Proyecto miUNQ: Implementación de una plataforma de Autenticación Centralizada para la utilización de servicios y aplicaciones de la UNQ

Alejandro Del Brocco, Nicolas Samus, Gabriel Guntin, Sergio Loyola, Gustavo Pilla, Hernan Slavich y Mariano Alvarez

Dirección de Servicios de Comunicación, Universidad Nacional de Quilmes, Buenos Aires, Argentina
alejandro@unq.edu.ar, dsi_dsr@listas.unq.edu.ar

Resumen. Este artículo servirá para presentar el proyecto miUNQ el cual pretende brindar una interfaz que sirve de contexto para que los usuarios de la Universidad puedan acceder a todos los servicios y aplicaciones mediante un único usuario y una única clave. Se explicarán todas las tareas previas de consolidación de la información, el modelo de implementación elegido, los procesos administrativos asociados y las estrategias de publicación utilizadas. Se presentará el entorno de trabajo que da contexto a la implementación y cómo se han utilizado distintos atributos de las identidades de cada persona para consumir información de los sistemas y presentarlos de una forma cómoda y amigable. Se describirán las experiencias de interacción con otras instituciones y la adopción del estándar OASIS SAML 2.0 para el desarrollo de la plataforma. Finalmente se dará un panorama del futuro de la implementación.

Palabras Clave: Single Sign On, SAML, CAS, Shibboleth, Interoperabilidad, Seguridad, Mellon, SIU, REST, SOAP.

1 Formulación del proyecto

La Universidad Nacional de Quilmes es una Universidad joven fundada en el año 1989. No obstante tiene una gran comunidad de usuarios definidos por 1200 docentes y 500 PAS (Personal administrativo y de servicios). A la vez, cuenta con más de 40 servicios y/o sistemas que les permiten el desarrollo de sus actividades diarias. En el año 2013 el Vicerrector de la Institución nos encomendó la tarea de facilitar los accesos a los distintos sistemas debido a que en cada uno de ellos la misma persona respondía a distintos usuarios. A modo de ejemplo, existía el usuario juan perez, el usuario jperez, el usuario juan.perez, etc. Entonces el desafío consistía en dejar de administrar usuarios para administrar identidades pero para ello era necesario definir una fuente de verdad exclusiva de la que se pudiera partir para anexar las atribuciones y habilidades correspondientes a cada persona. Sin embargo, entendimos que era

conveniente ampliar el alcance del proyecto para brindar además una herramienta de gestión potente y amigable que brinde acceso unificado y les permitiera tener información administrativa y académica a las personas y darle un contexto. Así nació la idea de un portal que aborde estas necesidades. Se planteó como base cumplir con estándares de seguridad, disponibilidad y ubiquidad para los accesos y la información de forma que se permitiera utilizar esta herramienta en cualquier parte del planeta.
Se estableció un equipo de trabajo de 5 personas que tendrían una dedicación exclusiva en el proyecto conformados por 3 administradores de red y 2 programadores.

Los lineamientos de la infraestructura que soportara este proyecto deberían: estar fundamentadas en un estándar, permitir múltiples proveedores de servicio de autenticación, e incluir la capacidad de formular contingencia y alta disponibilidad; todo esto utilizando íntegramente Software Libre.

El plazo establecido para la formulación del prototipo fue de 6 semanas.

2 Infraestructura y Despliegue

Al momento de comenzar con el proyecto la Universidad contaba con una base de datos de usuarios y un servicio de autenticación basado en OpenLDAP[1] administrado por una aplicación denominada Gosa[2].

Comenzamos a desarrollar la plataforma con la premisa de que fuera escalable y extensible por lo que se decidió en principio un diagrama de capas. Estas serían: la de origen de autenticación (base de datos de usuarios), la de la provisión de la identidad, la de la provisión de servicios y finalmente los servicios incluyendo el portal miUNQ.

La capa de *origen de autenticación* fue definida para utilizar nuestro directorio LDAP dejando abierta, a futuro, la posibilidad de incorporar otra fuente LDAP o reemplazarla eventualmente por otro tipo de base de datos tales como MySQL. En esta instancia se definen la autorización de acceso a las aplicaciones que utiliza la plataforma y son luego presentadas en el portal miUNQ.

La siguiente capa fue destinada a la *provisión de identidad*. Esta genera un ticket o token de autenticación que le será enviado luego a la capa de *provisión de servicios* para autenticar a todas aquellas a las que tenga permiso de acceso. Para ello se eligió un conjunto de soluciones que permitan múltiples tipos de conexión para la autenticación que garanticen independencia para elegir las aplicaciones que deseáramos basadas en el mismo estándar SAML. También es importante tener varias opciones de modo de poder utilizar el modelo nativo de autenticación de cada aplicación sin tener que modificar código para hacerlo compatible con el elegido. Para ello se utilizaron los siguientes proveedores de identidad: SAML, OpenID, Shibboleth, y CAS (Fig. 1).

---

[1] Es una implementación libre y de código abierto del protocolo Lightweight Directory Access Protocol (LDAP) desarrollada por el proyecto OpenLDAP.

[2] GOSa² es una herramienta GPL para la gestión de cuentas y sistemas sobre bases de datos LDAP

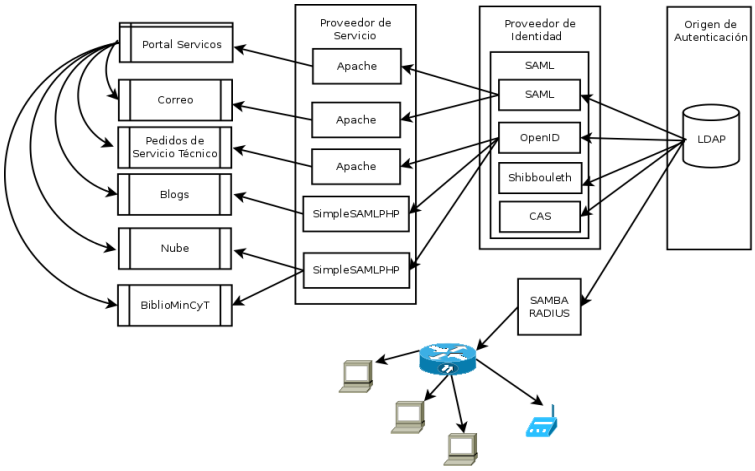

Fig. 1. Desarrollo de la plataforma miUNQ.

Por último la capa de *provisión de servicio* funciona como un intermediario que traduce el formato de la información de la persona al formato que entiende la aplicación a la que desee ingresar y valida el ticket recibido. Con éste se determina, o se deniega, el acceso a la aplicación.

Luego de la formulación de esta plataforma conseguimos un prototipo funcional que nos permitió probar con éxito la implementación.

Los servicios que se conectaron en primera instancia fueron el correo electrónico, a través de los clientes web Roundcube[3] y Horde[4], el servicio de gestión de incidencias, GLPI[5], el servicio de almacenamiento en nube, OwnCloud[6] y el servicio de blogs personales, WordPress[7].

Posteriormente se comenzó a trabajar en la conexión de los sistemas SIU para lo cual concertamos una entrevista con la coordinadora general del SIU María de Lujan Gurmendi y su equipo para contarles sobre el proyecto en que estábamos trabajando y de la necesidad de contar con un conector basado en el estándar SAML. Trabajamos intercambiando experiencias y finalmente en la versión 2.5 del framework de desarrollo SIU-TOBA[8] se incorporó el proveedor de identidad SAML 2.0.

Gracias a esto comenzamos a conectar los servicios del SIU siendo los primeros el SIU-Pilaga, gestión de presupuesto, SIU-Mapuche, gestión de recursos humanos y SIU -Diaguita, gestión de compras y patrimonio.

---

3 http://roundcube.net/

4 http://www.horde.org/apps/webmail

5 http://www.glpi-project.org/

6 https://owncloud.org/

7 https://es.wordpress.org/

8 http://www.siu.edu.ar/plataforma-estandar-de-desarrollo-siu-toba

3 Consumo de información a través de WebServices

Para poder avanzar en esta implementación resultaba imperioso realizar dos operaciones iniciales. La primera fue consolidar la identidad de las personas en todos los sistemas por lo que fue necesario realizar scripts de modificación masiva que aseguraran campos idénticos como nombre de usuario y legajo entre otros. La segunda fue garantizar la conexión de los sistemas SIU sobre todo el SIU-Mapuche el cual fue designado como fuente de verdad para la gestión de los usuarios. Tras realizar consultas directas con el SIU desde la versión 2.5 el framework TOBA incluye SAML y bastará modificar algunos parámetros de los archivos de configuración para conectarlos a nuestro servicio de autenticación.

Cumplidas estas consignas comenzamos a desarrollar el portal utilizando tecnologías libres. Las elegidas fueron Apache 2.4+,PHP 5.4+, Symphony 2+, Simple SAMLphp como proveedor de servicio, una pequeña base de datos basada en MySQL para registrar la sesión y algunas preferencias que pueden definirse en el portal, Memcached para la gestión de las sesiones, jQuery y Bootstrap para la vista del portal.

Teniendo ya configuradas las vistas del portal comenzamos a trazar la estrategia para consumir información de los sistemas SIU y presentarla de forma práctica al usuario. Para ello utilizamos una librería llamada Guzzle que consume servicios REST. Pero hasta el momento el sistema SIU-Mapuche utiliza SOAP para la gestión de los servicios web en lugar de REST y para conectarse es necesaria la librería WSF/PHP, a su vez esta librería no funciona con la versión PHP elegida. Para solucionar este inconveniente conectamos, miUNQ, mediante REST a una aplicación confeccionada en Silex que gestiona los servicios SOAP de MAPUCHE (Fig. 2)

Fig. 2. Solución para el consumo de servicios web con REST

4 Aspectos de seguridad y definición de plataforma

Desde la concepción del proyecto se consideró que la seguridad debía ser uno de los pilares del mismo, de este modo se llevaron a cabo distintas estrategias en los distintos frentes para mitigar de la mejor forma posible las vulnerabilidades al robo de identidad, acceso a servicios no autorizados por parte de un usuario válido, el acceso al directorio LDAP de la universidad con fines maliciosos y los ataques por denegación de servicio.

La infraestructura de red fue pensada de modo de garantizar una completa separación entre las redes de servicios (redes en la que se encuentran publicados los proveedores de servicios y el frontend (arreglo de proxys) atendiendo las peticiones destinadas al proveedor de identidad) y la red segura a la que solo tienen acceso las instancias de los proxys, los proveedores de identidad y los directorios LDAP replicados. De esta manera, se garantiza una única forma de acceder al servicio de provisión de identidad a través del frontend; el punto de contacto de ambos tipos de redes. El mismo cuenta con dos interfaces, cada una atendiendo en la vlan correspondiente al tipo y origen de la petición recibida. (Fig. 3).

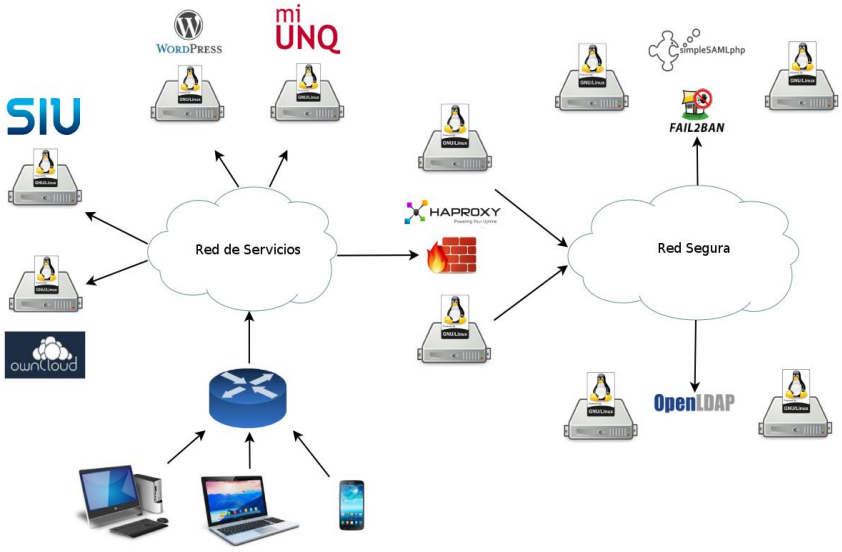

Fig. 3. Descripción de la infraestructura de red.

Para proteger a los proveedores de identidad de un ataque por denegación de servicio y la vulneración de credenciales por fuerza bruta se instaló en cada instancia del proxy un servicio open source de baneo por iptables basado en métricas sobre el origen, frecuencia y tipo de petición recibida llamado fail2ban. Este servicio, además envía una alerta al cuerpo técnico para notificarlo sobre el evento.

Los directorios LDAP están configurados con ACLs para brindar acceso a los proveedores de identidad en modo sólo lectura y requiriendo la autenticación por parte del usuario con sus credenciales para el acceso a su información. De esta forma se garantiza que ante un compromiso de la seguridad del sistema sobre una determinada cuenta de usuario no sea posible acceder a la información de los demás usuarios ni así tampoco la modificación de la misma. En el caso de los módulos de cambio y restitución por olvido de contraseña se utiliza un usuario LDAP con ACLs distintas que sólo le permiten al usuario hacer un cambio sobre su contraseña en el directorio.

Todas las comunicaciones tanto entre servidores como las peticiones realizadas desde los dispositivos de los clientes y sus respectivas devoluciones desde los proveedores de servicios y proveedores de identidad son realizadas de forma

encriptada por SSL. Todos los servidores web desplegados negocian sólo conexiones HTTPS con los clientes y a su vez el proveedor de identidad intercambia con los proveedores de servicio recíprocamente certificados x509 para garantizar la encriptación de los metadatos dado que en nuestra implementación los mismos son intercambiados por el cliente (Fig. 4)

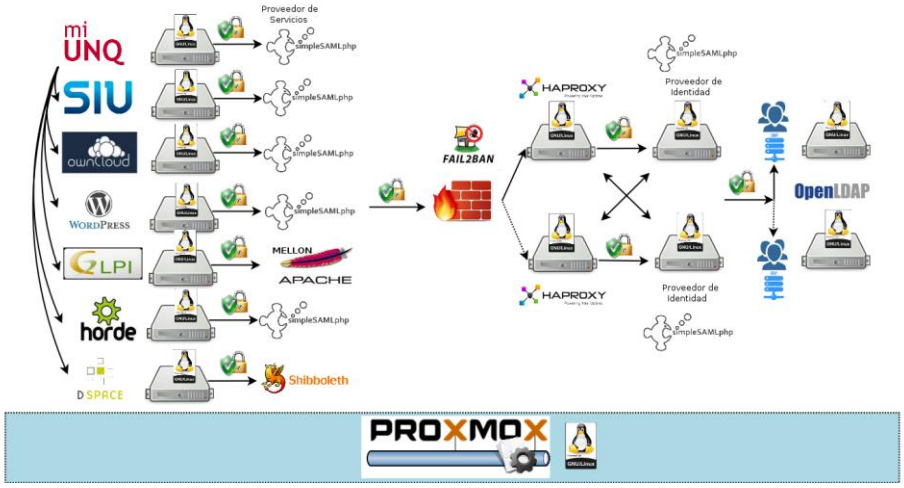

Fig. 4. Esquema final de la plataforma

5 Formulación del Portal miUNQ

La formulación del portal pretendía construir un espacio de trabajo cómodo, personalizable y adaptable a los distintos tipo de dispositivos y/o pantallas. Para ello se desarrolló un tema que contara con una distribución espacial que incluyera menús de opciones, buscadores, barras de alertas y bloques de notificaciones (Fig. 5)

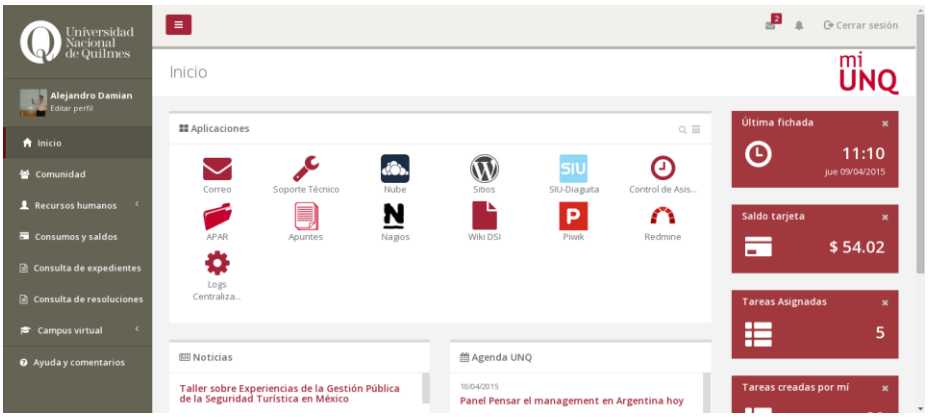

Fig. 5. Portada del sitio MiUnq.

A simple vista el usuario del portal tiene un pantallazo general de su información, puede ver el resumen de noticias y eventos de la Universidad, la cantidad de nuevos correos y notificaciones especiales.

El portal contiene información agrupada por interés y buscadores que consumen y presentan información resumida de otros sistemas permitiendo ampliar los resultados en los propios sistemas.

Para el acceso a los sistemas bastará con hacer click sobre el sistema deseado y se abrirá una nueva pestaña donde el proveedor de servicios del sistema elegido realizará la etapa de autorización utilizando las credenciales de sesión ya establecidas.

Los usuarios pueden definir sus preferencias incorporando los perfiles que tienen en cada red social de modo de poder ser buscados, a través de la sección comunidad (Fig. 6).

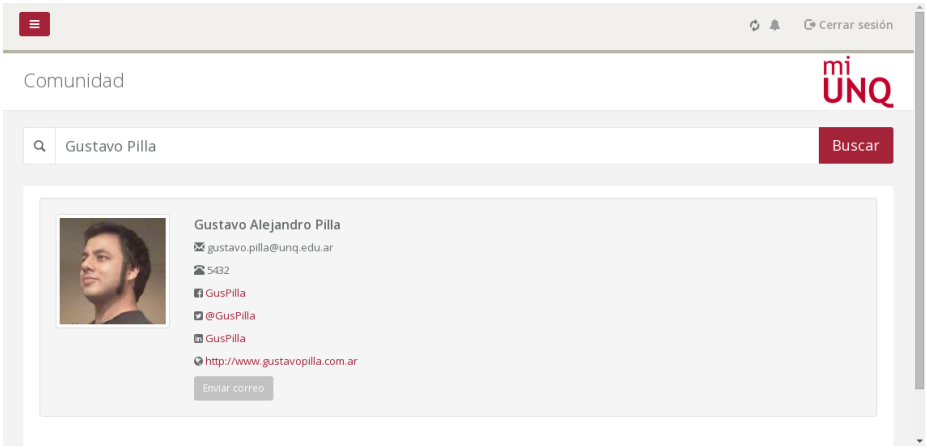

Fig. 6. Portada del sitio MiUnq.

En el apartado de recursos humanos los usuarios pueden consultar y descargar sus recibos de sueldo, que aparecen organizados de manera histórica, consultar su fichadas de ingreso y egreso, mediante un sistema de control de asistencia desarrollado por la Universidad, y las licencias solicitadas. También pueden consultar los datos de domicilios declarados como así también los familiares a cargo que constan en los sistemas de gestión.

6 Estado actual y vistas al futuro

El artículo hasta ahora ha enunciado el estado actual de la solución por lo que hemos reservado este apartado para contar que evolución pensamos. Podríamos primero enunciar qué nuevos sistemas y/o servicios se agregaran al portal, estos son: el servicio de listas de correo electrónico, Sympa[9], el servicio de Repositorio Institucional de Acceso Abierto, Dspace[10] y el servicio de plataforma social, Exo[11]. Adicionalmente estamos trabajando en la integración de herramientas de comunicación que permitan integrar notificaciones de llamadas y eventos generados por la central telefónica IP en el contexto del portal y la inclusión de una solución de web conference que les permita a los usuarios a permanecer en contacto con las personas de la institución aun a distancia para permitirle una integración completa y pueda así desarrollar sus actividades.

A su vez trabajamos para permitirle a los usuarios operar sobre la información suministrada mediante los web services tales como la gestión de licencias, entrega de formularios y solicitud de emisión de certificados de servicio, incorporar solicitudes de compra de bienes y servicios, informar y gestionar los bienes patrimoniales asociados, entre otras nuevas operaciones.

Pensando en los docentes integraremos tres herramientas, desarrolladas por la Universidad, la primera, les permiten acceder a un sistema de equivalencias que cuenta con antecedentes de aprobación de equivalencias cuestión que acelera la resolución de este trámite, la segunda, les brinda información respecto de la evaluación docente que se realiza en la institución y la última, les permite conocer la ocupación de las aulas y realizar reservas de las mismas. También estamos evaluando la posibilidad de consumir información del sistema de gestión académica, SIU-Guarani, para que los docentes puedan conocer los alumnos asociados a sus aulas y cargar notas desde el portal.

---

9 http://www.sympa.org/

10 http://www.dspace.org/

11 http://www.exoplatform.com/