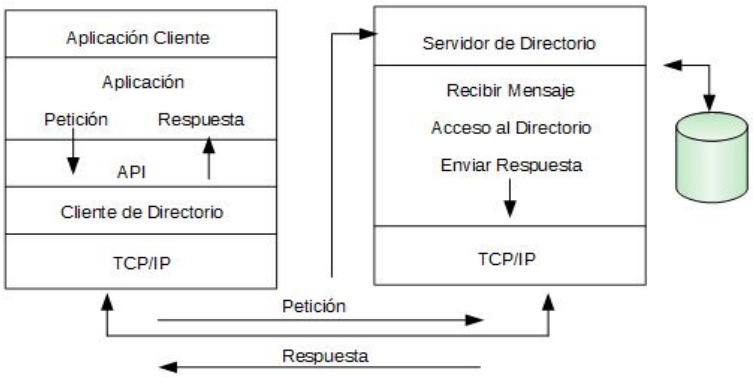

Figura 7: Estructura LDAP
Fuente: El Investigador

Siguiendo esta arquitectura el cliente no depende de la arquitectura del servidor y el servidor puede implementar el directorio de la forma más conveniente.

Directorios distribuidos.

El servicio de directorio puede estar centralizado o distribuido. En el caso de ser centralizado, un único servidor da todo el servicio de directorio, respondiendo a todas la consultas de los clientes. Si el directorio esta distribuido, varios servidores proporcionan el servicio de directorio. Cuando el servicio de directorio esta distribuido, los datos pueden estar fraccionados y/o replicados. Cuando la información esta fraccionada, cada servidor de directorio almacena un subconjunto único y no solapado de la información, es decir, una entrada es almacenada en un solo servidor. Cuando la información esta replicada, una entrada puede estar almacenada en varios servidores. Generalmente cuando el servicio de directorio es distribuido, parte de la información está fraccionada y parte está replicada.

Seguridad del directorio.

Algunos directorios deben permitir el acceso público, pero cualquier usuario no debe poder realizar cualquier operación. La política de seguridad define quién tiene qué tipo de acceso sobre qué información.
El directorio debe permitir las capacidades básicas para implementar la política de seguridad. El directorio puede no incorporar estas capacidades, pero debe estar integrado con un servicio de red fiable que proporcione estos servicios básicos de seguridad. Inicialmente se necesita un método para autenticar al usuario, una vez que se ha verificado la identidad del cliente, se puede determinar si esta autorizado para realizar la operación solicitada.

Generalmente las autorizaciones se encuentran en ACL (Access Control List); estas listas se pueden unir a los objetos y/o los atributos contenidos en el directorio, para facilitar su administración, los usuarios con los mismos permisos, son agrupados en grupos de seguridad[20].

Elementos del modelo de información

- **Entradas**: Unidades básicas de LDAP equivalentes a los nodos que conforman un árbol. Cada una de ellas refleja un concepto u objeto del mundo real (usuarios, organizaciones, hosts). Cada entrada está definida jerárquicamente de forma relativa a su nodo padre.

  Cada entrada tiene un nombre llamado Distinguished Name(DN), que la identifica unívocamente. Un DN consiste en una secuencia de partes más pequeñas llamadas Relative Distinguished Name (RDN), de forma similar a como el nombre de un fichero consiste en un camino de directorios en muchos sistemas operativos.

  Las entradas pueden ser organizadas en forma de árbol basándose en los Distinguished Name (DN), a este árbol de entradas de directorio se le conoce como Directory Information Tree (DIT).

- **Atributo**: Cada entrada está compuesta por una serie de atributos, cada uno de ellos formado por pares nombre:valor, estos puede ser multivaluados, es decir, cada atributo puede tener más de un valor asignado. En LDAP una entrada se puede definir mediante un archivo LDIF (LDAP interchange format) en el que se describen los diferentes atributos que lo componen. En cada archivo LDIF se pueden definir una o mas entradas, usando una línea en blanco como separador de entradas. Se puede distinguir dos tipos de atributos; atributos atómicos y de clase que indican el tipo de entrada que se está definiendo.

- **Clases:** Definen los atributos que tiene un tipo de entrada determinado. Toda entrada tiene que tener al menos un atributo objectclass que indica la clase a la que pertenece, y por lo tanto el resto de atributos que debe y puede tener. En una clase se definen los atributos como requeridos(obligatorios) o permitidos (opcionales). Cada objectclass tiene un identificador único[19].

2.2.6.1. Modelos de LDAP

Además de definir el protocolo de acceso al directorio, el estándar LDAP define cuatro modelos que permiten entender mejor el servicio de directorio.

- **Modelo de información**, describe la estructura de la información almacenada en el directorio LDAP.
- **Modelo de nombrado**, describe como se organiza e identifica la información en el directorio LDAP.
- **Modelo funcional**, describe que operaciones pueden ser realizadas sobre la información almacenada en el directorio LDAP.
- **Modelo de seguridad**, describe como puede protegerse la información contenida en el directorio LDAP frente a accesos no autorizados[20].

2.2.7. Active Directory

Active Directory almacena información acerca de los usuarios, equipos y recursos de red y permite el acceso a los recursos por parte de usuarios y aplicaciones. Proporciona una forma coherente de asignar nombres, describir, localizar, obtener acceso, administrar y proteger la información de estos recursos[9].

Funciones

- **Centralizar el control de los recursos de red.** Al centralizar el control de recursos como servidores, archivos compartidos e impresoras, sólo los usuarios autorizados pueden obtener acceso a los recursos de Active Directory.
- **Centralizar y descentralizar la administración de recursos.** Los administradores pueden manejar equipos cliente distribuidos, servicios de red y aplicaciones desde una ubicación central mediante una interfaz de administración coherente o pueden distribuir tareas mediante la delegación del control de los recursos.
- **Almacenar objetos de forma segura en una estructura lógica.** Active Directory almacena todos los recursos como objetos en una estructura lógica, jerárquica y segura.
- **Optimizar el tráfico de red.** La estructura física de Active Directory permite utilizar el ancho de banda de red de forma más efectiva. Por

ejemplo, garantiza que, cuando un usuario inicie una sesión en la red, la autoridad de autenticación más cercana a él lo autentique, reduciendo así la cantidad de tráfico de red[21].

Características

- **Escalabilidad:**Puede crecer y soportar un elevado número de objetos.
- **Integración con el DNS:**
  - Los nombres de dominio son nombres DNS y tienen que estar registrados en él.
  - Active Directory usa DNS como servicio de nombres y de localización.
  - Es necesario instalar DNS antes de poder instalar AD.
- **Extensible**: Permite personalizar las clases y objetos que están definidas dentro de Active Directory según las necesidades propias.
- **Seguridad**
- **Multimaestro:**
  - No distingue entre controladores de dominio primarios o secundarios.
  - Cualquier controlador de dominio puede procesar cambios del directorio.
  - Las actualizaciones o modificaciones realizadas en un controlador se replican al resto, siendo todos "iguales".
- **Flexible:**
  - Permite reflejar la organización lógica y física de la empresa u organización donde se instala.
  - Permite que varios dominios se conecten en una estructura de árbol o de bosque[9].

2.2.7.1. Componentes de la estructura lógica

- **Objetos:** Son los componentes más básicos de la estructura lógica. Un objeto es diferenciado por su nombre y representa un recurso de red. Cada clase de objetos se define mediante un grupo de atributos, que definen los posibles valores que se pueden asociar a un objeto[21].

- **Unidades organizativas:** Son contenedores que permiten ordenar los recursos u objetos dentro de un dominio. Mediante la estructuración de los objetos por unidades organizativas, se facilita su localización y administración. También se puede delegar la autoridad para administrar una unidad organizativa. Las unidades organizativas pueden estar anidadas en otras unidades organizativas, lo que simplifica la administración de objetos[21].

- **Dominios**: Se trata de las unidades funcionales centrales en la estructura lógica de Active Directory que son un conjunto de objetos definidos de forma administrativa y que comparten una base de datos, directivas de seguridad y relaciones de confianza comunes con otros dominios. Los dominios proporcionan las siguientes tres funciones:

  - Un límite administrativo para objetos.
  - Un medio de administración de la seguridad para recursos compartidos.
  - Una unidad de replicación para objetos[21].

- **Árboles de dominios:** Los dominios que están agrupados en estructuras jerárquicas se denominan árboles de dominios.

  Al agregar un segundo dominio a un árbol, se convierte en secundario del dominio raíz del árbol. El dominio al que está adjunto un dominio secundario se denomina dominio primario. Un dominio secundario puede tener a su vez su propio dominio secundario. El nombre de un dominio secundario se combina con el nombre de su dominio primario para formar su propio nombre único de Sistema de nombres de dominio (DNS, Domain Name System), de esta forma, el árbol dispone de un a espacio de nombres contiguo[21].

- **Bosques:** Un bosque es una instancia completa de Active Directory. Consta de uno o varios árboles.

  En un árbol de sólo dos niveles, todos los dominios secundarios se convierten en secundarios del dominio raíz de bosque para formar un árbol contiguo. El primer dominio del bosque se denomina dominio raíz de bosque. El nombre de ese dominio se refiere al bosque. De forma predeterminada, la información de Active Directory se comparte sólo dentro del bosque. De este modo, el bosque es un límite de seguridad para la información contenida en la instancia de Active Directory[21].

2.2.7.2. Componentes de la estructura física

- **Controladores de dominio.** Administran todas las facetas de las interacciones de los usuarios en un dominio (localización de objetos o validación de un intento de inicio de sesión). Cada controlador de dominio realiza funciones de almacenamiento y replicación. Un controlador de dominio sólo puede admitir un dominio. Para asegurarse de la disponibilidad continua de Active Directory, cada dominio debe disponer de más de un controlador de dominio[9].

- **Sitios de Active Directory**. Un sitio es una agrupación de equipos que están conectados físicamente por conexiones rápidas y de alta fiabilidad. Habitualmente equipos conectados en una LAN. Al establecer sitios, los controladores de dominio de un único sitio se comunican con frecuencia. Esta comunicación minimiza la latencia dentro del sitio, es decir, el tiempo necesario para que un cambio realizado en un controlador de dominio pueda replicarse en otros controladores de dominio. Se pueden crear sitios para optimizar el uso del ancho de banda entre los controladores de dominio que están en ubicaciones diferentes[9].

- **Particiones de Active Directory**: Cada controlador de dominio contiene las siguientes particiones de Active Directory:

  - La partición del dominio contiene replicados de todos los objetos de ese dominio. La partición del dominio sólo puede replicarse en otro controlador de dominio del mismo dominio.
  - La partición de configuración contiene la topología del bosque. La topología es un registro de todos los controladores de dominio y las conexiones entre ellos en un bosque.
  - La partición del esquema contiene el esquema de todo el bosque. Cada bosque tiene un esquema para que la definición de las clases de objetos sea coherente. Las particiones de configuración y del esquema pueden replicarse en los controladores de dominio del bosque.
  - Las particiones de aplicaciones opcionales contienen objetos no relacionados con la seguridad y utilizados por una o varias aplicaciones. Las particiones de aplicaciones pueden replicarse en controladores de dominio especificados del bosque[9].

Al analizar los diferentes escenarios de autenticación y servicios de directorios se puede concluir que la sustitución del Active Directory por Samba-OpenLdap

ofrece numerosas ventajas, no sólo por ser este un software amparado por licencias de libre distribución, sino por ser un sistema altamente configurable, que permite personalizar una organización en la medida exacta a través del directorio. La aplicación de servidor LDAP proporciona funcionalidad de Servicios de Directorios de una forma muy similar a los servicios de Microsoft Active Directory. Tales servicios incluyen gestionar las identidades y las relaciones entre los ordenadores, usuarios y grupos de ordenadores o usuarios que participan en la red. OpenLDAP puede usarse junto con SAMBA para proporcionar servicios de Archivo, Impresión y Directorio prácticamente de la misma forma que un Controlador de Dominio de Windows, si se compila SAMBA con soporte LDAP. OpenLDAP no tiene nada que envidiarle al Microsoft Active Directory, las herramientas están ahí, sólo hay que saberlas implementar y administrar, lo que sería su único costo (tiempo y paciencia).
RADIUS al recibir los datos proporcionados por un usuario, para realizar la Autentificación, puede verificarlos desde:

- **Mecanismos**: Active Directory, LDAP, Kerberos
- **Internal Database:** ID del usuario, contraseña, etc. se almacenan en la base de datos interna de RADIUS.
- **Autentificación de SQL** La información del usuario es almacenada en una base de datos SQL.

Además tiene la factibilidad de usar software de Base de Datos como OpenLDAP, PostgreSQL, Oracle En sus inicios debido a las soluciones tecnológicas del momento, se concibió para controlar de forma centralizada el acceso remoto de usuarios cuya conexión se realizaba mediante módems. A medida que se ha ido produciendo el desarrollo tecnológico, el protocolo RADIUS se ha implementado con éxito en escenarios de redes inalámbricas, ofreciéndoles la robustez y control necesarios en lo que a seguridad se refiere.

CAPÍTULO 3

Metodología

3.1. Modalidad Básica de la investigación

La realización de la presente investigación se basó en la investigación de campo la cual analiza el problema partiendo de hechos reales, para la obtención de información y requerimientos que evidencien los objetivos.

3.2. Población y muestra

La presente investigación por su característica no requiere población y muestra.

3.3. Recolección de información

Partiendo de que el objetivo de la investigación, es desarrollar un Sistema de Federaciones en la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, se realizó una entrevista no estructurada al Administrador de Redes de la Facultad a fin de constatar la necesidad de desarrollar dicho Sistemas en beneficio de la comunidad universitaria.
Además se realizó una revisión bibliográfica en documentos tales como: papers, libros y tesis correspondientes al tema, los mismos que proporcionaron la información necesaria para la estructuración del presente tema de investigación.

3.4. Procesamiento y análisis de datos

Una vez recolectada la información se procedió a su respectivo análisis obteniendo resultados satisfactorios los cuales fueron de gran importancia para la formulación de la propuesta. Los datos fueron analizados y procesados en relación al problema para poder establecer las respectivas conclusiones asegurando que los datos son lo más reales posibles.

3.5. Desarrollo del Proyecto

1. Analizar las aplicaciones y sistemas que posee la Facultad de Ingeniería en Sistemas, Electrónica e Industrial que son aptas para la aplicación de federaciones.
    - Elaboración de un inventario con las aplicaciones usadas por los estudiantes y docentes dentro de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.
    - Selección de las aplicaciones que requieran autenticación para la integración en el Sistema Federado.
2. Analizar el diccionario de datos en las aplicaciones y sistemas escogidos que posee la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.
    - Determinación de los mecanismos y campos de autenticación de cada aplicación.
3. Determinar los Sistemas de identidad federados de código abierto de libre acceso, disponibles en la actualidad y de mayor uso.
    - Estudio comparativo entre los Sistemas Federados de código abierto encontrados.
    - Determinación y revisión de las características técnicas de los Sistemas Federados de código abierto de mayor uso.
4. Desarrollar el Sistema de federaciones demostrativo para las plataformas utilizadas en la Facultad de Ingeniería en Sistemas, Electrónica e Industrial
    - Realización de la instalación y configuración de un servidor de autenticación para la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.
    - Determinación de los protocolos necesarios para la integración de las aplicaciones que serán parte del sistema de federado.
    - Ejecución de las pruebas respectivas para validar el servicio de federaciones.
    - Elaboración de ventajas y desventajas para la puesta en producción de un sistema de federaciones en la FISEI.

CAPÍTULO 4

Desarrollo de la propuesta

4.1. Datos Informativos

4.1.1. Tema de la Propuesta

"SISTEMA DE FEDERACIONES DE IDENTIDADES PARA LA FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL USANDO SOFTWARE DE CÓDIGO ABIERTO."

4.1.2. Institución Ejecutora

- Institución Educativa: Universidad Técnica de Ambato
- Nombre de la Institución: Facultad de Ingeniería en Sistemas, Electrónica e Industrial.
- Tipo de Organización: Pública
- Departamento: CEDIA

4.1.3. Beneficiarios

Universidad Técnica de Ambato Estudiantes, profesores y personal administrativo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

4.1.4. Ubicación

- Provincia: Tungurahua
- Cantón: Ambato
- Dirección: Av. Los Chasquis y Río Payamino
- Teléfono: 03 2415288

4.1.5. Equipo Responsable

- Tutor: Ing. David Guevara
- Investigador: Alexandra Cevallos

4.2. Análisis de las aplicaciones y sistemas que posee la FISEI

Para el análisis se establece una Entrevista no estructurada realizada por la autora Alexandra Cevallos, establecida directamente con el Ingeniero Eduardo Chaso administrador del Departamento de Redes de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

- ¿Existe algún mecanismo de Identidad Federada dentro de la Facultad?

  La facultad no cuenta con un sistema de Identidad Federada. Actualmente los docentes cuentan con una plataforma para el registro de notas y asistencia de los estudiantes, además para el registro control docente y su correo personal. Los estudiantes también ingresan a esta plataforma para rendir exámenes y subir tareas diarias, además poseen un correo institucional y el ingreso al un sistema de notas (utamático) para visualizar sus calificaciones durante su vida académica dentro de la institución.

- ¿Qué plataformas manejan estudiantes y docentes dentro de la FISEI?

  Dentro de la Facultad los docentes manejan plataformas tales como: Registro control docente, Utamático, Moodle, Correo Institucional, Repositorio Digital, Seguimiento a Graduados. Mientras que los estudiantes hacen uso de todas las anteriores excepto el registro control docente, pero con distintos privilegios.

Una vez terminada la entrevista se puede afirmar que la FISEI no dispone actualmente con un sistema de Identidad Federado que permita la autenticación directa con las distintas plataformas. La factibilidad de implementar este Sistema es contemplado en la entrevista como medio de investigación. Para ello se establece un análisis de las diferentes plataformas y aplicaciones con las que cuenta de la facultad, tanto de uso estudiantil como del personal docente, entre ellas se encuentra: Utamático Estudiante-Docente, Sistema Registro Control Docente, Correo Institucional.

APLICACIÓN	CAMPO	TIPO	TAM	DESCRIPCIÓN	MEDIO
PLATAFORMA VIRTUAL	Nombre de Usuario	Alfanumérico	20	Identifica el nombre de usuario	Moodle
	Contraseña	Alfanumérico	20	Generada al momento de crear el usuario	
UTAMÁTICO-DOCENTE	Usuario	Alfanumérico	10	Cédula de identidad que identifica al usuario.	SQL Server
	PIN	Alfanumérico	10	Proporcionado por el DIRA	
UTAMÁTICO-ESTUDIANTE	Usuario	Alfanumérico	10	Cédula de identidad que identifica al usuario.	SQL Server
	PIN	Alfanumérico	10	Proporcionado por el DIRA	
REGISTRO CONTROL DOCENTE	Usuario	Alfanumérico	10	Cédula de identidad que identifica al usuario.	PostgreSQL
	Contraseña	Alfanumérico	10	Proporcionado por el Administrador de Redes de la FISEI	

Tabla 2: Diccionario de Datos

Fuente: El Investigador

APLICACIÓN	CAMPO	TIPO	TAM	DESCRIPCIÓN
LDAP-MANAGER	Login	Alfanumérico	1000	cn="Manager" ,dc="dominio"
	Contraseña	Alfanumérico	1000	Contraseña proporcionada al momento de configurar LDAP
LDAP-USUARIO	Login	Alfanumérico	1000	uid="nombre_usuario", ou="grupo_pertenece" ,dc="dominio"
	Contraseña	Alfanumérico	1000	Contraseña proporcionada al momento de crear usuarios LDAP
ACTIVE DIRECTORY	Login	Alfanumérico	1000	CN=Common Name, OU=Organización, DC=Dominio
	Contraseña	Alfanumérico	1000	Contraseña proporcionada al momento de crear usuarios AD

Tabla 3: Sistemas de Autenticación

Fuente: El Investigador

4.2.1. Análisis de software de identidad federada

4.2.1.1. PAPI

Punto de Acceso a proveedores de información. Es una propuesta de RedIris para el acceso ubicuo a recursos de información. PAPI es un sistema que permite la autenticación y autorización de usuarios a través de una red de servicios Web. Sus principales características son la implementación de “single sign on” y la capacidad de actuar como "proxy de reescritura transparente al usuario". Actualmente se encuentra en desarrollo los mecanismos que lo hagan compatible con Shibboleth [22].

PAPI es un sistema de intercambio de datos de identidad digital, capaz de trabajar en modo federado. Las tareas de identificación y establecimiento de los datos pertinentes a un usuario (autenticación) se llevan a cabo en el entorno de la organización a la que pertenece, mientras que los procedimientos para establecer derechos de acceso a los recursos (autorización) están bajo el control de la organización que los proporciona. PAPI proporciona los mecanismos de transferencia de datos y de establecimiento de la confianza entre los participantes necesarios para que este esquema funcione.

PAPI es un sistema de autenticación y autorización que proporciona unos mecanismos para realizar el control de acceso a aquellos recursos que necesitan proteger cierta información y que están distribuidos en una red. Su principal objetivo es mantener la autenticación como una cuestión local a la organización a la que pertenece el usuario, mientras que los recursos realizarán el proceso de autorizar los accesos de dichos usuarios.

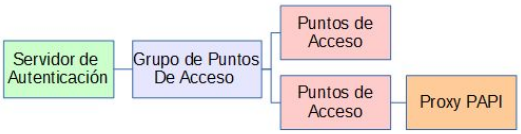

Figura 8: Componentes PAPI
Fuente: El Investigador

El sistema dispone de 4 componentes diferentes:

- **Servidor de autenticación (AS):** también llamado Proveedor de Identidad se encarga del proceso de autenticar al usuario, validando su identidad y asociándole una serie de atributos para que presente en los recursos protegidos.

- **Punto de Acceso (PoA):** este componente, conocido como Proveedor de Servicio, realiza la autorización del acceso a un recurso protegido comprobando la autenticación del usuario y sus atributos.
- **Grupo de Puntos de Acceso (GPoA)**: permite centralizar las políticas de autorización de una organización en un sólo punto, al cual preguntarán los Proveedores de Servicio de dicha organización.
- **Proxy PAPI:** es un proxy HTTP con re-escritura de los enlaces con respecto a un recurso web externo. De esta forma, recursos que sólo permiten autenticación por IP pueden integrarse también en una infraestructura de autenticación y autorización.

Las principales características de PAPI son:

- Infraestructura completa para desplegar un sistema de Single Sign-On dentro de una organización o entre diferentes organizaciones, proporcionando la tecnología necesaria para desplegar una federación de identidad digital.
- Proxy web con re-escritura de enlaces HTTP, permitiendo el acceso controlado a recursos externos que sólo disponen de mecanismos de autorización básicos como el control por IP.
- Protocolo abierto, ligero y documentado.
- Fácilmente interoperable con otros protocolos de autenticación y autorización, como SAML 1.1, SAML 2, OpenID y OAuth.
- Software abierto y disponible en diferentes lenguajes de programación: Perl, PHP, Java, ASP.NET, etc.
- Multitud de conectores disponibles para proveedores de servicio: MediaWiki, DokuWiki, Moodle, etc[23].

4.2.1.2. OAuth

Open Authorization (OAuth) es un estándar abierto que permite incluir seguridad en la autenticación para aplicaciones web y de escritorio.
OAuth implementa la forma de proteger no sólo un recurso web, sino también elementos de otras aplicaciones, como pueden ser las de escritorio o las móviles.
La diferencia entre OAuth y otros sistemas federados es que estos últimos ofrecen una identidad única para acceder a múltiples recursos, mientras que OAuth

permite a otras aplicaciones el acceso a un recurso, pero sin dar ningún tipo de información de carácter personal. Esto favorece a las aplicaciones web ofrecer sus servicios sin forzar a los usuarios a exponer sus contraseñas u otras credenciales. La estructura de autorización y autenticación mediante OAuth se basa en varios elementos básicos:

- **Proveedor de servicio (service provider)**. Es la aplicación web donde se encuentran los recursos que están protegidos mediante OAuth y se encarga de denegar o permitir el acceso a los mismos.
- **Usuario (user)**. Individuo que tiene una cuenta en la aplicación web proveedora del servicio.
- **Consumidor (consumer)**. Aplicación web que utiliza OAuth para acceder al proveedor de servicio en nombre del usuario.
- **Recurso protegido (protected resource)**. Datos controlados por el proveedor de servicio con OAuth a los que podrá acceder, mediante autenticación, el consumidor[24].

Para garantizar la seguridad al dar acceso a los recursos, OAuth define un método para validar la autenticidad de las peticiones HTTP. Este método se denomina signing request e intenta solventar los siguientes aspectos:

- Los datos enviados con las peticiones deben enviarse cifrados para evitar que una tercera persona pueda interceptarlos y hacer un uso ilícito de ellos.
- Debe existir un mecanismo que asocie una petición con unas credenciales concretas, ya que de no realizarse así, unas credenciales correctas podrían ser utilizadas en cualquier petición que se enviara.
- Debe permitirse interactuar con dos tipos de credenciales, las del consumidor, que garantizan que este es un consumidor autorizado previamente, y las del usuario, que lo certifican como usuario del proveedor del servicio.

Según el grado de seguridad del protocolo utilizado en la comunicación, el método varía. Si va sobre HTTPS, se sigue el método PLAINTEXT, que delega la mayor parte de la seguridad en la capa HTTPS. Cuando va sobre HTTP, el método de seguridad debe ser mucho más elaborado.
Para acreditar al consumidor, se utilizarán la consumer key y el consumer secret, que identificarán al consumidor ante el proveedor de servicio.

Para identificar al usuario, dispondremos de un token y del token secret. Estos elementos representarán al usuario, pero diferirán del nombre de usuario y contraseña originales en el proveedor de servicio. Esto permite al proveedor de servicio y al usuario más control y seguridad, dando acceso al consumidor, y además, permitiendo a un usuario revocar un token sin tener que cambiar contraseñas en otras aplicaciones.
Como método para garantizar la integridad, OAuth utiliza firmas digitales en vez de enviar las credenciales completas, verificándose así que el contenido de la petición no se ha modificado en el camino entre una aplicación y otra. La garantía de confianza dependerá del algoritmo de firma que se utilice y de la forma de aplicación del mismo.
Como dicha firma electrónica no verifica la identidad del que envía el mensaje, utilizamos la firma combinada con el secreto compartido. Para esto, será necesario que ambos elementos acepten un secreto que sólo conocerán ellos.
Para no permitir re-envíos por terceras personas, OAuth incorpora dos elementos: un número identificador para cada petición que el consumidor envíe al proveedor de servicio y una marca de tiempo que permitirá a los proveedores de servicio mantener los identificadores por un tiempo limitado
Existen tres métodos de firma diferentes:

- **PLAINTEXT**. Es el más simple de los tres y sólo se recomienda utilizar sobre HTTPS.
- **HMAC-SHA1**. Combina HMAC, que ofrece secreto compartido simétrico y SHA1 como algoritmo hash.
- **RSA-SHA1**. Es el más complejo de los métodos y combina RSA como mecanismo de seguridad de las claves y SHA1 como algoritmo de hash

La autenticación mediante OAuth es el proceso mediante el cual los usuarios conceden acceso a sus recursos protegidos sin compartir sus credenciales con el consumidor.
En vez de utilizar las credenciales del usuario en las peticiones a recursos protegidos, OAuth utiliza los tokens generados por el proveedor de servicio que denominamos request token y access token:

- **Requesttoken**. Utilizado por el consumidor para pedir al usuario acceso a los recursos protegidos. Una vez el request token es autorizado por el usuario, se intercambia por un access token, que debe utilizarse sólo una vez y no podrá usarse para otro cometido.

- **Accesstoken**. Utilizado por el consumidor para acceder a los recursos protegidos en nombre del usuario. Puede limitar a más de un recurso y tener un tiempo de vida limitado. Sólo el access token podrá usarse para acceder a los recursos protegidos, siendo éste susceptible de ser revocado[24].

4.2.1.3. SimpleSAMLPHP

SimpleSAMLphp es una aplicación escrita en PHP que implementa los estándares de SAML 2.0 y ofrece soporte para los dos escenarios: SAML como un proveedor de servicios y SAML como un proveedor de identidad. En caso de utilizar SimpleSAMLphp como un proveedor de servicios, este comunicará y delegará la autenticación con un Proveedor de Identidad SAML. Como SimpleSAMLphp está escrito en PHP, es una forma muy sencilla de integrar una Aplicación web basada en PHP dentro de una federación.
SimpleSAMLphp como un proveedor de identidad puede aceptar conexiones de Shibboleth y los servicios de SAML 2.0. Existen varios módulos de autenticación integrada, tales como LDAP, Servicio de CAS, autenticación Radius, autenticación SQL, OpenID y YubiKey. SimpleSAMLphp ofrece una Extensión API con el fin de permitir la personalización y integración con módulos de terceros.

- La flexibilidad soportortada por SimpleSAMLphp se centra en uno de los principales temas:
    - Módulos de autenticación: Permite implementar un módulo de autenticación personalizado, como Infraestructura de Clave Pública (PKI)
    - Filtros de procesamiento de autenticación: Permitir el procesamiento justo después de la autenticación
    - Temas: Permite personalizar el aspecto de las páginas
    - Módulos simpleSAMLphp: Permitir el desarrollo de nuevos protocolos de identidad, páginas, sistemas de registro, etc.

Además de la funcionalidad básica de un proveedor de servicios y de un proveedor de identidad, SimpleSAMLphp soporta otras características avanzadas, tales como: puente entre los protocolos, atributo de control, pruebas automatizadas y firma de metadatos. SimpleSAMLphp incluye bibliotecas para la integración con varios sistemas populares de Gestión de Contenidos (CMS), como Drupal, DokuWiki y MediaWiki[25].

SimpleSAMLPHP utiliza memcache, mecanismo que permite que las sesiones puedan ser distribuidos y replicadas entre varios servidores memcache, mediante el almacenamiento de múltiples copias redudantes de sesiones en diferentes servidores permitiendo el balanceo de carga y conmutación por error [26].

4.2.1.4. OpenID

OpenID es un estándar de autenticación de usuarios que, desde un punto de vista descentralizado, permite acceder a recursos que tienen desplegado un control de acceso. Además, dichos usuarios podrán acceder a diferentes recursos con una misma identidad digital, proveyendo de esta forma un sistema de single sign-on. El servicio donde el usuario se autentica se llama proveedor de OpenID u OpenID provider, mientras que el recurso protegido es conocido como Relaying Party.
La principal diferencia con los sistemas más comunes de federación de identidad digital es que OpenID no proporciona un único punto central para autenticar al usuario, sino que existen numerosos proveedores de OpenID desplegados en Internet que pueden ser utilizados para acceder a cualquier recurso protegido por esta tecnología.
Afortunadamente, contamos con una amplia colección de librerías abiertas para trabajar con OpenID en casi todas las plataformas, tanto en PHP, Python, Javao.NET.

Protocolo de autenticación

El protocolo de autenticación de OpenID disponible en su versión 2, se basa en el envío de mensajes HTTP utilizando tanto los métodos GET como POST.
El flujo de mensajes que se producen a la hora de acceder un usuario a un Relaying Party es el siguiente:

1. El usuario indica al Relaying Party cuál es su identificador OpenID, también llamado user-supplied identifier, mediante su navegador o agente. Por regla general, se establecerá este valor mediante un formulario HTML, el cual debería tener como nombre openid_identifier. De esta forma, el navegador podrá identificar claramente si existe la posibilidad de autenticarse en el Relaying Party mediante OpenID.

2. Una vez que el Relaying Party normaliza el identificador OpenID, que puede ser un eXtensible Resource Identifier (XRI) o un identificador de recursos uniforme (URI), realiza el proceso de discovery o descubrimiento. De esta

forma, obtiene información sobre la URL del proveedor de OpenID del usuario.

3. Opcionalmente, el proveedor de OpenID y el Relaying Party establecen una asociación que resulta en una clave secreta compartida por ambas partes. De esta forma, se elimina la necesidad de estar verificando las firmas digitales cada vez que se solicite la autenticación del usuario.

4. El Relaying Party redirige al usuario a través de su navegador o agente a su proveedor de OpenID por medio de un mensaje de petición de autenticación.

5. El usuario se autentica contra su proveedor de OpenID. Las cuestiones relativas al proceso de la autenticación están fuera del ámbito del protocolo, quedando delegado a las decisiones de los responsables de dicho proveedor.

6. El proveedor de OpenID redirige al usuario, por medio del navegador o agente, al Relaying Party que solicitó dicha petición de autenticación, indicando si la autenticación fue correcta o, en caso contrario, no fue posible.

7. El Relaying Party verifica la información que recibe del proveedor de OpenID a través del navegador o agente. Esta verificación implica comprobar los valores del mensaje que recibe, así como la firma digital de dicho mensaje, bien a través de la clave compartida obtenida en el paso 3 o bien enviando una petición directamente al proveedor de OpenID del usuario[24].

OpenID no se trata de una solución de identidad federada propiamente dicha ya que no especifica el mecanismo de autenticación, debido a que es un sistema de identificación digital descentralizado. Mediante OpenID un usuario puede identificarse en una página web a través de una URL y puede ser verificado por cualquier servidor que soporte el protocolo. Cuenta con el apoyo de Google, IBM, Microsoft, VeriSign y Yahoo entre otros [22].

4.2.1.5. Sun Access Manager

Producto originario de Sun Microsystems, que tiene a su vez una edición de código abierto llamado Open Single Sign-On.
Su objetivo es ofrecer una solución completa que ofrezca autenticación y autorización en entornos Web basados en Java, federados y basados en servicios web.

Aunque tiene una administración centralizada, Sun Access Manager se compone de los siguientes elementos:

- **Authentication Service:** Gestiona la identificación del usuario.
- **Policy Service:** Este servicio evalúa una política de acceso a un recurso protegido con respecto al usuario que intenta acceder a él.
- **User Session Management:** Una sesión de usuario es el intervalo entre el momento en el que el usuario accede a una aplicación protegida y el momento en el que sale de ella. Durante cada sesión, este servicio mantiene y gestiona información sobre las interacciones que realiza el usuario con dicha aplicación protegida.
- **SAML Service:** Este servicio se encarga de emitir información, tanto de identificación como de atributos, del usuario usando mensajes SAML.
- **Identity Federation Service:** Este servicio unifica las diferentes identificaciones que tiene para las aplicaciones y ofrece una aplicación global federada.
- **Logging Service:** Mantiene información sobre las acciones que realiza el usuario en el entorno protegido por el Sun Access Manager[27].

4.2.1.6. SPML

SPML son las siglas de service provisioning markup language, un lenguaje basado en XML para el aprovisionamiento automático de identidades en sistemas de información y la gestión de una identidad a lo largo de su ciclo de vida, desde crearla a revocarla, pasando por la modificación de la misma.
Se pueden identificar tres roles diferentes:

- **Requesting authority (RA):** la entidad que realiza la petición de aprovisionamiento.
- **Provisioning service provider (PSP):** software capaz de responder a peticiones SPML.
- **Provisioning service target (PST):** proveedor de las identidades. Este rol puede estar unido a Provisioning service provider (PSP), pero mientras que PSP necesita entender SPML, PST no.

SPML constituye un lenguaje de pregunta/respuesta, como SAML. Para ello necesitamos que Requesting authority y Provisioning service provider establezcan una relación de confianza, que puede ser representada también a través de SAML, introduciendo las aserciones correspondientes en la cabecera y las instrucciones SPML en el payload[24].
Tiene básicamente cinco operaciones:

1. <addRequest/>, utilizado para crear una cuenta.
2. <modifyRequest/>, se emplea para actualizar una cuenta.
3. <deleteRequest/>, utilizado para pedir el borrado de una cuenta.
4. <searchRequest/>, se utiliza para interrogar al PSP acerca de cuentas y sus propiedades.
5. <schemaRequest/>, permite pedir a la RA el esquema de aprovisionamiento de un PSP.

4.2.1.7. Shibboleth

Shibboleth surgió de la necesidad por parte de las instituciones de Internet2 de colaborar en proyectos on-line y se enmarca dentro de la Internet2 Middleware Initiative (I2-MI), la cual intenta conseguir el desarrollo de los principales servicios middleware en las universidades miembros de Internet2 (Universidad de Washington, Carnegie Mellon, la Universidad del Estado de Ohio, el Instituto de Tecnología de Massachusetts (MIT) y la Universidad de California).
El middleware es una capa de software entre la red y las aplicaciones. Este software ofrece servicios tales como la identificación, la autentificación, la autorización, los directorios y la seguridad. En la actualidad las aplicaciones web tienen que ofrecer estos servicios por sí mismas, lo que conlleva estándares opuestos e incompatibles. La iniciativa de Internet2 en este ámbito promueve la normalización y la interoperabilidad.
Shibboleth está por completo basado en SAML, proveyendo básicamente servicios de single sign-on y administración federada del acceso a recursos restringidos. Al estar basada su negociación en atributos, es un protocolo que tiene por diseño mecanismos para garantizar la privacidad. Esto contribuye a una tendencia reciente de tener en cuenta el diseño de los sistemas a la seguridad (security by design) y a la privacidad (privacy by design)[12].
Shibboleth permite a las organizaciones intercambiar información sobre los usuarios de forma segura y privada. Shibboleth es un sistema de inicio de sesión

único que accede a la información almacenada en el dominio de seguridad del usuario para autenticar a los visitantes de un sitio web. Esto permite a los usuarios acceder a información controlada de forma segura desde cualquier parte, sin contraseñas adicionales y sin poner en riesgo la privacidad innecesariamente[28].

- **Estándares y código abiertos**

La licencia que Shibboleth utiliza autoriza a cualquier persona a modificar y extender el código base. Dicho código se ha programado de forma modular, permitiendo su personalización para entornos existentes, mediante la conexión de nuevos módulos.
Basarse en estándares abiertos tiene la ventaja de que la información que se intercambia entre instituciones y organizaciones podría interoperar con aquella que provenga de otras soluciones. Shibboleth está diseñado para utilizar los siguientes estándares, la mayoría de los cuales están ya ampliamente extendidos:

- Hypertext Transfer Protocol (HTTP)
- Extensible Markup Language (XML)
- XML Schema
- XML Signature
- SOAP
- Security Assertion Markup Language (SAML)
- Secure Sockets Layer (SSL)
- Lightweight Directory Access Protocol (LDAP)

El uso de estándares abiertos es particularmente importante en el desarrollo de aplicaciones middleware, al mejorar la interoperabilidad de los diferentes sistemas e incrementar la compatibilidad.

- **SAML y OpenSAML**

SAML (Security Assertions Markup Language) es un entorno basado en XML para servicios Web que permite el intercambio de información de autorización y autenticación entre diferentes sitios Web.
SAML ofrece a los desarrolladores de espacios Web un estándar abierto que permitirá que los usuarios puedan visitar múltiples sitios Web sin necesidad de identificarse nada más que una vez.

Además permite, a los visitantes, visitar dichos sitios alojados por distintas compañías, facilitando la adquisición de productos o servicios en los mismos, al no requerir que estos usuarios tengan que registrarse y dar sus datos personales a través de Internet cada vez que entren en una Web.
SAML establece normas generales para la estructura de la información y para el intercambio de mensajes en el contexto de un protocolo. Shibboleth proporciona la infraestructura y el "modelo de confianza" necesarios para convertir a SAML en una aplicación útil.
Un componente básico de Shibboleth es **OpenSAML**, un conjunto de librerías Java y C++ de código abierto que pueden ser utilizadas para construir, transportar y analizar mensajes SAML. OpenSAML es capaz de almacenar individualmente los campos de información que componen un mensaje SAML y construir correctamente su representación XML, así como de llevar a cabo el proceso contrario, descomponiendo un documento XML en sus elementos individuales para entregarlos a un destinatario.
OpenSAML está diseñado para ser extensible y para poder integrar una amplia gama de "modelos de confianza" y requisitos de seguridad, aunque, por ahora, se orienta primordialmente a transacciones protegidas mediante PKI (Public Key Infrastructure) y TLS/SSL.

- **Intercambio de Atributos**

Cuando un usuario perteneciente a una institución (servidor, sitio o nodo de origen) trata de acceder a un recurso situado en otro dominio de seguridad (servidor, sitio o nodo de destino), Shibboleth envía información sobre dicho usuario a dicho dominio remoto, en vez de forzar al usuario a someterse a un proceso de autentificación en el destino. El sistema donde radica el recurso deseado puede utilizar esta información del usuario, para decidir si otorgar o no el acceso a dicho recurso.
Shibboleth permite al usuario elegir qué información sobre sí mismo se entregará al nodo de destino. Éste conocerá únicamente los atributos necesarios para llevar a cabo la decisión de control de acceso, protegiendo el anonimato del usuario en los casos en los que su identidad es menos importante que otros factores como formar parte de alguna institución o grupo de usuarios concreto.
En muchos casos, lo realmente importante a la hora de conceder o no acceso a un recurso es conocer un conjunto de características del usuario, no su identidad.

- **Seguridad**

Shibboleth trata con un tema especialmente sensible como es el acceso a recursos protegidos, de ahí que la seguridad sea una pieza fundamental a tener en cuenta. El código fuente ha sido cuidadosamente diseñado para hacerlo a prueba de ataques. Asimismo, se usan técnicas para proteger a los atributos en tránsito, que son contempladas por el propio estándar SAML.
Todos los servidores que intervienen en las transacciones se autentifican usando certificados digitales. En la arquitectura Shibboleth no se especifica el uso de certificados por parte de los clientes pero se contempla la posibilidad de usarlos, pudiendo incluso simplificar de alguna manera el funcionamiento del sistema.
Es importante resaltar que Shibboleth no limita de ninguna forma lo que el sitio de origen envía como atributos ni las acciones que el servidor de destino pueda llevar a cabo basándose en los atributos recibidos. El sistema proporciona medios para distribuir las características de los usuarios, utilizando certificados digitales y la asociación de los últimos con determinados sitios origen y destino. Una vez que se han entregado los atributos de forma segura en el destino deseado, Shibboleth no garantiza que el uso que se haga de ellos sea el adecuado. De la misma forma, no puede afirmar la veracidad de los atributos entregados, tan sólo que provienen de la autoridad apropiada y que dicha autoridad los remitió tal y como han aparecido en el destino.

- **Componentes de la arquitectura**
  - **Proveedor de Identidad o Identity Provider**: Emite aserciones que contienen afirmaciones de autentificación o de atributos a petición, principalmente, de un Proveedor de Servicios

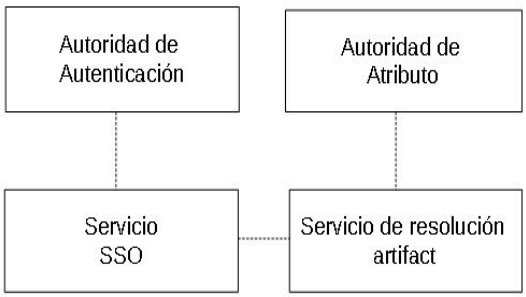

Figura 9: Componentes IdP en shibboleth
Fuente: El Investigador

Autoridad de Autenticación: Se encarga de expedir afirmaciones de autentificación. Interacciona con el Servicio Single-Sign On.

Servicio Single Sign-On (SSO): Constituye el primer punto de contacto del IdP. Inicia el proceso de autentificación y, en último lugar, redirige al cliente al Proveedor de Servicios.

Servicio de Resolución Artifact: En determinados situaciones, el Proveedor de Identidad devuelve un SAML artifact al Proveedor de Servicios, en lugar de la aserción propiamente dicha. El SP envía entonces dicho artifact al Artifact Resolution Service, utilizando algún canal alternativo de comunicación. Como respuesta, el Proveedor de Identidad le devuelve la aserción de autentificación requerida.

Autoridad de Atributo: Se encarga de procesar peticiones de atributos ("attribute requests") y emite aserciones de atributos.

- **Proveedor de Servicios o Service Provider** Gestiona recursos protegidos cuyo acceso se basa en la información que recibe del Proveedor de Identidad, en forma de aserciones.Contiene su propio recurso protegido ("Target Resource") en el interior de la estructura del Service Provider.

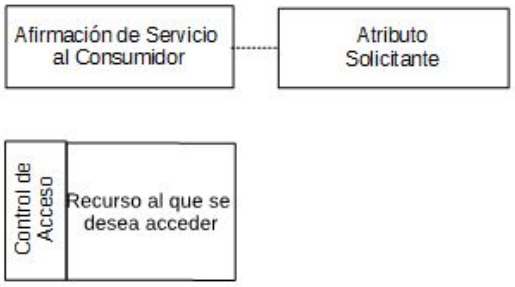

Figura 10: Componentes SP en Shibboleth
Fuente: El Investigador

Afirmación de Servicio al Consumidor Representa la interfaz utilizada para comunicarse con el Servicio Single Sign-On del Proveedor de Identidad. Procesa la aserción de autentificación devuelta por éste, inicia una petición de atributos al IdP (opcional), establece un contexto de seguridad en el Proveedor de Servicios para el usuario actual y redirige al cliente al recurso deseado.

Atributo Solicitante Una vez que ha sido establecido un contexto de seguridad en el Service Provider, el Atributo Solicitante puede llevar a cabo un intercambio de atributos comunicándose con la Autoridad de Atributo del Proveedor de Identidad.

Acceso de Control El Proveedor de Servicios debe proveer algún medio para evitar el libre acceso a los recursos protegidos, permitiendo la intervención del Proveedor de Identidad para supervisar el control de acceso.

- **Servidor WAYF:** Este servicio opcional opera independientemente del Proveedor de Servicios y del Proveedor de Identidad. Puede ser utilizado por el SP para determinar el IdP preferido por el usuario, ya sea con la intervención de éste o sin ella

- **Esquema de funcionamiento**

1. El usuario intenta acceder a un recurso protegido del Proveedor de Servicio, el cual se encuentra situado "detrás" de un control de acceso.
2. El control de acceso no conoce al usuario ni de qué sistema proviene, por lo que lo redirige al servidor WAYF.
3. El Servidor WAYF inicia un proceso para averiguar el Proveedor de Identidad que él usuario desea utilizar (aquél donde están sus datos personales o, en caso de existir más de uno, el preferido por el usuario).
4. El usuario le indica al Servidor WAYF en qué Proveedor de Identidad desea autentificarse.
5. El Servidor WAYF redirige al usuario al Proveedor de Identidad adecuado.
6. El Servicio Single Sign-On, que forma parte del IdP elegido, pregunta al usuario por sus credenciales en dicho sistema, con el fin de autentificarlo.
7. El usuario responde enviando al Proveedor de Identidad sus credenciales locales (por ejemplo, el nombre de usuario que posee en dicho sistema y su contraseña).
8. El Servicio Single Sign-On comprueba que las credenciales del usuario son correctas y envía una petición de autentificación SAML a la Autoridad de Autenticación dentro del mismo Proveedor de Identidad.
9. La Autoridad de Autenticación devuelve una aserción SAML de autentificación como respuesta a la petición del Servicio Single Sign-On
10. El Proveedor de Identidad genera un identificador único (ID) y redirige al usuario al Proveedor de Servicios, para que entregue la aserción de autentificación a la Afirmación del Servicio al Consumidor.
11. La Afirmación del Servicio al Consumidor valida la aserción que acaba de recibir, crea una sesión de seguridad para el usuario y transfiere el control de ejecución al Atributo Solicitante.

12. El Atributo Solicitante utiliza el identificador que generó el Proveedor de Identidad en el paso 10 para solicitar los atributos del usuario. La solicitud va dirigida a la Autoridad de Atributo, situada en el Proveedor de Identidad.

13. La Autoridad de Atributo del IdP responde con una aserción SAML de atributos. Qué y cuántos atributos componen la respuesta, depende de la política de entrega de atributos que establezca el Proveedor de Identidad.

14. El Proveedor de Servicio utiliza los atributos recibidos para decidir si permite al usuario acceder al recurso deseado, o bien rechaza dicho intento de acceso[29].

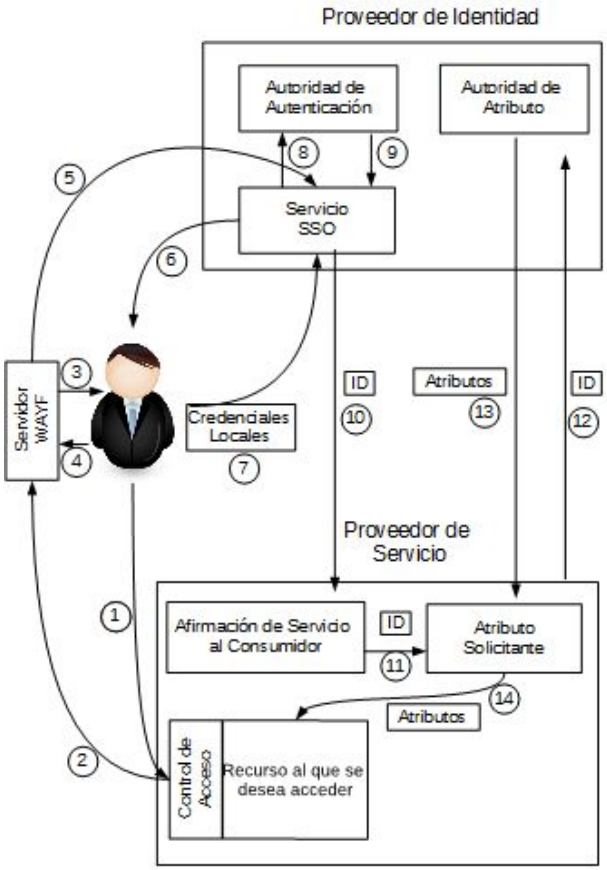

Figura 11: Shibboleth en Funcionamiento
Fuente: El Investigador

4.2.1.8. Cuadro Comparativo entre las distintas Aplicaciones para realizar Sistemas Federados

APLICACIÓN	SOPORTE	DOCUMENTACIÓN	OBSERVACIONES
PAPI	Fácilmente interoperable con otros protocolos de autenticación y autorización, como SAML 1.1, SAML 2, OpenID y OAuth. Software abierto y disponible en diferentes lenguajes de programación: Perl, PHP, Java, ASP.NET, etc. Multitud de conectores disponibles para proveedores de servicio: MediaWiki, DokuWiki, Moodle, etc.	Documentación de configuración propia en pagina web de PAPI: http://www.papisoftware.net/. En donde se puede encontrar Material de inicio, Documentación técnica y Presentaciones.	El funcionamiento de PAPI es bastante similar al Browser Post Profile de Liberty/SAML 2.0: la aserción es transmitida mediante el método POST de HTTP desde un proveedor de autenticación hasta los proveedores de servicio, solo que dicha aserción no es SAML (ni siquiera XML). Actualmente se encuentra en desarrollo los mecanismos que lo hagan compatible con Shibboleth.
OAuth	WebSphere Application Server actúa como proveedor de servicios de OAuth para gestionar las solicitudes de protocolo OAuth 2.0.	Documentación escasa proporcionada en http://www-01.ibm.com/	Permite a un proveedor de servicios/API facilitar a aplicaciones de terceros a que amplien sus servicios con aplicaciones que hacen uso de los datos de sus usuarios de manera segura y dejando al usuario la decisión de cuando y a quien, revocar o facilitar acceso a sus datos, creando así un ecosistema de aplicaciones alrededor del proveedor de servicios/API.
SimpleSAMLPHP	Aplicación escrita en PHP que implementa los estándares de SAML 2.0 y ofrece soporte para los dos escenarios: SAML como un proveedor de servicios y SAML como un proveedor de identidad. SimpleSAMLphp como un proveedor de identidad puede aceptar conexiones de Shibboleth y los servicios de SAML 2.0.	Amplia documentación de versiones, módulos, instalación y configuración de SimpleSAMLPHP https://simplesamlphp.org/	Usa memcache, mecanismo que permite que las sesiones puedan ser distribuidos y replicadas entre varios servidores memcache, mediante el almacenamiento de múltiples copias redudantes de sesiones en diferentes servidores permitiendo el balanceo de carga y conmutación por error. Dispone de una única aplicación que dependiendo de como sea configurada actúa como IdP, SP o WAYF.

Tabla 4: Aplicaciones para realizar Sistemas Federados

Fuente: El Investigador

APLICACIÓN	SOPORTE	DOCUMENTACIÓN	OBSERVACIONES
OpenID	Plataformas, tanto en PHP, Python, Javao.NET	Documentación en página web http://openid.net/	Sistema de identificación digital descentralizado. Problema de múltiple identidad para diferentes perfiles de navegación, el uso de identificadores no unidireccionales se convierten en datos identificativos, problemas de phishing
SunAcessManager	Entornos Web basados en Java, federados y basados en servicios web	Documentación en inglés en página de Oracle	Administración centralizada
SPML	SPML 1.0 está creado en base al Directory Services Markup Language V.2 de OASIS, que es una representación XML del protocolo LDAP. SPML se unirá a una familia de estándares diseñados para facilitar la implementación de Servicios Web, como son XACML, SAMI, UDDI, WSDI y SOAP	Escasa documentación. Archivo 2003 https://www.oasis-open.org/	SPML y SAML proporcionan un estándar para crear cuentas de usuario y validar a los usuarios como parte de una infraestructura de gestión de identidad. Los dos ofrecen la base para la integración de inicio de sesión único y aprovisionamiento de software para servicios Web.
Shibboleth	Soporta las versiones 1.1 y 2.0 de SAML. Implementación de perfiles basada en OpenSAML. Ofrece IdP en Java y SP en C++.	Está bien documentado. Facilita manuales de instalación del IdP y el SP. Tiene un API pública de clases para el IdP. Información del proyecto Shibboleth, especificaciones técnicas, demostraciones, etc. Cuenta también con una lista de correo y manuales para desarrolladores.	La licencia que Shibboleth utiliza autoriza a cualquier persona a modificar y extender el código base. Dicho código se ha programado de forma modular, permitiendo su personalización para entornos existentes, mediante la conexión de nuevos módulos. Shibboleth está diseñado estándares tales como: HTTP, XML, SOAP, LDAP, SAML, SSL, entre otros.

Tabla 5: Aplicaciones para realizar Sistemas Federados

Fuente: El Investigador

Después de haber estudiado las diferentes aplicaciones para realizar Sistemas Federados se ha llegado a la conclusión que para la realización del presente Proyecto de Investigación se opta por Shibboleth como herramienta de autenticación Single Sign On ya que ofrece una amplia documentación de instalación y configuración tanto para distribuciones Linux como Windows, además utiliza la biblioteca de cifrado OpenSSL, lo cual posibilita una fácil integración con otros sistemas por ejemplo, OpenCA y extensiones de OpenSSL, puesto que SAML no estandariza todos los aspectos en la gestión de identidad como los mecanismos para el establecimiento y gestión de cuentas y privilegios asociados, autenticación, control de acceso, etc.

Shibboleth integra un Proveedor de Servicio, Proveedor de identidad y WAYF en su estructura a diferencia de otras aplicaciones para Gestionar Identidades tales como SimpleSamlPHP y OAuth en donde la autenticación del usuario es realizada por un tercero lo que implica un mayor costo y dificultad de configuración e implementación, debido a que se debe integrar la aplicación con el proveedor de autenticación.

Shibboleth posse estándares abiertos que permiten el desarrollo de aplicaciones middleware, mejorarando la interoperabilidad de los diferentes sistemas e incrementar la compatibilidad, a diferencia de PAPI una herramienta que busca implementar a Shibboleth en su estructura para hacerla más robusta por sus estándares y protocolos.

4.3. Ejecución de la Propuesta

4.3.1. Esquema de Funcionamiento de un Sistema Federado en la UTA-FISEI

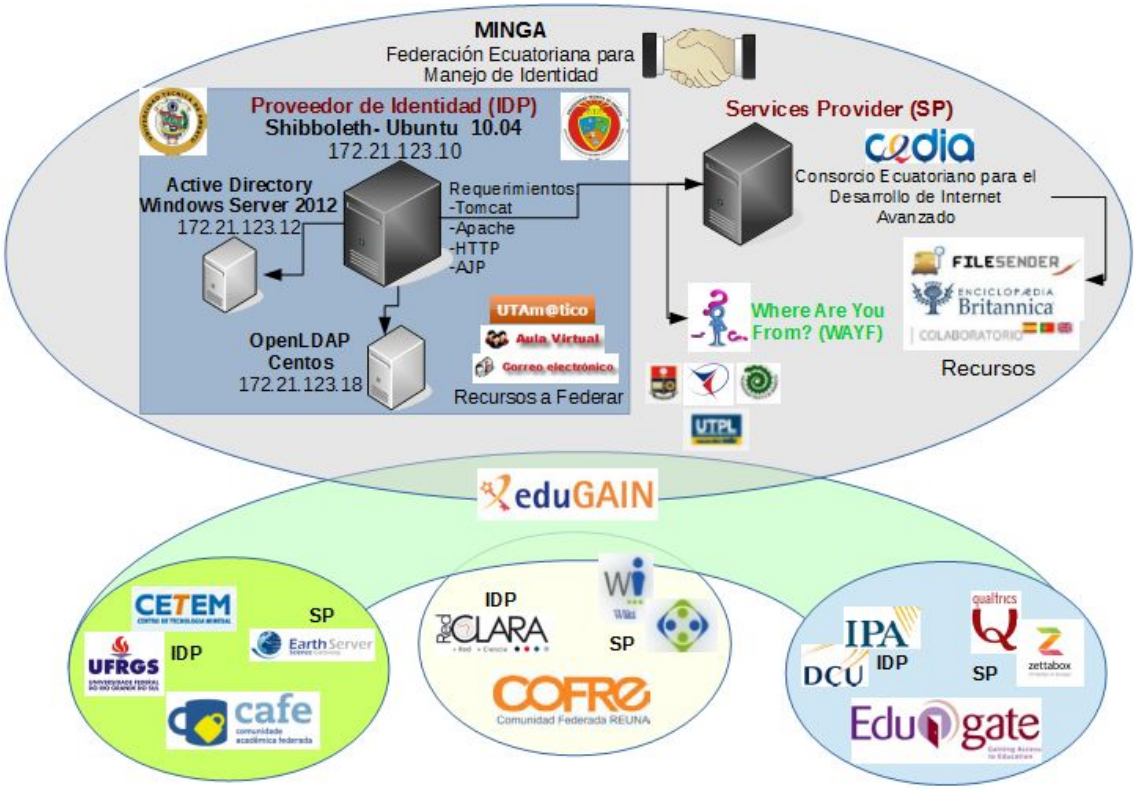

Figura 12: Esquema de Funcionamiento de Sistema Federado en la UTA-FISEI
Fuente: El Investigador

4.3.2. Esquema de Funcionamiento de Idp

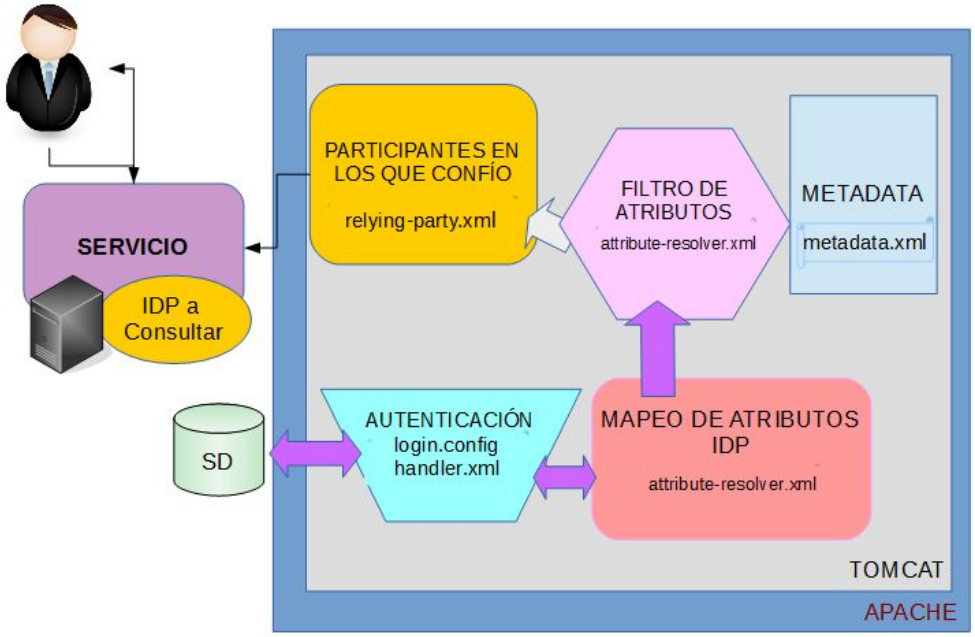

Figura 13: Esquema de Funcionamiento Idp
Fuente: El Investigador

4.3.3. Identity Provider Idp

Configuración de Fichero Hosts

Agregar una línea con la dirección IP del nuevo servidor y el dominio que se desea ver: 172.21.123.10 idp.uta.edu.ec

```
root@idp:/etc# cat hosts
127.0.0.1       localhost
127.0.1.1       idp.uta.edu.ec
172.21.123.10   idp.uta.edu.ec
# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Configuración del fichero Sources.list

Editar el fichero sources.list localizado en /etc/apt/sources.list, aquí se enlistan las "fuentes" o "repositorios" disponibles de los paquetes de software candidatos a ser: actualizados, instalados, removidos, buscados, sujetos a comparación de

versiones, etc. La herramienta APT administra el acceso a dichos paquetes, utilizando el fichero sources.list, para realizar las acciones previamente mencionadas. La palabra cd rom son referencias al cd de instalación, siempre vienen con las palabras "deb cdrom:" aunque se haya instalado a través de la red o de un usb. El término "deb http://" indica la dirección física del servidor o repositorio, es el nombre que recibe el servidor que contiene los paquetes, el término "deb src" indica la dirección de las fuentes de los programas[30].

```
deb http://archive.canonical.com/ lucid partner
```

Instalación de Paquetes Necesarios

- Actualizar el listado de todos los paquetes, a través del uso de una dirección específica para hacer la búsqueda y su posterior descarga sea más rápida en el ordenador.

  ```
  apt-get update
  ```

- Instalar Java Development Kit (JDK), el cual es un software que provee herramientas de desarrollo para la creación y compilación de programas java por ejemplo Apache Ant, Apache Maven, Eclipse

  ```
  apt-get install openjdk-6-jdk
  ```

- Dentro de la distribución Ubuntu se instala el VIM TINY por defecto el cual consta con las opciones básicas, pero no son suficientes al momento de desarrollar algo con PERL, C++, etc; para ello se utilza el comando[31]:

  ```
  apt-get remove [purge] nombre_paquete
  ```

  El mismo que elimina el paquete especificado del sistema. Admite el argumento –purge para que borre también los ficheros de configuración.

  ```
  apt-get remove --purge -y vim-tiny
  ```

- Actualizar los paquetes ya instalados que no necesitan, como dependencia, la instalación o desinstalación de otros paquetes.

  ```
  apt-get dist-upgrade y
  ```

- Instalación de paquetes necesarios paginando el texto en pantalla para que el usuario pueda leer sin mayores problemas, pudiendo avanzar o retroceder en el texto con las flechas de cursor del teclado

```
apt-get -y install less vim bzip2 zip unzip ssh dialog \
ldap-utils build-essential iptables-persistent
```

- En el fichero de configuración logrotate se lee la información necesaria sobre los ficheros de registro, las distintas aplicaciones que se ejecutan en un servidor suelen generar ficheros de log en los que se registran los eventos que han tenido lugar, generando un volumen importante de información en estos ficheros, por ello, es habitual establecer un procedimiento para el mantenimiento de los ficheros de log. En el fichero logrotate.conf descomentar la directiva compress, la misma que comprime los ficheros rotados,este utiliza gzip, por defecto, para realizar la compresión[32].

```
root@idp:/etc# cat logrotate.conf
# see "man logrotate" for details
# rotate log files weekly
weekly
# keep 4 weeks worth of backlogs
rotate 4
# create new (empty) log files after rotating old ones
create
# uncomment this if you want your log files compressed
compress
# packages drop log rotation information into this directory
include /etc/logrotate.d
# no packages own wtmp, or btmp -- we'll rotate them here
/var/log/wtmp {
    missingok
    monthly
    create 0664 root utmp
    rotate 1}
/var/log/btmp {
    missingok
    monthly
    create 0660 root utmp
    rotate 1}
# system-specific logs may be configured here
```

- Añadir las reglas IPTABLES que acepte el tráfico entrante que excluyan puertos de un determinado puerto de destino

```
iptables -A INPUT -p tcp -m tcp --dport 8443 -j ACCEPT
iptables -A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
iptables -A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
iptables -A INPUT -p tcp -m tcp --dport 8080 -j ACCEPT
```

- Guardar reglas IPTABLES

```
iptables-save > /etc/iptables/rules
```

- Agregar arranque automático del Firewall

```
update-rc.d iptables-persistent start 0 1 2 3 4 5 . stop 99 0 1 6 .
```

- Verificar zona horaria en el sistema

```
root@idp:~# date
mié jun 24 10:58:55 ECT 2015
```

- Añadir las variables de entorno necesarias para poder usar Java, Apache y Tomcat.

```
export JAVA_HOME="/usr/lib/jvm/java-6-openjdk"
export JRE_HOME="/usr/lib/jvm/java-6-openjdk"
export CATALINA_HOME="/usr/share/tomcat6"
export TOMCAT_HOME="/usr/share/tomcat6"
echo 'export JAVA_HOME="/usr/lib/jvm/java-6-openjdk"' >>/etc/
    profile
echo 'export JRE_HOME="/usr/lib/jvm/java-6-openjdk"' >> /etc/
    profile
echo 'export CATALINA_HOME="/usr/share/tomcat6"' >> /etc/
    profile
echo 'export TOMCAT_HOME="/usr/share/tomcat6"' >> /etc/profile
```

- Instalar Apache y Tomcat

```
apt-get install tomcat6 apache2 libapache2-mod-jk libxml2-utils
```

- Descomentar la siguiente línea de código dentro del fichero tomcat6, el mismo que se encuentra ubicado en /etc/default/tomcat6. El modo "Security Manager" ayuda a que los applets cargados por el cliente se ejecuten en su propio entorno, evitando así que accedan a ficheros del sistema. Además protege al servidor de errores involuntarios, trojan servlets, JSPs, JSP beans y librerías de etiquetas.

```
TOMCAT6_SECURITY=no
```

- Iniciar Tomcat

```
/etc/init.d/tomcat6 start
```

- Proceder a verificar la instalación correcta de Tomcat mediante un navegador, para esto digitar la siguiente dirección http://172.21.123.10:8080

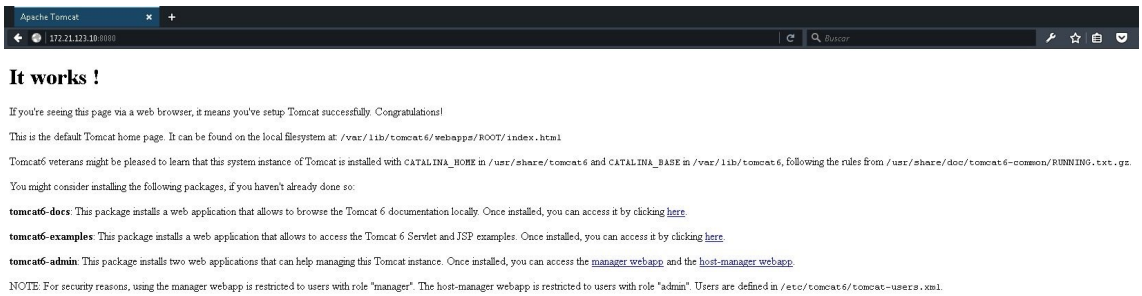

Figura 14: Tomcat Trabajando
Fuente: Investigador

- Editar el fichero **java.segurity**: En el se almacenan propiedades como: los proveedores de seguridad instalados en el sistema, la ubicación de los ficheros de configuración, nombre de la clase que implementa la política de seguridad, etc.

  Los proveedores instalados se registran añadiendo al fichero una línea con el formato[33]:

  ```
  security.provider.n=nombre_clase_provider
  ```

  donde n indica el número de proveedor.

  Editar el fichero java.segurity agregando los proveedores de seguridad instalados. En este fichero se almacena las propiedades necesarias para configurar la seguridad del sistema.

  ```
  security.provider.1=sun.security.provider.Sun
  security.provider.2=sun.security.rsa.SunRsaSign
  security.provider.3=com.sun.net.ssl.internal.ssl.Provider
  security.provider.4=com.sun.crypto.provider.SunJCE
  security.provider.5=sun.security.jgss.SunProvider
  security.provider.6=com.sun.security.sasl.Provider
  security.provider.7=org.jcp.xml.dsig.internal.dom.XMLDSigRI
  security.provider.8=sun.security.smartcardio.SunPCSC
  security.provider.9=sun.security.pkcs11.SunPKCS11 ${java.home}/
      lib/security/nss.cfg
  security.provider.10=edu.internet2.middleware.shibboleth.
      DelegateToApplicationProvider security.provider.11=org.
      bouncycastle.jce.provider.BouncyCastleProvider
  ```

- El fichero principal de configuración para Tomcat es server.xml, el cual contiene una amplia variedad de parámetros, dentro del mismo se procede a descomentar la siguiente línea de código la cual permite crear redireccionar puertos:

```
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443"
    />
```

  El elemento Connector representa las conexiones (Puertos TCP) que serán abiertas por Tomcat al arranque, a su vez dentro de cada elemento Connector se definen diversos atributos los cuales dan más detalles acerca de la conexión[34].

  Agregar un conector para el puerto 8443 a continuación de la linea previamente descomentada

```
<Connetor port="8443"
        maxHttpHeaderSize="8192"
        maxSpareThreads="75"
        scheme="https"
        secure="true"
        clientAuth="want"
        SSLEnabled="true"
        sslProtocol="TLS"
        keystoreType="PKCS12"
        keystoreFile="/opt/shibboleth-idp/credentials/idp.p12"
        keystorePass="changeit"
        truststoreFile="/opt/shibboleth-idp/credentials/idp.p12
            "
        truststorePass="changeit"/>
```

- Editar el fichero idp.xml el mismo que se encuentra en vi /etc/tomcat6/Catalina/localhost/idp.xml

```
<Context docBase="/opt/shibboleth-idp/war/idp.war"
        privileged="true"
        antiResourceLocking="false"
        antiJARLocking="false"
        unpackWAR="false"
        swallowOutput="true" />
```

- Editar el fichero idp-SSO en el cual se debe colocar la Dirección IP de Equipo, el nombre del Servidor y Dominio asignado por la institución, por ejemplo idp.uta.edu.ec. Las Llaves o keys deben ser compradas a una

empresa que venda certificados, es importante que no sea auto firmadas por comodidad de los usuarios.

```
<VirtualHost 192.168.123.10:443>
        ServerName idp.uta.edu.ec
        ServerSignature Off
        SSLEngine on
        SSLCertificateKeyFile /etc/ssl/private/idp.uta.edu.ec.
            key
        SSLCertificateFile /etc/ssl/certs/idp.uta.edu.ec.crt
        SSLCertificateChainFile /etc/ssl/certs/ca_eduroam_ec.
            crt
        DocumentRoot /var/www/vazio/
<Directory /var/www/vazio/>
        Options -Indexes -FollowSymLinks -MultiViews
        AllowOverride None
        Order deny,allow
        Deny from none
        Allow from all
</Directory>
JkMount /idp/* ajp13_worker
        CustomLog /var/log/apache2/access-idp-443.log combined
        LogLevel warn
        ErrorLog /var/log/apache2/error-idp-443.log
</VirtualHost>
```

- Crear el fichero idp.conf el cual se ubicará en: /etc/apache2/conf.d/ y digitar la siguiente información

```
JkWorkersFile /etc/libapache2-mod-jk/workers.properties
JkShmFile /var/run/apache2/jk-runtime-status.735
JkLogFile /var/log/apache2/mod_jk.log
JkLogLevel info
```

- Crear la carpeta vazzio como carpeta raíz del servidor web apache. Todos los documentos que se encuentren dentro de la carpeta raíz del servidor web, serán accesibles vía web.

```
mkdir /var/www/vazio/
```

- Desactivar el sitio web default en Apache para hacer del Virtual Host Apache creado.

```
a2dissite default
```

Ejecutado el comando anterior se puede visualizar que ya no esta incluido en los sitios activos:

```
root@idp:/var/www# cd /etc/apache2/
root@idp:/etc/apache2# ls sites-enabled/
idp-SSO
```

Para que la desactivación tenga efecto se debe cargar apache nuevamente mediante el comando:

```
service apache2 reload
```

Los sitios webs en el servidor se encuentran en un directorio llamado sites-available dentro de /etc/apache2, dentro de esta ubicación se crea y modifica la configuración de los mismos.

- Ejecutar el comando a2ensite (available2enablesite) el cual crea un enlace en sites-enable al site que le indiquemos (es decir, activa el virtualhost que acabamos de crear)[35].

```
a2ensite idp-SSO
```

Verificar que el sitio se encuentra activo

```
ls -al sites-enabled
total 8
drwxr-xr-x 2 root root 4096 2014-07-29 09:47 .
drwxr-xr-x 7 root root 4096 2014-10-11 21:04 ..
lrwxrwxrwx 1 root root   26 2014-06-18 21:40 idp-SSO -> ../
    sites-available/idp-SSO
```

- Apache es un servidor modular. Esto supone que en el núcleo del servidor sólo está incluida la funcionalidad más básica. Las características extendidas están disponibles a través de módulos que se pueden cargar en Apache. Al ejecutar el comando a2enmod se habilita un módulo de Apache, el comando a2dismod o deshabilita.

```
root@idp:/etc/apache2# a2enmod ssl
Module ssl already enabled

root@idp:/etc/apache2# a2enmod jk
Module jk already enabled
```

- Visualizar módulos funcionales

```
root@idp:/etc/apache2# ls mods-enabled
alias.conf          authz_default.load     autoindex.conf   deflate.conf
    env.load     negotiation.conf   setenvif.conf   status.conf
alias.load          authz_groupfile.load   autoindex.load   deflate.load
    jk.load      negotiation.load   setenvif.load   status.load
auth_basic.load   authz_host.load        cgid.conf        dir.conf
        mime.conf   reqtimeout.conf    ssl.conf
authn_file.load   authz_user.load        cgid.load        dir.load
        mime.load   reqtimeout.load    ssl.load
```

Certificados Autorizados

Un certificado de clave pública es un punto de unión entre la clave pública de una entidad y uno o más atributos referidos a su identidad. El certificado garantiza que la clave pública pertenece a la entidad identificada y que la entidad posee la correspondiente clave privada.
Los certificados de clave pública se denominan comúnmente Certificado Digital, ID Digital o simplemente certificado. La entidad identificada se denomina sujeto del certificado o subscriptor (si es una entidad legal como, por ejemplo, una persona).
Los certificados digitales sólo son útiles si existe alguna Autoridad Certificadora (Certification Authority o CA) que los valide, debido a que si uno se certifica a sí mismo no hay ninguna garantía de que su identidad sea la que anuncia, y por lo tanto, no debe ser aceptada por un tercero que no lo conozca. Es importante ser capaz de verificar que una autoridad certificadora ha emitido un certificado y detectar si un certificado no es válido. Para evitar la falsificación de certificados, la entidad certificadora después de autentificar la identidad de un sujeto, firma el certificado digitalmente. Los certificados digitales proporcionan un mecanismo criptográfico para implementar la autentificación; también proporcionan un mecanismo seguro y escalable para distribuir claves públicas en comunidades grandes [36].

- Agregar los certificados en los java (CA) va a confiar.

  Certificados tomados de la ubicación /etc/ssl/certs. Ejemplos:

```
ca_cedia.pem
ca-certificates.crt
CA_Disig.pem
```

```
CA_Disig_Root_R1.pem
CA_Disig_Root_R2.pem
ca_eduroam_ec.crt
idp.uta.edu.ec.crt
IGC_A.pem
Izenpe.com.pem
java
```

Instalación Shibboleth

- Descargar shibboleth-identityprovider-2.4.0 y copiar en root, además de la APIs de Java BouncyCastle (bcprov-jdk16-144.jar) necesario para los recursos de cifrado de la clave pública.
- Ejecutar el siguiente código, en el cual se indica el hostname y la clave de instalación de shibboleth:

```
root@idp:~/shibboleth-identityprovider-2.4.0/src/installer/resources
# cat install.properties
idp.home=/opt/shibboleth-idp
idp.hostname=idp.uta.edu.ec
idp.hostname.input=idp.uta.edu.ec
idp.home.input=/opt/shibboleth-idp
idp.keystore.pass=changeit
```

- Editar el fichero web.xml en la sección init- param en el cuál se indicará las direcciones IP que pueden administrar el sistema

```
<init-param>
  <param-name>AllowedIPs</param-name>
  <param-value>172.21.0.0/16 10.0.1.0/24 172.16.15.0/24 127.0.0.1/32
      ::1/128</param-value>
</init-param>
```

- Instalar shibboleth a través del comando ./install.sh

```
root@idp:~/shibboleth-identityprovider-2.4.0# ./install.sh
Buildfile: src/installer/resources/build.xml

install:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Be sure you have read the installation/upgrade instructions on the
Shibboleth website before proceeding.
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
skipping input as property idp.home.input has already been set.
The directory '/opt/shibboleth-idp' already exists.
Would you like to overwrite this Shibboleth configuration? (yes, [no
    ])
yes
skipping input as property idp.hostname.input has already been set.
skipping input as property idp.keystore.pass has already been set.
Updating property file:
/root/shibboleth-identityprovider-2.4.0/src/installer/resources/
    install.properties
Generating signing and encryption key, certificate, and keystore.
Copying 5 files to /opt/shibboleth-idp/bin
Copying 8 files to /opt/shibboleth-idp/conf
Copying 1 file to /opt/shibboleth-idp/metadata
Copying 46 files to /opt/shibboleth-idp/lib
Copying 5 files to /opt/shibboleth-idp/lib/endorsed
Copying 1 file to /root/shibboleth-identityprovider-2.4.0/src/
    installer
Building war: /root/shibboleth-identityprovider-2.4.0/src/installer/
    idp.war
Copying 1 file to /opt/shibboleth-idp/war
Deleting: /root/shibboleth-identityprovider-2.4.0/src/installer/web.
    xml
Deleting: /root/shibboleth-identityprovider-2.4.0/src/installer/idp.
    war

BUILD SUCCESSFUL
Total time: 6 seconds
```

- Otorgar permisos necesarios a los ficheros logs y metadata de shibboleth

```
# chown tomcat6.tomcat6 /opt/shibboleth-idp/logs/
# chown tomcat6.tomcat6 /opt/shibboleth-idp/metadata/
```

- Iniciar el servicio: |http://172.21.123.10:8080/idp/status

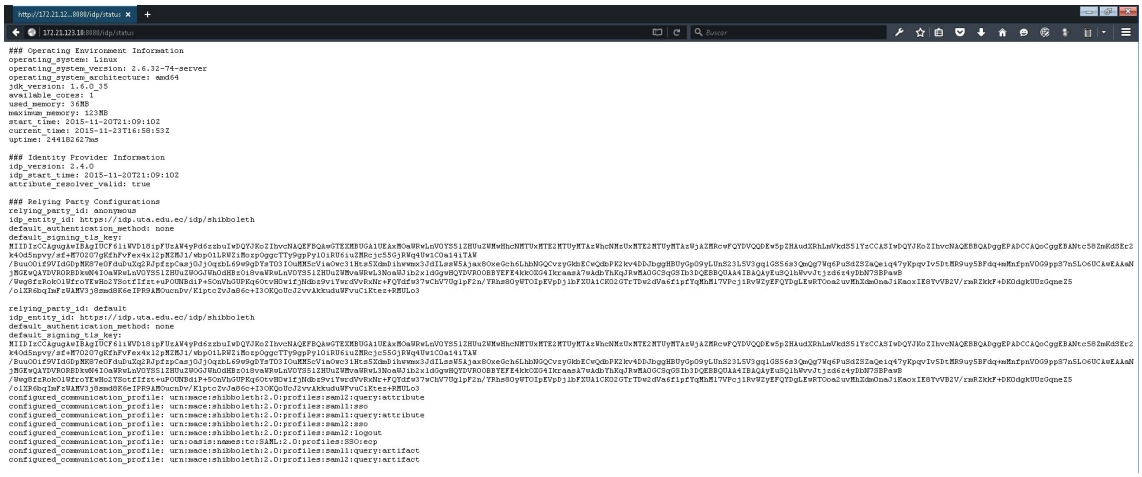

Figura 15: Iniciar Servicio Shibboleth Funcionando Puerto 8080
Fuente: El Investigador

Configuración de la autenticación de Shibboleth

ACTUALIZACIÓN DEL FICHERO HANDLER.XML

- En el fichero handler se habilita el tipo de autenticación que se quiere utilizar en Shibboleth.
    - Con respecto a los manejadores del proceso de Login bajo el comentario de

      <!– Login Handlers –>, se comentará el relativo a phRemoteUser, y descomentará la sección phUsernamePassword.

```
 <!-- Login Handlers -->
<!--
  <ph:LoginHandler xsi:type="ph:RemoteUser">
        <ph:AuthenticationMethod>urn:oasis:names:tc:SAML:2.0:ac:
            classes:unspecified
  </ph:AuthenticationMethod>
    </ph:LoginHandler>
-->

<ph:LoginHandler xsi:type="ph:UsernamePassword"
                 jaasConfigurationLocation="file:///opt/shibboleth-
                     idp/conf/login.config">
        <ph:AuthenticationMethod>urn:oasis:names:tc:SAML:2.0:ac:
            classes:PasswordProtectedTransport
```

```
    </ph:AuthenticationMethod>
     </ph:LoginHandler>
```

ACTUALIZACIÓN DEL FICHERO LOGIN.CONFIG

- El fichero login.config se comprobarán las credenciales que el usuario enviará en el formulario de login.
- Shibboleth IdP se basa en módulos JAAS, por lo que se podrá utilizar cualquiera que esté disponible dentro del classpath de dicho software. JAAS se encarga de definir cuales son los recursos a los que cada usuario puede acceder a través del rol o roles asignado[37].
- La única configuración que debe existir dentro del fichero es relativo al módulo "ShibUserPassAuth".

```
 ShibUserPassAuth {
   edu.vt.middleware.ldap.jaas.LdapLoginModule required
       ldapUrl="ldap://172.21.123.18:389"
       baseDn="ou=People,dc=uta,dc=edu,dc=ec"
       ssl="false
userFilter="uid={0}";
userField="uid"
serviceUser="cn=alexandra,dc=uta,dc=edu,dc=ec"
serviceCredential="alexandra"
subtreeSearch="false";
};
```

Configuración del Fichero RELYING-PARTY.XML

- En este fichero se establece los proveedores de servicio en los cuales se confía. Actualiza la configuración relativa al uso de metadatos externos, el acceso hacia cada uno de los servicios (googleaps, bibliotecas, servicios internos, externos, etc)
- Para esto entro de "Metadata Configuration" abajo de <!– Example metadata provider. –> agregar el servidor de pruebas:

```
<metadata:MetadataProvider id="testshib" xsi:type="metadata:
    FileBackedHTTPMetadataProvider"
        metadataURL="http://www.testshib.org/metadata/testshib-
            providers.xml"
        backingFile="/opt/shibboleth-idp/metadata/testshib.xml">
<metadata:MetadataFilter xsi:type="metadata:ChainingFilter">
```

```
<metadata:MetadataFilter xsi:type="metadata:EntityRoleWhiteList">
<metadata:RetainedRole>samlmd:SPSSODescriptor</metadata:RetainedRole
    >
</metadata:MetadataFilter>
</metadata:MetadataFilter>
</metadata:MetadataProvider>
```

Configuración de la política de emisión de atributos

ACTUALIZACIÓN DEL FICHERO ATTRIBUTE-RESOLVER.XML

- Este fichero establece con qué atributos trabajará el Proveedor de Identidad, y posee tres esquemas:

  - Schema: Core schema attributes
  - Schema: inetOrgPerson attributes
  - Schema: eduPerson attributes

- Dentro del fichero descomentar los 20 atributos correspondientes al esquema Core, debido a que con estos atributos trabajara el Idp y serán enviados posteriormente al SP.

- Colocar la conexión a la Base de Datos dentro de la sección DataConnector

```
<resolver:DataConnector id="myLDAP" xsi:type="dc:LDAPDirectory"
        ldapURL="ldap://172.21.123.18:389"
        baseDN="ou=Group,dc=uta,dc=edu,dc=ec"
       principal="cn=Manager,dc=uta,dc=edu,dc=ec"
        principalCredential="alexidp15">
        <dc:FilterTemplate>
            <![CDATA[
                (uid=$requestContext.principalName)
            ]]>
        </dc:FilterTemplate>
    </resolver:DataConnector>
```

Certificado Apache

- Dentro de /etc/apache2/sites-available/idp-SSO se configuró previamente las llaves privada (KeyFile), publica(File). Debido a que estas son las llaves que son vistas desde el mundo es recomendable que sean emitidas por un

CA público. En el presente proyecto estos certificados privado y público serán generados por el CA privado y enviado a los participantes.

```
SSLCertificateKeyFile /etc/ssl/private/idp.uta.edu.ec.key
SSLCertificateFile /etc/ssl/certs/idp.uta.edu.ec.crt
```

- Otorgar los permisos necesarios al certificado privado mediante el siguiente comando:

```
chmod 640 /etc/ssl/private/idp.uta.edu.ec.key
```

Certificado Tomcat

- En el fichero server.xml se configuró el conector 8443 en el cual se indica la ubicación del fichero keystoreFile, el mismo que almacena las claves para transacciones SSL, por lo que es necesario crear el fichero idp.p12, para ello se debe copiar el certificado público y privado (entregado por CEDIA) en /opt/shibboleth-idp/credentials, con los nombres idp.key e idp.crt. Y ejecutar el siguiente comando para crear idp.p12

```
openssl pkcs12 -export -in idp.crt -inkey idp.key -out idp.p12 -name
    idp -caname selfsigned
```

- Otrogar permisos al usuario tomcat6

```
chown tomcat6.tomcat6 /opt/shibboleth-idp/credentials/*
chown tomcat6.tomcat6 /opt/shibboleth-idp/metadata
```

Iniciar servicios apache y tomcat

```
/etc/init.d/tomcat6 restart
/etc/init.d/apache2 restart
```

- Apache2 Funcionando: https://172.21.123.10/idp/status

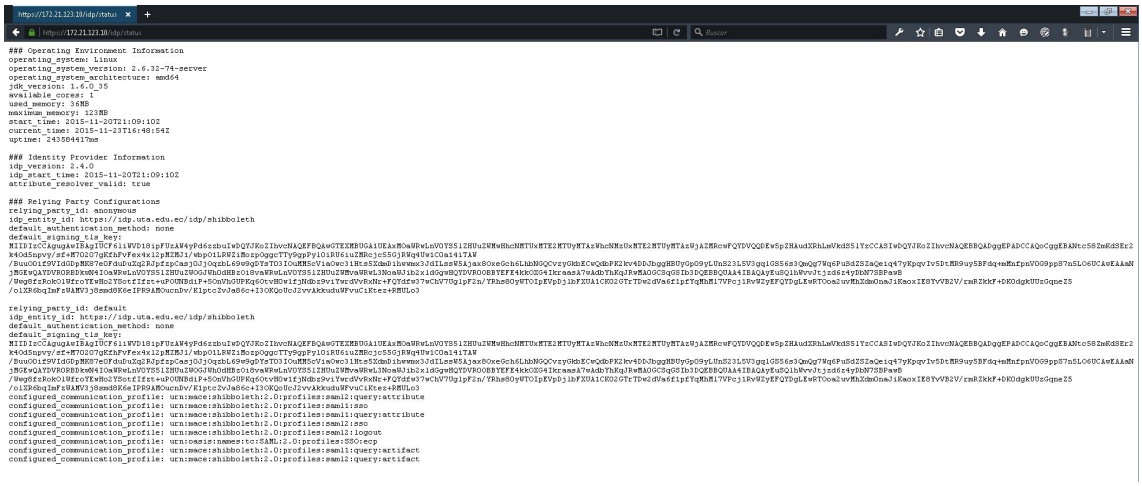

Figura 16: Apache2 Funcionando
Fuente: El Investigador

4.3.4. Configuración de OpenLDAP como servidor de autenticación

Instalar o actualizar, el equipamineto lógico necesario a través del comando:

```
yum -y install openldap openldap-clients openldap-servers
```

- Copiar el fichero DB_CONFIG a la carpeta ldap otorgándole los permisos necesarios, para ello ejecutar lo siguiente:

```
cp /usr/share/openldap-servers/DB_CONFIG.example/var/lib/ldap/
    autenticar/DB_CONFIG
```

```
chown ldap. /var/lib/ldap/DB_CONFIG
```

- Iniciar el servicio ldap a través del comando y añadir éste al resto de los servicios que arrancan junto con el sistema

```
/etc/rc.d/init.d/slapd start
chkconfig slapd on
```

Creación de claves de acceso administrador OpenLDAP

- El usuario administrador del directorio de LDAP posee una clave de acceso, para su creación se debe ejecutar el comando

  ```
  slappasswd
  ```

- Se obtendrá un criptograma, el cual será usado como clave de acceso para el usuario Manager, quien tendrá todos los privilegios sobre el directorio.

```
{SSHA}Oi1EsLGiNDutn6LhiLnb1y3hcxSIanoM
```

- Crear el fichero chrootpw.ldif añadiendo la clave generada en la sección olcRootPW.

```
dn: olcDatabase={0}config,cn=config
changetype: modify
add: olcRootPW
olcRootPW: {SSHA}Oi1EsLGiNDutn6LhiLnb1y3hcxSIanoM
```

- Los clientes y servidores OpenLDAP son capaces de utilizar Transport Layer Security (TLS), marco para proporcionar integridad y confidencialidad de protección de apoyo a la autenticación LDAP utilizando el mecanismo externo SASL; para brindar ello ejecutar el siguiente comando[37]:

```
ldapadd -Y EXTERNAL -H ldapi:/// -f chrootpw.ldif
SASL/EXTERNAL authentication started
SASL username:
gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={0}config,cn=config"
```

Establecer un nombre de dominio en la DB LDAP

- Generar la contraseña del Administrador de Directorios a través del comando:

  ```
  slappasswd
  ```

- Se obtendrá un criptograma el cual deberá ser reemplazado en el fichero de configuración chdomain.ldif.

  ```
  {SSHA}7DPefm43z2KQEFaIlY1IY9ztBPOSjgay
  ```

- Crear el fichero chdomain.ldif en el cual se debe llenar los campos dc por el nombre del dominio, y en el campo olcRootPW la contraseña de nombre de dominio generada.

```
dn: olcDatabase={1}monitor,cn=config
changetype: modify
replace: olcAccess
olcAccess: {0}to * by dn.base="gidNumber=0+uidNumber=0,cn=peercred,
    cn=external,cn=auth"
  read by dn.base="cn=Manager,dc=uta,dc=edu,dc=ec" read by * none

dn: olcDatabase={2}bdb,cn=config
changetype: modify
replace: olcSuffix
olcSuffix: dc=uta,dc=edu,dc=ec

dn: olcDatabase={2}bdb,cn=config
changetype: modify
replace: olcRootDN
olcRootDN: cn=Manager,dc=uta,dc=edu,dc=ec

dn: olcDatabase={2}bdb,cn=config
changetype: modify
add: olcRootPW
olcRootPW: {SSHA}7DPefm43z2KQEFaIlY1IY9ztBPOSjgay

dn: olcDatabase={2}bdb,cn=config
changetype: modify
add: olcAccess
olcAccess: {0}to attrs=userPassword,shadowLastChange by
  dn="cn=Manager,dc=uta,dc=edu,dc=ec" write by anonymous auth by
      self write by * none
olcAccess: {1}to dn.base="" by * read
olcAccess: {2}to * by dn="cn=Manager,dc=uta,dc=edu,dc=ec" write by *
     read
```

- Utilizamos el mecanismo externo de autenticación sobre el fichero chdomain.ldif

```
ldapmodify -Y EXTERNAL -H ldapi:/// -f chdomain.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=
    auth
SASL SSF: 0
```

```
modifying entry "olcDatabase={1}monitor,cn=config"
modifying entry "olcDatabase={2}bdb,cn=config"
modifying entry "olcDatabase={2}bdb,cn=config"
modifying entry "olcDatabase={2}bdb,cn=config"
```

- Creamos el fichero basedomain.ldif en el cual se indica el nombre del dominio en los campos dc, la organización a la pertenece (o:UTA) y el nombre del servidor (dc:uta).

```
dn: dc=uta,dc=edu,dc=ec
objectClass: top
objectClass: dcObject
objectclass: organization
o: UTA
dc: uta

dn: cn=Manager,dc=uta,dc=edu,dc=ec
objectClass: organizationalRole
cn: Manager
description: Directory Manager

dn: ou=People,dc=uta,dc=edu,dc=ec
objectClass: organizationalUnit
ou: People

dn: ou=Group,dc=uta,dc=edu,dc=ec
objectClass: organizationalUnit
ou: Group
```

- Añadir el dominio y el usuario manager el fichero basedomain.ldif

```
ldapadd -x -D cn=Manager,dc=uta,dc=edu,dc=ec -W -f basedomain.ldif
Enter LDAP Password:

adding new entry "dc=uta,dc=edu,dc=ec"
adding new entry "cn=Manager,dc=uta,dc=edu,dc=ec"
adding new entry "ou=People,dc=uta,dc=edu,dc=ec"
adding new entry "ou=Group,dc=uta,dc=edu,dc=ec"
```

- Autenticación de usuario Manager a través de la dirección 172.12.123.18/phpldapadmin/

Figura 17: Usuario Manager Ingresando a phpLDAPadmin
Fuente: El Investigador

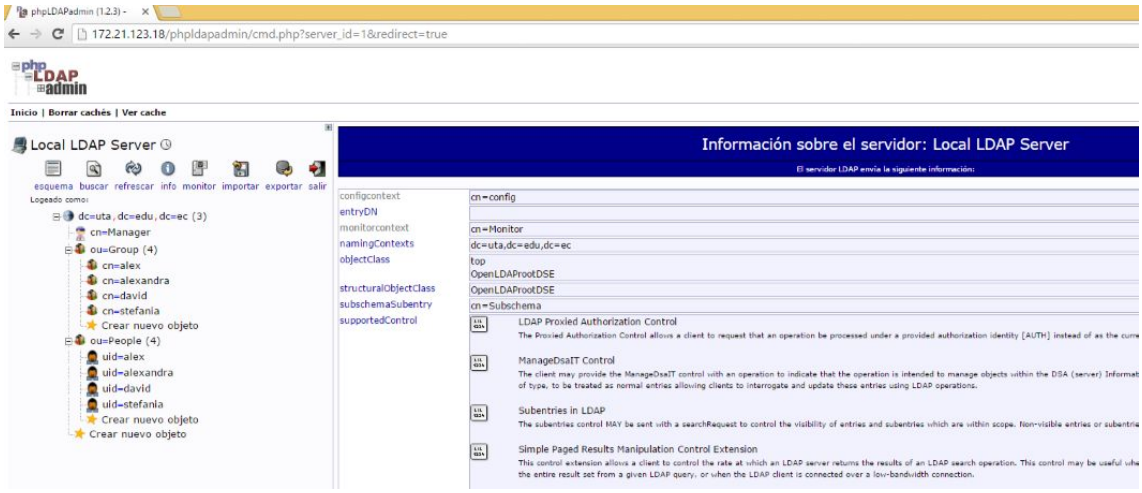

Figura 18: Pantalla de Ingreso Manager
Fuente: El Investigador

Añadir Clientes en el Servidor OpenLDAP

Permite que los usuarios accedan desde cualquier máquina a través de su login, frente al servidor LDAP.

- Crear el fichero ldapuser.ldif y añadir el siguiente código el mismo que permitirá crear usuarios dentro del servidor LDAP; para ello digitar en dc el dominio a utilizar.

```
dn: uid=cent ,ou=People ,dc=uta ,dc=edu ,dc=ec
objectClass: inetOrgPerson
```

```
objectClass: posixAccount
objectClass: shadowAccount
cn: Cent
sn: Linux
userPassword: {SSHA}Oi1EsLGiNDutn6LhiLnb1y3hcxSIanoM
loginShell: /bin/bash
uidNumber: 1000
gidNumber: 1000
homeDirectory: /home/cent

dn: cn=cent,ou=Group,dc=uta,dc=edu,dc=ec
objectClass: posixGroup
cn: Cent
gidNumber: 1000
memberUid: cent
```

- Agregar al fichero ldapuser.ldif el usuario Manager y el dominio a usar:

```
ldapadd -x -D cn=Manager,dc=uta,dc=edu,dc=ec -W -f ldapuser.ldif
Enter LDAP Password:
adding new entry "uid=cent,ou=People,dc=uta,dc=edu,dc=ec"
adding new entry "cn=cent,ou=Group,dc=uta,dc=edu,dc=ec"
```

- Fichero ldapuser.ldif después de ejecutar sentencia ldapadd:

```
[root@ldap ~]# vi ldapuser.ldif
shadowMax: 99999
shadowLastChange: 16678

dn: uid=stefania,ou=People,dc=uta,dc=edu,dc=ec
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
sn: stefania
givenName: stefania
cn: stefania
displayName: stefania
uidNumber: 502
gidNumber: 502
userPassword: {crypt}$6$DQl4awHL$m5AyVkfMW//
rGBmPljbY/8EBSqf9uM1.XLEn/.rMnOWxUo6PA7n43amBhGBYjKqGY.
mQsCuU7CyNmVVKuMlMk/
gecos: stefania
loginShell: /bin/bash
```

```
homeDirectory: /home/stefania
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 0
shadowMax: 99999
shadowLastChange: 16678

dn: cn=david,ou=Group,dc=uta,dc=edu,dc=ec
objectClass: posixGroup
cn: david
gidNumber: 500
memberUid: david

dn: cn=alexandra,ou=Group,dc=uta,dc=edu,dc=ec
objectClass: posixGroup
cn: alexandra
gidNumber: 501
memberUid: alexandra

dn: cn=stefania,ou=Group,dc=uta,dc=edu,dc=ec
objectClass: posixGroup
cn: stefania
gidNumber: 502
memberUid: stefania
```

- Añadir usuarios y grupos en el directorio LDAP a través del siguiente bash, el cual extrae los usuarios locales y grupos del fichero ldapuser.ldif [38]:

```
#!/bin/bash
SUFFIX='dc=uta,dc=edu,dc=ec'
LDIF='ldapuser.ldif'
echo -n > $LDIF
for line in `grep "x:[5-9][0-9][0-9]:" /etc/passwd | sed -e "s/ /%/g
    "`
do
    LUID="`echo $line | cut -d: -f1`"
    NAME="`echo $line | cut -d: -f5 | cut -d, -f1`"

    if [ ! "$NAME" ]
    then
        NAME="$LUID"
    else
        NAME=`echo "$NAME" | sed -e 's/%/ /g'`
    fi
```

```
    SN=`echo "$NAME" | awk '{print $2}'`
    [ ! "$SN" ] && SN="$NAME"

    LASTCHANGEFLAG=`grep $LUID: /etc/shadow | cut -d: -f3`
    [ ! "$LASTCHANGEFLAG" ] && LASTCHANGEFLAG="0"
    SHADOWFLAG=`grep $LUID: /etc/shadow | cut -d: -f9`
    [ ! "$SHADOWFLAG" ] && SHADOWFLAG="0"

    echo "dn: uid=$LUID,ou=People,$SUFFIX" >> $LDIF
    echo "objectClass: inetOrgPerson" >> $LDIF
    echo "objectClass: posixAccount" >> $LDIF
    echo "objectClass: shadowAccount" >> $LDIF
    echo "sn: $SN" >> $LDIF
    echo "givenName: `echo $NAME | awk '{print $1}'`" >> $LDIF
    echo "cn: $NAME" >> $LDIF
    echo "displayName: $NAME" >> $LDIF
    echo "uidNumber: `echo $line | cut -d: -f3`" >> $LDIF
    echo "gidNumber: `echo $line | cut -d: -f4`" >> $LDIF
    echo "userPassword: {crypt}`grep $LUID: /etc/shadow | cut -d: -
        f2`" >> $LDIF
    echo "gecos: $NAME" >> $LDIF
    echo "loginShell: `echo $line | cut -d: -f7`" >> $LDIF
    echo "homeDirectory: `echo $line | cut -d: -f6`" >> $LDIF
    echo "shadowExpire: `passwd -S $LUID | awk '{print $7}'`" >>
        $LDIF
    echo "shadowFlag: $SHADOWFLAG" >> $LDIF
    echo "shadowWarning: `passwd -S $LUID | awk '{print $6}'`" >>
        $LDIF
    echo "shadowMin: `passwd -S $LUID | awk '{print $4}'`" >> $LDIF
    echo "shadowMax: `passwd -S $LUID | awk '{print $5}'`" >> $LDIF
    echo "shadowLastChange: $LASTCHANGEFLAG" >> $LDIF
    echo >> $LDIF
done

for line in `grep "x:[5-9][0-9][0-9]:" /etc/group`
do
    CN="`echo $line | cut -d: -f1`"
    LGID="`echo $line | cut -d: -f3`"

    echo "dn: cn=$CN,ou=Group,$SUFFIX" >> $LDIF
    echo "objectClass: posixGroup" >> $LDIF
    echo "cn: $CN" >> $LDIF
    echo "gidNumber: $LGID" >> $LDIF
    echo "memberUid: `grep ":$LGID:" /etc/passwd | cut -d: -f1`" >>
        $LDIF
```

```
    users="`echo $line | cut -d: -f4`"
    if [ "$users" ]
    then
        for user in `echo "$users" | sed 's/,/ /g'`
        do
            [ ! "$CN" = "$user" ] && echo "memberUid: $user" >>
                $LDIF
        done
    fi
    echo >> $LDIF
done
```

- Autenticación de Usuario: stefania a través de la dirección 172.12.123.18/phpldapadmin/

Figura 19: Pantalla de Logeo Usuario LDAP
Fuente: El Investigador

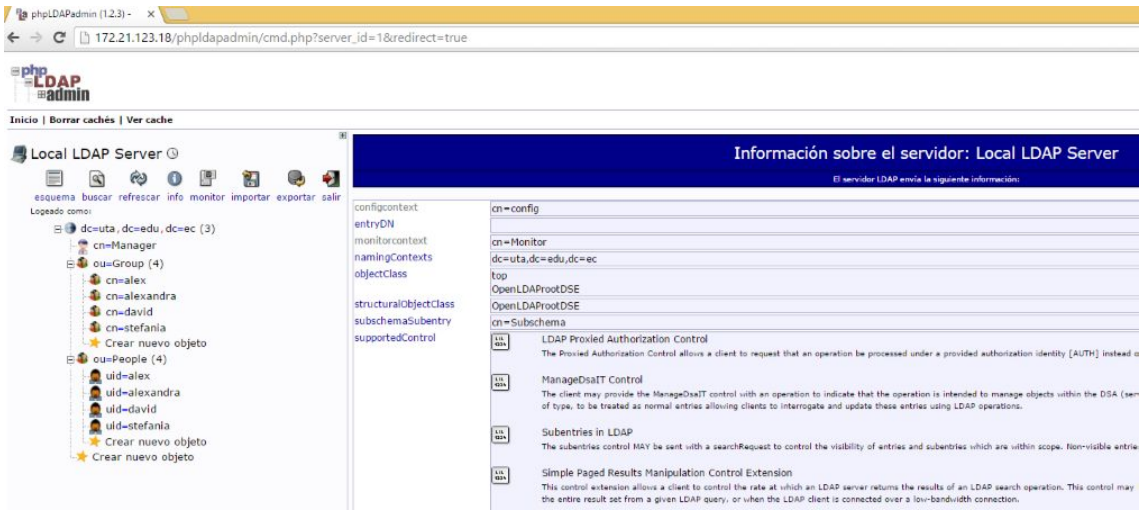

Figura 20: Pantalla de Ingreso Usuario LDAP
Fuente: El Investigador

4.3.5. Instalación Services Provider (SP)

- Instalar el demonio de Shibboleth a través de paquetes mediante el siguiente código:

```
apt-get install libapache2-mod-shib2
```

- Definir el entityID (nombre único) para distinguir el service provider entre los otros miembros de la federación.

- REMOTE_USER: contiene la lista de posibles atributos que pueden utilizarse para autenticar usuarios que se conectan a su sitio.

```
<ApplicationDefaults id="default" policyId="default"
        entityID="https://idp.uta.edu.ec/idp"
        REMOTE_USER="eppn␣persistent-id␣targeted-id"
        signing="true" encryption="true">
```

- Definir parámetros de sesión:

  - handlerSSL (booleano) (por defecto es true) Cuando es verdadero, sólo las peticiones web a través de SSL / TLS serán procesados por los manipuladores.

    Otras solicitudes se pueden bloquear, o posiblemente ignoran (y por lo general resultan en un error 404) en función del servidor web, pero nunca serán procesados.

    Esto es útil para los sitios que quieren proteger el tráfico de protocolo SAML.

  - exportLocation: Permite apoyar las operaciones de búsqueda local del aserciones SAML almacenadas en caché.

  - idpHistoryDays (tiempo en días) Determina el tiempo que las cookies persistirán. Si no se establece el númerp de días, caducará cuando el navegador se cierra [39].

```
<Sessions lifetime="28800" timeout="3600" checkAddress="false
    "
            handlerURL="/Shibboleth.sso" handlerSSL="true"
            exportLocation="http://172.21.123.76/federacion"
                exportACL="127.0.0.1"
            idpHistory="false" idpHistoryDays="9">
```

- Definir Iniciador de Sesión:
  - El elemento <SessionInitiator> se utiliza para configurar los controladores que son
  - responsables de iniciar el proceso de autenticación en el SP y el establecimiento de una sesión con el mismo.
  - WAYF SessionInitiator: Indicado por type = "WAYF" , se refiere al navegador a un servicio Shibboleth WAYF.
    - **atributos**
      - ◇ URL (URL absoluta): La URL de un servicio WAYF [40].

```
<SessionInitiator type="Chaining" Location="/Login" isDefault="
    true" id="Intranet"
    relayState="cookie" entityID="https://idp.uta.edu.ec/idp"
        forceAuthn="true">
  <SessionInitiator type="SAML2" acsIndex="1" template="
      bindingTemplate.html"/>
  <SessionInitiator type="Shib1" acsIndex="5"/>
</SessionInitiator>
<!-- An example using an old-style WAYF, which means Shib 1
    only unless an entityID is provided. -->
<SessionInitiator type="Chaining" Location="/WAYF" id="WAYF"
    relayState="cookie">
 <SessionInitiator type="SAML2" acsIndex="1" template="
     bindingTemplate.html"/>
  <SessionInitiator type="Shib1" acsIndex="5"/>
   <SessionInitiator type="WAYF" acsIndex="5" URL="https://
       federacion.uta.edu.ec/WAYF"/>
</SessionInitiator>
```

- Definir el fichero metadata:
  - Crear un fichero xml dentro de /etc/shibboleth

```
vi federacion.uta.edu.ec.xml
```

  - Generar un fichero de texto xml que contiene los metadatos necesarios para el SP mediante la siguiente línea de código:

```
shib-metagen -c /etc/ssl/certs/idp.uta.edu.ec.crt -h
    172.21.123.76.uta.edu.ec > /etc/shibboleth/federacion.uta.
    edu.ec.xml
```

En donde: -c indica la ubicación del certificado público que va a ser otorgado para la generación del fichero xml; -h indica el nombre del SP

- Definir recursos medata
  - El elemento <MetadataProvider> configura una fuente de metadatos para el uso del SP.
  - La "porción" XML es un recurso recargable , lo que significa que el contenido XML se puede suministrar en línea, en un fichero local o un fichero remoto, y se puede monitorizar los cambios y recargar en marcha [41].

```
<MetadataProvider type="XML" uri="https://federacion.uta.edu.ec/
    federacion.uta.edu.ec.xml"
                  backingFilePath="/etc/shibboleth/federacion.uta.edu
                      .ec.xml" reloadInterval="7200">
                <MetadataFilter type="RequireValidUntil"
                    maxValidityInterval="2419200"/>
                <MetadataFilter type="Signature" certificate="
                    fedsigner.pem"/>
            </MetadataProvider>

<MetadataProvider type="XML" file="/etc/shibboleth/federacion.uta.
    edu.ec.xml
"/>
```

- Configurar Apache2 para permitir Shibboleth mediante el comando : **a2enmod shib2**

```
Enabling module shib2.
Run '/etc/init.d/apache2 restart' to activate new configuration!
```

- Se procede a crear un directorio (dip) que será visto desde cualquier navegador dentro de /var/www
  - Editar el archivo /etc/apache2/sites-available/default con el siguiente contenido:
  -
```
Alias /idp/ "/var/www/idp"
        <Directory "/var/www/idp">
        Options Includes
        AllowOverride All
        Order allow,deny
        Allow from all
        </Directory>
```

- Crear un archivo nuevo dentro de la carpeta /var/www , la misma que contendrá un archivo .htaccess que permitirá modificar o agregar funciones a directorios, con la siguiente sintaxis:

```
AuthType shibboleth
Require valid-user
```

En donde:

- AuthType: Tipo de autentificación de usuarios
- Require: Selecciona qué usuarios autentificados pueden acceder a un recurso

Figura 21: Página Principal de Autenticación Sistema Federado (SP)
Fuente: El Investigador

4.3.6. Servicios del Sistema Federado

4.3.6.1. File Sender

FileSender es una aplicación basado en web que permite a los usuarios autenticados enviar de forma segura y sencilla archivos arbitrariamente grandes a otros usuarios.
Los usuarios sin una cuenta reciben un comprobante, por un usuario autenticado, que permite subir archivos y ser enviados.
FileSender se ha desarrollado para las necesidades de la comunidad de enseñanza superior e investigación.

El propósito del programa es enviar archivos de gran tamaño, tener ese archivo disponible para su descarga durante un cierto número de descargas o una cierta cantidad de tiempo, y después se elimine automáticamente el archivo.
El software no pretende ser una plataforma de publicación de archivos permanente [42].

Funcionamiento:

Los archivos son compartidos con las personas seleccionadas, de modo que el remitente envía un mensaje al correo electrónico, el que adjuntará una URL que corresponde a la ubicación del archivo a descargar.
El número máximo de destinatarios es 100 por envío.

Beneficios:

Esta herramienta permite el envío de archivos de hasta 100GB por cada envío.
Transferencia rápida de información, que no puede ser compartida por las limitaciones típicas de capacidad de almacenamiento asociadas a usuarios en repositorios o buzones de correo electrónico [43].

4.3.6.2. Enciclopedia Británica

Britannica Academic Edition

Diseñado específicamente para cumplir con los requisitos de investigación y productividad de universidades y bibliotecas académicas [44].

- **Sitios de la Web recomendados**: Los editores de Britannica seleccionan y examinan más de 100,000 sitios Web externos para asociarlos a artículos y resultados de investigación.
- **Ebooks y fuentes primarias**: Miles de libros electrónicos (muchos de ellos ilustrados) además de documentos históricos y documentos asociados con artículos.
- **Analista de Datos Mundiales:** Una base de datos exclusiva con datos estadísticos actuales y pasados que explora los países del mundo.
- **Diarios y Artículos de Revistas Íntegros**: Más de 700 títulos, a través de una asociación con EBSCO. Los títulos son seleccionados especialmente para cubrir las necesidades universitarias y cuentan con artículos que cubren hasta tres años. Estos artículos son incorporados a la herramienta de búsqueda de Britannica y correlacionados a artículos de referencia específica.

- **Atlas Mundial Interactivo:** Acceso a los detallados mapas de Britannica y a los datos de países de forma simultánea.
- **Workspace**: El espacio de trabajo exclusivo de Britannica es un organizador de investigaciones para guardar diferentes contenidos de Britannica.
- **Diccionario y Tesauro Merriam-Webste's Collegiate:** Incorporado a las bases de datos con pronunciación de audio y resulta accesible desde cualquier palabra.
- **Diccionario de Citas Merriam-Webster:** Ofrece una viva colección de más de 4,000 citas, tanto contemporáneas como clásicas, para informes y presentaciones.

Britannica Image Quest

ImageQuest ofrece una colección única de imágenes organizadas por temas en un solo sitio web. Empresas como Bridgeman Art Gallery, Dorling Kindersley Images, Getty Images, the National Portrait Gallery of London, the National Geographic Society y otras entidades renombradas se han unido con Britannica para ofrecer la mejor y más amplia colección de imágenes. ImageQuest permite que los estudiantes accedan a millones de imágenes de 60 proveedores con la misma suscripción [45].

Enciclopedia Moderna

Británica Enciclopedia Moderna es un portal digital en español ideal para investigaciones. Las herramientas de investigación en este portal ofrecen el acceso rápido a información fiable en español, todo en un sitio Web fácil de usar. Británica Enciclopedia Moderna da acceso a miles de artículos, recursos multimedia, mapas y mucho más. El sitio web es ideal para estudiantes y profesores que necesitan acceso a información confiable en español. Enciclopedia Moderna es un portal de referencia online en español, creado especialmente para atender las necesidades de la comunidad académica en América Latina [46].

Escolar Online

Británica Escolar es un portal digital en español que ayuda a enriquecer el aprendizaje de los estudiantes de primaria y secundaria. El contenido actualizado de Británica Escolar está organizado por niveles académicos para ayudar a

mejorar el rendimiento de los estudiantes, facilitar la instrucción diferenciada y maximizar el uso de la tecnología en el aula.
Británica Escolar permite que los estudiantes completen sus trabajos escolares usando los más de 15.000 artículos de la enciclopedia y 9.000 elementos multimedia que incluyen imágenes, videos, audio y mapas detallados. Los estudiantes también pueden disfrutar de una gran variedad de herramientas útiles para el aprendizaje desarrolladas por especialistas en la educación [47].

4.3.6.3. Colaboratorio Red Cedia

Portal desarrollado para el apoyo y fomento de la colaboración científico-académica latinoamericana. Colaboratorio de Red Cedia es un nexo que une a los usuarios que lo integran, y les permite utilizar las distintas herramientas y servicios que la red avanzada ofrece para la concreción de sus objetivos y los de sus investigaciones colaborativas.
Mediante las herramientas y servicios que Colaboratorio pone a su disposición, podrá acceder y ser parte de las discusiones y eventos de las comunidades pertenecientes a Red Cedia, crear y participar de conferencias web, reservar salas multipunto para conferencias H.323, buscar y encontrar documentos de Red Cedia y de las comunidades que la integran, transferir archivos pesados, postular a oportunidades de fondos para proyectos, ir al encuentro de socios y colaboradores para su investigación y proyectos [48].

4.3.7. Ventajas y Desentajas de uso de Sistema Federado dentro de la FISEI

Ventajas

1. **Ventajas para los usuarios:**
    - **Identidad única para todos los servicios federados**: Una única clave que le da acceso a todos los servicios.
    - **Single Sign ON (SSO) Web**. Una vez identificado el usuario en un sistema federado tendrá acceso al resto de servicios hasta que se finalice la sesión (log out) sin tener que volver a introducir sus credenciales de acceso.
    - **Single Log Out (SLO)**. Al cerrar sesión de una aplicación se cerrará la sesión de todas las aplicaciones federadas, mejorando así la seguridad del sistema.

- **Fiable, fácil y rápido**. Al usuario se le presenta un único sistema de autenticación que conoce.

2. **Ventajas para administradores de sistemas:**
   - **Facilita los procedimientos**. Se despliega un escenario controlado en el que los accesos están monitorizados y todos el procesos controlados.
   - **Menor número de incidencias:** Al existir una clave única los administradores dejan de atender a incidencias relacionadas con pérdidas y reseteos de claves. Los datos de los usuarios pasan a estar en un punto común verificados y actualizados por lo que se reducen las duplicidades de cuentas y los conflictos.
   - **Mayor control de los datos del usuario.** Mediante la definición de ARPs (Attribute Release Policies) adecuadas el administrador puede decidir, dentro del conjunto de datos que posee de cada usuario, cuáles enviar a un servicio concreto.

3. **Ventajas para las organizaciones**:
   - **Mayor interoperabilidad / productividad**. Fácil integración con multitud de sistemas heterogéneos. la tecnología SAML2 se erige como el futuro de los sistemas de federación de identidades. Un ejemplo son los exitodos sistemas de acceso unificado de Facebook o Google, que permiten acceder a todos sus servicios bajo el protocolo SAML2.
   - **Reducción de riesgos de seguridad**. Las comunicaciones que envían información del usuario siempre van cifradas incluso cuando se accede por protocolos no seguros como HTTP. La contraseña del usuario nunca viaja entre los distintos nodos de la federación. Se utiliza tecnología PKI para todo este proceso de cifrado de comunicaciones [29].

4. Reducción de tiempo y número de procedimientos para proveer acceso a un recurso compartido a otras instituciones o dentro de la misma. En el campus universitario, los recursos digitales pueden ser cuentas de correo, plataformas educativas (sistemas e-learning), bases de datos de las bibliotecas, equipos informáticos, entre otros; para poder acceder a cada uno de estos recursos, el usuario (alumno o docente), requiere autenticarse. Haciendo uso de un sistema de autenticación centralizado, el usuario es capaz de acceder a cada uno de los recursos haciendo uso de un mismo

usuario y una misma contraseña. Además el usuario puede hacer uso de sus mismas credenciales para poder acceder a recursos compartidos entre distintas instituciones.

Desventajas

1. Mayor complejidad para instalar y configurar Shibboleth como Proveedor de Identidad.
2. Mayor mantenimiento.
3. Puede requerir hardware adicional para instalar el servidor de federación.
4. Se requiere actualización de software o versiones diferentes a las actualizadas para implementar una nueva configuración.
5. Requieren una configuración amplia para Single Sign On.

CAPÍTULO 5

Conclusiones y Recomendaciones

5.1. Conclusiones

- Después de haber realizado un estudio comparativo entre las diferentes herramientas Open Source que permiten federar aplicaciones se concluyó que Shibboleth es mejor alternativa debido a que brinda seguridad y privacidad al momento de intercambiar información entre el SP y las instituciones participantes, manteniendo la integridad de los datos de los usuarios.

- Las asociaciones facilitan el intercambio de recursos entre las diferentes organizaciones, promoviendo así la cooperación entre los participantes en un círculo de confianza.

- A través de la identidad federada se simplifica el acceso por parte del usuario a los recursos, ya que fomentan la autenticación única con Single Sign-On.

- El presente proyecto de investigación sirve como guía de un sistema federado, para acceder a los diferentes servicios que oferta la comunidad universitaria tales como bibliotecas, repositorios, revistas científicas, entre otros, a través del DITIC (Dirección de Tecnología de Información y Comunicación) de la Universidad Técnica de Ambato y en conjunto con CEDIA (Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado) institución encargada de proporcionar el acceso a estos recursos por medio de MINGA quien maneja las identidades dentro del Ecuador; cabe añadir que al momento de culminar el proyecto de investigación, CEDIA está implementando nuevos servicios para los Sistemas Federados del Ecuador motivo por el cual no todos estos han sido añadidos al sistema, sin embargo la aplicación cuenta con las configuraciones necesarias para la implementación de nuevos servicios en un futuro.

5.2. Recomendaciones

- Es aconsejable que la Facultad y Universidad a través de CEDIA u otra institución que ofrezca aplicaciones aptas para la comunidad educativa, realice convenios para adquirir servicios tales como: repositorios virtuales, aplicaciones de investigación, revistas científicas o portales de empresas de software, que ofrecen paquetes gratuitos a universitarios, entre otros; que puedan ser federados en la institución.

- Shibboleth puede ser considerada inicialmente como una herramienta compleja por tal motivo, se requiere realizar un análisis detallado sobre su funcionamiento y estructura.

- El presente proyecto de investigación sirve como una guía para la instalación y configuración de Shibboleth, sistema de federación de código abierto, el mismo que fue elegido después de haber sido analizado y comparado con otros sistemas que ofrecen este aplicativo, en dicho proyecto se detalla la configuración de los archivos principales de Shibboleth como proveedor de identidad y como proveedor de servicios; además se anexa instalación de LDAP como servidor de autenticación y Active Directory en Windows Server 2012 con un dominio y usuarios para futuras conexiones que permitirá el acceso a diferentes recursos ofrecidos por CEDIA a través de MINGA y cualquier institución que pueda ofrecer servicios a la comunidad educativa.

- Diseñar un plan de contingencia integral que relacione equipamiento físico(hardware), equipamiento lógico (software) e infraestructura, debido a que, si el servidor de federación está fuera de servicio, los usuarios no podrán autenticarse.

Bibliografia

[1] C. Teixeira y J. Sousa Pinto F. Pimenta. Globalid federated identity provider associated with national citizens card, 2010.

[2] V. Choyi y Y. Shah Y. Targali. Seamless authentication and mobility across heterogeneous networks using federated identity systems, 2013.

[3] D. Jain y V. Tejaswi N. Satyanarayana, N. Gupta. *Design and development of collaborative educational network Global virtual institution using grid, federated identity management and virtual meeting techonologies.* Web Technologies Centre for Development of Advanced Computing Hyderabad, India, 2012.

[4] Galvez Nicolas. Estado del arte: Identity management options in current and future internet. `https://scm.labit.inf.utfsm.cl/trac/sc2011/wiki/IdentityManagement#no1`, 2013. [Online; accessed 13-Abril-2015].

[5] P. L. M. Aurélio. Federacao de identidades e computacao em nuvem: Estudo de caso usando shibboleth, 2012.

[6] Arlindo L. Marcon Jr Maicon S., Altair O. Integral federated identity management for cloud computing, 2012.

[7] . G. E. C. E. Feliciano Guilherme A. L., . O. L. Uma arquitetura para gerencia de identidades em nuvens híbridas, 2011.

[8] Osmosis Latina. Server.xml. `http://www.osmosislatina.com/tomcat/configuracion.htm`, 2005. [Online; accessed 06-Junio-2015].

[9] Jaime Valenzuela. *Introducción a las infraestructuras de Active Directory.* Región Metropolitana, Chile, 2008.

[10] Torres V País L, Ribeiro S. Gestion de identidad: Modelos. `http://www.gta.ufrj.br/grad/11_1/geren-id/index.php?file=kop1.php`, 2011. [Online; accessed 29-Julio-2015].

[11] Diario Linux. Hosts virtuales en apache 2 (ubuntu). `http://diariolinux.com/2007/05/29/hosts-virtuales-en-apache-2-ubuntu/`, 2007. [Online; accessed 07-Junio-2015].

[12] Daniel García Moreno. *SSH SOBRE FEDERACIÓN DE IDENTIDAD.* Sevilla, 2008.

[13] José Oliver Julio Pons. Instalación y configuración de un servidor radius. `http://www.grc.upv.es/docencia/tra/PDF/Radius.pdf`, 2012. [Online; accessed 06-Julio-2015].

[14] TeleInfo. Servidores radius. `http://trabajotele08.blogspot.com/`, 2008. [Online; accessed 07-Julio-2015].

[15] Cisco. ¿cómo el radius trabaja? `http://www.cisco.com/cisco/web/support/LA/102/1024/1024966_32.html`, 2014. [Online; accessed 08-Julio-2015].

[16] Rafael Calzada. Introduccion al servicio de directorio. `https://www.rediris.es/ldap/doc/ldap-intro.pdf)`, 2013. [Online; accessed 29-Mayo-2016].

[17] Microsoft. Introduction to lightweight directory access protocol (ldap). `https://support.microsoft.com/en-us/kb/196455)`, 2015. [Online; accessed 30-Mayo-2016].

[18] Celida Romero. *Analisis Comparativo entre productos que proveen servicio de directorio pertenecientes aTecnologias propietaria y de libre acceso, aplicado a laboratorios en ambientes educativos.* Escuela Superior Politecnica del Litoral, 2008.

[19] J. Gil D. Marcos J. Berna J. Monllor H. Ramos A. Albaladejo A. Hernandez F. Macia, F. Mora. *Administración de servicios de Internet: De la teoría a la práctica.* Universidad de Alicante,España, 2008.

[20] Rafael Calzada. Introducción al servicio de directorio. `https://www.rediris.es/ldap/doc/ldap-intro.pdf`, 2015. [Online; accessed 25-Junio-2015].

[21] Pilar Gonzalez. Configuración de active directory. `http://www.ditec.um.es/aso/teoria/tema13.pdf`, 2007. [Online; accessed 02-Julio-2015].

[22] LA COFA. Identidad 2.0. `https://lacofa.fundaciontelefonica.com/2008/05/23/identidad_federada/`, 2008. [Online; accessed 10-Enero-2016].

[23] PAPI. Papi. http://www.papisoftware.net/doku.php, 2011. [Online; accessed 08-Enero-2016].

[24] José María Palazón Romero. Single sign-on y federación de identidades. https://www.exabyteinformatica.com/uoc/Dactiloscopia/Identidad_digital/Identidad_digital_(Modulo_4).pdf, 2010. [Online; accessed 10-Enero-2016].

[25] Claudiu Nisipasiu Ionut Andronache. Web single sign-on implementation using the simplesamlphp application. http://www.jmeds.eu/index.php/jmeds/article/viewFile/Web-Single-Sign-On-Implementation-Using-the-SimpleSAMLphp-Application/pdf, 2011. [Online; accessed 10-Enero-2016].

[26] simpleSAMLphp. simplesamlphp installation and configuration. https://simplesamlphp.org/docs/1.9/simplesamlphp-install, 2010. [Online; accessed 10-Enero-2016].

[27] Teresa Matamoros. Papoid: Papi openid server. https://www.rediris.es/ptyoc/res/store/dl20/PAPOID-PFC.pdf, 2008. [Online; accessed 10-Enero-2016].

[28] Tecnológico Nacional de México. ¿qué es internet 2? https://www.tecnm.mx/telecomunicaciones/que-es-internet-2, 2012. [Online; accessed 14-Junio-2015].

[29] Sixto Martín. Curso para operadores de proveedores de servicio. https://confia.aupa.info/docs/cursos/2012/noviembre/index.html, 2012. [Online; accessed 16-Junio-2015].

[30] Alvaro Soto. *Configuración de una infraestructura basada en SAML para el acceso seguro a una Federación de Sistemas*. Universidad de Sevilla, 2005.

[31] Blackboard. Tipo de proveedor de autenticación shibboleth. http://help.blackboard.com/es-es/Learn/9.1_2014_04/Administrator/070_Server_Management_and_Integrations/Authentication/030_Auth_Implementing/Shibboleth_Authentication_Provider_Type, 2015. [Online; accessed 16-Julio-2015].

[32] Joaquín García. El repositorio y el sources.list de ubuntu. http://ubunlog.com/repositorios-de-ubuntu/, 2013. [Online; accessed 04-Junio-2015].

[33] Aitor Iriarte. Instala un vim más completo. http://aitoreus.blogspot.com/2011/01/instala-un-vim-mas-completo.html, 2011. [Online; accessed 04-Junio-2015].

[34] Open Alfa. Cómo configurar la rotación de logs en linux. http://blog.openalfa.com/como-configurar-la-rotacion-de-logs-en-linux, 2014. [Online; accessed 05-Junio-2015].

[35] Sergio Talens. Ficheros de configuración. http://www.uv.es/sto/cursos/seguridad.java/html/sjava.html#toc6, 2000. [Online; accessed 06-Junio-2015].

[36] Sergio Tales. Introducción a los certificados digitales. http://www.accv.es/noticias/certificadosdigitales.pdf, 2007. [Online; accessed 10-Diciembre-2015].

[37] Cecilio Álvarez. Seguridad y jass. http://www.arquitecturajava.com/seguridad-y-jaas/, 2013. [Online; accessed 13-Noviembre-2015].

[38] Server World. Add ldap user accounts. http://www.server-world.info/en/note?os=CentOS_6&p=ldap&f=7, 2015. [Online; accessed 05-Diciembre-2015].

[39] Nate Klingenstein. Nativespsessions. https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPSessions, 2015. [Online; accessed 27-Marzo-2016].

[40] Nate Klingenstein. Nativespsessioninitiator. https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPSessionInitiator#NativeSPSessionInitiator-WAYFSessionInitiator(DiscoveryHandler), 2015. [Online; accessed 27-Marzo-2016].

[41] Nate Klingenstein. Nativespmetadataprovider. https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPMetadataProvider), 2015. [Online; accessed 27-Marzo-2016].

[42] Xander Jansen. Filesender home. https://www.assembla.com/spaces/file_sender/wiki, 2016. [Online; accessed 20-Marzo-2016].

[43] Cedia. Envío de archivos. https://www.cedia.org.ec/colaboratorio/envio-de-archivos, 2016. [Online; accessed 20-Marzo-2016].

[44] Britannica Digital Learning. Britannica academic: Base de datos completa e ideal para cualquier uso académico. http://www.britannica.es/products/online/BritannicaAcademic.html, 2016. [Online; accessed 22-Marzo-2016].

[45] Britannica Digital Learning. Britannica imagequest: Acceso a casi tres millones de imágenes ideales para cualquier uso educativo. http://www.britannica.es/products/online/ImageQuest.html, 2016. [Online; accessed 22-Marzo-2016].

[46] Britannica Digital Learning. Britannica enciclopedia moderna: Portal de referencia completamente en español. http://www.britannica.es/products/online/EnciclopediaModerna.html, 2016. [Online; accessed 22-Marzo-2016].

[47] Britannica Digital Learning. Britannica escolar. http://www.britannica.es/products/online/BritannicaEscolar.html, 2016. [Online; accessed 22-Marzo-2016].

[48] Red Clara. Colaboratorio red clara. http://www.redclara.net/index.php/productos-y-servicios/servicios-para-la-colaboracion, 2016. [Online; accessed 22-Marzo-2016].

[49] RedCLARA. Sepa más sobre las comunidades en redclara. http://www.redclara.net/index.php/conocimiento-e-innovacion/colaboracion-en-red/temas/sepa-mas-comunidades, 2016. [Online; accessed 23-Marzo-2016].

[50] Renata. Servicios sivic. https://www.renata.edu.co/index.php/component/content/article/70-servicios/7204-sivic-agendamiento-de-multiconferencia, 2016. [Online; accessed 22-Marzo-2016].

[51] Renata. Herramientas de colaboración-envio. https://www.renata.edu.co/index.php/component/content/article/147-servicios-star/herramientas-de-colaboracion/7256-envio, 2016. [Online; accessed 22-Marzo-2016].

Anexos y Apéndices

Anexo A

Configuración Active Directory

- Dentro de Administrador del Servidor en el Panel se encuentra la opción Instalación basada en características o roles.

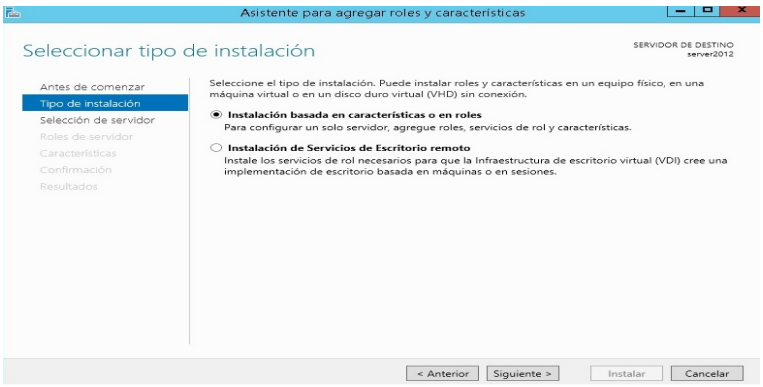

Figura 22: Instalación Basada en Características o Roles
Fuente: El Investigador

- Seleccionar el servidor destino a utilizar.

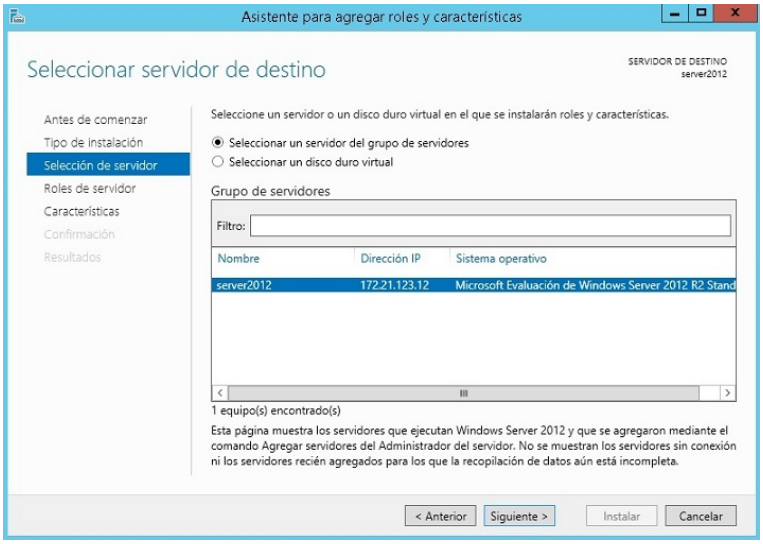

Figura 23: Servidor destino
Fuente: El Investigador

- Instalar Servicios de Dominio Active Diretory, solicitará la instalación de componentes adicionales

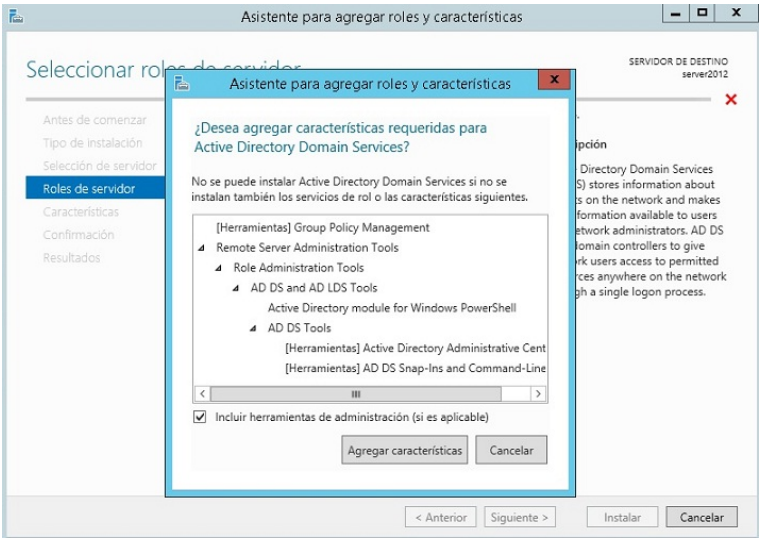

Figura 24: Servicio de Dominio Active Directory
Fuente: El Investigador

- Agregar características que necesita instalar para promoverlo a DC

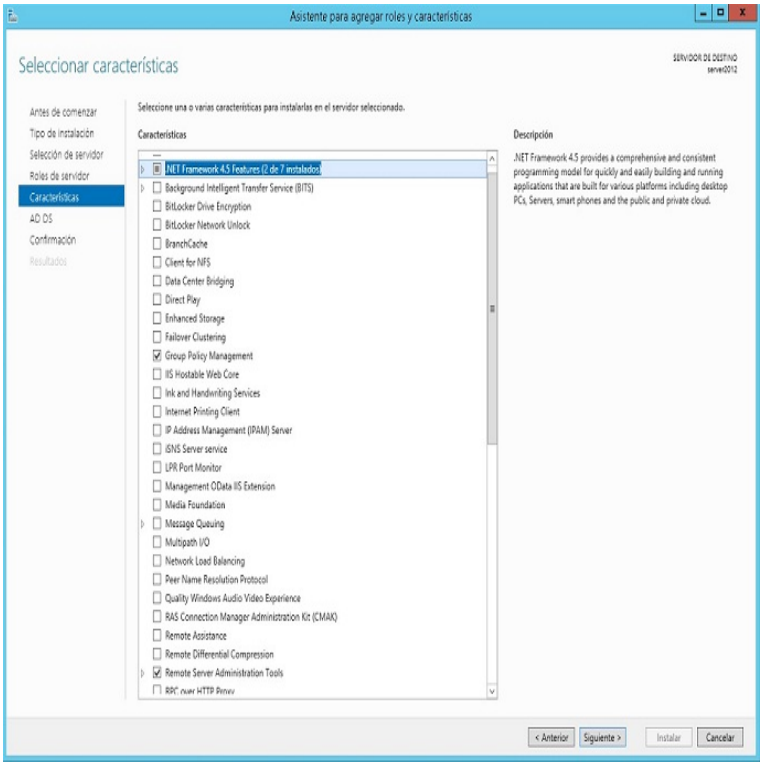

Figura 25: Características DC
Fuente: El Investigador

- Se visualizará un resumen detallando las características de lo que se va instalar.

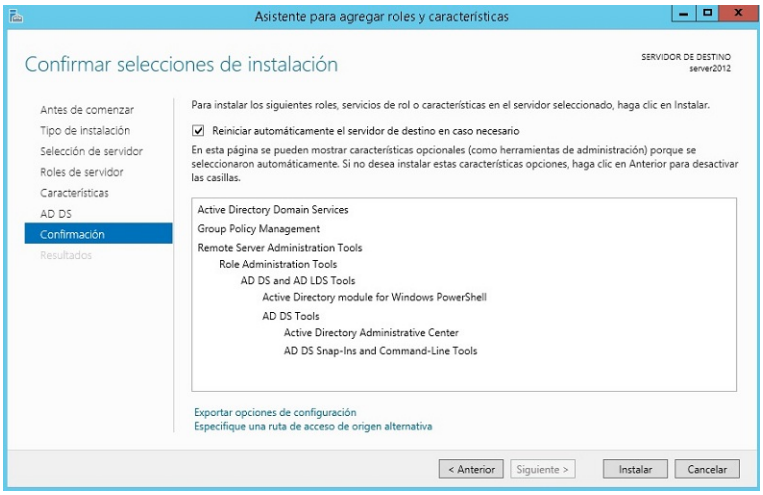

Figura 26: Confirmar selección de aplicación
Fuente: El Investigador

- Finalizada la instalación, y ya en el último paso, se debe promover al equipo como Controlador de Dominio configurándolo de acuerdo a la necesidad.

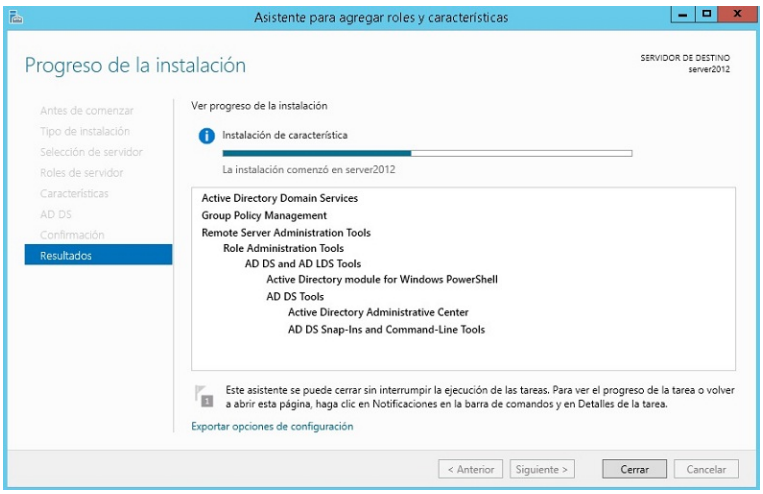

Figura 27: Progreso de la Instalación AD
Fuente: El Investigador

- La opción ofrecida por omisión es crear un nuevo Bosque (“Forest”), que es lo que se debe seleccionar cuando se está creando el primer Dominio Active Directory. Se debe ingresar el nombre del Dominio a crear: uta.edu.ec.

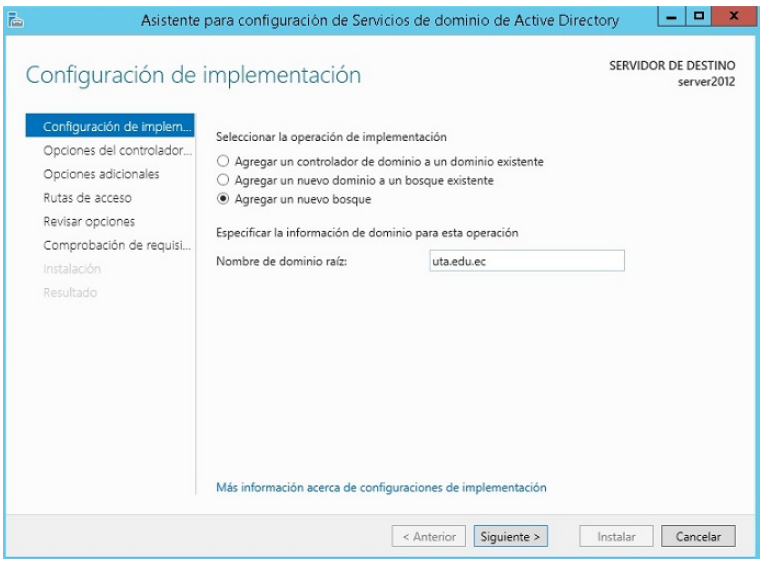

Figura 28: Nombre del Dominio
Fuente: El Investigador

- Salvo que posteriormente se vaya a instalar Controladores de Dominio con versiones anteriores del sistema operativo, no conviene disminuir los niveles funcionales. Es de gran importancia colocar una contraseña segura de "Directory Service Restore Mode" (DSRM). Esta contraseña es necesaria en caso de hacer una restauración desde una copia de seguridad del Controlador de Dominio, esta no tiene relación con la cuenta de administrador del Dominio, no se sincroniza, y es individual para cada Controlador de Dominio.

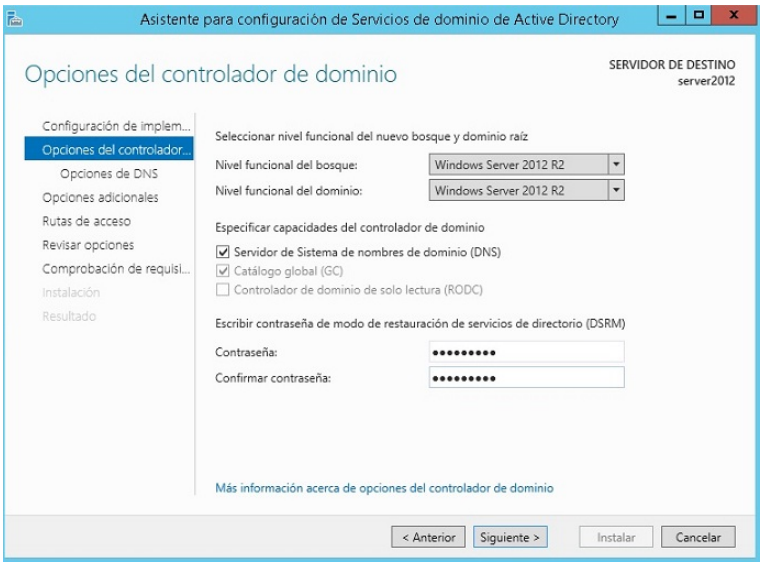

Figura 29: Controlador de Dominio
Fuente: El Investigador

- Al crear una zona DNS es normal que no pueda efectuar la delegación en el DNS superior.

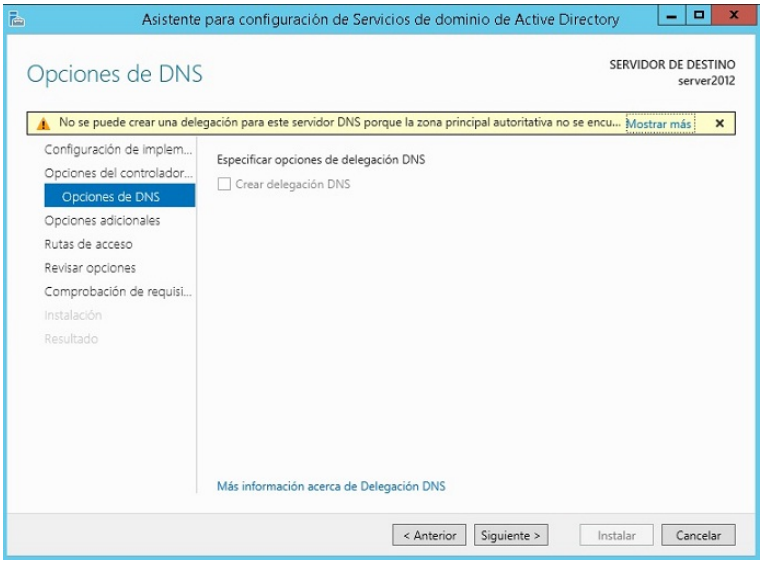

Figura 30: DNS
Fuente: El Investigador

- Agregar el nombre NetBIOS, se sugiere el nombre del Dominio, salvo que esté duplicado en la red, siempre será la parte más a la izquierda del nombre de Dominio que se haya colocado.

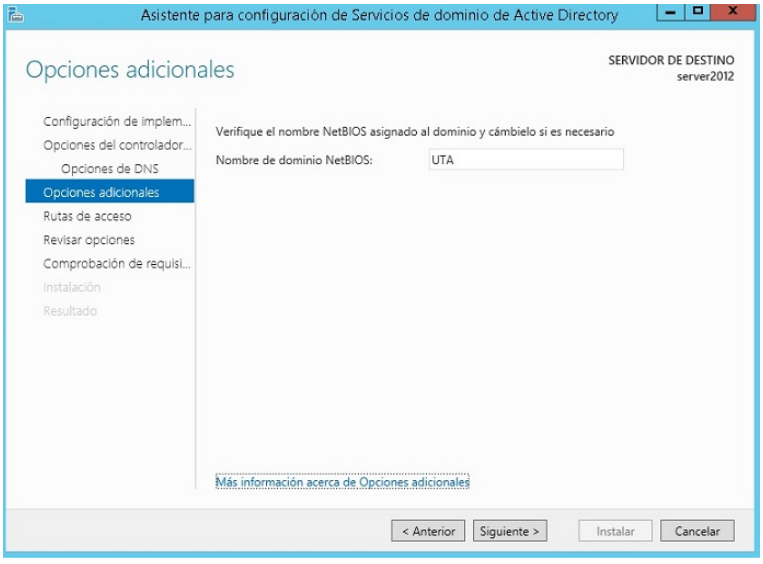

Figura 31: Nombre NetBIOS
Fuente: El Investigador

- Salvo que se tenga en el servidor más de un disco físico y se espere que el Active Directory sea “muy grande”, no conviene cambiar las ubicaciones de los archivos. Como aclaración: mover la base y los logs es muy sencillo luego, pero cambiar la ubicación de SYSVOL es problemático. Para la aplicación debido al espacio sobrante en la partición C: se optó por cambiar a la unidad D:

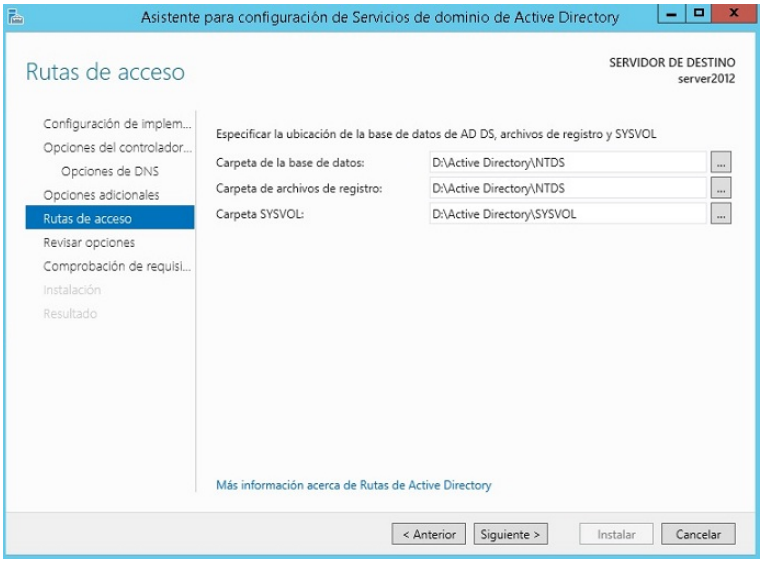

Figura 32: Ubicación Base de Datos del AD
Fuente: El Investigador

- Verificar si lo seleccionado es lo deseado para la creación del nuevo dominio, seguido se reiniciará la máquina automáticamente con el nombre del nuevo dominio.

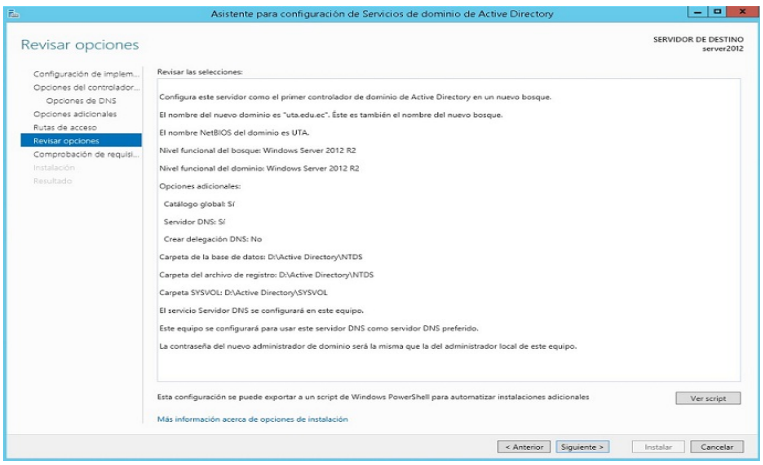

Figura 33: Revisar opciones nuevo Dominio
Fuente: El Investigador

Creación de Usuarios

- Dentro de Usuarios y Equipos de Active Directory, en el dominio uta.edu.ec se creará un contenedor de usuarios; en el mismo se agregará usuarios de prueba siguiendo estos pasos:

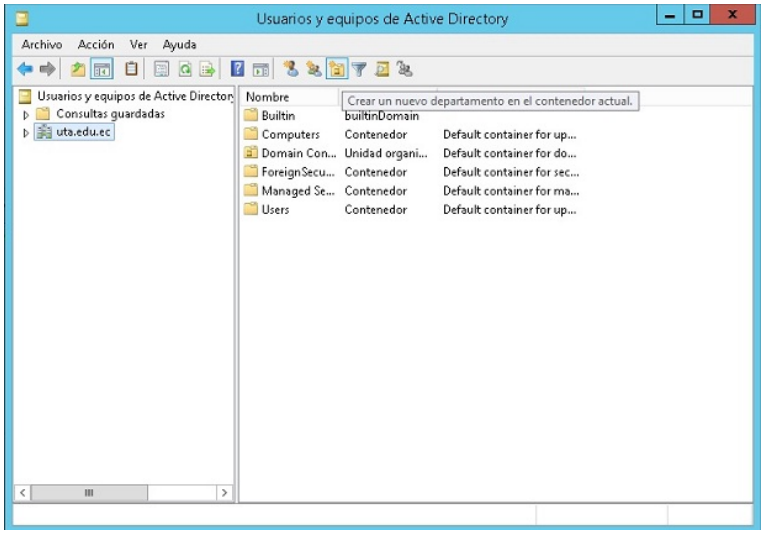

Figura 34: Contenedor de Usuarios
Fuente: El Investigador

- Dar un nombre de pila, apellidos, iniciales, nombre de inicio de sesión de usuario.

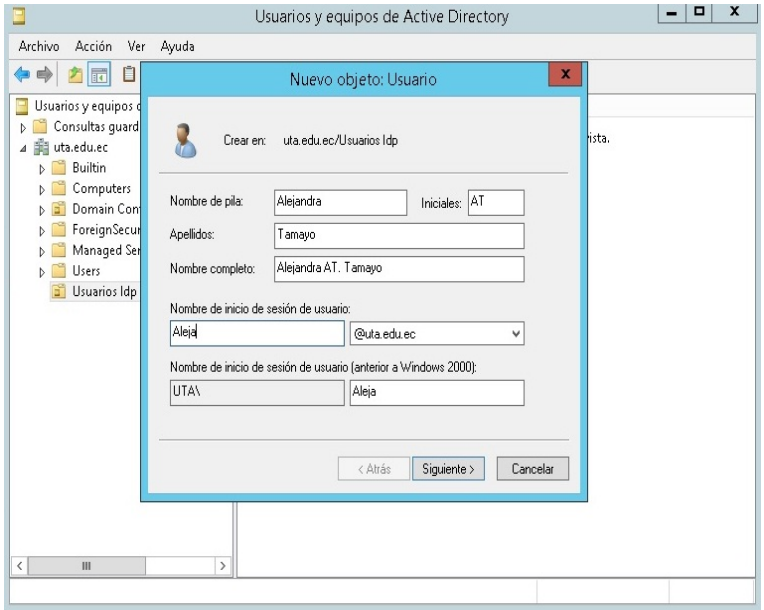

Figura 35: Datos Personales del Usuario
Fuente: El Investigador

- Establecer una contraseña e indicar que la contraseña nunca expira.

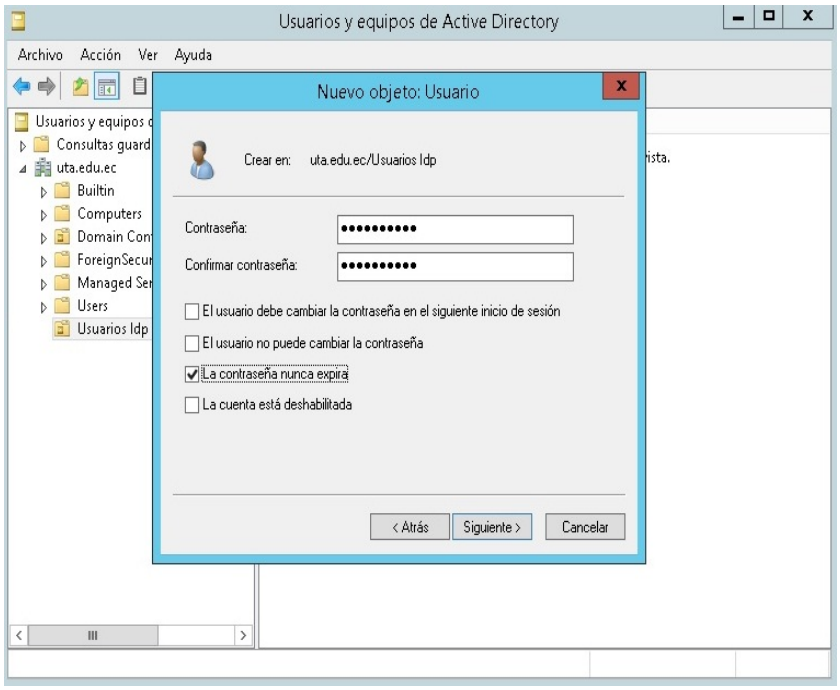

Figura 36: Establecer Contraseña al Usuario
Fuente: El Investigador

- Finalmente se muestra la información detallada del usuario

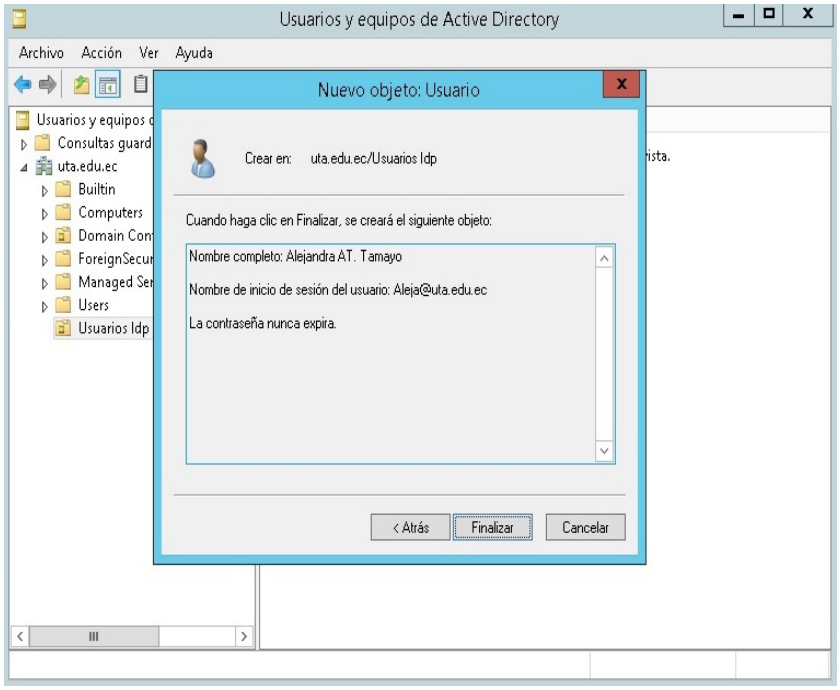

Figura 37: Información detallada del Usuario
Fuente: El Investigador

- Se ha creado cuatro usuario como ejemplo

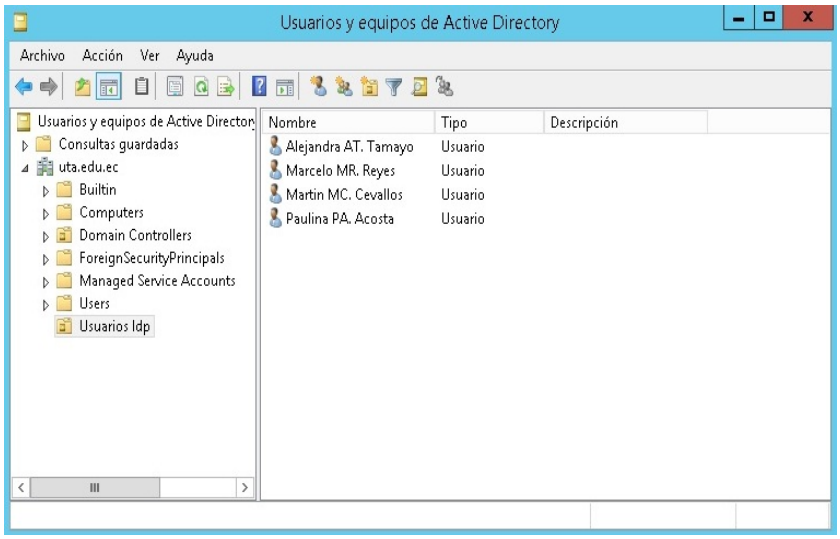

Figura 38: Ejemplos de Usuarios Windows Server 2012
Fuente: El Investigador

Unir un cliente Windows 7 al dominio

- Ingresar a Propiedades de la conexión de área local TCP/IPv4, y señalar la dirección IP de máquina y como DNS la IP del servidor 172.21.123.12.

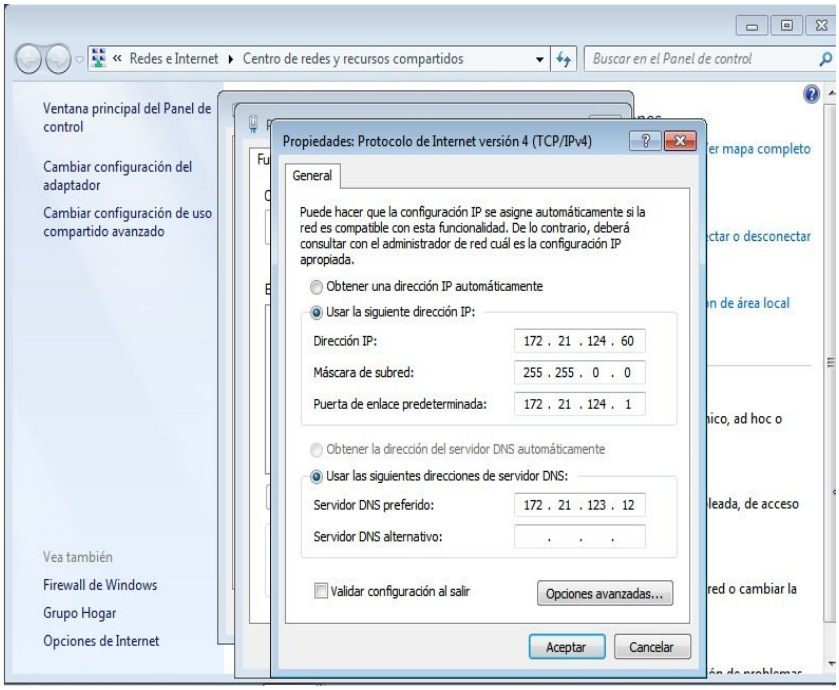

Figura 39: Propiedades de la conexion de área local
Fuente: El Investigador

- Dentro de Propiedades del Sistema se procede a cambiar el nombre del equipo y nombre del dominio.

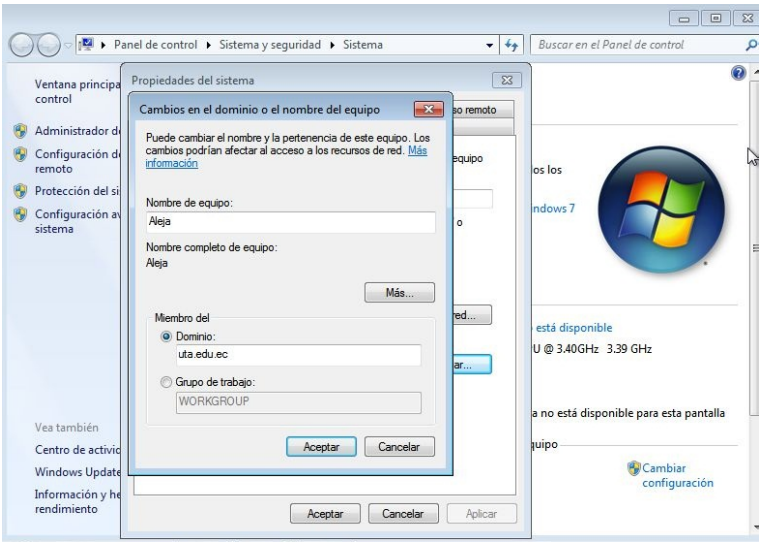

Figura 40: Nombre de equipo y dominio
Fuente: El Investigador

- En ese momento, Windows 7 busca en la red el dominio especificado. Si no lo encuentra, aparecerá un mensaje de aviso; si lo encuentra, se debe escribir un nombre de usuario y una contraseña, perteneciente al dominio, que tenga privilegios suficientes para unir el equipo cliente.

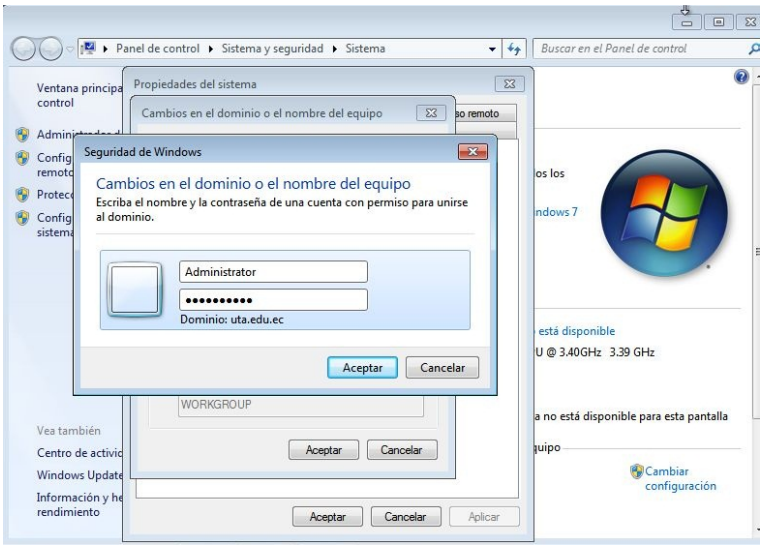

Figura 41: Autenticación para unirse al dominio
Fuente: El Investigador

- La ventana de autenticación se cierra y en su lugar aparece un mensaje indicando que el equipo se ha unido correctamente al dominio. Si se comete algún error en el nombre de usuario o en la contraseña, en lugar del mensaje siguiente, aparecerá uno de error y se tendrá que volver a intentar.

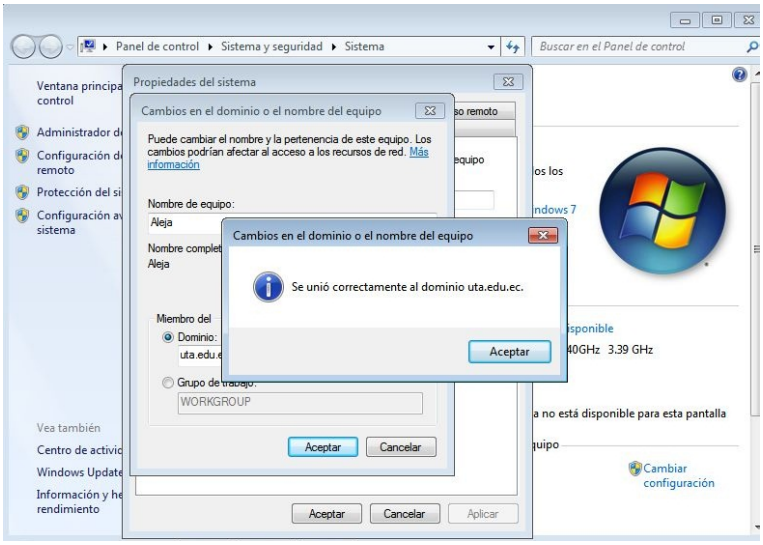

Figura 42: Autenticación exitosa
Fuente: El Investigador

Anexo B

Uso de Recursos dentro del Sistema Federado

B.1. FileSender

- **Envío de un archivo**

Para Enviar un archivo debe escribir la dirección de destino, indicar la fecha de expiración del archivo y seleccionar el archivo a subir.
El destinatario recibirá un correo con un enlace para descargar el archivo.

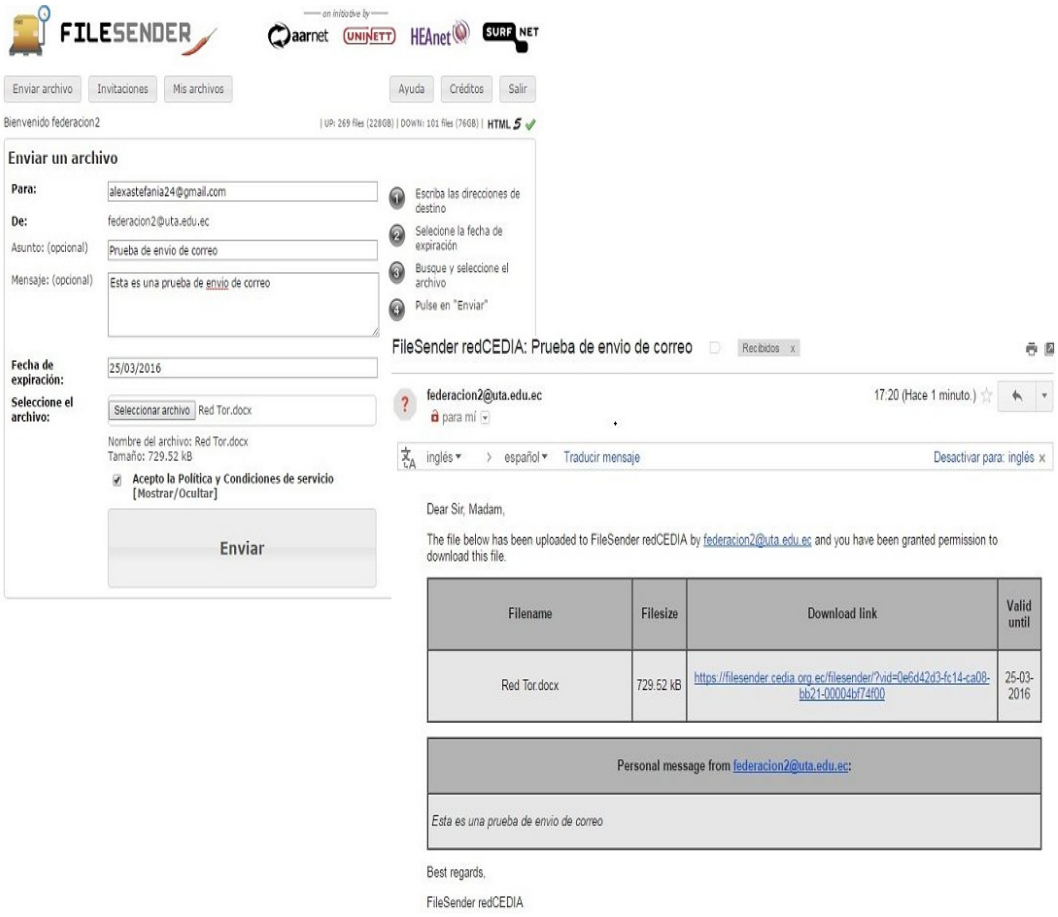

Figura 43: Envió de un archivo
Fuente: El Investigador

Dentro del enlace el usuario accede como invitado y puede descargar el archivo recibido.

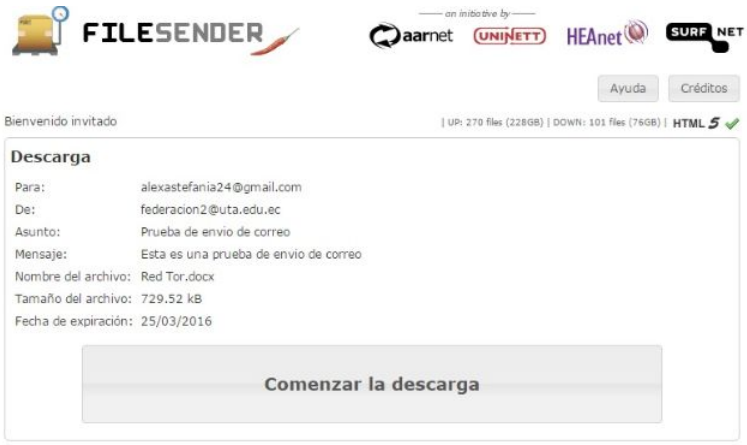

Figura 44: Descarga de Archivo Recibido
Fuente: El Investigador

- **Invitaciones de envío**

Con las "Invitaciones de envío", cualquiera puede enviarle un archivo. Para generar una "Invitación de envío", se escribe una dirección de correo, a continuación se pulsa en "Enviar la Invitación". El destinatario recibirá un correo con un enlace a la Invitación.

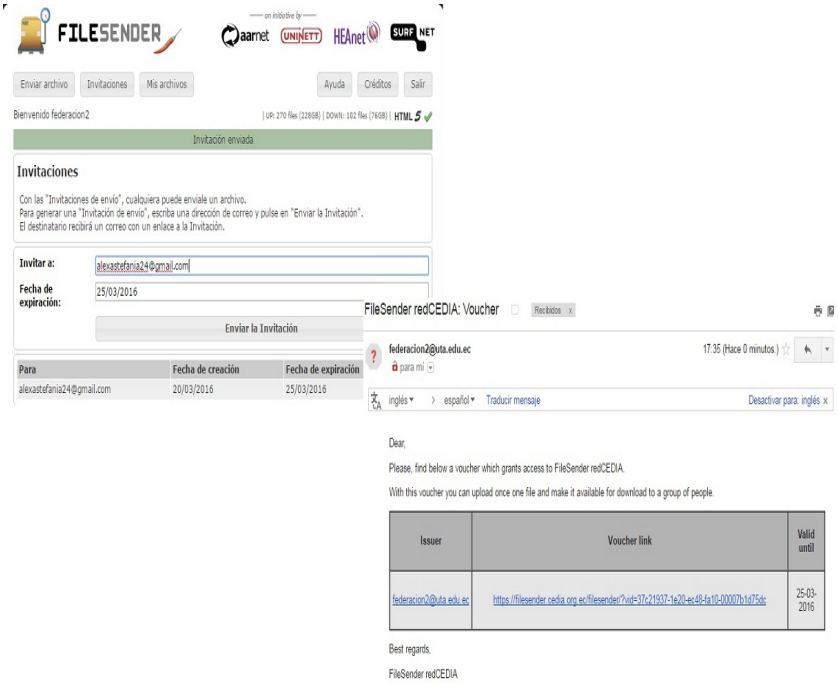

Figura 45: Invitación de Envío
Fuente: El Investigador

Dentro del enlace, se encuentra una pantalla de envió de correo en la cual se introduce la dirección destino, fecha de expiración y el archivo a enviar

Figura 46: Envío Correo Electrónico desde cuenta invitada
Fuente: El Investigador

- **Mis Archivos**

Dentro de la pestaña “Mis Archivos” se puede encuentra los Archivos enviados o recibidos con su detalle: Nombre del archivo, Tamaño, asunto, mensaje, fecha de creación y expiración.

Figura 47: Mis Archivos
Fuente: El Investigador

B.2. Enciclopedia Británica

B.2.1. Britannica Academic Edition

- **Página Principal**

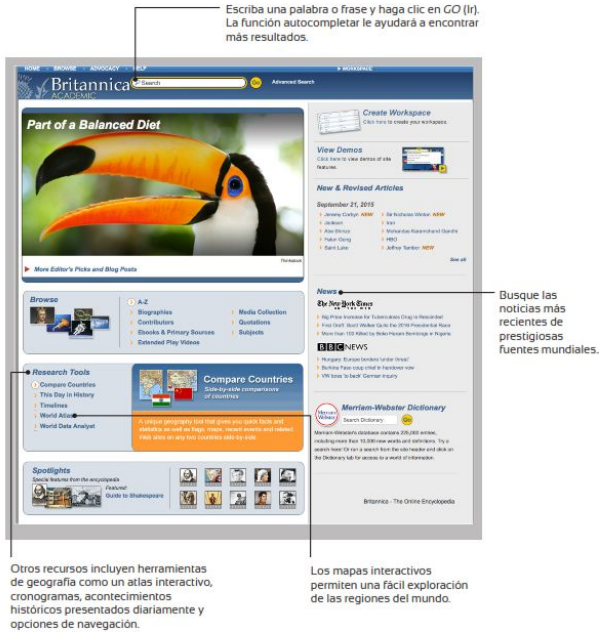

Figura 48: Página Principal Academic Edition
Fuente: El Investigador

- **Página de Resultados de Búsqueda**

Muestra opciones relevantes al buscar un artículo dentro de Academic Edition

Figura 49: Página de Búsqueda
Fuente: El Investigador

Figura 51: Referencias
Fuente: El Investigador

- **Página de Artículos**

Indica las diferentes opciones que se muestran al desplegar un artículo, tal como: videos e imágenes, web links, widgets, dictionary, entre otros.

Figura 50: Página de Artículos
Fuente: El Investigador

- **Referencia o Citación de un artículo**

Muestra las diferentes formas de citar un artículo, pudiendo ser estas: MLA, APA, Harvard y Chicago Manual of Style.

- **Historia de Actualización de Artículos**

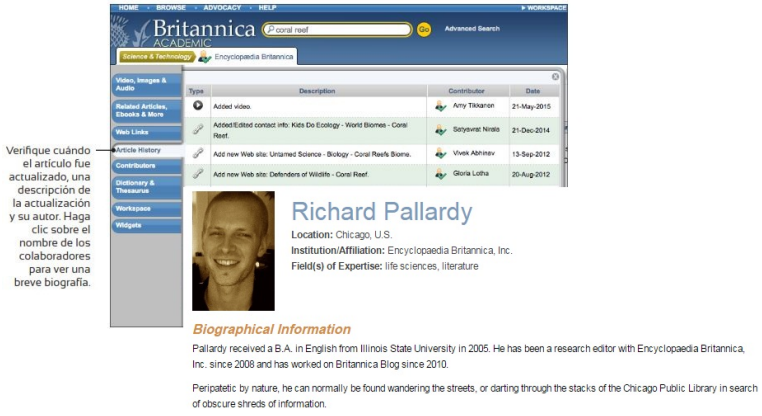

Figura 52: Historial de Actualización de Artículos
Fuente: El Investigador

B.2.2. Británica Image Quest

- **Página Principal**

Figura 53: Página Principal Image Quest
Fuente: El Investigador

- **Búsqueda Flexible**

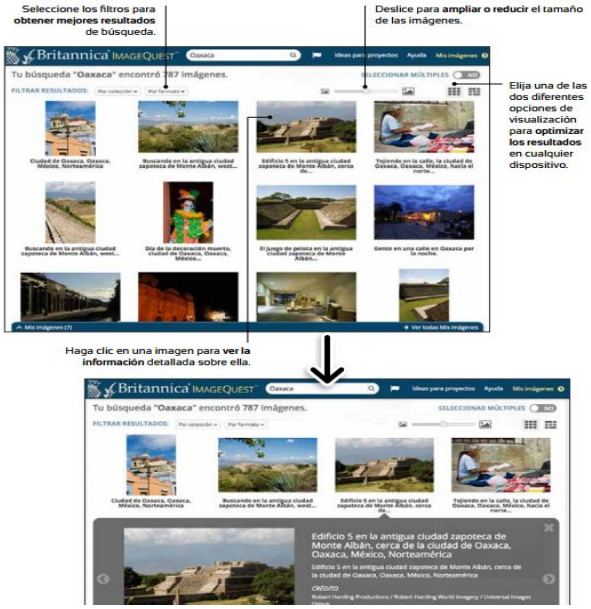

Figura 54: Búsqueda Flexible Image Quest
Fuente: El Investigador

- **Detalles de la Imagen**

Todos los datos importantes sobre las imágenes están ubicados en una sola página.

Figura 55: Detalles de la Imagen
Fuente: El Investigador

- **Mis Imágenes**

Figura 56: Selección de Múltiples Imágenes
Fuente: El Investigador

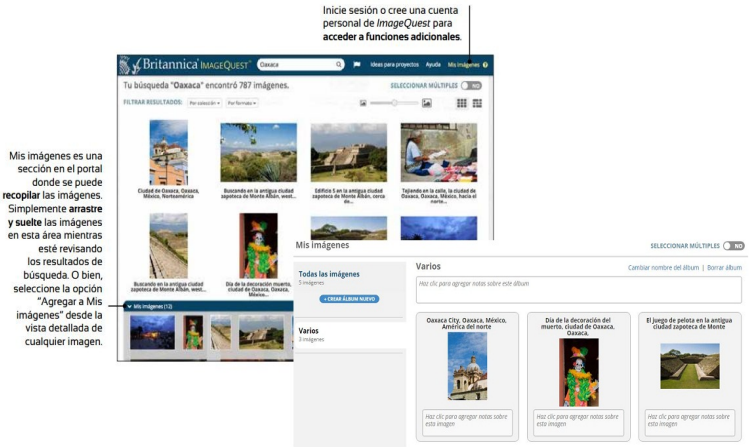

Figura 57: Mis Imágenes
Fuente: El Investigador

B.2.3. Británica Enciclopedia Moderna

- **Página Principal**

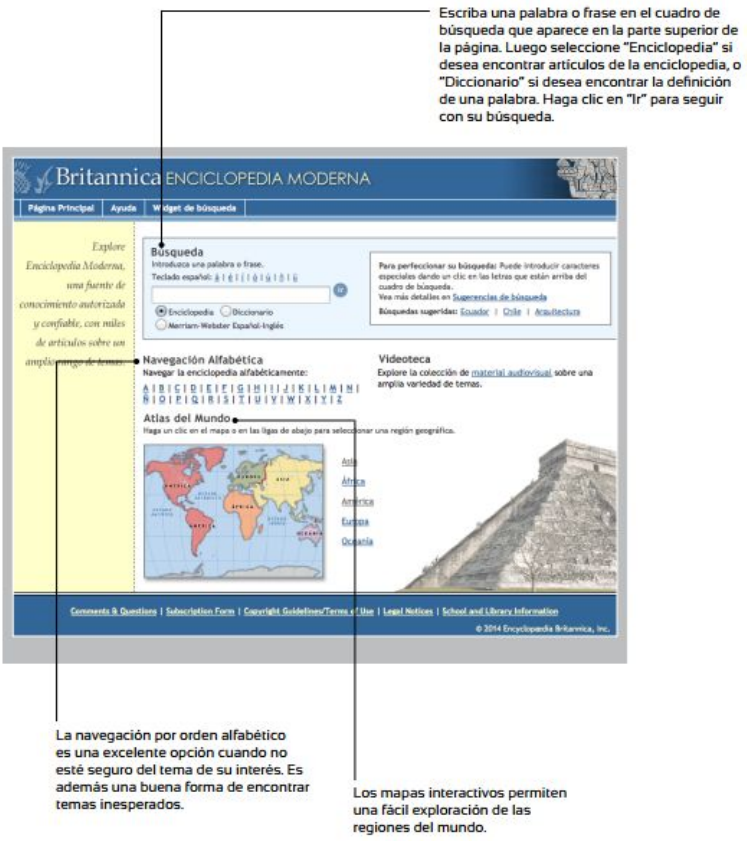

Figura 58: Página Principal Británica Moderna
Fuente: El Investigador

- **Búsqueda**

Figura 59: Página de Resultados de Búsqueda
Fuente: El Investigador

- **Artículo Enciclopedia Moderna**

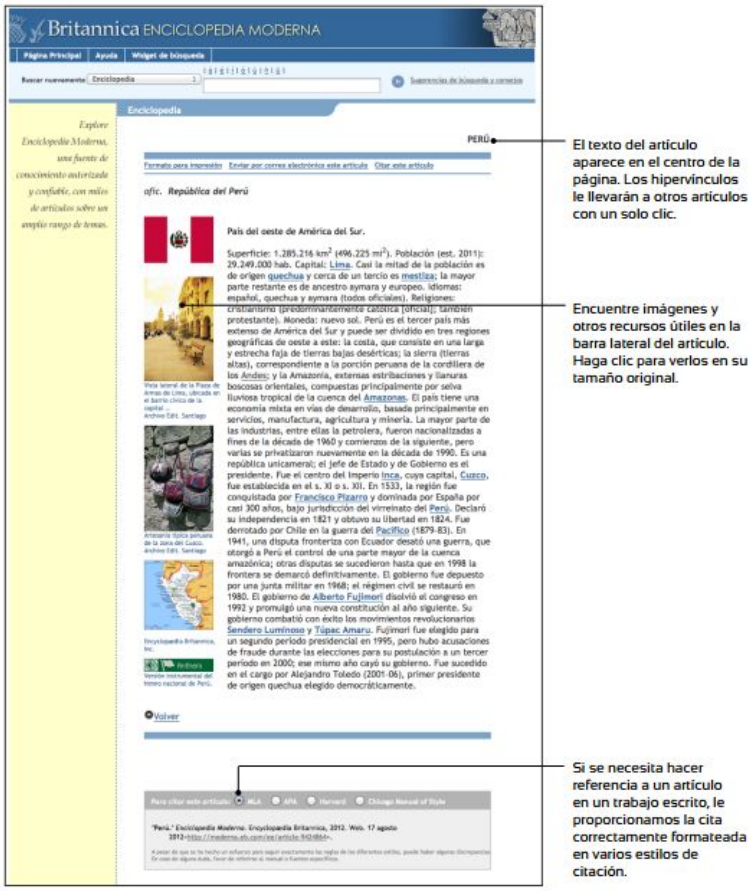

Figura 60: Página de artículos
Fuente: El Investigador

Es posible enviar un artículo a través de correo electrónico para ello se digita al dirección de correo a enviar, el nombre de quien lo envia y su respectivo mail.

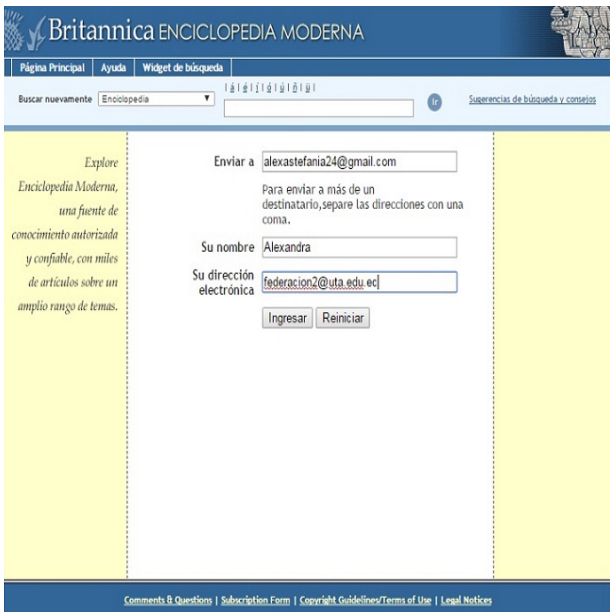

Figura 61: Envío de Artículo
Fuente: El Investigador

- **Atlas del mundo**

Desde la página principal, se puede realizar clic sobre un continente o seleccionar uno de los enlaces que se muestran en la parte derecha. En el mapa del continente, seleccionar cualquiera de los países y el mapa del país reemplazará el del continente.

Figura 62: Atlas del mundo
Fuente: El Investigador

- **Widget de Búsqueda**

Para los suscriptores de Britannica: Los estudiantes y profesores pueden realizar búsquedas en el portal de Enciclopedia Moderna directamente desde el sitio web de su escuela o biblioteca con esta herramienta exclusiva. Los administradores de sitios web de su institución se pueden insertar este widget de búsqueda por copiando y pegando el código en sus sitios web.

<iframe
src="http://moderna.eb.com/sboxes/html/Moderna.html"frameborder=0
width=280 height=90 scrolling=no></iframe>

Figura 63: Widget
Fuente: El Investigador

B.2.4. Británica Escolar Online

- **Página Principal**

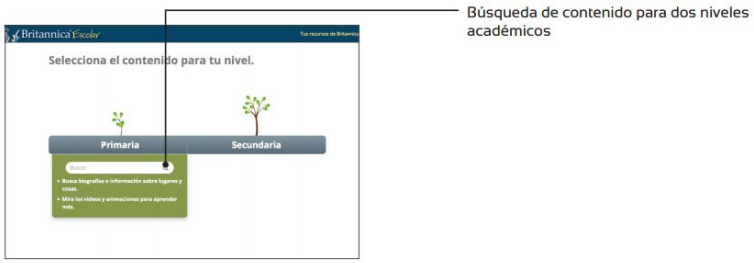

Figura 64: Menú Primaria o Secundaria de Británica Escolar
Fuente: El Investigador

- **Página Principal Primaria**

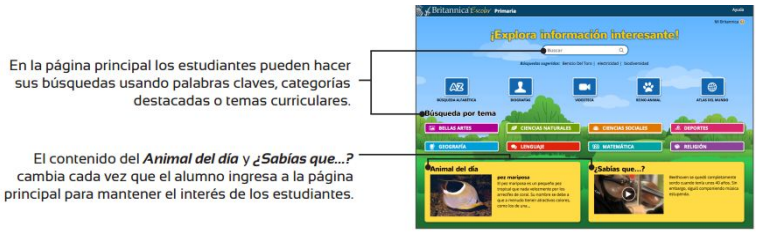

Figura 65: Página Principal Primaria
Fuente: El Investigador

- **Búsqueda Artículos Primaria**

Para empezar a usar el portal se utiliza el cuadro de búsqueda en la parte superior de cada página; además se puede realizar la búsqueda por orden alfabético, tema, biografía, grupo animal o su hábitat, o lista de videos educativos.

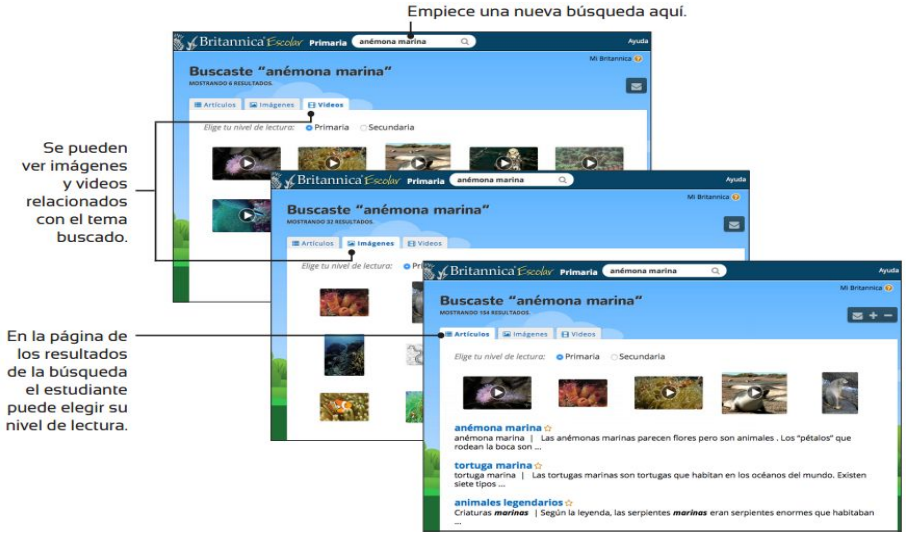

Figura 66: Búsqueda Artículos de Primaria
Fuente: El Investigador

- **Artículos Británica Escolar Primaria**

Británica Escolar Primaria cuenta con artículos que se destacan por su contenido informativo y por sus relevantes elementos multimedia

Figura 67: Artículo Escolar Primaria
Fuente: El Investigador

- **Búsqueda por Orden Alfabético Escolar Primaria**

Se puede buscar artículos por orden alfabético

Figura 68: Búsqueda por Orden Alfabético (Primaria)
Fuente: El Investigador

- **Búsqueda por Biografía Escolar Primaria**

Es posible hacer búsquedas de biografías por orden alfabético

Figura 69: Búsqueda por Biografía (Primaria)
Fuente: El Investigador

- **Atlas del mundo Escolar Primaria**

Es posible buscar información sobre los diferentes países del mundo usando el Atlas del mundo interactivo.

Figura 70: Atlas del mundo (Primaria)
Fuente: El Investigador

- **Videoteca Escolar Primaria**

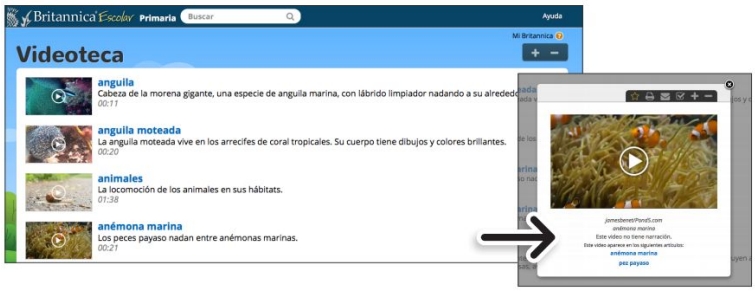

Figura 71: Videoteca Escolar Primaria
Fuente: El Investigador

- **Reino Animal Escolar Primaria**

Figura 72: Reino Animal Escolar Primaria
Fuente: El Investigador

- **Búsqueda Por Tema Escolar Primaria**

Hacer clic en el tema para ver una lista de artículos relacionados

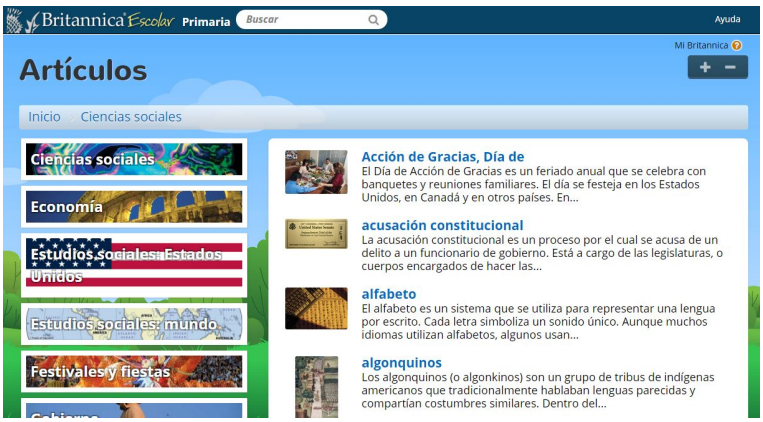

Figura 73: Búsqueda por Tema en Escolar Primaria
Fuente: El Investigador

- **Página Principal Secundaria**

Este nivel ofrece artículos de contenido más avanzado, además de imágenes, mapas, audio y videos para ayudar a los estudiantes a analizar y evaluar múltiples fuentes de evidencia.

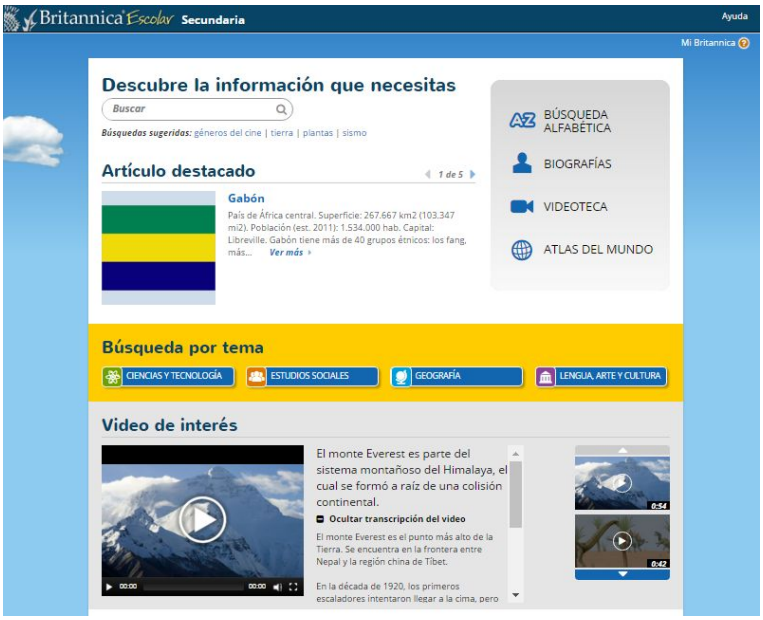

Figura 74: Página Principal Secundaria
Fuente: El Investigador

Para empezar a usar el nivel de secundaria del portal se utiliza el cuadro de búsqueda en la parte superior de la página; además es posible realizar la búsqueda por orden alfabético, tema, biografía o lista de videos educativos.

Figura 75: Búsqueda Escolar Secundaria
Fuente: El Investigador

Los artículos en este nivel son del contenido más avanzado y apoyan el aprendizaje de los estudiantes de secundaria.

Figura 76: Artículos Escolar Secundaria
Fuente: El Investigador

- **Búsqueda por Orden Alfabético y Biográfico Escolar Secundaria**

Figura 77: Búsqueda por Orden Alfabético y Biográfico Escolar Secundaria
Fuente: El Investigador

- **Videoteca Escolar Secundaria**

Figura 78: Videoteca Secundaria
Fuente: El Investigador

- **Atlas del Mundo Escolar Secundaria**

Figura 79: Atlas del Mundo Escolar Secundaria
Fuente: El Investigador

B.2.5. Colaboratorio Red Cedia

- **Comunidades**

Red Cedia impulsa la formación de comunidades de investigación regional y apoya el trabajo de aquellas ya establecidas. Para ello pone a disposición de científicos e investigadores de la región, y de forma gratuita, sus aplicaciones y servicios, todos desarrollados para potenciar la colaboración y el trabajo en red.
Red Cedia provee un ambiente virtual de colaboración de forma gratuita a todas las comunidades de investigación de América Latina, este ambiente es Colaboratorio, una plataforma web en la que cada comunidad integrante posee su propio espacio de interacción. Mediante las herramientas y servicios que se ofrecen dentro de Colaboratorio, usted podrá participar en las discusiones, foros y eventos de su comunidad y de todas aquellas que integre en Red Cedia, crear y participar conferencias web (VC Espresso), reservar salas multipunto para conferencias H.323, transferir archivos que pesen hasta 10GB (eNVIO), conocer y recibir avisos de fondos de financiamiento para la realización de proyectos y fortalecer su red de contactos y de socios profesionales [49].

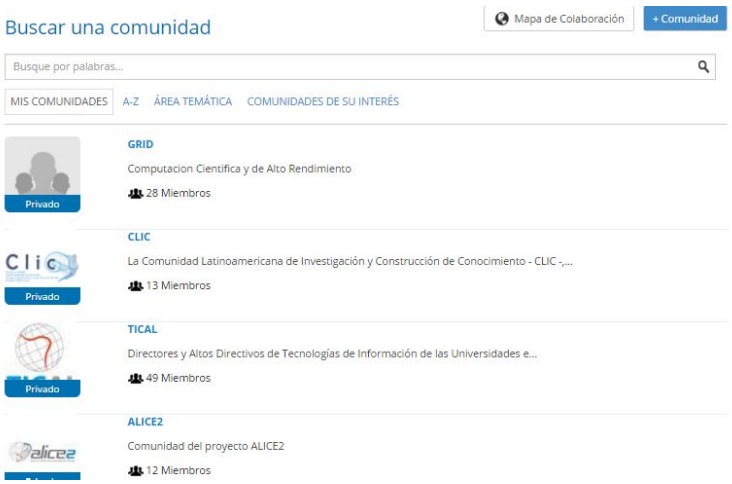

Figura 80: Comunidades Red Cedia
Fuente: El Investigador

- **Busco Socios**

Herramienta que permite buscar oportunidades de financiamiento para el desarrollo de proyectos de investigación e identificar, entre los usuarios del Colaboratorio, potenciales interesados en trabajar conjuntamente en las áreas de interés del usuario. Actualmente, el servicio es parte de la plataforma de colaboración de Red Cedia, Colaboratorio, y al desplegarse presenta tres elementos:

1. **Convocatorias-Fondos:** con información de los llamados a presentar proyectos hechos por diversas fuentes de financiamiento, cuyas fechas de vencimiento estén próximas. Usando las opciones disponibles el usuario puede ordenarlas alfabéticamente, desde las más recientes o las más antiguas. Además, si conoce una fuente de financiamiento que no aparezca entre las opciones, puede sugerir incroporar dicho fondo a la base de datos, enviando una URL y un mensaje al administrador.

2. **Busco Socios:** listado de posibles contactos, filtrados desde la base de datos de usuarios de Colaboratorio, de acuerdo a la información de perfil ingresada por los usuarios.

3. **Avisos:** publicaciones hechas por otros usuarios que buscan encontrar nuevos miembros para sus proyectos o que han anunciado su disponibilidad para sumarse a otras búsquedas ya existentes. El usuario, si lo desea, puede también publicar un aviso, especificando la disciplina, su país de procedencia, y dando una breve descripción de sus intereses

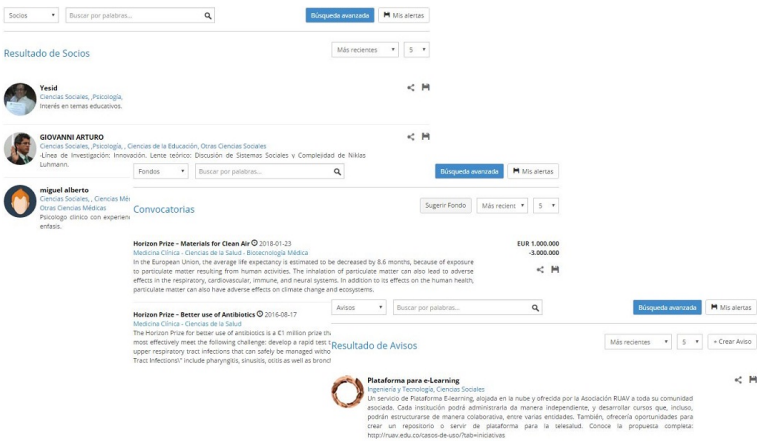

Figura 81: Busco Socios
Fuente: El Investigador

- **VC Espresso - Conferencia Web**

Servicio de videoconferencia web exclusivo para los miembros de las comunidades de Red Cedia. Con VC Espresso, usted podrá comunicarse en tiempo real, con imagen y sonido, y por el tiempo que desee, con los miembros de su comunidad de investigación. No importa si su reunión es con una sola persona o con 20, VC Espresso facilitará sus encuentros gracias a que pone sobre su navegador web de preferencia, la aplicación que le permitirá mantener contacto permanente con los integrantes de su comunidad, o bien, de otros grupos de investigación de América Latina.

VC Espresso le permitirá compartir con los asistentes a su reunión presentaciones PDF, PowerPoint e imágenes en los formatos frecuentemente utilizados. Adicionalmente, usted podrá mostrarles su escritorio con el fin de realizar demostraciones en vivo, gestionar el perfil de los asistentes, utilizar herramientas de toma de notas, pizarra colaborativa y chat. Todo de forma independiente de su sistema operativo, gracias a que es un cliente web que funciona con navegadores como Google Chrome, Mozilla Firefox e Internet Explorer en sus últimas versiones y sus correspondientes complementos Flash. Por último, si requiere un registro de su actividad, en VC Espresso usted siempre puede grabar en video sus sesiones [48].

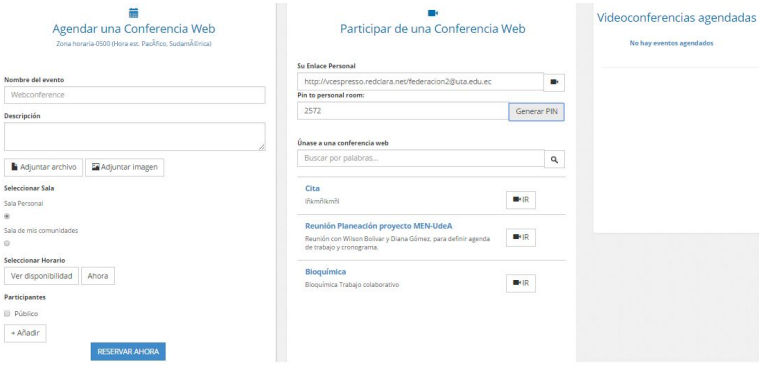

Figura 82: VC Espresso
Fuente: El Investigador

- **SIVIC - Agendamiento de Multiconferencia**

El sistema de reserva de salas de Videoconferencias H323 permite facilitar la búsqueda de salas habilitadas con unidades multipunto para este tipo de videoconferencias en Latinoamérica con el fin de maximizar recursos para la gestión del equipo de trabajo o la integración de la comunidad de investigación. SIVIC permitirá, en un mismo espacio, organizar videoconferencias en diversos países, permitiendo a todos los participantes reservar sus propias salas de videoconferencia en la región.

SIVIC posee el primer clúster colaborativo de soporte multiconferencia en Latinoamérica: cuatro países comparten aquí los puertos de sus soportes multiconferencia, garantizando una disponibilidad de hasta 50 puntos de conexión estándar simultánea y diez puntos de conexiones en alta definición.

SIVIC, está disponible las 24 horas al día, los 365 días del año, y permitirá a los usuarios de su institución realizar reservas de salas de videoconferencia certificadas para llevar a cabo sus reuniones y eventos en línea de mayor calidad. SIVIC garantiza la gestión efectiva de las reservas y el uso apropiado de las salas, según las políticas de uso de cada institución. A través de este sistema, los usuarios también pueden enviar invitaciones a terceros y hacer pública la actividad, ampliando la visibilidad de su evento [50].

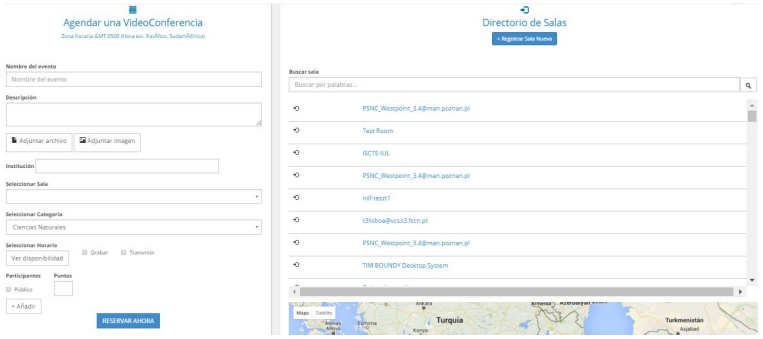

Figura 83: SIVIC
Fuente: El Investigador

- **eNVIO - FileSender**

El servicio eNVIO le permite a usted transferir archivos de gran tamaño, aquellos que, al adjuntarlos, superan la capacidad de envío de los sistemas de correo.
eNVIO trabaja cargando grandes cantidades de información a un servidor temporal de Red Cedia que entrega una dirección Web desde donde cualquier persona o grupo que usted decida, podrá descargar su material cuantas veces lo requiera.El servicio se encuentra disponible para la carga y transferencia de archivos por cualquier usuario registrado en Colaboratorio de Red Cedia.
Usted podrá enviar el enlace privado de descarga (link / URL – dirección Web) a un máximo de 100 correos electrónicos. El sistema soporta las extensiones zip, .rar, .doc, .xls, .pdf, .docx, .odt, .xlsx, .mov y un tamaño máximo de 10GB. Los archivos permanecerán albergados en el sistema por la cantidad de días que usted defina, hasta un límite máximo de 20; cumplido el plazo ellos serán eliminados automáticamente por el sistema, asegurando la privacidad y seguridad de la información [51].

Anexo C

Recursos Económicos

N°	DETALLE	UNIDAD	CANT.	V.U	TOTAL	PRESP
1	Uso de Internet	horas	1650	0,50	825,00	250,00
2	Impresiones B/N	c/u	500	0,05	25,00	10,00
3	Impresiones Color	c/u	100	0,10	10,00	3,00
4	Copias	c/u	100	0,02	2,00	1,00
5	Medios de almacena-miento	c/u	1	10,00	10,00	10,00
6	Computador portátil	c/u	1	12000,00	1200,00	1200,00
7	Carpetas	c/u	6	1,00	6,00	6,00
8	CPU ACER CORE i7	c/u	1	900,00	900,00	900,00
9	Desarrollador del Proyecto	horas	1280	17,80	22784,00	7565,00
				Subtotal	25762,00	9945,00
				I.V.A (12 %)	3091,44	1193,40
				TOTAL	28853,44	11138,40

Tabla 6: Cuadro de Costo Real Vs Presupuesto

Fuente: El Investigador

Anexo D

Cronograma de Actividades

N°	Nombre de la Tarea	Duración	Comienzo	Fin	Pred
1	Diseño de la entrevista no estructurada	4 días	mar 12/05/15	vie 15/05/15	
2	Aplicación de la entrevista no estructura al Administrador de Redes de la FISEI	2 días	lun 18/05/15	mar 19/05/15	1
3	Levantamiento de Diccionario de Datos	17 días	mié 20/05/15	jue 11/06/15	2
4	Estudio de las aplicaciones de identidad federada	8 días	vie 12/06/15	mar 23/06/15	
5	Elaboración de cuadro comparativo de las distintas aplicaciones para realizar identidad federada	11 días	mié 24/06/15	mié 08/07/15	4
6	Corrección de distintos puntos en marco teórico	3 días	jue 09/07/15	lun 13/07/15	
7	Instalación de las máquinas virtuales para el desarrollo de la propuesta	24 días	dom 12/07/15	jue 13/08/15	
8	Configuración Tomcat	6 días	jue 13/08/15	jue 20/08/15	7
9	Configuración Apache	5 días	vie 21/08/15	jue 27/08/15	8
10	Configuración puertos necesarios	5 días	vie 28/08/15	jue 03/09/15	9
11	Configuración de llaves certificadas	6 días	vie 04/09/15	vie 11/09/15	10
12	Instalación Shibboleth	14 días	sáb 12/09/15	jue 01/10/15	11
13	Configuración de ficheros shibboleth	8 días	jue 01/10/15	lun 12/10/15	12

Tabla 7: Cronograma de Actividades

Fuente: El Investigador

N°	Nombre de la Tarea	Duración	Comienzo	Fin	Pred
14	Instalación OpenLDAP	9 días	lun 12/10/15	jue 22/10/15	12
15	Configuración OpenLDAP	10 días	vie 23/10/15	jue 05/11/15	7
16	Instalación phpLDAPadmin	4 días	vie 06/11/15	mié 11/11/15	14
17	Instalación Windows Server 2012	22 días	jue 12/11/15	vie 11/12/15	15
18	Creación de active directory en Windows server 2012	15 días	sáb 12/12/15	vie 01/01/16	7
19	Creación de dominio en WS 2012	7 días	vie 01/01/16	lun 11/01/16	17
20	Creación de usuario en Windows server 2012	11 días	mar 12/01/16	mar 26/01/16	18
21	Corrección de varios puntos en el documento del proyecto de investigación	12 días	mié 27/01/16	jue 11/02/16	19
22	Clonación de máquina virtual ubuntu 10.04	5 días	vie 12/02/16	jue 18/02/16	6
23	Configuración del SP	7 días	vie 19/02/16	lun 29/02/16	7
24	Creación de manual de usuario (Anexo B) de los recursos que posee el Sistema Federado	9 días	mar 01/03/16	vie 11/03/16	22
25	Configuración archivos Services Provider	22 días	sáb 12/03/16	mar 12/04/16	
26	Correcciones de conclusiones y recomendaciones del Proyecto de investigación.	10 días	mar 12/04/16	lun 25/04/16	23
TOTAL DE DÍAS		256 días			

Tabla 8: Cronograma de Actividades

Fuente: El Investigador