Séptima Conferencia de Directores de Tecnología de Información, TICAL 2017 Gestión de las TICs para la Investigación y la Colaboración, San José, del XX al XX de julio de 2017

Plataforma de Gestión de Identidad y Acceso Federado para la Universidad de Cuenca

Ma. José Torres [bc], Andrés de los Reyes [c],
Luis Espinoza [c], Victor Saquicela [a]

[a] Departamento de Ciencias de la Computación, Universidad de Cuenca,
Av. 12 de Abril y Av. Loja, 010112
Cuenca, Ecuador.

[b] Facultad de Ingeniería, Universidad de Cuenca,
Av. 12 de Abril y Av. Loja, 010112
Cuenca, Ecuador.

[c] Dirección de Tecnologías de Información y Comunicación, Universidad de Cuenca,
Av. 12 de Abril y Av. Loja, 010112
Cuenca, Ecuador.

mariajose.torres@ucuenca.edu.ec
andres.delosreyes@ucuenca.edu.ec
luis.espinoza@ucuenca.edu.ec
victor.saquicela@ucuenca.edu.ec

Resumen. Con el crecimiento del portafolio de servicios de Tecnologías de Información y Comunicación ofrecidos a la comunidad universitaria, el sistema de autenticación basado en usuario y contraseña para cada sistema va quedando obsoleto, debido principalmente a la inconsistencia de los datos de usuario que se almacenan en los diferentes repositorios. Tras definir el problema que afecta la prestación de este servicio, se propone como solución la construcción de una plataforma de gestión de identidad y acceso federado (***IAA***) basada en la recomendación de la iniciativa ***Trust and Identity in Education and Research*** de ***Internet2***. La validez de la arquitectura propuesta se estableció a través de varias pruebas de concepto que contemplan la configuración de los componentes de la plataforma en un ambiente controlado, pero considerando pruebas de aplicación real con aplicaciones desarrolladas en casa, así como con sistemas de código abierto como ***Moodle*** y ***uPortal***.

Palabras Clave: federación de identidad, single sign on, autenticación única, Shibboleth, uPortal, doble factor de autenticación, Moodle federado, Grouper, VOOT, SSO

Eje temático: Seguridad de la información

1 Introducción

Los sistemas de información y comunicación en la Universidad de Cuenca - Ecuador facilitaron la ejecución de las tareas administrativas implementados en la segunda mitad de la década de los años 90. Para ese entonces, la naciente seguridad

informática sugería la utilización de un sistema de autenticación basado en contraseñas en el que el usuario (probador) solicita el acceso a un sistema de información (verificador); en caso de coincidir las palabras ingresadas, el sistema permite al usuario acceda a diferentes recursos. Este sistema de autenticación, va quedando obsoleto debido a que el portafolio de servicios crece y genera incidencias al tener que usar contraseñas distintas para acceder a cada sistema; por lo que los usuarios se ven obligados a preocuparse de mantener sus credenciales en apuntes de fácil acceso que causan un riesgo potencial de autenticación indebida. También, es necesario mencionar que los sistemas utilizados por la comunidad universitaria se pueden clasificar en tres categorías. La primera, agrupa a sistemas que solo pueden ser utilizados dentro de la red de la institución; como son las Bases de Datos Digitales suscritas por la Universidad de Cuenca. Para acceder a este servicio se utiliza la autenticación basada en EzProxy[1]. Un segundo grupo, está constituido por sistemas que sólo puede ser utilizados por usuarios específicos. En este caso, la gestión de roles y perfiles ha sido delegada al administrador del sistema, que realiza una configuración manual para conceder los permisos requeridos puesto que la configuración está almacenada en la base de datos de cada sistema. Finalmente, el portafolio de servicios incluye sistemas provistos por terceros que son de utilidad para la institución, como es el caso de G Suite de Google, a los que se debe aprovisionar las credenciales de autenticación cada vez que se da un mantenimiento de usuarios.

Por otra parte, es necesario mencionar que la Universidad de Cuenca cuenta con más de 40000 cuentas de usuario distribuidos en dos dominios de autenticación: ucuenca.edu.ec y ucuenca.ec. En el primero, se alojan las cuentas del personal docente, de investigación y administrativo; mientras que en el dominio ucuenca.ec están alojadas las cuentas de los estudiantes.

Inicialmente, se consideró juntar los usuarios de los dos dominios en uno sólo -ucuenca.edu.ec-, con el fin de optimizar los esfuerzos y recursos para mantener las credenciales de acceso e implementar el servicio de autenticación única. Para lograr este propósito, se realizó un análisis de los datos obtenidos de las fuentes de autenticación mencionadas en la Fig. 1, de donde se encontró inconvenientes como la existencia de nombres de usuario repetidos entre los dominios de autenticación; es decir, que el mismo nombre de usuario ***UID*** corresponde a dos personas diferentes. También se detectó que se tienen personas repetidas: una misma persona tiene más de una cuenta de usuario, ya sea en el mismo dominio, o una en cada dominio. A lo que se agrega el desconocimiento del número de usuarios que deben estar activos en las fuentes de autenticación: primero porque no se cuenta con una política institucional de gestión de usuarios, y luego porque el número de usuarios registrados en las fuentes de autenticación difiere notablemente. Existen reportes de incidencias en la Mesa de Soporte de TI que muestran credenciales inconsistentes por la utilización de caracteres especiales como ñ, vocales tildadas, o caracteres codificados en los ***UID***, lo que ocasiona que al crear cuentas en los servicios de ***G Suite*** se genere una excepción y no se cree la cuenta, o no se pueda modificar sus datos personales.

---

[1] EZproxy es un servidor proxy web utilizado por bibliotecas para dar acceso desde el exterior de la red informática de la biblioteca, a un sitio web de acceso restringido que auténtica los usuarios por dirección IP (Online Computer Library Center, Inc.)

Desde el punto de vista de acceso y autorización, se debe mencionar que cada sistema gestiona sus credenciales y concede acceso a los recursos de acuerdo a la información de una o más tablas de su base de datos. Esta configuración genera inconvenientes al momento de generar nuevos roles o perfiles porque no se cuenta con un proceso de autenticación, autorización y acceso único. De aquí surge la necesidad de implementar un mecanismo que permita gestionar la identidad de los usuarios de la comunidad universitaria de manera centralizada y automática a través de la dotación de un Servicio de Gestión de Identidad y Acceso federado a la Universidad de Cuenca que permita acceder a los servicios informáticos institucionales y otros servicios federados suscritos.

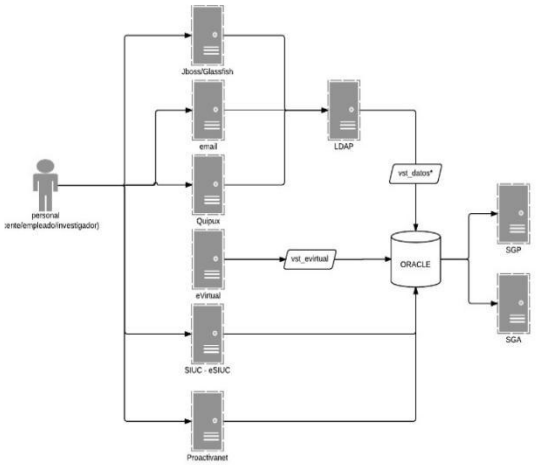

Fig. 1: Arquitectura utilizada para la autenticación de usuarios en los diferentes servicios provistos por la DTIC para la Universidad de Cuenca.

2 Antecedentes y Trabajos Relacionados

La Red de Investigación y Educación de América -***Internet2***- define a la gestión de Identidades (***IdM***) así: *"...sistema integrado de procesos, políticas y tecnologías que permiten a las organizaciones facilitar y controlar el acceso de los usuarios a sus recursos y aplicaciones, permitiendo a la vez proteger su información confidencial, tanto personal como profesional, de usuarios no autorizados*...". Adicionalmente, (Suess J., 2009) postula que para que un sistema de gestión de identidad y acceso sea exitoso se debe tener una concepción holística sobre las entidades y las interdependencias que existen entre ellos. Tal ambiente requiere que tres aspectos estén en su lugar para una protección y confianza adecuadas:

- Identificación: Asegurar que las credenciales electrónicas para el acceso a un sistema se concedan sólo a la persona correcta.
- Autenticación: Comprobar la validez de estas credenciales en el momento del acceso.
- Autorización: Determinar que a la persona así identificada se le ha otorgado la autoridad para realizar las acciones solicitadas.

Como complemento a este concepto, las redes académicas han adoptado la noción de una federación de identidades con el afán de apoyar la movilidad académica y el uso de servicios. Una federación es un grupo o conjunto de entidades que comparten la tecnología, estándares y casos de uso que permiten transmitir información de identidad de un usuario de manera segura facilitando la identificación, autenticación y autorización entre diferentes dominios. En una federación de identidades se establece un círculo de confianza que permite que un usuario (sujeto) autenticado en un organismo de la federación acceda a recursos (objeto) de otro organismo de la misma federación. La identificación se realiza en los Proveedores de Identidad (***IdP***). El Proveedor de Servicio (***SP***) al que accede el usuario confía en los datos del usuario que le son suministrados por el ***IdP*** y en función de los mismos autoriza al usuario a hacer uso de los recursos. Además, para que esta arquitectura sea efectiva es necesario definir una tabla de capacidades que tiene un determinado sujeto a los diferentes recursos protegidos por un sistema.

Para promover estas ideas, ***Internet2*** mantiene el programa ***Trust and Identity*** en Educación e Investigación ***TIER*** (Internet2, 2017) que ofrece recomendaciones y un paquete de componentes para gestionar la identidad y el acceso federado en entornos universitarios abarcando los aspectos fundamentales de la federación de identidades. Para la capa de identificación y autorización recomienda utilizar ***Shibboleth*** (Jisc Services Limited, 2017) que es un proyecto de código abierto que proporciona capacidades de inicio de sesión único y permite a los sitios tomar decisiones de autorización informadas para el acceso individual de recursos protegidos de manera que preserven la privacidad. Para la gestión de capacidades o acceso, se ha trabajado en el proyecto ***Grouper*** (Internet2, 2016) que maneja grupos y administra acceso a través de aplicaciones y rastrea información como afiliaciones o roles en el campus. ***COmanage*** (Internet2, 2016) es una plataforma que permite a los grupos de colaboración agilizar y gestionar los requisitos de las herramientas comunes de colaboración a los que tienen acceso. Los esquemas ***eduPerson*** y ***eduOrg*** (Internet2, 2016) diseñados para incluir atributos de persona y organización utilizados comúnmente en la educación superior y así facilitar el intercambio de información entre federaciones. ***MACE Registres*** (Internet2, 2016) para la identificación de esquemas de atributos de usuario personalizados para las instituciones que deseen implementarlo. ***Multifactor Authentication*** (Internet2, 2016) complementa la identificación tradicional al solicitar adicionalmente un código ***-token-*** generado aleatoriamente en un dispositivo móvil o en el navegador del usuario.

La adopción de este modelo, depende de la generación de una estructura de datos estandarizada para brindar interoperabilidad. Así, cada sistema o aplicación posee la misma infraestructura de identidad y acceso, con lo que se simplifica notablemente su administración y mantenimiento.

2.1 Trabajos Relacionados

La implementación de federación de identidades está bien documentada en el sitio REFEDS (REFEDS, 2017). En América existen seis federaciones registradas: CAFe Federation (Brasil), CAF Federation (Canadá), COFRe Federation (Chile), RENATA Federation (Colombia), MINGA (Ecuador), InCommon Federation (Estados Unidos), siendo esta última la más grande con 2356 ***IdP*** y 6969 entidades registradas. A través de este visor de metadatos, se conoce que varias organizaciones han implementado ***Shibboleth*** para la gestión de la identidad y autenticación, pero se desconoce los mecanismos de control que se utilizan para gestionar la autorización y acceso a los recursos protegidos de los servicios de TI. Para citar casos de éxito basados en la propuesta ***IAA***, la documentación de ***Internet2*** indica que en Estados Unidos se ha difundido ampliamente la implementación de ***Grouper, EduPerson o EduOrg*** para la construcción de plataformas ***IAA*** (Internet2, 2017) **.** En lo relacionado al Ecuador, la documentación oficial de ***CEDIA*** (CEDIA - Red Nacional de Investigación y Educación del Ecuador, 2017), no detalla la implementación de una plataforma de gestión de identidad; pero, si se conoce de la implementación local de ***Shibboleth*** como en el caso de la Universidad Técnica Particular de Loja. Es así, que la Universidad de Cuenca es pionera en la implementación de una plataforma ***IAA*** para integrarla a sus sistemas de información y al esquema de federación de identidades a través de ***MiNGA*** (CEDIA - Red Nacional de Investigación y Educación del Ecuador, 2017)**.** Además, una vez puesto en producción el ***IdP*** en la Universidad de Cuenca, y tras ajustarlo a las normas de ***MiNGA*** se pudo establecer la relación de confianza con la federación europea ***Gèant*** para el dominio ucuenca.edu.ec, siendo los primeros en lograr independencia en la provisión de identidad para los usuarios con otras federaciones.

Este documento se detalla la experiencia obtenida en la ejecución del proyecto para la dotación de una plataforma de gestión de identidad y acceso federado, y está organizado de la siguiente manera: en el apartado 3 se describe el estado del arte propuesto por la asociación ***Internet2,*** quienes proponen el uso de un conjunto de herramientas complementarias que abordan los tres aspectos requeridos para que la gestión de identidades sea exitosa. En el apartado 4, se describen las pruebas de concepto realizadas con cada herramienta, como se integraron entre ellas y como se integrarán con los sistemas de información realizados en casa.

3 Arquitectura para la Gestión de Identidades y Acceso Federado

Entre sus objetivos estratégicos, la Dirección de Tecnologías de Información y Comunicación de la Universidad de Cuenca (***DTIC)*** se ha planteado la creación de una arquitectura orientada a servicios para cumplir con la demanda de sistemas de información impuestas por el modelo de negocio de la Universidad de Cuenca. Por esta razón, es necesario contar con una plataforma de soporte para la gestión de identidad y acceso federado robusta, segura e interoperable que permita gestionar el acceso a los recursos informáticos. Además, deberá fortalecer la seguridad

informática, apegada a las recomendaciones dadas por ***MiNGA*** para fomentar la colaboración interinstitucional.

Para definir el alcance de la intervención, fue necesario plantear el escenario en el que se trabajará. Esto se realizó a través de dos acciones iniciales: la primera es consolidar la identidad de los miembros de la comunidad universitaria en una sola base de datos; la segunda es definir la granularidad para el control de acceso al que se pretende llegar con los sistemas que se implementen a futuro. Entonces, se establece la ruta que se debe seguir a través de la implantación conjunta de los siguientes proyectos:

- Implementar un sistema de aprovisionamiento que permita alimentar el Directorio Institucional y que refleje una política institucional para la gestión de identidad y control de acceso.
- Implementar ***Shibboleth*** para la gestión de autenticación lo que contempla el proceso de pruebas y contingencia del servicio.
- Implementar ***Grouper*** para la gestión de roles en base a la estructura institucional.
- Implementar ***uPortal*** para la publicación de micro servicios que doten de recursos a los usuarios en virtud de su rol.

Estos proyectos abarcan los diferentes componentes que integran una solución de gestión de identidad, autenticación y autorización. En la Fig. 2, se ilustra la forma en la cual los componentes interactúan entre sí para dar como resultado una arquitectura integrada, robusta y confiable. Es necesario mencionar que la alta disponibilidad de la plataforma estará gestionada por un sistema de replicación del centro de datos.

La arquitectura propuesta está conformada por cinco macro componentes, agrupados en dos eventos. En el evento ***Aprovisionamiento***, se define el sistema de aprovisionamiento de usuarios (1) que alimentará según sea necesario el Directorio Institucional (2) y al sistema de gestión de roles y accesos Grouper (3). Por otro lado, el evento ***Identificación, Autenticación y Autorización***, que se desencadenará cada vez que un usuario solicite acceso a una aplicación a través de un navegador de internet, evento que consumirá la información definida en (2) y (3) a través ***Shibboleth*** para conceder el acceso a los recursos en ***uPortal*** u otra aplicación según corresponda.

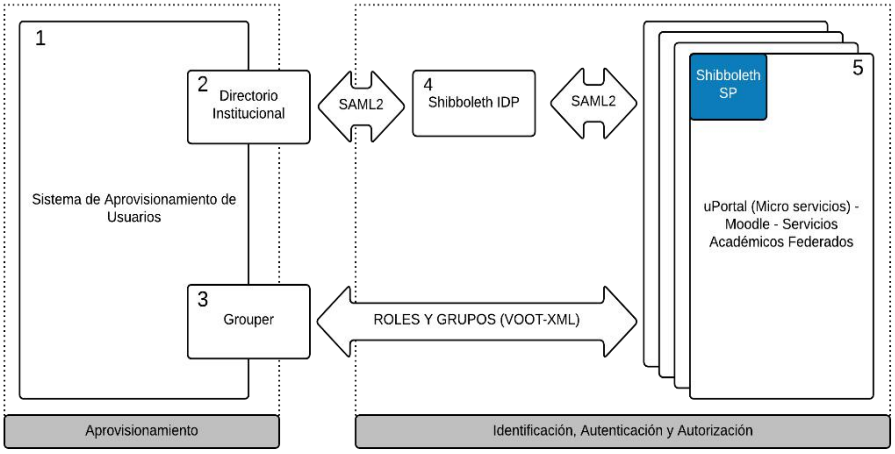

Fig. 2 Arquitectura propuesta para la plataforma de gestión de identidad y acceso federado para la Universidad de Cuenca.

La construcción de la plataforma ***IAA*** comienza por establecer la información requerida para alimentar el directorio institucional. La recomendación de ***Internet2*** para la interoperabilidad, incluye los esquemas comunes ***Person, OrgPerson, inetOrgPerson*** que vienen por defecto en una instalación ***LDAP***. Sobre estos, estarán los esquemas ***eduPerson*** donde se definen los atributos federados. El esquema ***Schac***, promocionado por la comunidad europea ***TERENA***, incluye otros atributos para el intercambio de datos interinstitucionales (REFEDS, 2016). Sobre estos se presentan los esquemas nacionales, que para el caso de Ecuador no están definidos.

Luego, es necesario levantar cada componente por separado, modelar el comportamiento esperado para finalmente integrarlo y verificar si la funcionalidad obtenida es la esperada.

4 Pruebas de Concepto

La validez de la arquitectura propuesta se estableció a través de varias pruebas de concepto –***PoCx.x***- que contemplan la configuración de los componentes de la plataforma en un ambiente controlado, pero considerando pruebas de aplicación real. La configuración de una ***PoC*** implicó investigación y revisión extensa de las funcionalidades de cada uno de los componentes involucrados en los eventos de la plataforma ***IAA***; incluyendo el examen del modelo de datos y el control de los eventos internos requeridos para viabilizar el comportamiento esperado.

La primera, ***PoC1.0***, o prueba de concepto base, consistió en la configuración de dos fuentes de autenticación: ***OpenLDAP*** y ***AD*** en Shibboleth IdP. Para cada caso, es necesario ajustar las plantillas de autenticación debido a que los ***OID*** de los atributos liberados no son iguales. Para ajustar la plataforma a los esquemas recomendados por ***TIER*** (Internet2, 2017), se mapean los atributos en el ***IDP*** entre el esquema utilizado

en el ***AD*** y el esquema ***eduPerson*** por la facilidad de implementación al no requerir modificación del sistema de aprovisionamiento de usuarios.

3.1 Prueba de Concepto Inicial –*PoC1.1*-

La ***PoC1.1*** validó la configuración de ***Shibboleth SP*** en dos servidores de aplicaciones web: ***Apache*** y ***Tomcat*** sobre Linux. En ambos casos, su configuración implica la aceptación de la metadata del ***SP*** para la configuración de "***Relying Party***" en el ***IdP***. De esta manera se pudo determinar que ***Tomcat*** no soporta nativamente la instalación de un ***SP***, por lo que, para capturar los atributos liberados por el ***IdP*** tras la autenticación, es necesario instalar un proxy sobre Apache. Este módulo adicional, se encargará de capturar las peticiones dirigidas al recurso protegido, interactuar con el ***IdP*** para obtener los atributos liberados para el ***SP***, y pasarlos hacia ***Tomcat***; desde aquí dependerá de la aplicación.

3.2 Prueba de Concepto de Doble Factor de Autenticación –*PoC1.2*-

El fortalecimiento de la seguridad y confidencialidad se puede lograr a través de la implementación de un sistema de doble autenticación que complementa la autenticación tradicional en los servicios de TI. En otras palabras, además de requerir un nombre de usuario y contraseña, solicita el ingreso de un segundo factor de autenticación, como puede ser un código de seguridad. Generalmente, este código se genera en un dispositivo del usuario que luego debe ingresarlo para validar su identidad en el sistema. Para la ***PoC1.0*** se integró ***Shibboleth-IdP3TOTP-Auth*** (Korteke, 2017) en el ***IdP***. Este es paquete permite modificar el flujo de usuario - contraseña, al solicitar un código generado por una aplicación móvil o el complemento de ***Google Chrome*** para ***Google Authenticator***. La primera vez que el usuario accede al servicio, le solicita la creación de la semilla del código en su ***Google Authenticator***. Al leer el código ***QR***, se genera el enlace requerido para las siguientes solicitudes de acceso. En el tercer paso, luego de que el ***IdP*** valide la identidad del usuario, se notifica la entrega de los atributos listados al ***SP***. El usuario deberá aceptar este paso, para ser promocionado al recurso protegido.

3.3 Prueba de Concepto con Moodle –*PoC1.3*-

Una vez construida la plataforma, fue necesario validar la funcionalidad con uno de los servicios que ofrece la ***DTIC***: el entorno virtual de aprendizaje basado en ***Moodle LMS***. El proyecto de mejoramiento del entorno virtual, entre otros objetivos, trata de integrarlo con el sistema de gestión académica para recuperar la información de usuarios (docentes o estudiantes), cursos, carreras y contenidos de las asignaturas con el objetivo de integrar los servicios de TI y brindar una mejor experiencia a los usuarios de la comunidad universitaria. Para esto se han analizado dos métodos: El primero a través del aprovisionamiento utilizando los servicios web provistos por

Moodle, y el segundo a través del plugin para enrolamiento utilizando el protocolo ***VOOT***[2] (GEANT, 2017).

En la ***PoC1.3,*** el servidor web utilizado es un ***Apache***, que pasa a través de un Proxy con balanceo de carga, lo que requiere una configuración adicional en el ***SP.*** Para el evento ***Aprovisionamiento,*** se preparó la plataforma ***Moodle*** para el mantenimiento de cursos, docentes y estudiantes a través del plugin ***VOOT.*** Esta configuración requiere que en ***Grouper***, se creen carpetas (que representan los cursos y carreras), sus miembros y permisos. Sin embargo, es importante notar que ***Moodle*** necesita conocer a los usuarios antes de aprovisionar los cursos, por lo que los usuarios deben pasar por el evento de ***IAA*** a menos una vez o se presentará el error "usuario desconocido." [3]. Este evento es gestionado por ***Shibboleth,*** que reportará los atributos requeridos por el ***SP***. El ***plugin*** de autenticación deberá configurarse de tal manera que mapee los atributos recibidos desde el ***IdP*** con los campos de usuario definidos en su base de datos. Una vez finalizado este evento, se presenta el espacio personal del usuario en la plataforma virtual, con los cursos en donde se ha enrolado y los datos personales mapeados en la base de datos local.[4]

3.4 Prueba de Concepto con uPortal –*PoC1.4*-

La nueva arquitectura de sistemas de información está basada en el desarrollo de microservicios. Se espera que, a mediano plazo, se pueda desplegar un portal único de acceso a Servicios de TI. De esta manera, los usuarios podrán recordar una única dirección URL, en la que luego de autenticarse les presentará los servicios a los cuales tienen permisos de acceso. Las aplicaciones basadas en microservicios publicados en el portal permiten a los usuarios acceder a un conjunto de recursos protegidos en virtud de su rol. Entre otras, los usuarios acceden a la visualización de información básica personal, la visualización de información corporativa de seguridad o los mecanismos de cambio de contraseña, tanto propias como de cuentas genéricas de las que el usuario es responsable. Para probar este concepto se preparó el ***PoC1.3***, donde se integra la plataforma ***IAA***, con el proyecto ***uPortal*** desarrollado por la comunidad Apereo (Apereo, 2017).

Para la ***PoC1.4,*** se utiliza un servidor ***Tomcat*** detrás de un proxy sobre ***Apache***. La configuración interna de ***uPortal***, permite capturar los atributos liberados por el ***IdP*** y así gestionar la identidad del usuario en el contexto de la aplicación.

3.5 Prueba de Concepto con aplicaciones basadas en microservicios –*PoC1.5*-

---

[2] ***VOOT*** es un protocolo para intercambiar información de grupos a aplicaciones, definidas dentro de ***GN3-JRA3-T2*** (Tarea de Federaciones de Identidad) de la comunidad europea ***Gèant***. El ***plugin*** desarrollado para Grouper implementa la versión 0.9 del protocolo ***VOOT.***

[3] Mayor información sobre el procedimiento para realizar esta configuración la encontrará en (GEANT, 2017)

[4] Luego de cada IAA exitosa, los atributos de usuarios serán actualizados.

En la ***PoC1.5*** se evalúa la factibilidad de integración de la herramienta ***Grouper*** con aplicaciones desarrolladas en casa. Primero, se plantea la posibilidad de delegar la administración de grupos a diferentes usuarios con el objetivo de descentralizar el control de roles y así agilizar el trabajo de las diferentes unidades de la Universidad. Adicional a la configuración realizada en la ***PoC1.3***, se considera utilizar a ***Grouper*** para gestionar los roles de los usuarios y el acceso a los recursos protegidos en las aplicaciones que se están desarrollando. Dado que se han definido una gran cantidad de grupos, se desarrolló un servicio web en ***JAVA*** que filtre los grupos que de interés y les exponga como un objeto ***JSON*** a los aplicativos. Este servicio no recibe como parámetro el usuario, pues al superar el evento ***IAA*** obtiene este dato de las cabeceras ***HTML***, luego consume los servicios web de ***Grouper***, filtra y formatea la información. Como resultado se tiene una interfaz gestionada en base al rol del usuario.

Conclusiones y Trabajos Futuros

La utilización de herramientas de código abierto y acceso gratuito permiten que las instituciones cubran necesidades similares con menor esfuerzo, ya que el trabajo de sus grupos de desarrollo se enfocará en la integración de herramientas de software con sus necesidades. Es así que en este caso, la adopción de las recomendaciones propuestas por la iniciativa ***TIER*** permite que la Universidad de Cuenca cuente con una plataforma robusta para la gestión de identidad y acceso federado evitado el esfuerzo de un desarrollo en casa, pero siempre apegado a la innovación.

Otro factor de éxito en este proyecto fue la adquisición de destrezas por parte de los técnicos involucrados. En fase experimental, fue posible jugar con los diferentes parámetros que ofrecen las herramientas para su implementación e integración fomentando el aprendizaje por ensayo y error; de tal manera, que los técnicos involucrados en el proyecto han adquirido destrezas tanto para la administración de la plataforma construida como para definir propuestas de trabajo que amplíen su alcance inicial planteado, y además la personalización del código.

Por otro lado, si bien las pruebas de concepto descritas en este documento están aún en una fase beta de producción, en cada integración requerida por el equipo de desarrolo se van afinando los detalles de funcionalidad esperada de tal manera que puedan ser puestos en producción sin mayor complicación, y así completar el conjunto de herramientas necesarias ***IAA.***

Finalmente, quedan pendientes por desarrollar proyectos como la adopción de ***CoManage*** y la estandarización del Directorio Activo con los esquemas ***eduPerson***, ***Schac*** y la construcción del portal de usuario sobre ***uPortal*** las aplicaciones basadas en microservicios.

También, una vez que la federación ***Gèant*** ha reconocido el ***IdP*** de la Universidad de Cuenca, es posible suscribir acuerdos con servicios de red avanzada internacionales que favorezcan a la docencia e investigación de nuestra comunidad universitaria, y así fortalecer el concepto de federación de identidades que busca este proyecto entre sus objetivos.

Agradecimientos

Este trabajo es parte del Plan Operativo 2017 de la Dirección de Tecnologías de Información de la Universidad de Cuenca, y ha sido apoyado por la investigación realizada para la tesis "Diseño de Procesos Estrategia de Estrategia de Servicios" que actualmente está en desarrollo.

Referencias

Apereo. (2017). *uPortal Documentation*. Obtenido de https://www.apereo.org/projects/uportal/uportal-documentation

GEANT. (2017). *Cross Domain Group Information Exchange.* Obtenido de https://wiki.geant.org/display/gn3pjra3/VOOT+-+Cross+Domain+Groupinformation+Exchange

GEANT. (2017). *How to integrate Moodle with Grouper.* Obtenido de https://wiki.geant.org/download/attachments/24215762/HOWTO%20Integrate%20Moodle%20with%20Grouper%20on%20Ubuntu%20Linux%2012.04.pdf?version=2&modificationDate=1416492228317&api=v2

Internet2. (08 de 2016). *Comanage*. Obtenido de http://www.internet2.edu/products-services/trust-identity/comanage/

Internet2. (2016). *EduPerson & EduOrg.* Obtenido de http://www.internet2.edu/products-services/trust-identity/eduperson-eduorg/

Internet2. (21 de 12 de 2016). *Grouper Wiki Home*. Obtenido de https://spaces.internet2.edu/display/Grouper/Grouper+Wiki+Home

Internet2. (2016). *INCOMMON MULTIFACTOR AUTHENTICATION.* Obtenido de http://www.internet2.edu/products-services/trust-identity/incommon-multifactor-authentication/

Internet2. (2016). *Mace Registries*. Obtenido de http://www.internet2.edu/products-services/trust-identity/mace-registries/

Internet2. (13 de 03 de 2017). *Trust and Identity in Education and Research.* Obtenido de http://www.internet2.edu/vision-initiatives/initiatives/trust-identity-education-research/

Internet2. (2017). *Use Cases by Category.* Obtenido de https://spaces.internet2.edu/display/Grouper/Use+Cases+by+Category

Jisc Services Limited. (2017). *Shibboleth*. Obtenido de https://shibboleth.net/about/basic.html

Korteke. (2017). *Korteke Shibboleth Totp Auth complement*. Obtenido de https://github.com/korteke/ShibbolethIdP3-TOTP-Auth

Online Computer Library Center, Inc. (s.f.). *http://www.oclc.org/en/ezproxy/features.html.* Recuperado el 03 de 2017

Red Nacional de Investigación y Educación del Ecuador. (13 de 03 de 2017). *cedia.org.ec*. Obtenido de https://www.cedia.org.ec/minga

REFEDS. (2016). *REFEDS SCHAC - SCHema for ACademia* . Obtenido de https://wiki.refeds.org/display/STAN/SCHAC+Releases

REFEDS. (2017). *REFEDS - Research and Education FEDerations group.* Obtenido de https://met.refeds.org

Suess J., M. K. (2009). IAM. *Identity Management and Trust Services: Foundations for Cloud Computing, 44*, 5.

Switch - AAI. (2017). *Switch AAI Interfederation International Attributes*. Obtenido de https://www.switch.ch/aai/docs/interfederation/international-attributes.html?homeOrg=ucuenca.edu.ec&homeOrgType=university#setupForm