Congreso Universidad
ISSN: 2306-918X | RNPS: 2318 | Vol. 11 No. 4 2025 e43 (enero-abril)

Presentado en el X Taller Internacional "La transformación digital y las tecnologías de avanzada en la Educación Superior"

Artículo científico

Servicio de federación de identidades para la red de investigación y educación del Ministerio de Educación Superior

Identity federation service for the research and education network of the Ministry of Higher Education

Alain Lamadrid Vallina[1] 0000-0003-3036-5265 lamadrid@reduniv.edu.cu

Jorge Daniel Villa Hernández[1] villa@reduniv.edu.cu

José Gregorio Liendo Gutiérrez[2] josegregorioliendo1999@gmail.com

[1] Ministerio de Educación Superior. La Habana, Cuba.

[2] Universidad Tecnológica de La Habana. La Habana, Cuba.

Recibido: 2/10/2024

Aceptado: 19/12/2024

RESUMEN

La federación de identidades es un sistema de confianza entre dos o más partes, capaz de autenticar a los usuarios; así como de transmitir la información necesaria para autorizar su acceso a los recursos brindados por proveedores de servicio, de una manera más segura y eficiente. Para ello, comparten y distribuyen información relativa a identidad y atributo de los usuarios, a través de diferentes dominios de confianza, según ciertas políticas establecidas. El presente trabajo tuvo la finalidad de diseñar 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. Para ello, se realizó 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 analizaron federaciones de identidad implementadas por organizaciones similares, para tomar algunas de sus experiencias, como punto de partida. 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 implementó la federación, se procedió a diseñar el servicio, y se tomaron en cuenta los requerimientos establecidos para el mismo.

Palabras clave: federación de identidad; gestión de identidad; redes académicas.

ABSTRACT

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 the resources provided by service providers, in a more secure and efficient way. To this end, they share and distribute information related to user identity and attributes, through different trust domains, according to certain established policies. The purpose of this work was to design an identity federation service for the national network of research and advanced education of the Ministry of Higher Education of the Republic of Cuba. For this purpose, a study was made of the main elements that make up identity federations, as well as the standards and architectures most commonly used in their implementation. In order to carry out the design, identity federations implemented by similar organizations were analyzed to take some of their experiences as a starting point. After carrying out a study of the aspects involved in this identity management model and analyzing the particularities of the network where the federation was implemented, we proceeded to design the service, and took into account the requirements established for it.

Keywords: identity federation; identity management; academic 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.

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

Para su implementación es necesario el establecimiento de acuerdos de confianza entre organizaciones 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, repositorios de objetos de aprendizaje, 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 y 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 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, se busca 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, ello provoca la duplicación de recursos y esfuerzos. Con el objetivo de enfrentar la problemática expresada, se propone el diseño de un servicio de federación de identidades para REDUNIV.

MATERIALES Y MÉTODOS

Se realizó un estudio de los principales elementos que conformaron las federaciones de identidad, así como de los estándares y arquitecturas más utilizados en la implementación de las mismas. Con este fin, se realizó el diseño y se analizaron federaciones de identidad implementadas por organizaciones similares a REDUNIV.

La implementación del servicio de federación de identidad de REDUNIV, se concibió en cuatro etapas que permitieron construir cada uno de los componentes, incorporar gradualmente nuevos usuarios y servicios, y realizar un ejercicio frecuente de capacitación técnica.

La selección de instituciones involucradas en cada etapa, así como la lista de tareas a desarrollar, se determinaron a partir de las condiciones tecnológicas (equipamiento y equipo de administración), las que constituyeron una base para consolidar el proceso 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.

RESULTADOS Y DISCUSIÓN

Las redes nacionales y regionales conforman una malla con alcance global que se estructura mediante 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 los espacios de colaboración compartidos.

A nivel global, se encuentran en operación más de 140 RNIE, en la región de Latinoamérica y el Caribe se destacan la red brasileña para la educación y la 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 RNIE son miembros de la cooperación latinoamericana de redes avanzas (RedCLARA)[6], la red de investigación y educación de la región (Cadenas, 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 RNIE son pioneras en el uso de federaciones de identidad; permiten a los usuarios autenticarse una vez, para tener acceso a múltiples servicios; mejoran su experiencia de conexión; y disminuyen la complejidad y los costos asociados a la emisión y gestión de credenciales (Bedoya, 2018).

[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

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

- La comunidad académica federada (CAF) es la federación de identidad que reúne instituciones de enseñanza e investigación brasileñas[7].
- La comunidad federada de REUNA (COFR) es la plataforma para instituciones académicas y de investigación chilenas[8].
- La federación de identidad mexicana (FENIX), operada por CUDI[9].
- Las 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.

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 SSO, al de federación de identidad, también conocido como gestión de identidad federada (FIM).

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, 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 como el correcto aseguramiento de los datos, usuarios y procesos involucrados (Dib y Toumi, 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 IDP es el encargado de gestionar los datos de identidad de una organización, es un servicio al cual son redirigidos los usuarios de una organización para ser autenticados, brindan servicio de autenticación a las aplicaciones y se necesita al menos uno por cada organización participante (con una comunidad de usuarios) en una federación (Cevallos, 2016).

[7] https://memoria.rnp.br/es/servicios/cafe.html

[8] https://www.reuna.cl/cofre

[9] https://www.fenix.org.mx

En general están conectados a servicios de directorios (tales como directorio activo o LDAP), los que 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, y permite el acceso a los recursos (Haddouti, 2015).

Servicio de descubrimiento*:* Posibilita a los usuarios (a partir de un listado), elegir el IDP 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 la caracterizan 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).
- Videoconferencias.

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.
- Permite 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.

- Permite 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, se relacionan los principales componentes del servicio de federación de identidad de REDUNIV.

Tabla 1. 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. • A partir de 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.

Las siguientes figuras 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).

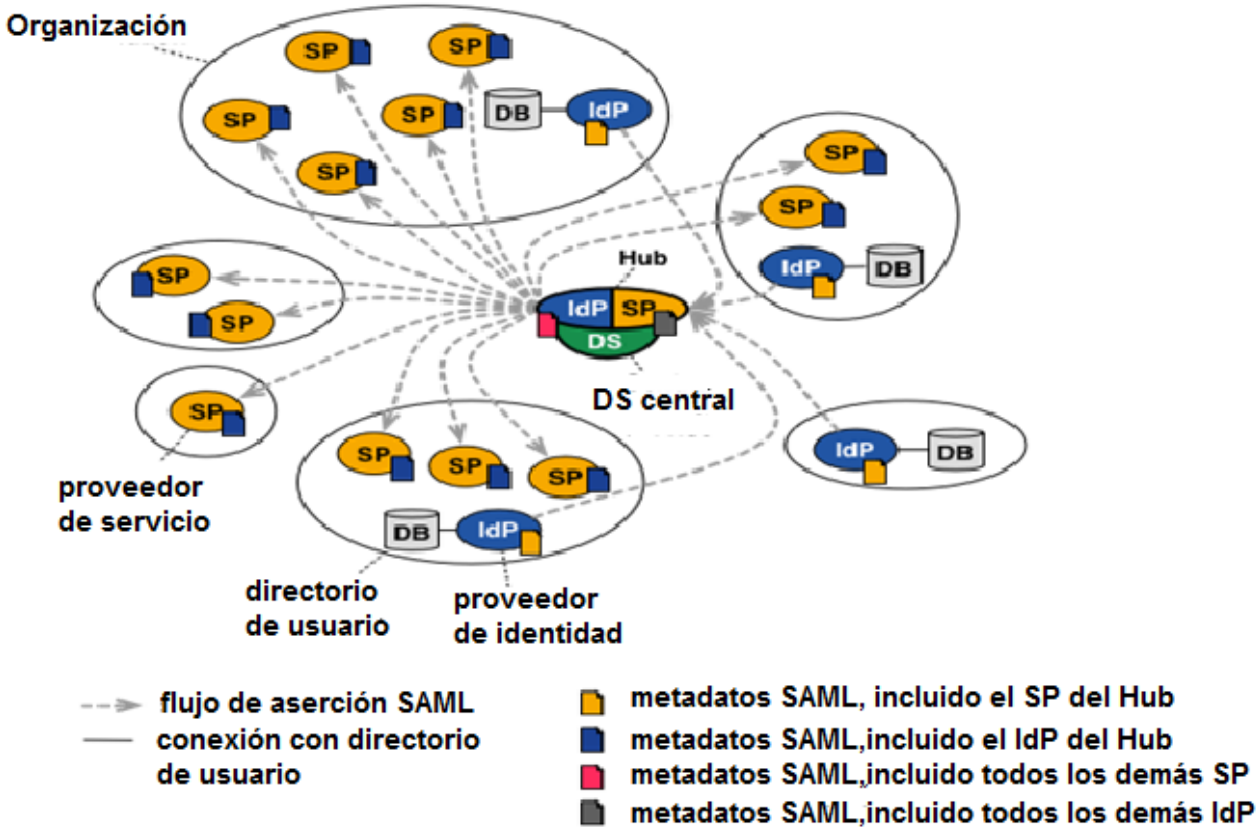

Figura 1. Arquitectura propuesta para la federación de REDUNIV

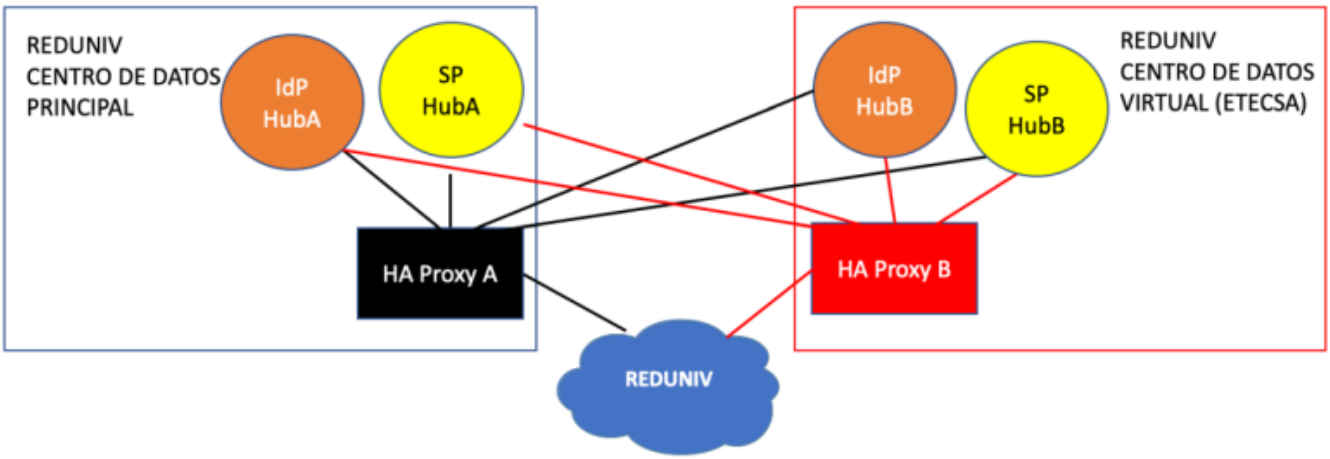

Figura 2. Implementación de Proveedores de identidad y servicios en hub de la federación de identidad de REDUNIV

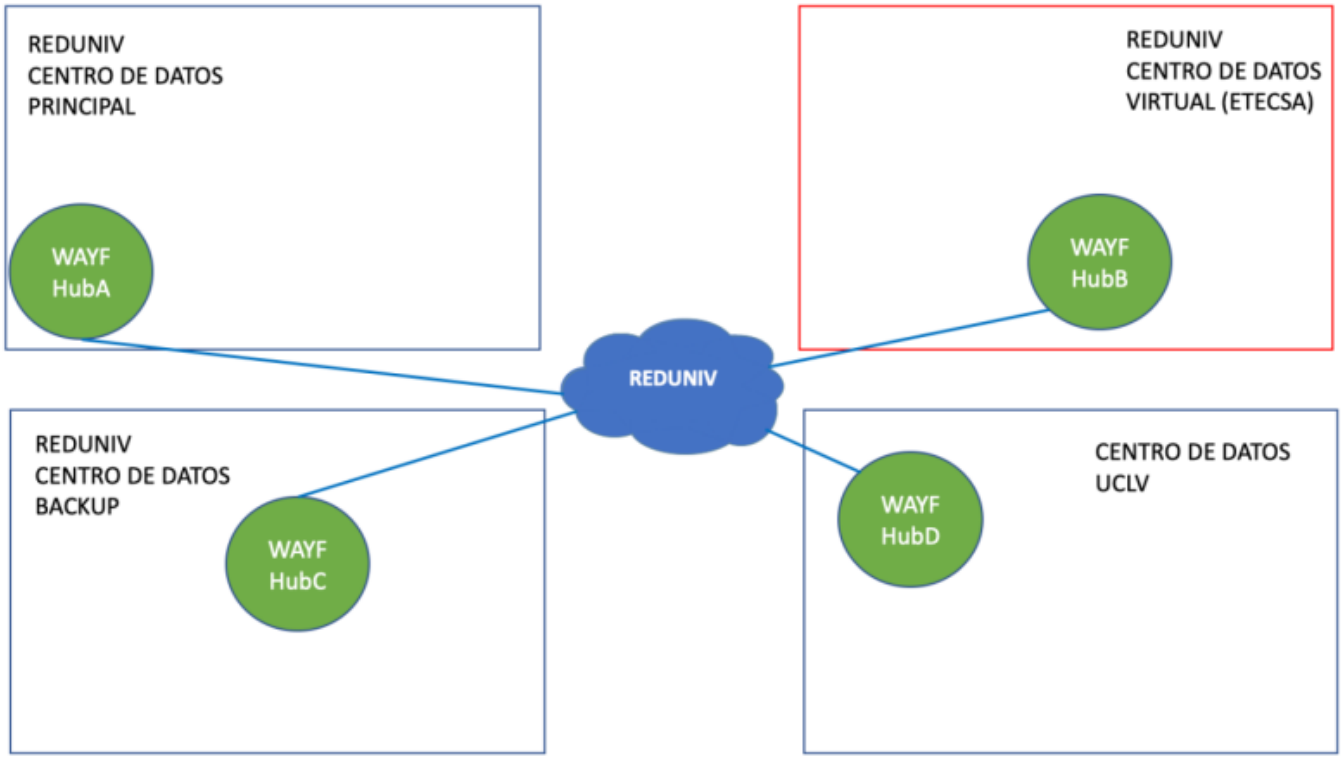

Figura 3. Implementación de Servicio WAYF en hub de la federación de REDUNIV

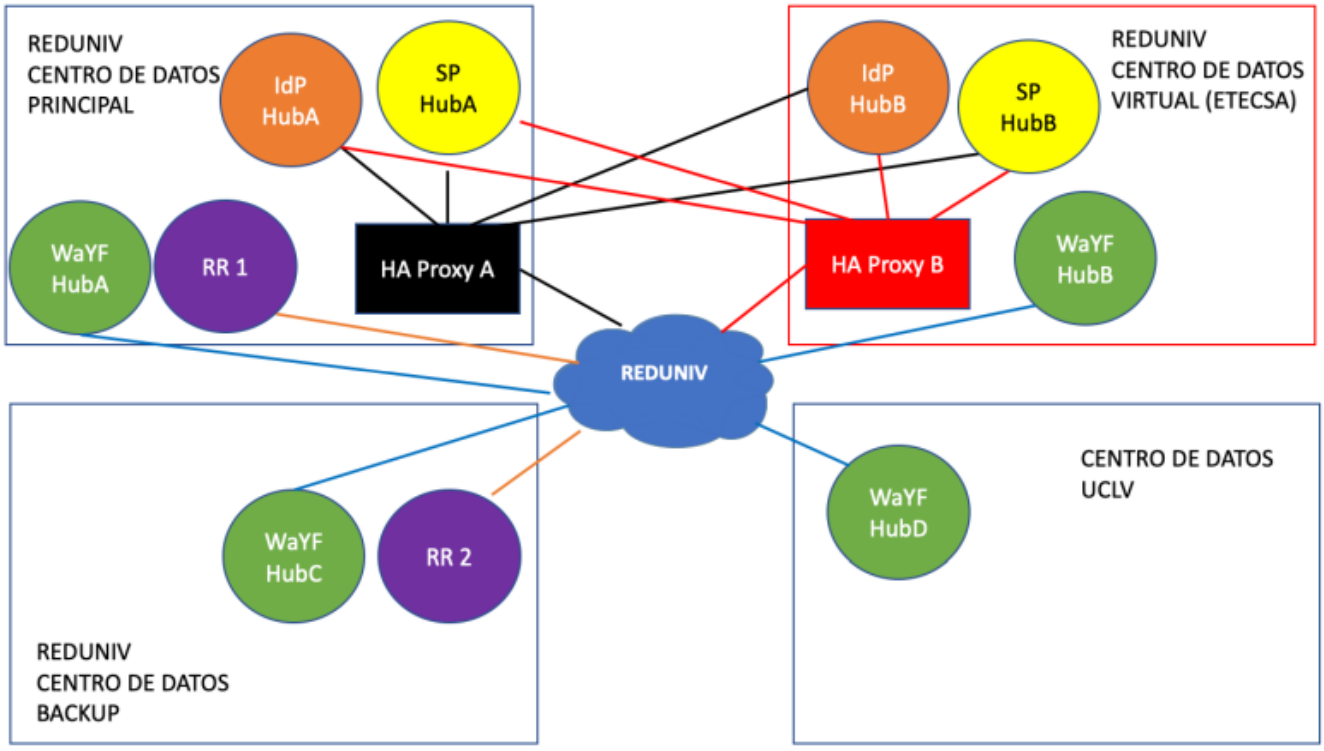

Figura 4. Implementación de servicios en el hub en la federación de identidad de REDUNIV

La implementación del servicio de federación de identidad de REDUNIV, se concibe en cuatro etapas que permitieron 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 determinaron a partir de las condiciones tecnológicas (equipamiento y equipo de administración), las que constituyeron una base para consolidar el proceso. De igual manera, fue importante resaltar el carácter novedoso de estas tecnologías en el país; por lo que fue 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: seis meses)

- Se crea en REDUNIV, de servicios de la federación (IDP, SP, WAYF) en centro de datos principal de la red. En esta etapa, únicamente se instala una instancia de cada servicio y se preparan 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.
- Se habilita servidor de tiempo (NTP) en REDUNIV.
- Se capacita a los administradores de todas las redes componentes de REDUNIV.
- Se crea 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.
- Se elabora de las normativas de participación en la federación; así como para publicar servicios.

Etapa 2 (tiempo estimado de duración: seis meses)

- Se valida el diseño y se realizan las correcciones que sean pertinentes.
- Se instalan proveedores de identidad en la Universidad de Granma (UDG), Universidad de Pinar del Río (UPR), Universidad Agraria de la Habana (UNAH), Universidad de Guantánamo (UG), Universidad de Ciego de Ávila (UNICA) y Universidad de Camagüey (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.
- Se crea y pone en funcionamiento, la primera instancia del registro de recursos de la federación.
- Se identifican posibles servicios adicionales a federar.

Etapa 3 (tiempo estimado de duración: 6 meses)

- Se valida el diseño y se realizan las correcciones que sean pertinentes.
- Se agregan nuevos proveedores de servicios (identificados en la segunda etapa).
- Se agregan proveedores de identidad, en todas las Instituciones pertenecientes a REDUNIV, que aún no se han conectado a la federación.
- Se instala el compilador de metadatos en centro de datos principal de REDUNIV.
- Se instalan las dos instancias restantes del servicio WAYF (en centro de datos backup de REDUNIV y en centro de datos de UCLV).

- Se instala 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.
- Se diseñar y realiza el ejercicio de interconexión con otra federación.

Etapa 4 (tiempo estimado de duración: 12 meses)

- Participación en federaciones regionales/internacionales.

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 que a través del establecimiento de relaciones de confianza entre las organizaciones que los desarrollan, se interconectan entre sí y permiten 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 seleccionaron como estándar para su implementación en REDUNIV, propuesta que se estructuró en cuatro etapas bien definidas que permitieron la introducción gradual de la tecnología. El diseño presentado satisfizo las condiciones establecidas, donde los bajos requerimientos en cuanto a recursos tecnológicos y humanos para su implementación hicieron muy viable su introducción en un corto período de tiempo.

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

REFERENCIAS BIBLIOGRÁFICAS

Cadenas, L. E. (2020). El rol de las redes nacionales de investigación y educación en las Ciencias Sociales. *Disertaciones*, 13(1) https://doi.org/10.12804/revistas.urosario.edu.co/disertaciones/a.7608

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.

Simone. (2022). Digital *Identity: The international landscape of active systems*. Politecnico Milano.

Dib, O. y Toumi, K. (2020). Decentralized Identity Systems: Architecture, Challenges, Solutions and Future Directions, *AETiC*, 4(5), pp. 19-40. https://doi.org/10.33166/AETiC.2020.05.002

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.

Haddouti, S. E. (2015). Towards an Interoperable Identity Management Framework: a Comparative Study. *International Journal of Computer Science Issues*, 12(6), 2015. https://arxiv.org/abs/1902.11184

Geant. (2023). *Federation Architectures* - eduGAIN - GÉANT federated confluence. https://wiki.geant.org/display/eduGAIN/Federation+Architectures

Conflicto de intereses

Los autores declaran no tener conflictos de intereses.

Contribución de los autores

Todos los autores revisaron la redacción del manuscrito y aprueban la versión finalmente remitida.