SERVICIO DE FEDERACIÓN DE IDENTIDADES PARA REDUNIV

REDUNIV IDENTITY FEDERATION SERVICE

Alain Lamadrid Vallina, lamadrid@reduniv.edu.cu, Ministerio de Educación Superior, Cuba, Master en Ciencia, Director General de Információn, Comunciación e Informatización.

Jorge Daniel Villa Hernández, villa@reduniv.edu.cu, Ministerio de Educación Superior, Cuba, Master en Ciencia, Asesor.

José Gregorio Liendo Gutiérrez, josegregorioliendo1999@gmail.com, Universidad Tecnológica de La Habana (CUJAE), Cuba, Estudiante de Pregrado.

Resumen

La federación de identidades es un sistema de confianza entre dos o más partes, capaz de autenticar a los usuarios; así como transmitir la información necesaria para autorizar su acceso a los recursos brindados por proveedores de servicio, en una manera más segura y eficiente. Para ello, comparten y distribuyen información relativa a identidad y atributos de los usuarios a través de diferentes dominios de confianza, según ciertas políticas establecidas. El presente trabajo de diploma tiene la finalidad de realizar el diseño de un servicio de federación de identidades para la Red Nacional de Investigación y Educación de Avanzada del Ministerio de Educación Superior de la República de Cuba (REDUNIV). Para ello se ha realizado un estudio de los principales elementos que conforman las federaciones de identidad, así como de los estándares y arquitecturas más utilizados en la implementación de las mismas. Con el fin de realizar el diseño, se analizan federaciones de identidad implementadas por organizaciones similares a REDUNIV: con el objetivo de tomar algunas de sus experiencias, como punto de partida para este trabajo. Después de llevar a cabo un estudio de los aspectos involucrados en este modelo de gestión de identidad y de analizar las particularidades de la red donde se va a implementar la federación, se procede a diseñar el servicio, tomando en cuenta los requerimientos preestablecidos para el mismo.

Palabras claves: Federación de identidad, gestión de identidad, RNIE, Redes Académicas.

Abstract

An Identity federation is a trust system between two or more parties, capable of authenticating users; as well as transmitting the necessary information to authorize their access, to resources offered by service providers, in a more secure and efficient way. These services, usually share and distribute information related to the identity and attributes of users through different trusted domains, according to certain established policies. The purpose of this thesis, is to design an identity federation service for the Advanced NREN of the Ministry of Higher Education of the Republic of Cuba (REDUNIV). The proposal includes a study of the main elements on identity federations, as well as the most used standards and architectures. To create the current design, some identity federation implementations in similar organizations to REDUNIV were reviewed; trying to find elements that might be used as starting point for this work. The study of topics related with identity federation management models and analyzing the design prerequisites and the current infrastructure, allowed us to come up with a proposal of an identity federation service for REDUNIV.

Keywords: Identity federation, identity management, NREN, Academics Networks.

Introducción

En un mundo donde el trabajo colaborativo entre instituciones ha tenido un auge sin precedentes y el acceso a servicios fuera de los límites institucionales es cada vez más necesario, ha surgido la necesidad de que un usuario perteneciente a un dominio de identidad[1], pueda acceder a recursos de otros dominios en los que se confía. Es aquí donde surge la necesidad de federar identidades, a partir de integrar y coordinar centralmente diferentes dominios de identidad; para lograr una mejor gestión de usuarios y un efectivo control de acceso. Para su implementación, es necesario el establecimiento de acuerdos de confianza entre organizaciones; tal que permitan a cualquier usuario de una federación, acceder a los recursos y servicios de cualquier organización federada (tales como laboratorios remotos, fondos bibliográficos, Entornos Virtuales de Enseñanza y Aprendizaje (EVEA), repositorios de objetos de aprendizaje (ROA), servicios de videoconferencia, entre otros), siempre y cuando tenga autorización, gracias a una identidad digital única común. La federación de identidad es utilizada en diferentes campos de la actividad humana; en sectores tales como: salud, gobierno, educación, comercio, entre otros.

El Ministerio de Educación Superior de la República de Cuba (MES) cuenta con una Red Nacional de Investigación y Educación (REDUNIV) que tiene como miembros a todas las Universidades y Entidades de Ciencia, Tecnología e Innovación (ECTI) adscriptas de este organismo. Generalmente, cada una de estas instituciones miembro de REDUNIV cuenta con un servicio local de directorio para la gestión de identidades. Los usuarios aceden a los servicios, recursos y contenidos mediante sistemas de credenciales, construidos de forma personalizada; buscando emplear un sistema único de autenticación a través de todos los servicios publicados en la red de su institución. Sin embargo, lograr accesos a recursos privados, ubicados fuera de las fronteras de la Universidad o ECTI de origen; demanda un elevado nivel de gestión (con bajo nivel de productividad y éxito). En general, se requiere de la creación de credenciales de acceso local en cada nueva institución. De esta forma, se desperdician oportunidades de compartir experiencias y conocimientos entre entidades homólogas, provocando la duplicación de recursos y esfuerzos.

Con el objetivo de enfrentar la problemática expresada anteriormente, de forma general, los autores proponen el diseño de un servicio de federación de identidades para REDUNIV.

Algunas Federaciones de Identidad implementadas en las Redes de Investigación y Educación de la región latinoamericana.

Las redes nacionales y regionales conforman una malla con alcance global que se estructura a partir de la interconexión de redes de alcance nacional con redes regionales, que a su vez se interconectan entre sí a distintos niveles. Este mallado, concibe la conexión física, las capacidades de procesamiento y gestión de datos, y espacios de colaboración compartidos.

A nivel global, se encuentran en operación más de 140 RNIEs. En la región de Latinoamérica y el Caribe se destacan la Red Brasileña para la educación y la

[1] contenedor para gestionar usuarios y roles, aprovisionar usuarios y proteger la integración de aplicaciones.

investigación (RNP)[2], la Red para la investigación y educación de Chile (REUNA)[3], la Red Nacional de Educación e Investigación de México (CUDI)[4] y la Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia (CEDIA)[5]. Estas RNIEs son miembros de la Cooperación Latinoamericana de Redes Avanzas (RedCLARA)[6], la Red de Investigación y Educación de la región. (Cadenas, L. E., 2020)

En Cuba existen diferentes proyectos sectoriales con alcance nacional (que incluyen actividad académica), tales como REDUNIV, RIMED (Ministerio de Educación), CUBARTE (Ministerio de Cultura), INFOMED (Ministerio de Salud Pública) y RedCien (Ministerio de Ciencia, Tecnología, Innovación y Medio Ambiente).

Las RNIEs han sido pioneras en el uso de federaciones de identidad, permitiendo a los usuarios autenticarse una vez, para tener acceso a múltiples servicios; mejorando su experiencia de conexión y disminuyendo la complejidad y los costos asociados a la emisión y gestión de credenciales. (Bedoya Ortiz, D. H.,2018)

A continuación, se relacionan los sistemas de federación de identidad que los autores utilizaron como referentes para el desarrollo de la investigación:

- La Comunidad Académica Federada (CAFe) es la federación de identidad que reúne instituciones de enseñanza e investigación brasileñas.[7]
- La Comunidad Federada de REUNA (COFRe) es la plataforma para instituciones académicas y de investigación chilenas.[8]
- La federación de identidad mexicana (FENIX), operada por CUDI.[9]
- La Federaciones de identidad para redes de Educación Latinoamericanas (FIEL) operada por RedCLARA provee y promueve el acceso a federaciones entre sus redes socias y las instituciones afiliadas a ellas.

Un acercamiento al Servicio de Federación de Identidad.

El empleo de mecanismos de Inicio de Sesión Único (SSO) se produce de forma exitosa, fundamentalmente dentro del ámbito de una organización o entorno controlado (dígase una universidad); tal que sea posible conectar directamente las aplicaciones y servicios con su comunidad de usuarios. Cuando se requiere el acceso a recursos y servicios en múltiples aplicaciones, es necesario escalar el concepto simple de Inicio de Sesión Único, al de Federación de Identidad, también conocido como Gestión de Identidad Federada (FIM, según sus siglas en inglés).

La federación de identidad es una tecnología específica de los sistemas de gestión de identidades, que se construye sobre la base de relaciones de confianza entre dos o más organizaciones para compartir aplicaciones y servicios. (Simone, P., 2022) Las organizaciones que participan en una federación de identidad, lo hacen a partir de un grupo de reglas explícitas, que garantizan el correcto funcionamiento del proceso; así

[2] https://www.rnp.br/es/
[3] https://www.reuna.cl/
[4] https://cudi.edu.mx/
[5] https://cedia.edu.ec/
[6] https://www.redclara.net/index.php/es/
[7] https://memoria.rnp.br/es/servicios/cafe.html
[8] https://www.reuna.cl/cofre
[9] https://www.fenix.org.mx/

como el correcto aseguramiento de los datos, usuarios y procesos involucrados. (Dib O. y Toumi K., 2020)

En el ámbito de la identidad federada existen varios elementos que se encuentran estrechamente relacionados entre sí y que representan la esencia de las federaciones de identidad:

Proveedor de identidad (IDP): El proveedor de identidad es el encargado de gestionar los datos de identidad de una organización. Un IDP es un servicio al cual serán redirigidos los usuarios de una organización para ser autenticados. Los proveedores de identidad brindan servicio de autenticación a las aplicaciones. Se necesita al menos un proveedor de identidad por cada organización participante (con una comunidad de usuarios) en una federación. (Cevallos A. S, 2016)

En general, están conectados a servicios de directorios (tales como Directorio Activo o LDAP), los cuales almacenan los perfiles de los usuarios.

Proveedor de servicios (SP): En un esquema federado, no es más que un proceso que corre en cada aplicación; y se encarga de verificar y validar las credenciales de autenticación de los usuarios, permitiendo el acceso a los recursos. (Haddouti, S. E., 2015)

Servicio de descubrimiento: Posibilita a los usuarios (a partir de un listado), elegir el proveedor de identidad de su organización. El servicio lo redirige hacia la página de inicio de sesión de la institución seleccionada, a fin de realizar la autenticación. Este proceso, es también conocido como servicio De dónde eres (WAYF, por sus siglas en inglés).

Proxy proveedor de identidad: Es un componente que puede incluirse de forma opcional. Recibe solicitudes de autenticación dentro de la federación, y las redirecciona adecuadamente hacia el IDP de la organización del usuario en cuestión.

Diseño del Servicio de Federación de Identidad de RedUniv.

RedUniv, se formalizó como la Red Nacional de Investigación y Educación de Avanzada del MES en la resolución 65/2021[10] del ministro del ramo. Algunos aspectos que caracterizan a RedUniv son:

- Verdaderamente nacional.
- Interconecta a 25 IES y el Grupo Empresarial del MES.
- Su comunidad está conformada por más de 200 mil estudiantes, docentes e investigadores.
- Inteligencia distribuida
- Red-Laboratorio, abierta a la innovación y experimentación
- Amplio espectro de interconexión, con énfasis en el acceso a otras redes académicas nacionales e instituciones académicas.

Algunos elementos que caracterizan las condiciones actuales en RedUniv son:

- La mayoría de las instituciones componentes de RedUniv poseen soluciones de SSO para que sus usuarios accedan a los servicios locales de forma sencilla y controlada.

[10] http://reduniv.edu.cu/wp-content/uploads/2022/01/RESOLUCION-65-REDUNIV.pdf

- Básicamente se emplean dos soluciones para servicios de directorios: Directorio Activo (solución comercial de Microsoft para Windows Server y Azure) y LDAP (estándar abierto de Internet, en implementaciones de código abierto).
- En el área de comunicaciones y servicios de información y red, fundamentalmente se trabaja con Linux (en diferentes distribuciones) y aplicaciones de código abierto.
- Cada institución cuenta con un equipo técnico, que opera toda la infraestructura, servicios y usuarios de la institución.
- Las políticas de operación de la infraestructura de red y servicios de cada institución, se rige por políticas nacionales emitidas por la Dirección de Informatización y Desarrollo Digital del MES; pero la implementación se realiza a partir de disposiciones emitidas localmente por la dirección de cada entidad.
- Buena conectividad desde todos los campus centrales de las universidades; así como desde las ECTI.

De los servicios publicados en RedUniv, se identifican como posibles a federar en una etapa inicial:

- Plataformas de educación a distancia
- Repositorios de objetos de aprendizaje
- Repositorios institucionales
- Servicio de computación de alto rendimiento (HPC)
- Videoconferencia

El diseño del servicio de federación parte de las siguientes premisas:

- Que brinde una mejor experiencia a los usuarios en la interacción con recursos ubicados en las IES conectadas a RedUniv.
- Solución distribuida (siempre que sea posible) y centralizada (siempre que deba serlo).
- Escalable en cuanto a cantidad de usuarios y servicios.
- Posible de mantener con un mínimo de recursos humanos.
- Costos razonables en cuanto a infraestructura.
- Posible de implementar sin generar alteraciones significativas a las infraestructuras existentes en cada red.
- Que permita el trabajo con diferentes opciones de autenticación (contraseñas, certificados, doble factor de autenticación, etc.)
- Basada en *HTTP/HTTPS redirects.*
- Basada fundamentalmente en soluciones de software libre.
- Que permita la futura integración con otras redes académicas dentro y fuera del país.
- Capaz de conservar la privacidad de los usuarios y contenidos.

Hasta el momento, en Cuba, no existe ninguna implementación de federación de identidad en redes académicas, por lo que no se puede establecer un punto de partida basado en la experiencia local.

En la siguiente tabla relacionan los principales componentes del servicio de federación de identidad de RedUniv:

Componentes	**Principales elementos de la selección**

Estándar: SAML 2.0	Requisitos a tener en cuenta en la selección del estándar: • Solución Basada en HTTP/HTTPS redirects • Solución que permita el trabajo con diferentes opciones de autenticación (contraseñas, certificados, doble factor de autenticación, etc.) • Solución que posibilite la implementación, sin generar alteraciones significativas a las infraestructuras existentes en cada red. • Solución capaz de conservar la privacidad de los usuarios y contenidos. • Solución que permita la futura integración con otras redes académicas dentro y fuera del país Otros aspectos considerados: • Todas las Federaciones académicas nacionales o regionales, anteriormente expuestas, implementan SAML
Arquitectura: *hub and spoke* con inicio de sesión distribuido	Los principales aspectos que se tuvieron en cuenta para la selección de la arquitectura, a partir de las características de RedUniv son: • Las instituciones que forman RedUniv, de forma general, cuentan con servicios de Inicio único de sesión • Crear una base de datos central para los usuarios de RedUniv, es realmente inviable. • La cantidad de servicios y usuarios que se prevé federar, en una primera etapa, es baja. • Teniendo en cuenta la implementación de otros servicios, se recomienda que la gestión de la federación sea centralizada. RedUniv asume todo el trabajo de coordinación de la federación; y para garantizar el correcto funcionamiento de la misma, debe poner en funcionamiento los siguientes servicios: • Proveedor de identidad (IdP). Tiene la responsabilidad de estar en contacto con los diferentes proveedores de servicio existentes • Proveedor de servicios (SP). • Servicio WAYF (Discovery Service) • Registro de Recursos • Servidor de tiempo (NTP) • Compilador de Metadatos (Metadata Aggregator)
Plataforma: Shibboleth	• La selección se basa en los requerimientos del diseño planteados con anterioridad • El requisito explícito sobre emplear soluciones de software libre, eliminan de la evaluación a un grupo importante de soluciones que se emplean actualmente; entre las que puede mencionarse Okta

	Identity Management, VMware Workspace One Access, Ping Identity PingOne y Auth0. • Se evaluaron diversas soluciones basadas en *software* libre; entre ellas SimpleSAMLphp, SATOSA, Keycloak, OpenIAM, FreeIPA y Gluu. • Shibboleth, SimpleSAMLphp y SATOSA, están desarrolados sobre SAML; aunque solamente los dos primeros, pueden implementar exitosamente proveedores de servicio e identidad. • Shibboleth es la herramienta empleada por las federaciones académicas anteriormente expuestas.

En los anexos se muestran los gráficos relacionados con la arquitectura seleccionada como parte del diseño de Federación de Identidad de RedUniv. La Figura 1 tiene como base, el diseño de la figura presentada en Geant (2023)

La implementación del servicio de federación de identidad de RedUniv se concibe en cuatro etapas, que permitirán construir con solidez cada uno de los componentes, incorporar gradualmente nuevos usuarios y servicios, así como realizar un ejercicio frecuente de capacitación técnica. La selección de instituciones involucradas en cada etapa, así como la lista de tareas a desarrollar, se determinarán a partir de las condiciones tecnológicas (equipamiento y equipo de administración), las cuales deben constituir una base para consolidar el proceso posteriormente. De igual manera, es importante resaltar, el carácter novedoso de estas tecnologías en el país; por lo cual, es un proceso necesariamente gradual, para lograr un cambio de visión, en referencia con la gestión de identidad y las formas de proveer servicios seguros a una amplia comunidad de usuarios.

ETAPA 1 (tiempo estimado de duración: 6 meses)

- Se crea en REDUNIV, hub de servicios de la federación (IdP, SP, WAYF) en centro de datos principal de la Red. En esta etapa, únicamente se instalará una instancia de cada servicio, preparándose condiciones técnicas para avanzar en la implementación del diseño de forma total.
- Se instalan proveedores de identidad y servicios en REDUNIV y en las redes de la Universidad Central Marta Abreu de Las Villas (UCLV), Universidad de Oriente (UO), Universidad Tecnológica de la Habana (CUJAE) y Universidad de Ciencias Informáticas (UCI).
- Se establecen políticas de tráfico en centro de datos de REDUNIV, para garantizar acceso al Hub.
- Habilitar servidor de tiempo (NTP) en REDUNIV.
- Capacitación a los administradores de todas las redes componentes de REDUNIV.
- Crear una máquina virtual personalizada, para facilitar (en el futuro) un rápido despliegue de proveedores de Identidad y Servicio, en todas las instituciones conectadas a REDUNIV; así como para la realización de actividades de superación.
- Elaboración de las normativas de participación en la federación; así como para publicar servicios.

ETAPA2 (tiempo estimado de duración: 6 meses)

- Validar el diseño realizado y realizar las correcciones que sean pertinentes.
- Se instalan proveedores de identidad en la Universidad de Granma (UDG), Universidad de Pinar del Río Hermanos Saiz (UPR), Universidad Agraria de la Habana (UNAH), Universidad de Guantánamo (UG), Universidad de ciengo de Ávila (UNICA), Universidad de Camagüey Ignacio Agramonte y Loynaz (UC).
- Se instala (en centro de datos virtual de RedUniv). la segunda instancia del servicio WAYF; así como del proveedor de los proveedores de identidad y servicio.
- Se instala el servicio HA Proxy en centro de datos principal de RedUniv
- Crear y poner en funcionamiento, la primera instancia del Registro de Recursos de la Federación.
- Identificar posibles servicios adicionales a federar.

ETAPA3 (tiempo estimado de duración: 6 meses)

- Validar el diseño realizado y realizar las correcciones que sean pertinentes
- Agregar nuevos proveedores de servicios (identificados en la segunda etapa)
- Agregar proveedores de identidad, en todas las Instituciones pertenecientes a RedUniv, que aún no se han conectado a la federación.
- Instalar el Compilador de Metadatos en centro de datos principal de RedUniv
- Se instalan las 2 instancias restantes del servicio WAYF (en centro de datos backup de RedUniv y en centro de datos de UCLV)
- Se instalará la segunda instancia del registro de recursos (en centro de datos backup de RedUniv)
- Se instala el servicio HA Proxy en centro de datos virtual de RedUniv
- Diseñar y realizar, ejercicio de interconexión con otra federación

ETAPA 4 (tiempo estimado de duración: 12 meses)

- Participación en federaciones regionales/internacionales

Conclusiones.

Las redes académicas y de investigación suponen una solución óptima para las demandas de conectividad de universidades y centros de investigación en una nación. Además ofrecen servicios de federación de identidad que promueven la colaboración entre sus participantes y un mayor aprovechamiento de los recursos.

En las federaciones de identidad intervienen dos actores importantes: los proveedores de servicio y los proveedores de identidad, los cuales a través del establecimiento de relaciones de confianza entre las organizaciones que los desarrollan; se interconectan entre sí permitiendo a los usuarios acceder a múltiples servicios, en múltiples dominios, con solo un juego de nombre de usuario y contraseña

Los estándares más utilizados para las federaciones de identidad son OAuth, SAML 2.0 y OpenID Connect, en especial estos dos últimos debido a que son protocolos de autenticación y autorización.

Como parte del diseño, SAML 2.0 se ha seleccionado como estándar para su implementación en RedUniv; propuesta que se ha estructurado en cuatro etapas bien definidas, que permitirán la introducción gradual de la tecnología.

El diseño presentado, satisface las condiciones establecidas para el diseño; donde, los bajos requerimientos en cuanto a recursos tecnológicos y humanos para su implementación, hacen muy viable su introducción en un corto período de tiempo.

El proceso de diseño de la federación sienta las bases de este tipo de infraestructuras, para las redes académicas del país, y define los principales elementos a tener en cuenta para la posterior implementación del servicio.

Bibliografía

1. Cadenas, L. E. (2020) El rol de las redes nacionales de investigación y educación en las Ciencias Sociales», Disertaciones, vol. 13, n.o 1, ene. 2020, doi: 10.12804/revistas.urosario.edu.co/disertaciones/a.7608.
2. Bedoya Ortiz, D. H. (2018), Estado y prospectiva académica de las redes nacionales de tecnología avanzada pioneras en Iberoamérica. (Tesis de maestría). Universidad Nacional de Quilmes, Bernal, Argentina
3. Simone (2022) Digital Identity: The international landscape of active systems, Politecnico Milano, 2022.
4. Dib O. y Toumi K. (2020) «Decentralized Identity Systems: Architecture, Challenges, Solutions and Future Directions», AETiC, vol. 4, n.o 5, pp. 19-40, dic. 2020, doi: 10.33166/AETiC.2020.05.002.
5. Cevallos A. S (2016), Sistema de Federaciones de Identidades para la facultad de ingeniería en sistemas, electrónica e industrial usando software de código abierto, Universidad Técnica de Ambato, Ecuador, 2016.
6. Haddouti, S. E. (2015) Towards an Interoperable Identity Management Framework: a Comparative Study, International Journal of Computer Science Issues, vol. 12, n.o 6, 2015.
7. Geant (2023) Federation Architectures - eduGAIN - GÉANT federated confluence. https://wiki.geant.org/display/eduGAIN/Federation+Architectures (accedido 29 de mayo de 2023)

Anexos.

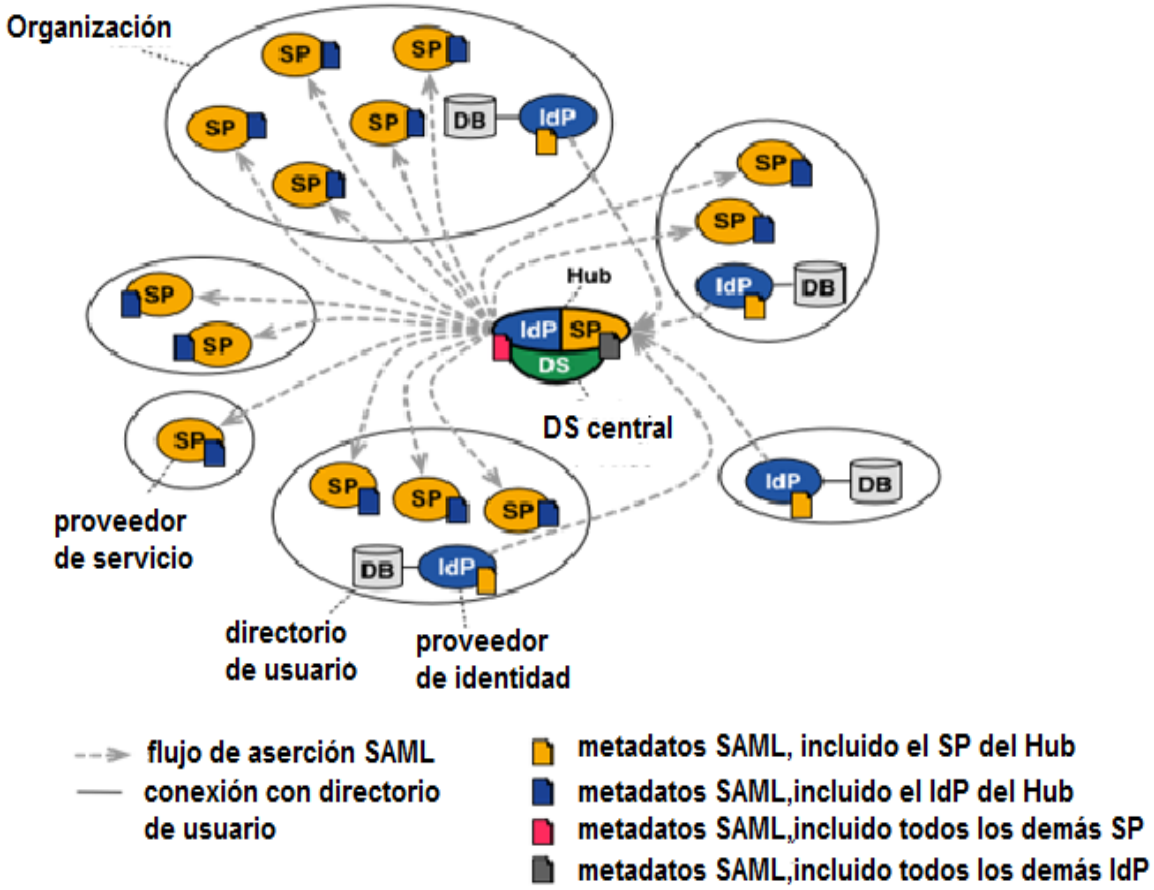

Figura 1. Arquitectura propuesta para la federación de RedUniv.

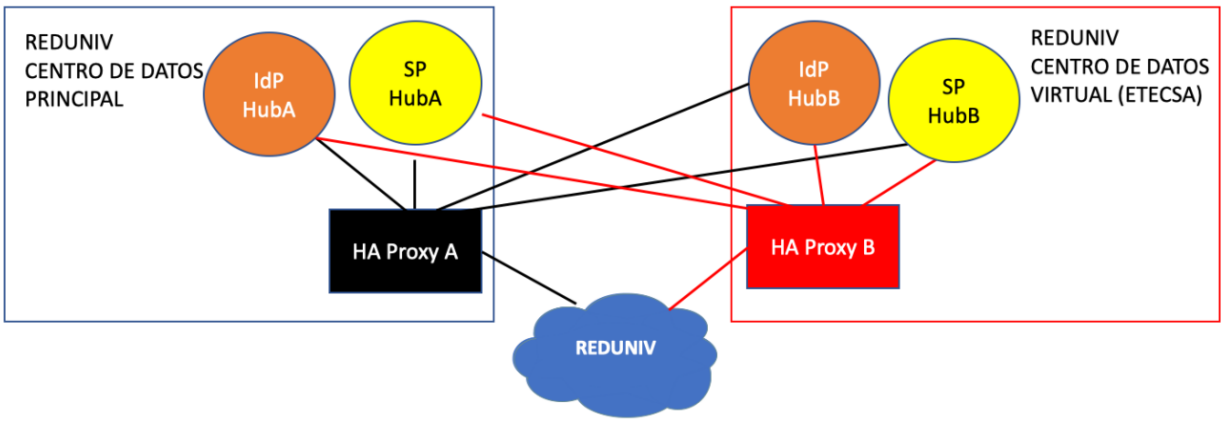

Figura 2. Implementación de Proveedores de identidad y servicios en hub de Federación de Identidad de RedUniv.

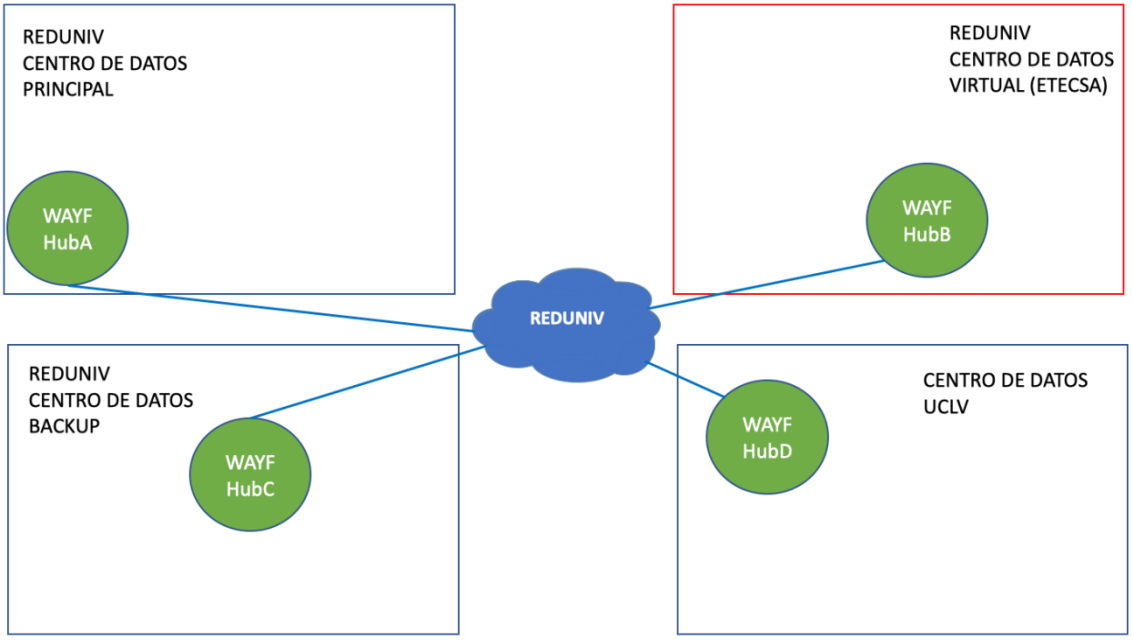

Figura 3. Implementación de Servicio WAYF en hub de Federación de RedUniv.

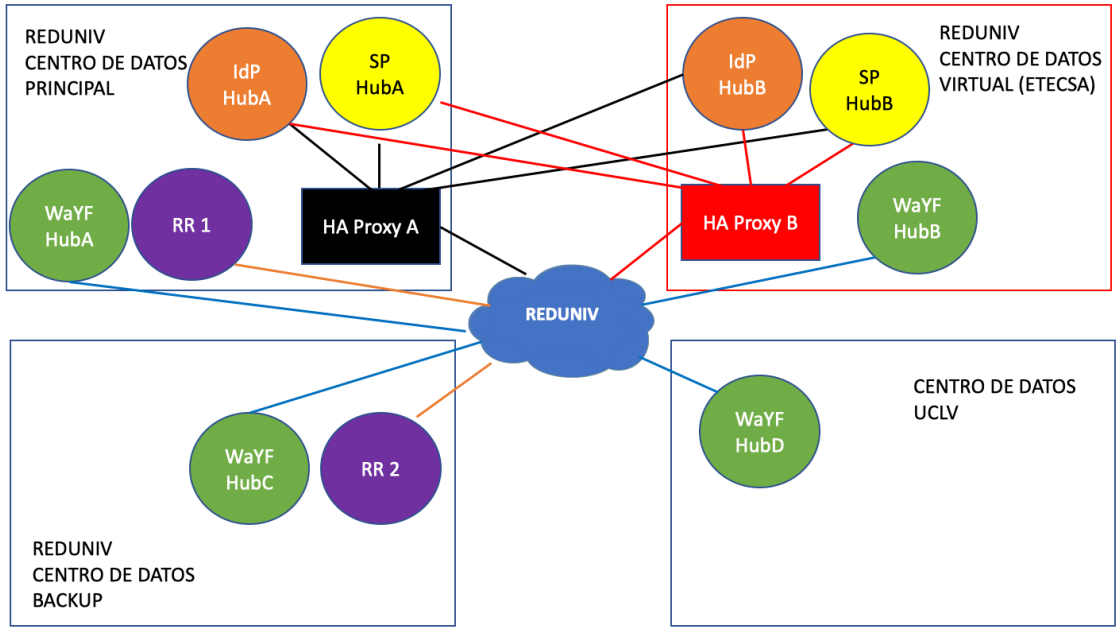

Figura 4. Implementación de servicios en el hub en la Federación de Identidad de RedUniv.