



## COFRe: Comunidad Federada REUNA

### Apéndice WebSSO para Organizaciones Proveedoras de Identidad

Versión 2.1 - 21/01/2021



Este documento está bajo licencia [Creative Commons Attribution-ShareAlike3.0 Unported License](https://creativecommons.org/licenses/by-sa/3.0/).

## Tabla de Contenido

1. Definiciones y Terminología.....	3
2. Introducción.....	3
3. Obligaciones de la Organización Proveedora de Identidad para el perfil WebSSO.....	4
3.1 Obligaciones y Derechos del Operador de la Federación.....	4
3.2 Obligaciones y Derechos de la Organización Proveedora de Identidad.....	4
4. Elegibilidad.....	5
5. Modificación.....	5

## 1. Definiciones y Terminología

En el contexto de este documento

Atributo	Pieza de información que describe al Usuario Final, sus propiedades y/o sus roles dentro de una Organización.
Autenticación	Proceso mediante el que se verifica la identidad de un Usuario Final previamente registrado.
Autorización	Proceso de garantizar o denegar a un Usuario Final previamente autenticado, derechos de acceso a un servicio.
Usuario Final	Una persona natural afiliada a una Organización Proveedora de Identidad, e.g. empleado, investigador, profesor o estudiante, haciendo uso del o los servicios de un Proveedor de Servicio.
Federación	La Federación de Identidad. Una asociación de organizaciones las que se unen para intercambiar información, tanto de sus usuarios como de sus recursos, según lo convenido, con la finalidad de permitir la colaboración y transacciones.
Operador de la Federación	Organización que provee de la Infraestructura para la Autenticación y Autorización de el o los Miembros de la Federación.
Miembro de la Federación	Una organización que se ha unido a la Federación aceptando por escrito las Reglas de la Federación. Dentro de la Federación, un Miembro de la Federación puede ser una Organización Proveedora de Identidad y/o un Proveedor de Servicio.
Organización Proveedora de Identidad o IdP	Organización en la cual un Usuario Final está afiliado. Esta organización es responsable de la autenticación del Usuario Final y de administrar la Identidad Digital de sus Usuarios Finales.
Administración de la Identidad	Proceso de emitir y administrar las identidades digitales de usuarios finales.
Proveedor de Servicio o SP	Organización responsable de ofrecer al Usuario Final el o los servicios que este pretende usar. Los SP pueden confiar en el resultado de la autenticación y atributos que los IdP validan de sus Usuarios Finales.
Metadata de la Federación	Archivo en formato SAML/XML que contiene información respecto de los Miembros de la Federación.
Servicio de Descubrimiento	Servicio administrado por el Operador de la Federación pensado para los Miembros de la Federación que actúan como Proveedores de Servicio, el que ofrece una lista de las Organizaciones Proveedoras de Identidad de la Federación.
Perfiles de Nivel de Garantía	Modelos o buenas prácticas usados por la Organización Proveedora de Identidad como guía en el proceso de validación y aseguramiento de una identidad digital con un Usuario Final (e.g. NIST 800-63-3)

## 2. Introducción

Este documento describe los pasos involucrados en el proceso de afiliación de una Organización Proveedora de Identidad para el perfil de WebSSO.

### **3. Obligaciones de la Organización Proveedora de Identidad para el perfil WebSSO**

#### **3.1 Obligaciones y Derechos del Operador de la Federación**

Esta Federación es operada por REUNA, la Red Nacional para Investigación y Educación Chilena.

Además de lo señalado en cualquier otra sección de las Reglas de la Federación, REUNA es responsable de:

- La gestión operativa segura y confiable de la Metadata de la Federación y del Servicio de Descubrimiento.
- Publicar la información acerca de los Atributos necesarios para cada Proveedor de Servicio.

#### **3.2 Obligaciones y Derechos de la Organización Proveedora de Identidad**

Además de lo señalado en cualquier otra sección de las Reglas de la Federación, si un Miembro de la Federación es una Organización Proveedora de Identidad, ella:

- Se encargará de entregar y gestionar las credenciales de Autenticación de sus Usuarios Finales, así como de autenticarlos, tal y como se especifica en sus perfiles de nivel de garantía.
- Debería entregar su Declaración de Práctica de Gestión de Identidades a REUNA, que a su vez la facilitará a otros Miembros de la Federación si la solicitan. La Declaración de Práctica de Gestión de Identidades es una descripción del ciclo de vida de la Gestión de Identidades, que incluye una descripción de cómo las identidades digitales individuales se registran, mantienen y eliminan del sistema de gestión de identidades. La declaración deberá contener descripciones de los procesos administrativos, las prácticas y las tecnologías significativas que se utilizan en el ciclo de vida de la gestión de identidades y que deberán ser capaces de contribuir a un ciclo de vida de la gestión de identidades seguro y consistente. Los perfiles de nivel de garantía podrán imponer requisitos específicos.
- Garantizará que un Usuario Final cumple con la Política de Uso Aceptable de la Organización Proveedora de Identidad.
- Tendrá operativo un Centro de Asistencia Técnica para sus Usuarios Finales, con respecto a cuestiones relacionadas con los servicios de la Federación. Se anima a las Organizaciones Proveedoras de Identidad a que mantengan un Centro de Asistencia Técnica para responder a las consultas de los usuarios, al menos durante el horario de oficina normal en la zona horaria local. Las Organizaciones Proveedoras de Identidad no deberán remitir las consultas de los Usuarios Finales directamente a REUNA, y deberán esforzarse al máximo por garantizar que los

correspondientes contactos de la Organización Proveedora de Identidad solo envíen problemas y consultas relevantes a REUNA.

- Se encargará de asignar valores de Atributos a los Usuarios Finales y de gestionar los valores para asegurarse de que están actualizados.
- Se encargará de comunicar los Atributos a los Proveedores de Servicio.
- Se encargará de mantener su Metadata actualizada. Si hay algún cambio en esta, el responsable técnico deberá notificar a REUNA de este hecho.
- Al momento de cancelar su membresía con la Federación, deberá enviar una lista de los Proveedores de Servicio con los cuales estaba relacionada.

#### **4. Elegibilidad**

Las instituciones socias de REUNA pueden solicitar directamente aplicar como Organización Proveedora de Identidad. Para otras instituciones, su solicitud deberá ser estudiada y se tomará la resolución, la cual será informada vía correo electrónico en un plazo máximo de 15 días, desde la recepción de esta.

#### **5. Modificación**

REUNA tiene derecho a corregir eventualmente las Reglas de la Federación. Dichos cambios deberán ser revisados por REUNA y deberán comunicarse por escrito a todos los Miembros de la Federación, en un plazo de, al menos, 90 días antes de que entren en vigor.