



Ministério da  
**Cultura**

Ministério da  
**Saúde**

Ministério da  
**Educação**

Ministério da  
**Ciência, Tecnologia  
e Inovação**



# Creación de Federación de Identidad para las Redes Académicas

Julho/2013



## Índice – Parte 1

- Introdução y presentación
- Sobre el curso
- Federaciones de identidad
- Elementos y conceptos de una federación
- Arquitectura de una federación



# Introducción y presentación



# Sobre el curso

Ministério da  
Cultura

Ministério da  
Saúde

Ministério da  
Educação

Ministério da  
Ciência, Tecnologia  
e Inovação

GOVERNO FEDERAL  
**BRASIL**  
PAÍS RICO É PAÍS SEM POBREZA

# Sobre el curso

- Conceptos básicos sobre federaciones
- Primeros pasos para el SSO
- Actividades técnicas
- Configuración de entidades



# Federaciones de Identidad

Ministério da  
Cultura

Ministério da  
Saúde

Ministério da  
Educação

Ministério da  
Ciência, Tecnologia  
e Inovação

GOVERNO FEDERAL  
**BRASIL**  
PAÍS RICO É PAÍS SEM POBREZA

# Federaciones de Identidad

- Motivación para la creación de federaciones
  - Acceso a recursos y servicios restringido a dominios específicos
  - Controlar el acceso de un usuario a un recurso

# Federaciones de Identidad

- Soluciones posibles...
  - Una cuenta para cada servicio, por usuario
    - Problema para el usuario: debe acordarse de muchos nombres y contraseñas
    - Problema para el administrador del sistema: definición de permisos diferentes para cada cuenta de cada usuario
  - Cuenta única para departamentos o para clases de usuarios
    - Problema para el usuario: no hay como diferenciar los derechos de un usuario
    - Problema para el administrador del sistema: no hay como hacer una auditoría



# Federaciones de Identidad

... o una federación!



# Federaciones de Identidad

... o una federación!

- ¿Qué es?
  - Red de confianza en que cada institución es responsable por realizar la autenticación y proveer informaciones sobre sus usuarios hasta servicios autorizados
  - Sus conceptos están basados en una infraestructura de autenticación y autorización interdomínios, que permite a los usuarios que mantengan todos sus atributos en la institución de origen y acceder a los recursos ofrecidos por la federación
  - Los servicios de la federación deben estar basados en las relaciones de confianza definidas por la RNIE

# Federaciones de Identidad

- Federaciones existentes actualmente

Austria - ACOnet	Hungría - eduID.hu
Australia - AAF	Irlanda - Edugate
Bélgica - Belnet	Italia - IDEM
Brasil - CAFE	Japón - GakuNin
Canadá - CAF	Letonia - LAIFE
Suiza - SWITCHaai	Holanda - SURFfederatie
Chile - COFRe	Noruega - FEIDE
República Checa - eduID.cz	Nueva Zelanda - Tuakiri New Zealand Access Federation
Alemania - DFN-AAI	Portugal - RCTSaai
Dinamarca - WAYF	Suecia - SWAMID
Estonia - TAAT	Eslovaquia - ArnesAAI Slovenska
España - SIR	Reino Unido - UK Access Management Federation for Education and Research
Finlandia - Haka	Estados Unidos - InCommon
Francia - Fédération Éducation-Recherche	Internacional - IGTF
Grecia - GRNET	
Croacia - AAI@EduHr	

30 federaciones, más 6 federaciones piloto

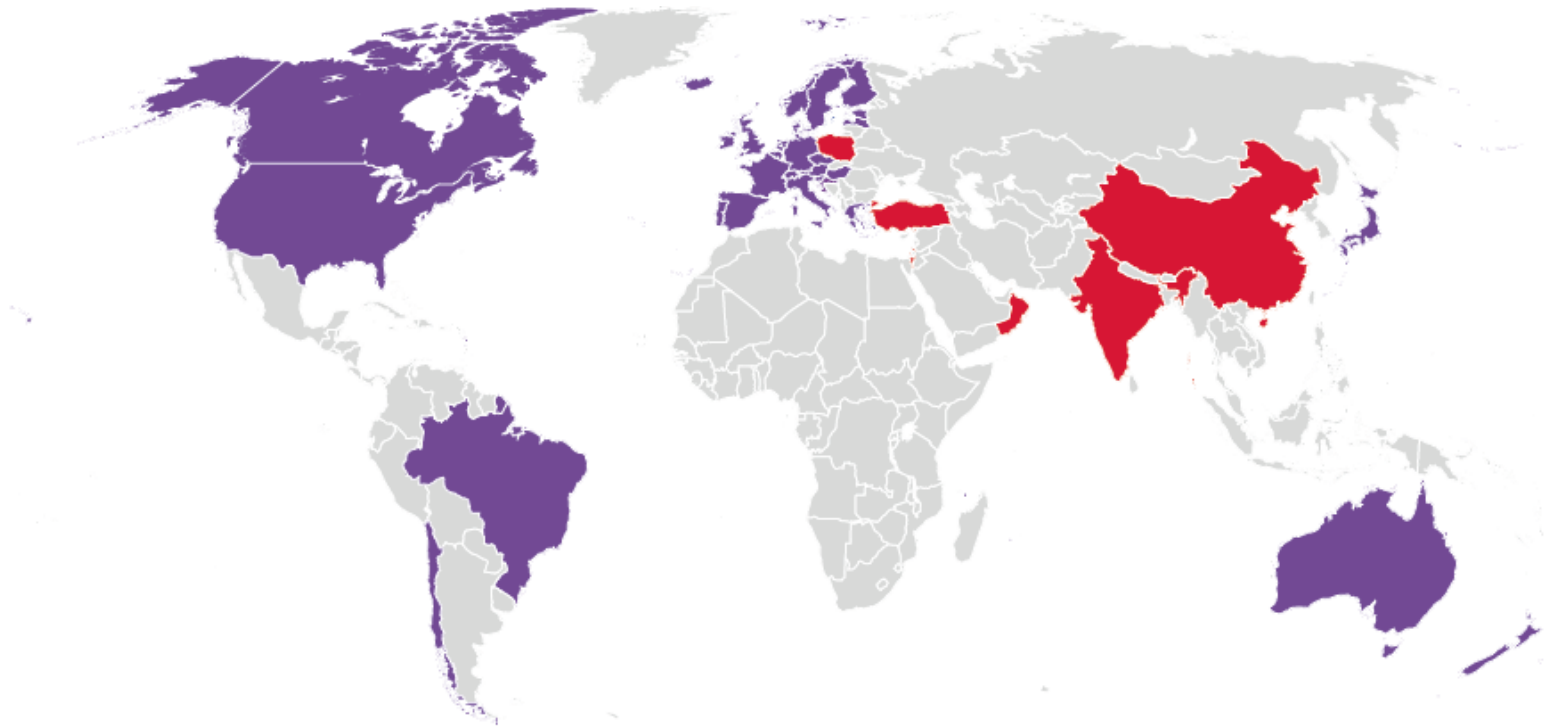
# Federaciones de Identidad

- REFEDS - Research and Education Federations
  - Tiene por objetivo el cambio de procesos, prácticas y políticas de federaciones de identidad, y también de favorecer la discusión de modos de facilitar la comunicación entre federaciones
  - REFEDS mantiene una lista de todas las federaciones que trabajan asociadas a instituciones de enseñanza y investigación



# Federaciones de Identidad

- REFEDS – Mapa de instituciones



**REFEDS**

# Federaciones de Identidad

- REFEDS – Discovery Guide
  - Una documentación recién publicada por REFEDS es el *Discovery Guide*, una guía sobre como presentar la identidad federada a sus usuarios, buenas prácticas en federaciones y ejemplos de como tener una buena experiencia de utilización

<http://discovery.refeds.org/>

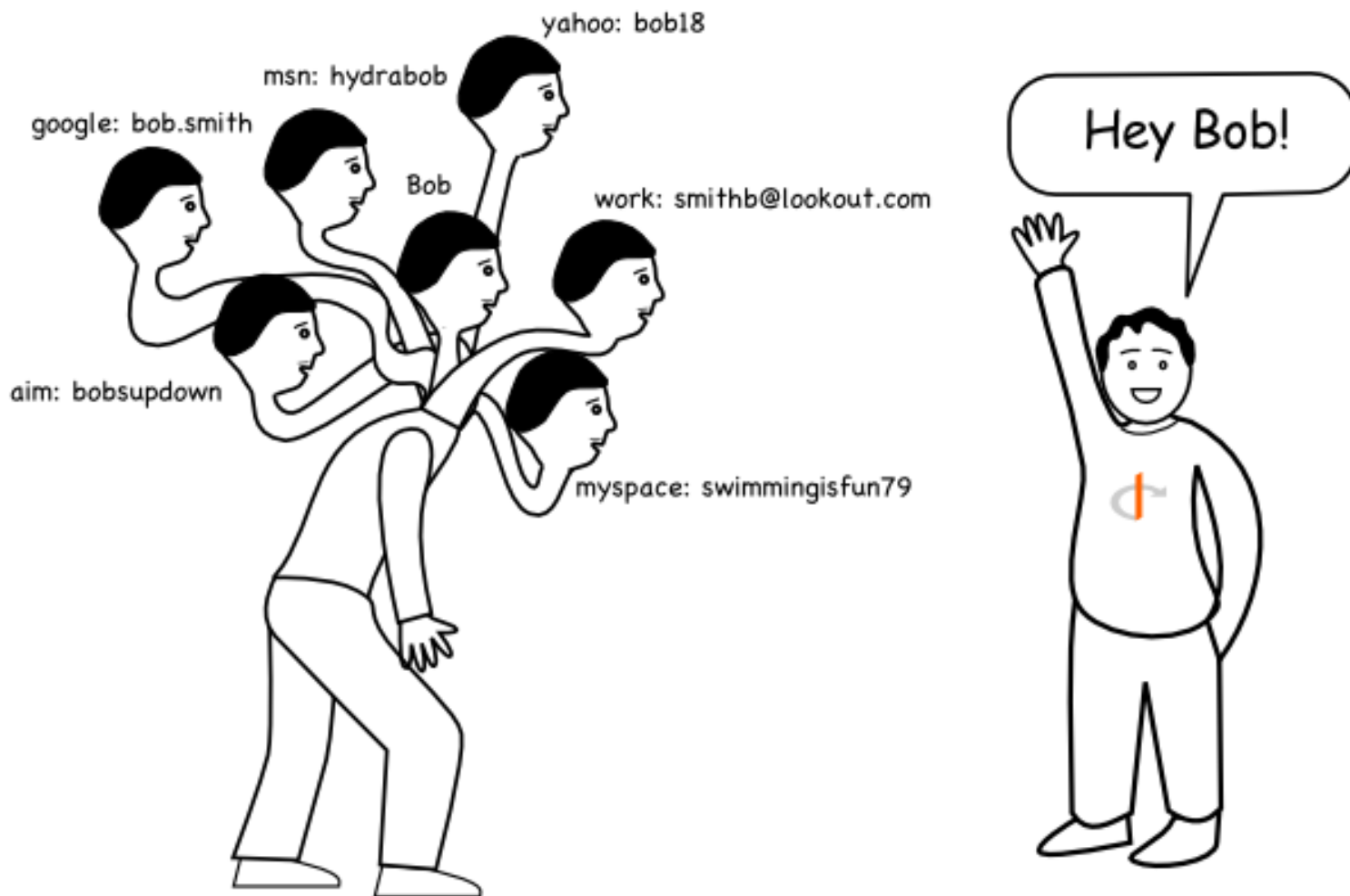




# Elementos y conceptos de una federación

# Elementos y conceptos de una federación

- Single Sign-on (SSO)





# Elementos y conceptos de una federación

- Single Sign-on (SSO)
  - Mecanismo que posibilita que un usuario pueda acceder a múltiples servicios con una única acción de autenticación
  - Mientras el token de autenticación sea válido, el usuario no tendrá que se autenticar de nuevo en cualquier servicio de la federación
  - Utilización de las credenciales académicas para acceso a todos los servicios de la federación
  - Asociación con la base de datos académica a través de un LDAP
  - Definición de esquemas para uniformizar la comunicación y el cambio de atributos

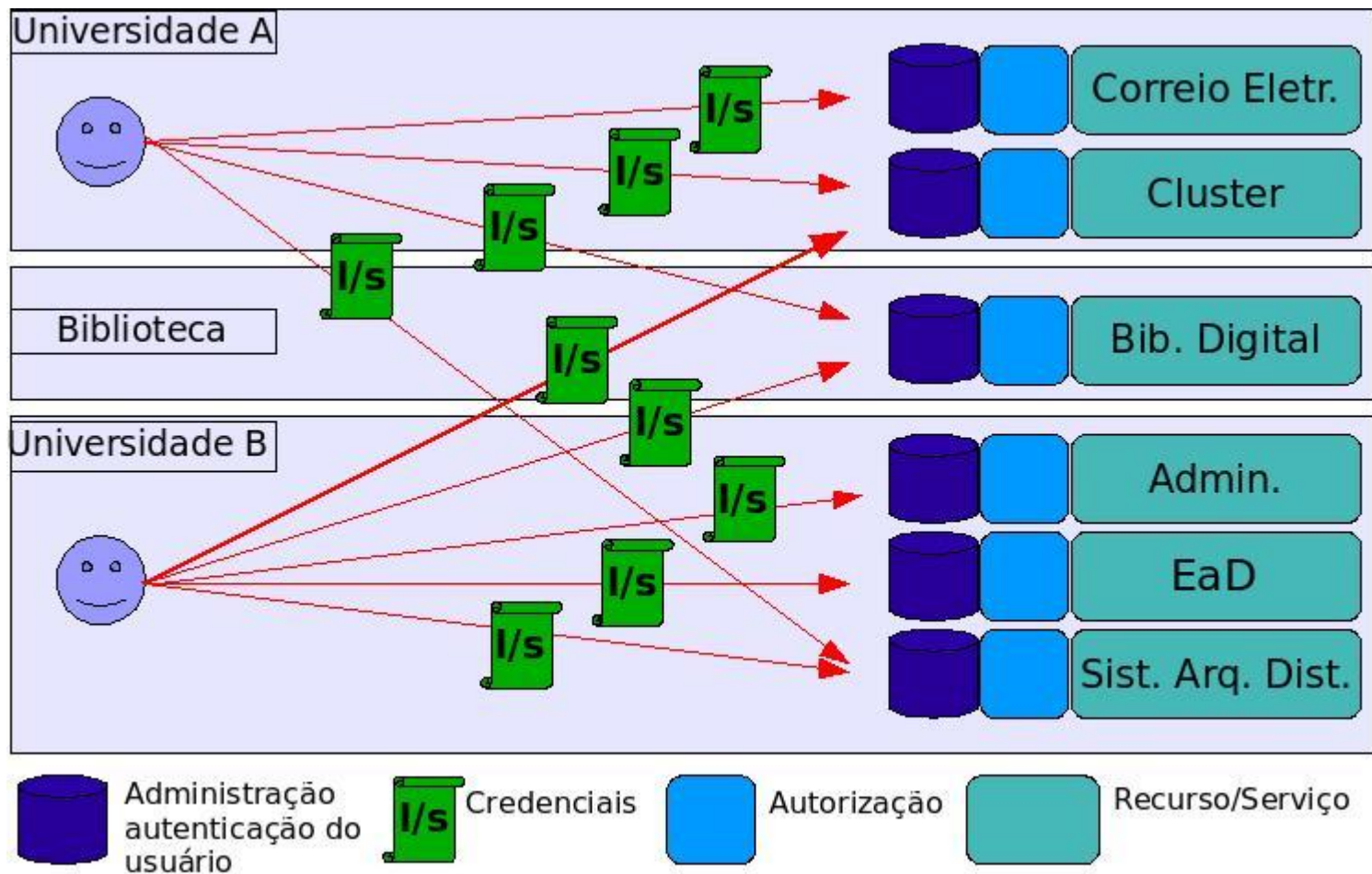
# Elementos y conceptos de una federación

- Single Sign-on (SSO): herramientas más utilizadas en federaciones académicas



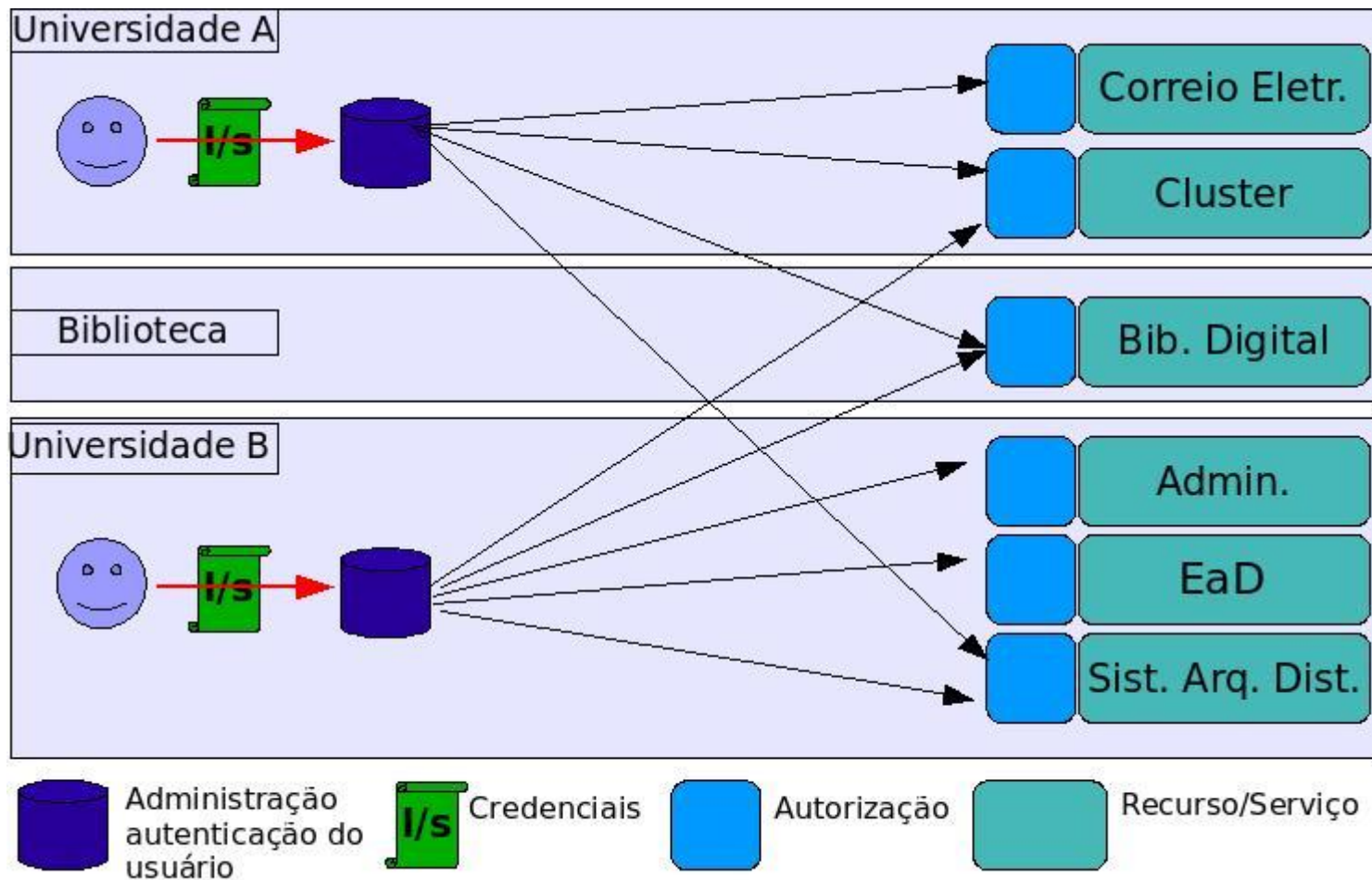
# Elementos y conceptos de una federación

- Single Sign-on (SSO): antes...



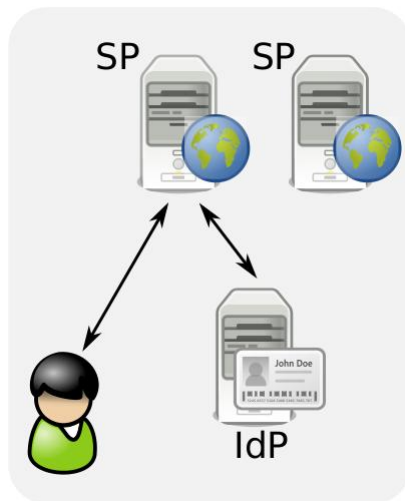
# Elementos y conceptos de una federación

- Single Sign-on (SSO): ... y después



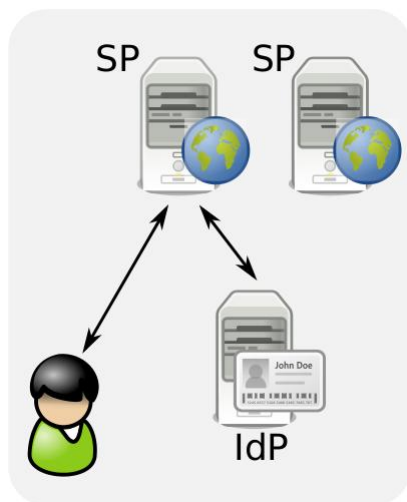
# Elementos y conceptos de una federación

- Proveedor de identidad (IdP)
  - Elemento que realiza la autenticación del usuario y fornece sus atributos al servicio
  - Fornece un token de autenticación al servicio, conteniendo informaciones como los atributos del usuario
  - Integrase con el sistema de autenticación institucional para proveer autenticación y atributos a un servicio



# Elementos y conceptos de una federación

- Proveedor de identidad: ejemplos
  - Proveedor de una RNIE: RNP, InCommon, REUNA
  - Proveedor de una universidad: USP, INICTEL, PUC
  - Proveedor de otras instituciones de enseñanza e investigación: ministerios, museos, laboratorios, centros de investigación, ...



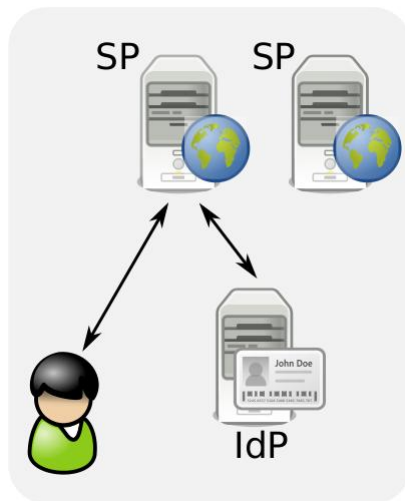
# Elementos y conceptos de una federación

- LDAP (Lightweight Directory Access Protocol)
  - Directorio que mantiene las credenciales de autenticación y de los atributos de cada usuario
  - Es consultado por el IdP para realizar la autenticación



# Elementos y conceptos de una federación

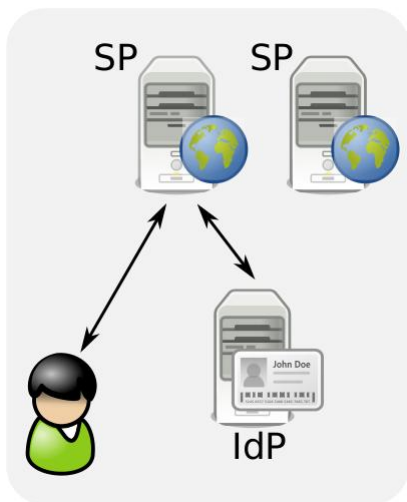
- Proveedor de servicios
  - Representa un servicio que puede ser utilizado por los miembros de la federación
  - Después de recibir los atributos de un usuario, enviado por su IdP, puede hacer su autorización para uso del servicio
  - Puede también restringir el acceso del usuario a recursos de acuerdo con los atributos recibidos





# Elementos y conceptos de una federación

- Proveedor de servicios: ejemplos
  - Sistemas académicos, acceso a bibliotecas de universidades, repositorios y bancos de publicaciones
  - Compra de libros y software con beneficios a instituciones
  - Almacenamiento y cambio de archivos



# Elementos y conceptos de una federación

- Discovery Service
  - Servicio para descubierta de la institución de origen del usuario
  - El usuario es direccionado a la página de autenticación de su institución



# Elementos y conceptos de una federación

- Discovery Service: ejemplos  
— EDS (Shibboleth)

Meu Espaço

Acesso remoto ao Portal de Periódicos via CAFe - RNP

Selecione uma instituição

ENVIAR

Tutorial

Para utilizar a identificação por meio da CAFe, sua instituição deve aderir a esse serviço provido pela Rede Nacional de Ensino e Pesquisa (RNP).

[Clique aqui para mais informações.](#)

Selecione uma instituição

Selecione uma instituição

ASSOCIAÇÃO INSTITUTO NACIONAL DE MATEMÁTICA PURA E APLICADA  
COORDENAÇÃO DE APERFEIÇOAMENTO DE PESSOAL DE NÍVEL SUPERIOR  
ESCOLA BAHIANA DE MEDICINA E SAÚDE PÚBLICA  
ESCOLA NACIONAL DE CIÊNCIAS ESTATÍSTICAS  
FUNDAÇÃO UNIVERSIDADE FEDERAL DE MATO GROSSO DO SUL  
FUNDAÇÃO UNIVERSIDADE FEDERAL DO AMAPÁ  
INSTITUTO BRASILEIRO DE INFORMAÇÃO, CIÊNCIA E TECNOLOGIA  
INSTITUTO EVANDRO CHAGAS  
INSTITUTO FEDERAL DE GOIÁS  
INSTITUTO FEDERAL DE MATO GROSSO  
INSTITUTO FEDERAL DO ESPÍRITO SANTO  
INSTITUTO FEDERAL DO PIAUÍ  
INSTITUTO NACIONAL DE PESQUISAS DA AMAZÔNIA  
MUSEU DE ASTRONOMIA E CIÊNCIAS AFINS  
OBSERVATÓRIO NACIONAL  
PONTIFÍCIA UNIVERSIDADE CATÓLICA DE CAMPINAS  
PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS  
PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL  
REDE NACIONAL DE ENSINO E PESQUISA

# Elementos y conceptos de una federación

- Discovery Service: ejemplos
  - EDS
  - DiscoJuice (UNINETT)





Sign in to Foodle  
Select your Provider

- UFPA - Universidade Federal do Para  
Brazil Nas proximidades
- PUCMINAS - Pontificia Universidade Catolica de Minas Gerais  
Brazil Nas proximidades
- UNIR - Universidade Federal de Rondonia  
Brazil Nas proximidades
- RNP - Rede Nacional de Ensino e Pesquisa  
Brazil Nas proximidades
- UVA - Universidade Estadual Vale do Acaraú  
Brazil Nas proximidades
- ENCE - Escola Nacional de Ciencias Estatísticas (IBGE)  
Brazil Nas proximidades
- UFGD - Universidade Federal da Grande Dourados  
Brazil Nas proximidades
- UPF - Universidade de Passo Fundo  
Brazil Nas proximidades
- UNIFAP - Universidade Federal do Amapá  
Brazil Nas proximidades
- INPA - Instituto Nacional de Pesquisas da Amazonia

Q pu pesquise um fornecedor de identidade, como por exemplo Universi

▸ Preciso de ajuda, não encontro o meu fornecedor de identidade

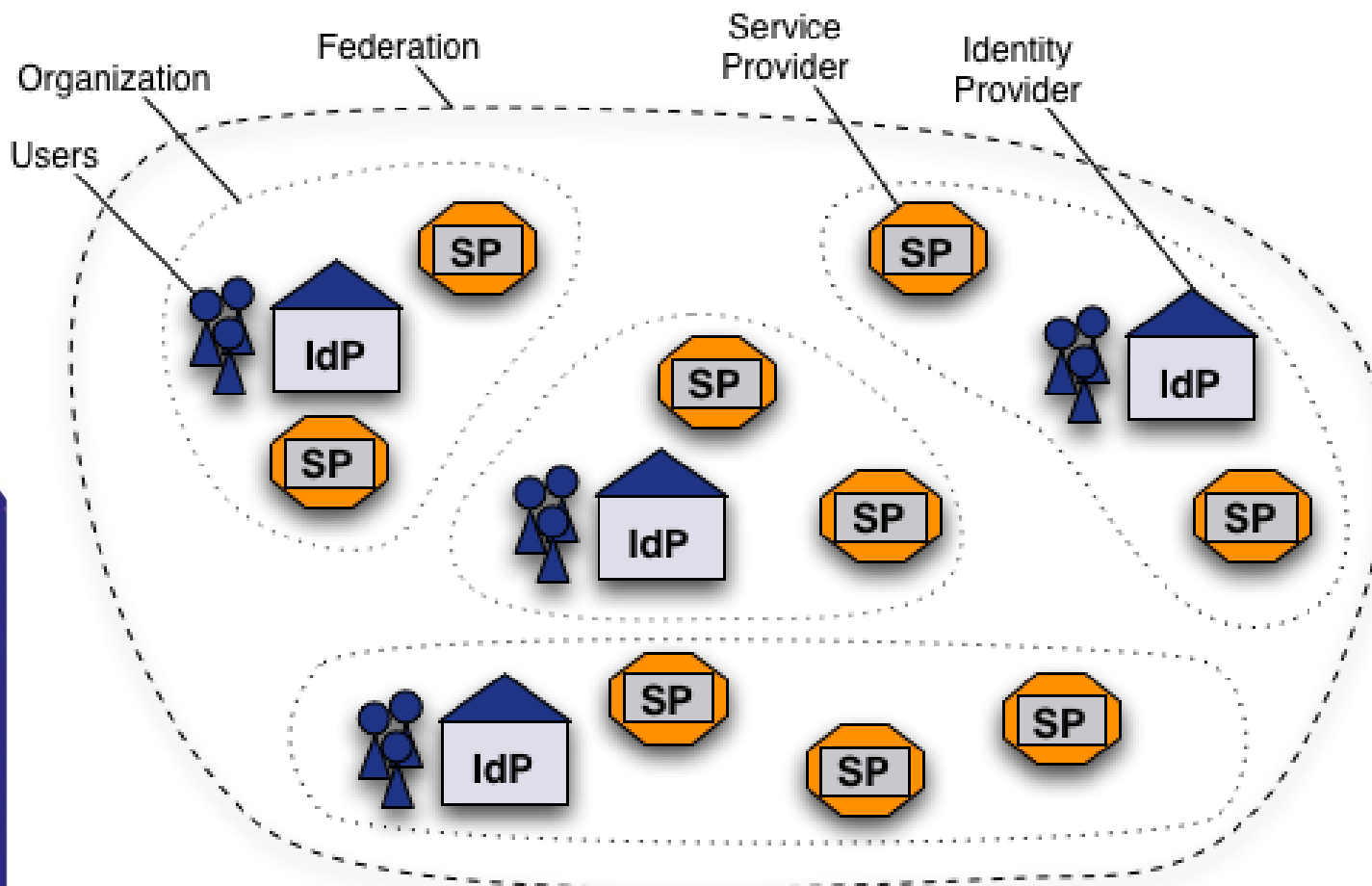
 Identificar a minha localização e visualizar os fornecedores de identidade nas proximidades

Visualizar fornecedores de identidade em  

visualizar todos os países

# Elementos y conceptos de una federación

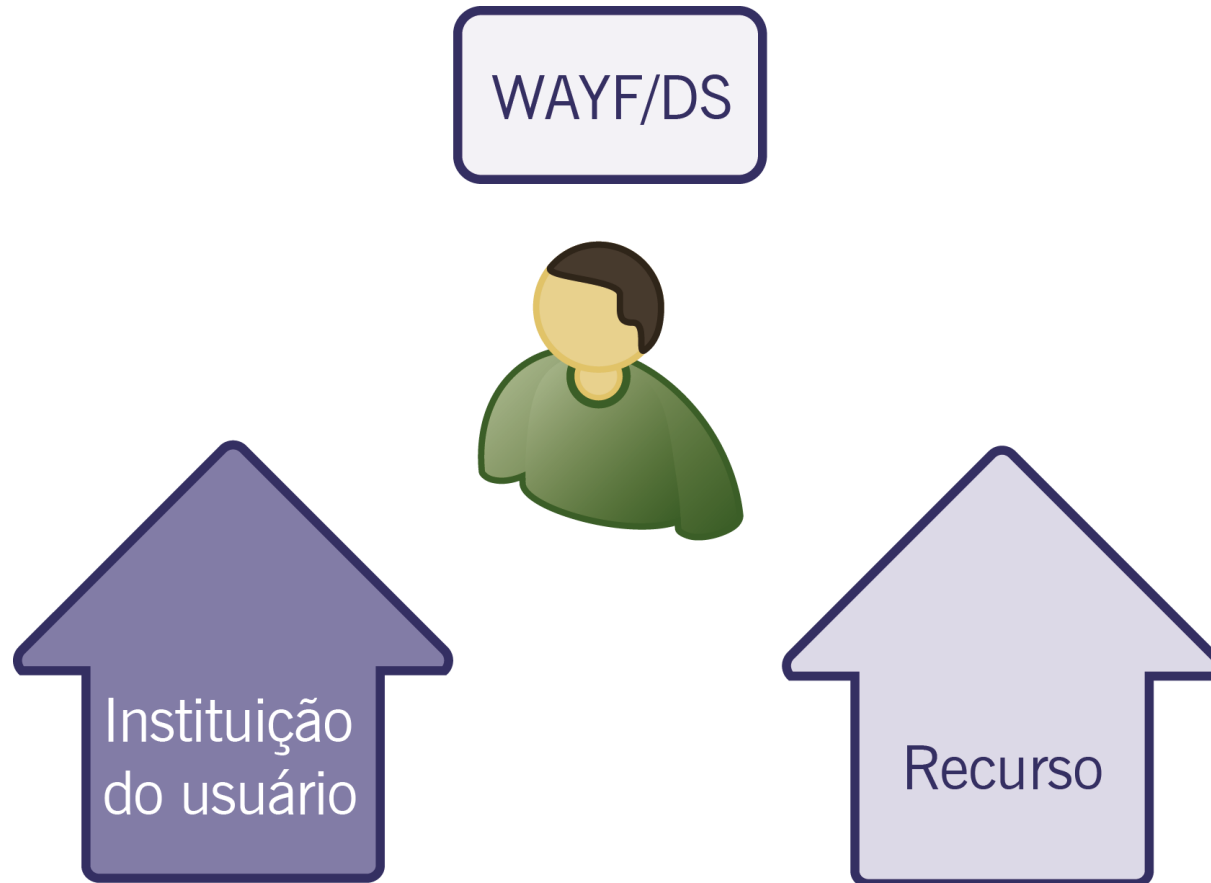
- La interconexión de todas las entidades



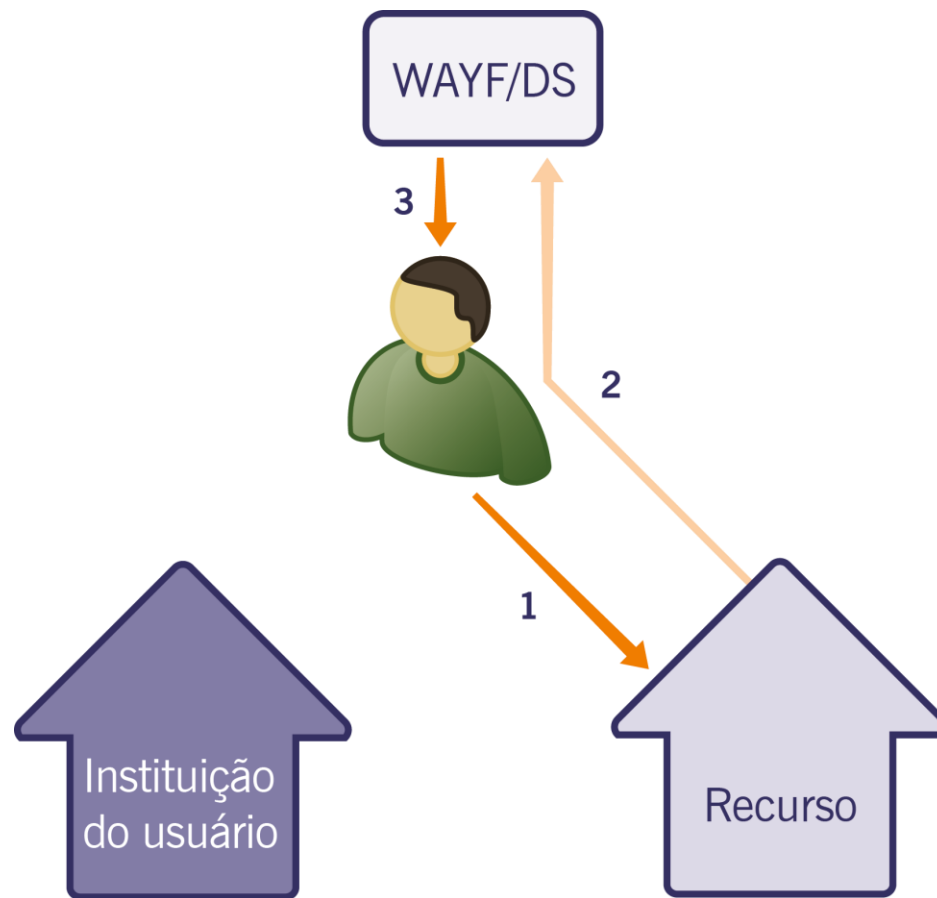


# Arquitectura de una federación

# Arquitectura de una federación



# Arquitetura de uma federação

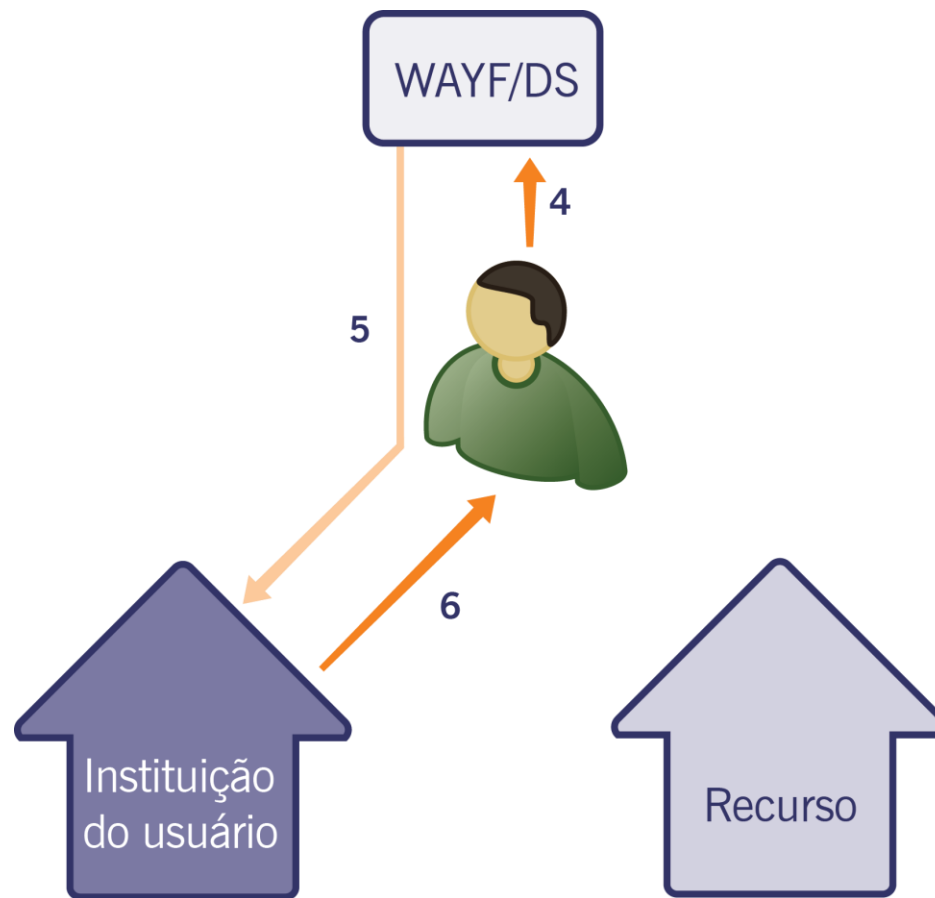


- ➔ Requisição/Resposta HTTP
- ➔ Redirecionamento HTTP
- ➔ Conexão servidor/servidor

Fuente: ESR-RNP



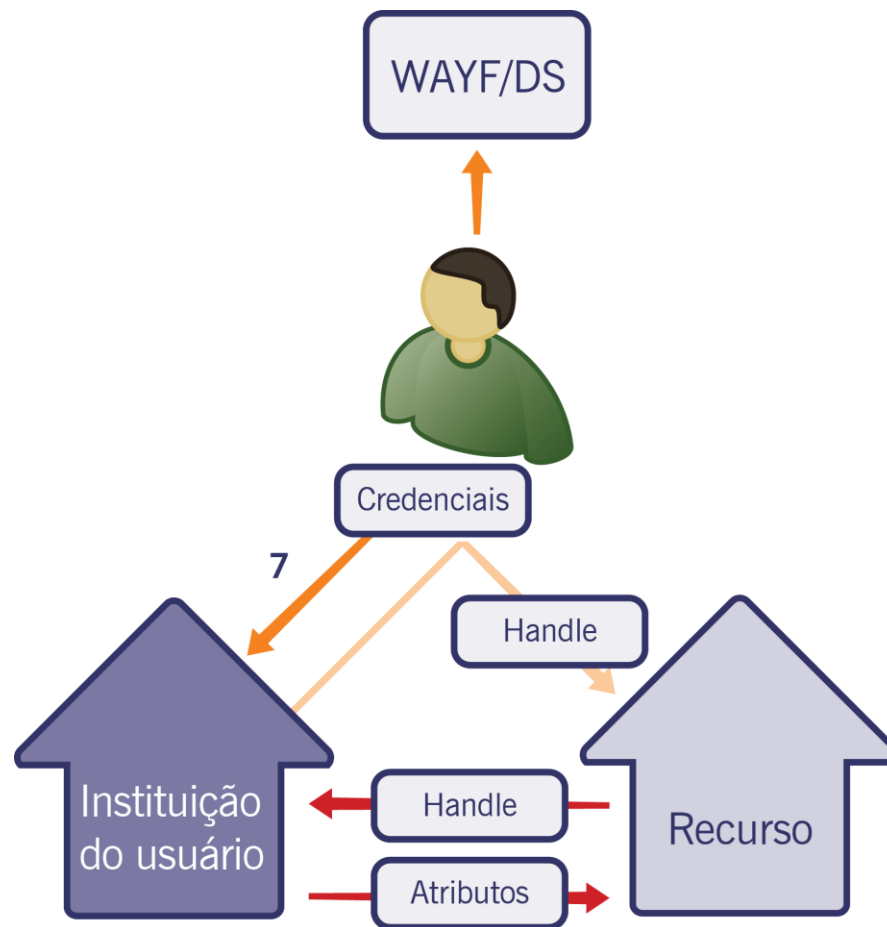
# Arquitetura de uma federação



- ➔ Requisição/Resposta HTTP
- ➔ Redirecionamento HTTP
- ➔ Conexão servidor/servidor

Fuente: ESR-RNP

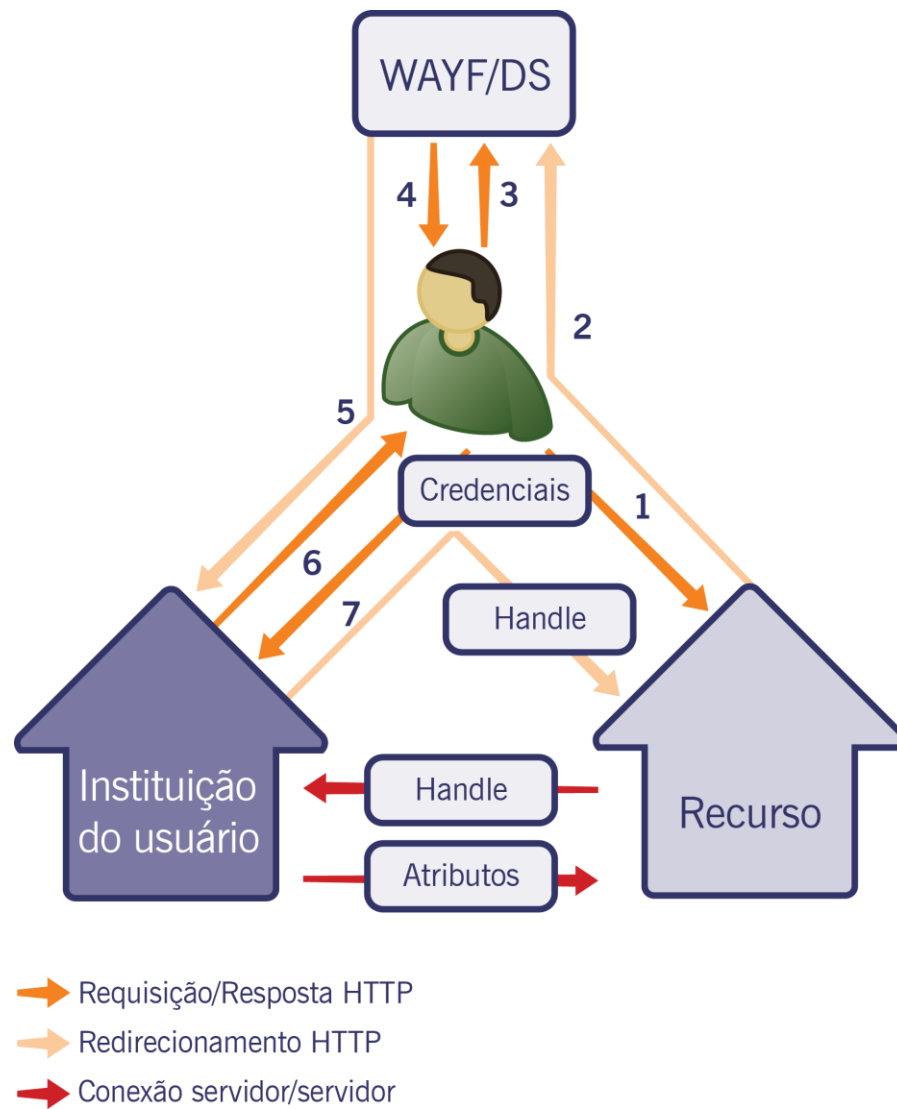
# Arquitectura de una federación



- ➔ Requisição/Resposta HTTP
- ➔ Redirecionamento HTTP
- ➔ Conexão servidor/servidor

Fuente: ESR-RNP

# Arquitetura de una federación



# Arquitectura de una federación

- Demostración de autenticación y autorización – Portal CAPES

The screenshot displays the CAPES Periodicos portal. At the top, there is a navigation bar with the logo 'periodicos.' and 'CAPES'. To the right, there are links for 'MAPA DO SITE', 'FALE CONOSCO', 'MEU ESPAÇO', 'TAMANHO' (with 'A+' and 'A-' buttons), and 'CONTRASTE' (with 'A' and 'A-' buttons). Below this is a secondary navigation bar with 'PÁGINA INICIAL', 'INSTITUCIONAL', 'ACERVO', 'BUSCA', 'NOTÍCIAS', and 'SUPPORTO'. A breadcrumb trail indicates 'Você está aqui: [Página inicial](#)'. The main content area is divided into four search sections: 'Buscar assunto', 'Buscar periódico', 'Buscar livro', and 'Buscar base'. Each section has a search input field, a 'BUSCAR' button, and a 'Busca avançada' link. The 'Buscar periódico' and 'Buscar livro' sections also feature an alphabetical index (A-Z) and a 'Lista Completa' link. To the right of the search sections is a photograph of a woman, Daniela Savassi, sitting on a bench and using a laptop. A vertical caption reads 'Foto: Gustavo Leite'. Below the search sections are three columns of featured content: 'Notícias' with the article 'Pesquisas das engenharias na Begell House', 'Coleções' with 'American Society for Microbiology (ASM)' and 'Gale Virtual Reference Library', and 'Treinamentos' with 'Treinamento do Portal de Periódicos - UFMT'. The bottom right corner features the RNP logo.

# Arquitetura de uma federação

- Demonstração de autenticação e autorização – Portal CAPES



The screenshot shows the 'Meu Espaço' (My Space) login page of the CAPES Portal. At the top, there is a navigation bar with the CAPES logo and links for 'MAPA DO SITE', 'FALE CONOSCO', 'MEU ESPAÇO', 'TAMANHO', and 'CONTRASTE'. Below this is a secondary navigation bar with links for 'PÁGINA INICIAL', 'INSTITUCIONAL', 'ACERVO', 'BUSCA', 'NOTÍCIAS', and 'SUPORTE'. A breadcrumb trail indicates the user is on the 'Página inicial'. A secondary menu contains links for 'Missão e objetivos', 'Quem participa', 'Histórico', 'Documentos', and 'Estatísticas de uso'. The main content area is titled 'Meu Espaço' and contains two columns of text. The left column explains that this option allows saving content of interest and using other portal resources. It includes a login form with fields for 'Nome do usuário' and 'Senha', an 'ENVIAR' button, and links for 'Esqueci minha senha' and 'NOVO USUÁRIO'. The right column explains that this option allows remote access to the portal's content for the user's institution. It features the 'cafe' logo (comunidade acadêmica federada) and the text 'Usar identificação da minha instituição via federação CAFE - RNP'. At the bottom, there is a footer with contact information and a copyright notice for 2010.

MAPA DO SITE | FALE CONOSCO | **MEU ESPAÇO** | TAMANHO | CONTRASTE  
A+ A- | A A

PÁGINA INICIAL | INSTITUCIONAL | ACERVO | BUSCA | NOTÍCIAS | SUPORTE

Você está aqui: [Página inicial](#) | [Missão e objetivos](#) | [Quem participa](#) | [Histórico](#) | [Documentos](#) | [Estatísticas de uso](#)

## Meu Espaço

Esta opção permite guardar conteúdo de interesse no Meu Espaço e utilizar outros recursos do Portal.

Nome do usuário :

Senha:

**ENVIAR** [Esqueci minha senha](#)

**NOVO USUÁRIO** [\(Caso ainda não seja um usuário identificado.\)](#)

[Não recebi meu e-mail de confirmação de cadastro](#)

Esta opção permite o acesso remoto ao conteúdo do Portal de Periódicos disponível para sua instituição.

 **cafe** comunidade acadêmica federada

Usar identificação da minha instituição via federação [CAFe - RNP](#)

Setor Bancário Norte, Quadra 2, Bloco L, Lote 06, 11º andar - CEP 70040-020 - Brasília/DF - Tel (61)2022.6200 | FAX:(61)2022.6220  
© Copyright 2010 Periodicos.capes.gov.br

# Arquitetura de uma federação

- Demonstração de autenticação e autorização – Portal CAPES

Meu Espaço

Acesso remoto ao Portal de Periódicos via CAFe - RNP

Selecione uma instituição

ENVIAR

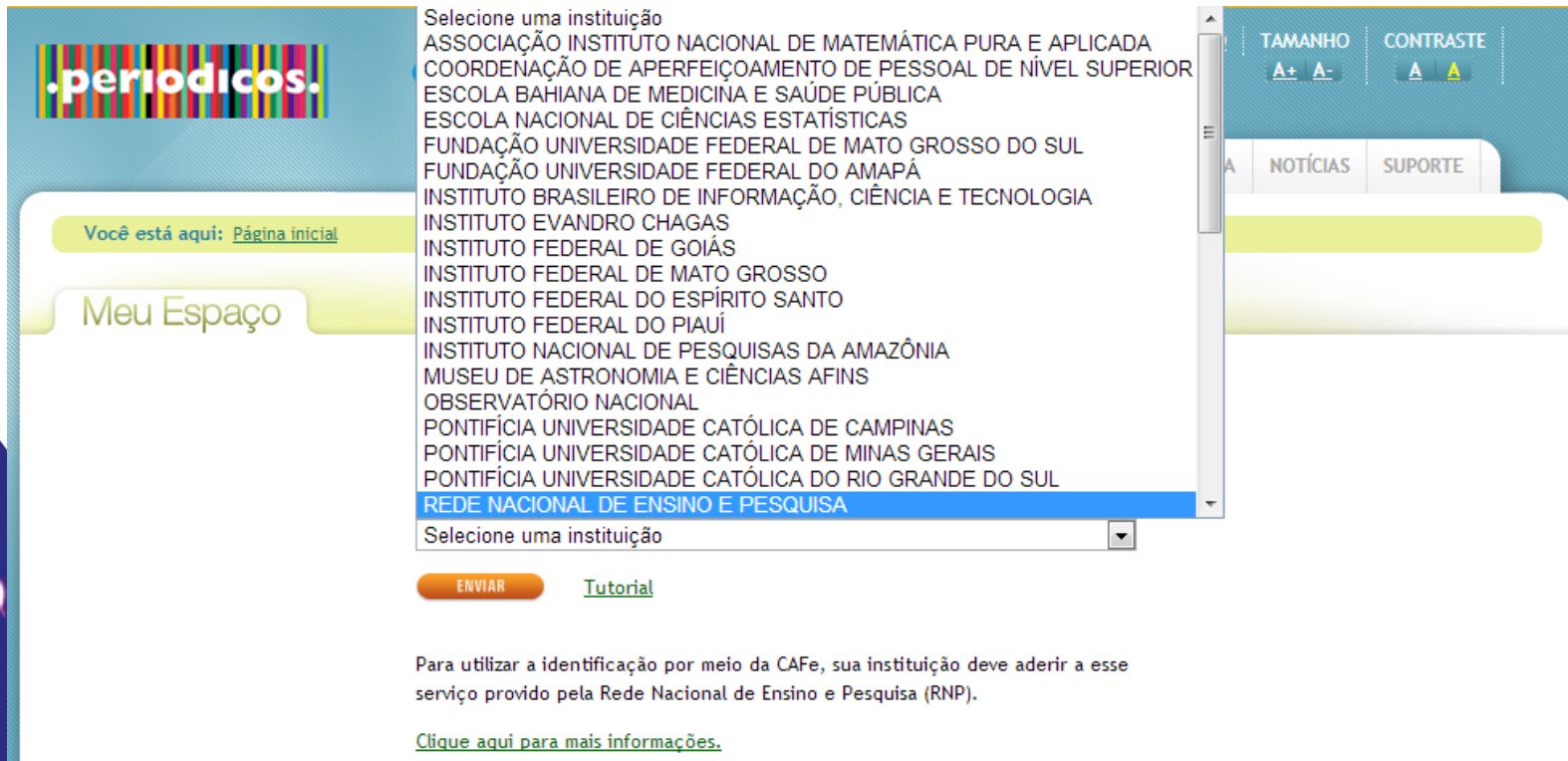
[Tutorial](#)

Para utilizar a identificação por meio da CAFe, sua instituição deve aderir a esse serviço provido pela Rede Nacional de Ensino e Pesquisa (RNP).

[Clique aqui para mais informações.](#)

# Arquitectura de una federación

- Demostración de autenticación y autorización – Portal CAPES



The screenshot displays the CAPES portal interface. On the left, there is a logo for ".periodicos." and a navigation bar with "Você está aqui: [Página inicial](#)" and "Meu Espaço". The main content area features a dropdown menu titled "Selecione uma instituição" with a list of institutions. The "REDE NACIONAL DE ENSINO E PESQUISA" option is highlighted in blue. Below the dropdown is an "ENVIAR" button and a "Tutorial" link. At the bottom, there is a paragraph of text and a link "Clique aqui para mais informações." On the right side of the page, there are controls for "TAMANHO" (font size) and "CONTRASTE" (contrast), and a navigation bar with "NOTÍCIAS" and "SUPPORTO".

Selecione uma instituição

ASSOCIAÇÃO INSTITUTO NACIONAL DE MATEMÁTICA PURA E APLICADA  
COORDENAÇÃO DE APERFEIÇOAMENTO DE PESSOAL DE NÍVEL SUPERIOR  
ESCOLA BAHIANA DE MEDICINA E SAÚDE PÚBLICA  
ESCOLA NACIONAL DE CIÊNCIAS ESTATÍSTICAS  
FUNDAÇÃO UNIVERSIDADE FEDERAL DE MATO GROSSO DO SUL  
FUNDAÇÃO UNIVERSIDADE FEDERAL DO AMAPÁ  
INSTITUTO BRASILEIRO DE INFORMAÇÃO, CIÊNCIA E TECNOLOGIA  
INSTITUTO EVANDRO CHAGAS  
INSTITUTO FEDERAL DE GOIÁS  
INSTITUTO FEDERAL DE MATO GROSSO  
INSTITUTO FEDERAL DO ESPÍRITO SANTO  
INSTITUTO FEDERAL DO PIAUÍ  
INSTITUTO NACIONAL DE PESQUISAS DA AMAZÔNIA  
MUSEU DE ASTRONOMIA E CIÊNCIAS AFINS  
OBSERVATÓRIO NACIONAL  
PONTIFÍCIA UNIVERSIDADE CATÓLICA DE CAMPINAS  
PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS  
PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL  
**REDE NACIONAL DE ENSINO E PESQUISA**

Selecione uma instituição

[ENVIAR](#) [Tutorial](#)

Para utilizar a identificação por meio da CAFe, sua instituição deve aderir a esse serviço provido pela Rede Nacional de Ensino e Pesquisa (RNP).

[Clique aqui para mais informações.](#)

# Arquitectura de una federación

- Demostración de autenticación y autorización – Portal CAPES



**Shibboleth Identity Provider Login to Service Provider <https://www.periodicos.capes.gov.br/shibboleth>**

Username:

Password:



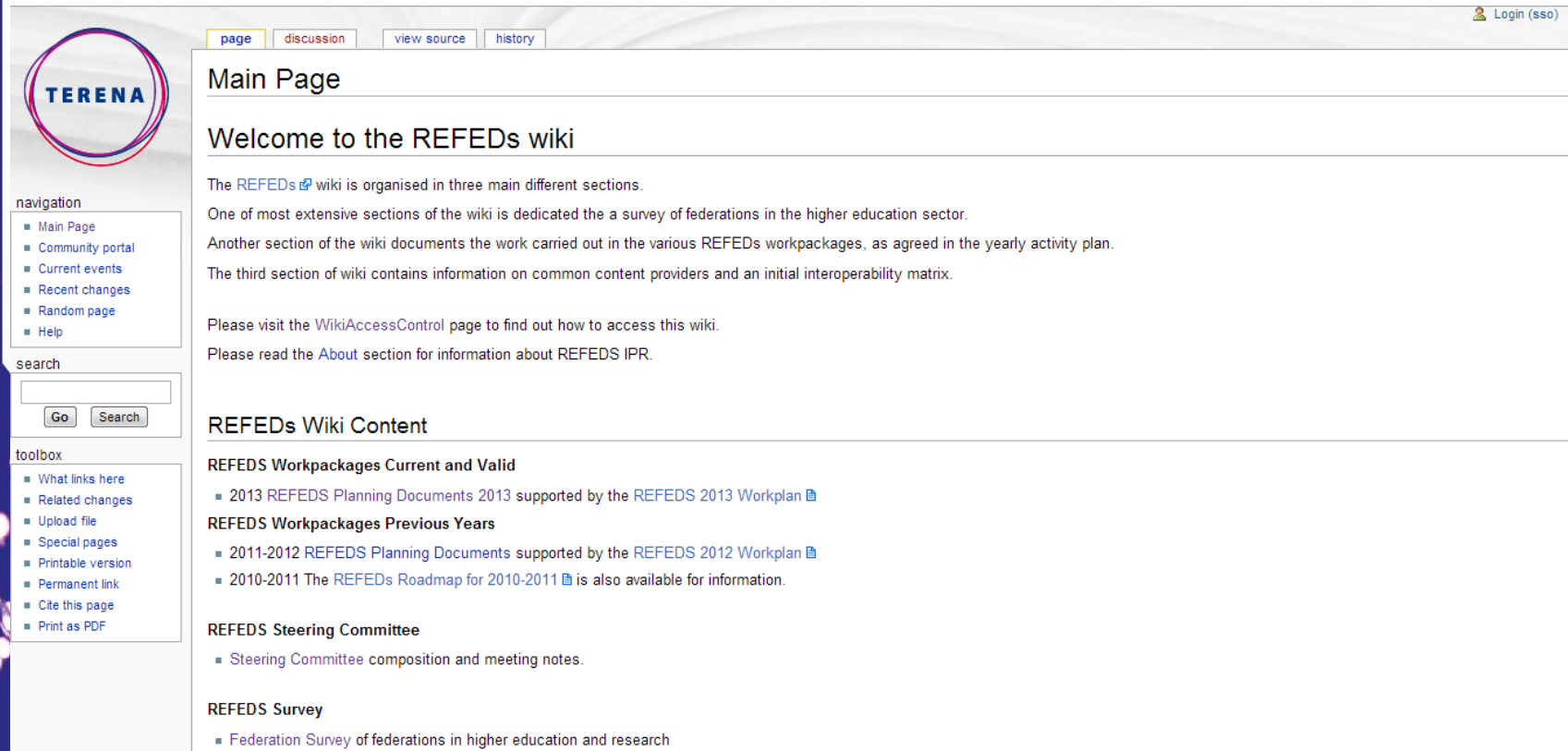
# Arquitectura de una federación

- Demostración de autenticación y autorización – Portal CAPES

The screenshot displays the CAPES Portal de Periódicos interface. At the top, the logo for 'periodicos.' and 'CAPES' is visible. Navigation links include 'MAPA DO SITE', 'FALE CONOSCO', 'MEU ESPAÇO', 'TAMANHO', and 'CONTRASTE'. A user is logged in, with the name 'Camila Fausto da Motta Santos' highlighted in a red box. Below the navigation, there are links for 'PÁGINA INICIAL', 'INSTITUCIONAL', 'ACERVO', 'BUSCA', 'NOTÍCIAS', and 'SUPORTE'. The main content area features four search sections: 'Buscar assunto', 'Buscar periódico', 'Buscar livro', and 'Buscar base'. Each section has a search input field, a 'BUSCAR' button, and a 'Busca avançada' link. The 'Buscar periódico' and 'Buscar livro' sections also include an alphabetical index and a 'Lista Completa' link. On the right, there is a photograph of a woman sitting on the grass using a laptop, with the caption 'Talita acessa o Portal de Periódicos do Parque Olhos D'água, em Brasília'. Below the search sections, there are three columns of news and training information: 'Notícias', 'Coleções', and 'Treinamentos'. The 'Treinamentos' section lists a training course at UFMT. The RNP logo is in the bottom right corner.

# Arquitectura de una federación

- Demostración de Single Sign-on



The screenshot displays the main page of the REFEDs wiki. At the top right, there is a 'Login (sso)' link. Below it, navigation tabs for 'page', 'discussion', 'view source', and 'history' are visible. The main heading is 'Main Page', followed by 'Welcome to the REFEDs wiki'. The introductory text explains the wiki's structure and provides links to 'WikiAccessControl' and 'About' sections. A 'REFEDs Wiki Content' section lists 'REFEDs Workpackages Current and Valid' (including 2013 documents) and 'REFEDs Workpackages Previous Years' (including 2011-2012 and 2010-2011 documents). It also mentions the 'REFEDs Steering Committee' and the 'REFEDs Survey'.

**TERENA**

navigation

- Main Page
- Community portal
- Current events
- Recent changes
- Random page
- Help

search

Go Search

toolbox

- What links here
- Related changes
- Upload file
- Special pages
- Printable version
- Permanent link
- Cite this page
- Print as PDF

page discussion view source history

## Main Page

### Welcome to the REFEDs wiki

The REFEDs [wiki](#) is organised in three main different sections.

One of most extensive sections of the wiki is dedicated the a survey of federations in the higher education sector.

Another section of the wiki documents the work carried out in the various REFEDs workpackages, as agreed in the yearly activity plan.

The third section of wiki contains information on common content providers and an initial interoperability matrix.

Please visit the [WikiAccessControl](#) page to find out how to access this wiki.

Please read the [About](#) section for information about REFEDS IPR.

### REFEDs Wiki Content

#### REFEDs Workpackages Current and Valid

- 2013 REFEDS Planning Documents 2013 supported by the [REFEDS 2013 Workplan](#)

#### REFEDs Workpackages Previous Years

- 2011-2012 REFEDS Planning Documents supported by the [REFEDS 2012 Workplan](#)
- 2010-2011 The [REFEDs Roadmap for 2010-2011](#) is also available for information.

#### REFEDs Steering Committee

- [Steering Committee composition and meeting notes.](#)

#### REFEDs Survey

- [Federation Survey of federations in higher education and research](#)

Login (sso)

# Arquitectura de una federación

- Demostración de Single Sign-on



Escolheu autenticar-se anteriormente em **RNP - Rede Nacional de Ensino e Pesquisa**

[Entrar em RNP - Rede Nacional de Ensino e Pesquisa](#)

All Chile Nordic countries Spain UK US Italy NZ AU NL eduGAIN Guest providers Miscellaneous

1033 entries

Incremental search...

♥ [RNP - Rede Nacional de Ensino e Pesquisa](#)

[AAF standalone attribute authorities](#)

[AAF standalone attribute authorities](#)

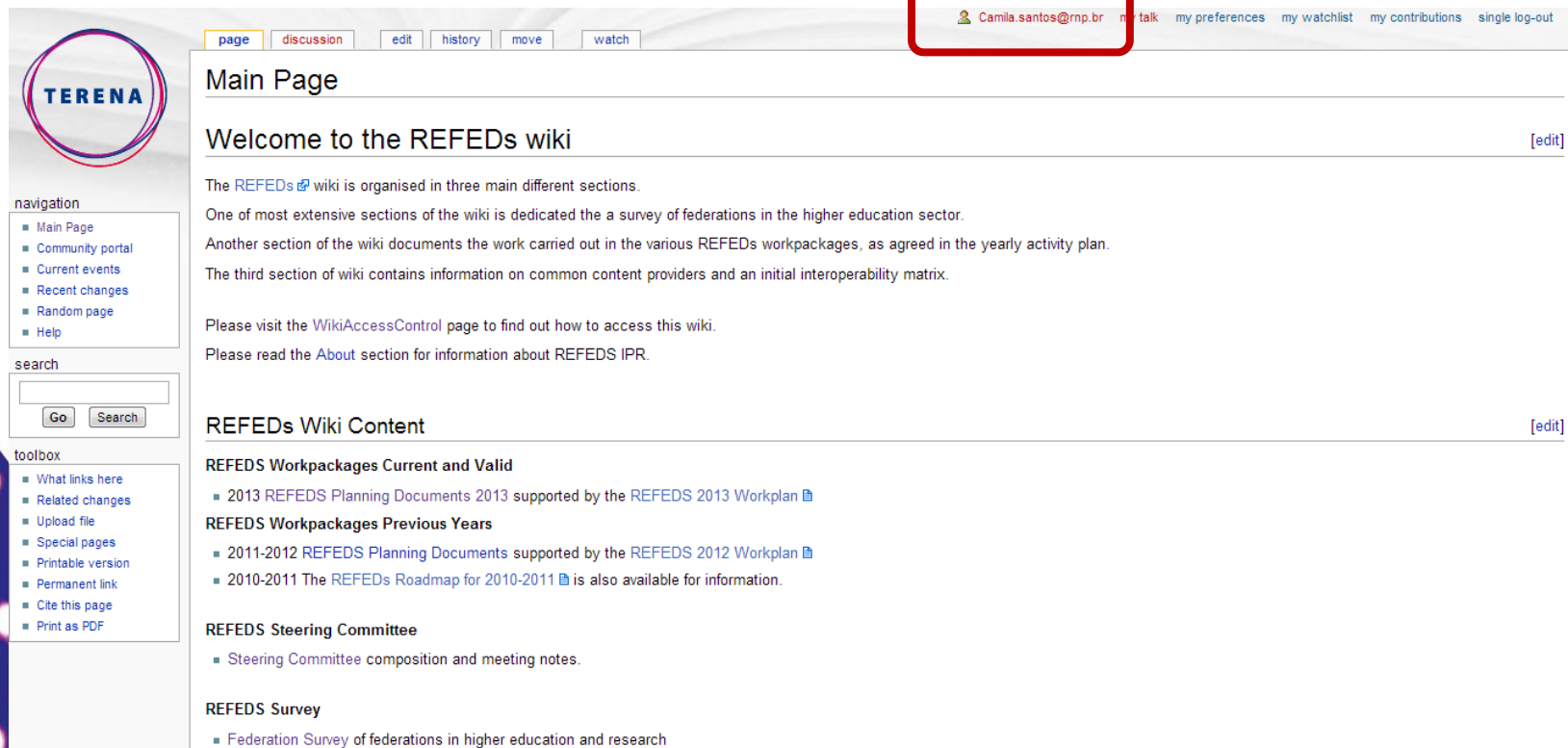
[AAF standalone attribute authorities](#)

[AAF Virtual Home](#)

[AAI@EduHr Single Sign-On Service](#)

# Arquitectura de una federación

- Demostración de Single Sign-on



The screenshot displays the main page of the REFEDs Wiki. At the top right, a user is logged in as **Camila.santos@rnp.br**, which is highlighted with a red box. The page features a navigation menu with options like 'page', 'discussion', 'edit', 'history', 'move', and 'watch'. The main content area includes a welcome message, a brief overview of the wiki's structure, and a list of content categories such as 'REFEDs Workpackages Current and Valid', 'REFEDs Workpackages Previous Years', 'REFEDs Steering Committee', and 'REFEDs Survey'. A sidebar on the left provides navigation and search tools.

**TERENA**

page discussion edit history move watch

Camila.santos@rnp.br talk my preferences my watchlist my contributions single log-out

## Main Page

### Welcome to the REFEDs wiki [edit]

The REFEDs wiki is organised in three main different sections.

One of most extensive sections of the wiki is dedicated the a survey of federations in the higher education sector.

Another section of the wiki documents the work carried out in the various REFEDs workpackages, as agreed in the yearly activity plan.

The third section of wiki contains information on common content providers and an initial interoperability matrix.

Please visit the [WikiAccessControl](#) page to find out how to access this wiki.

Please read the [About](#) section for information about REFEDS IPR.

### REFEDs Wiki Content [edit]

#### REFEDs Workpackages Current and Valid

- 2013 REFEDS Planning Documents 2013 supported by the [REFEDS 2013 Workplan](#)

#### REFEDs Workpackages Previous Years

- 2011-2012 REFEDS Planning Documents supported by the [REFEDS 2012 Workplan](#)
- 2010-2011 The [REFEDs Roadmap for 2010-2011](#) is also available for information.

#### REFEDs Steering Committee

- Steering Committee composition and meeting notes.

#### REFEDs Survey

- Federation Survey of federations in higher education and research

navigation

- Main Page
- Community portal
- Current events
- Recent changes
- Random page
- Help

search

Go Search

toolbox

- What links here
- Related changes
- Upload file
- Special pages
- Printable version
- Permanent link
- Cite this page
- Print as PDF

# Arquitetura de uma federación

- Servicio de teste de atributos

## Homologação de atributos - Chimarrao

Shib-Application-ID -> default

Shib-Session-ID -> \_dd8a18e2e32a30a8a51f96e41cd19d59

Shib-Identity-Provider -> https://idp.rnp.br/idp/shibboleth

Shib-Authentication-Instant -> 2013-07-03T18:49:46.639Z

Shib-Authentication-Method -> urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport

Shib-AuthnContext-Class -> urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport

eduPerson-eduPersonPrincipalName -> be741859c288b52d4b4cd2ea9e8b3ed4@rnp.br

inetOrgPerson-cn -> Camila Fausto da Motta Santos

inetOrgPerson-mail -> camila.santos@rnp.br

inetOrgPerson-sn -> da Motta Santos

# Arquitetura de uma federación

- Servicio de teste de atributos

## Homologação de atributos - Chimarrao

Shib-Application-ID -> default

Shib-Session-ID -> \_dd8a18e2e32a30a8a51f96e41cd19d59

Shib-Identity-Provider -> https://idp.rnp.br/idp/shibboleth

Shib-Authentication-Instant -> 2013-07-03T18:49:46.639Z

Shib-Authentication-Method -> urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport

Shib-AuthnContext-Class -> urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport

eduPerson-eduPersonPrincipalName -> be741859c288b52d4b4cd2ea9e8b3ed4@rnp.br

inetOrgPerson-cn -> Camila Fausto da Motta Santos

inetOrgPerson-mail -> camila.santos@rnp.br

inetOrgPerson-sn -> da Motta Santos

# Arquitectura de una federación

- Comunicación entre los elementos
  - SAML (Security Assertion Markup Language): Padrón que describe los mensajes XML enviados e recibidos por los elementos de la federación
  - Estos mensajes posibilitan el cambio de datos para autenticación y autorización entre productores y consumidores de aserciones



## Índice – Parte 2

- Definição de políticas
- Definição del esquema
- Provedores de identidade y de servicio
- *Discovery Service*
- Certificados





# Definição de políticas

# Definición de políticas

- ¿Qué es una política?
  - Definición de las reglas de una federación: cómo adherir, cómo salir, obligaciones y derechos de los miembros y de la federación, etc.
  - Documento formal que define los acuerdos entre los miembros de una federación y de ellos con la propia federación
  - Debe también garantizar que la utilización de los servicios no viole las reglas definidas por la RNIE o mismo por el país del usuario

# Definición de políticas

- Modelos de documentos de políticas (inglés)

Ejemplos:

<http://www.terena.org/activities/eurocamp/oct12/slides/Identity%20Federation%20Policy%20Template%20v0.4.pdf>

Cómo hacer:

[https://refeds.terena.org/index.php/Identity\\_Federation\\_Policy\\_-\\_template\\_document](https://refeds.terena.org/index.php/Identity_Federation_Policy_-_template_document)



# Definição del esquema

# Definición del esquema

- ¿Qué es un esquema?
  - Colección de atributos que pueden calificar un objeto
  - Definición del nombre y formato de los atributos
  - Cada atributo debe tener un OID (*Object Identifier*) asociado, ya definido, caso sea un atributo existente, o atribuido dentro de un registro definido para la institución
  - Informaciones sobre el registro de atributos:  
<http://www.oid-info.com/faq.htm>

# Definición del esquema

- Dependencia de los esquemas
  - Ya existen esquemas definidos para algunos objetos: personas, organizaciones, eventos, etc.
  - No es necesario crear un esquema todo nuevo, siempre se puede buscar hacer adaptaciones
  - En 2001, Internet2 creó la primera versión de el esquema eduPerson, para utilización dentro del ámbito académico, a partir de otros esquemas existentes

# Definición del esquema

- Esquema eduPerson

<b>eduPerson (200312) OIDs 1.3.6.1.4.1.5923.1.1.*</b>	<b>Allocation</b>
1.3.6.1.4.1.5923.1.1.2	eduPerson
1.3.6.1.4.1.5923.1.1.1.1	eduPersonAffiliation
1.3.6.1.4.1.5923.1.1.1.7	eduPersonEntitlement
1.3.6.1.4.1.5923.1.1.1.2	eduPersonNickname
1.3.6.1.4.1.5923.1.1.1.3	eduPersonOrgDN
1.3.6.1.4.1.5923.1.1.1.4	eduPersonOrgUnitDN
1.3.6.1.4.1.5923.1.1.1.5	eduPersonPrimaryAffiliation
1.3.6.1.4.1.5923.1.1.1.8	eduPersonPrimaryOrgUnitDN
1.3.6.1.4.1.5923.1.1.1.6	eduPersonPrincipalName
1.3.6.1.4.1.5923.1.1.1.9	eduPersonScopedAffiliation
1.3.6.1.4.1.5923.1.1.1.10	eduPersonTargetedID

# Definición del esquema

- Esquema eduPerson: ejemplo de atributo creado

**2.2.1. eduPersonAffiliation** (defined in eduPerson 1.0); *OID*: 1.3.6.1.4.1.5923.1.1.1.1

*RFC4512 definition*

(1.3.6.1.4.1.5923.1.1.1.1

NAME 'eduPersonAffiliation'

DESC 'eduPerson per Internet2 and EDUCAUSE'

EQUALITY caseIgnoreMatch

SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )

*Application utility class*: standard; # of values: multi

*Definition*

Specifies the person's relationship(s) to the institution in broad categories such as student, faculty, staff, alum, etc. (See controlled vocabulary).

*Permissible values*

faculty, student, staff, alum, member, affiliate, employee, library-walk-in



# Definición del esquema

- Esquema eduPerson: ejemplo de atributo de otro esquema

3.2. **cn** (commonName, included in person); *OID: 2.5.4.3*

*Application utility class: core; # of values: multi*

*Definition*

Common name.

According to RFC4519, "The 'cn' ('commonName' in X.500) attribute type contains names of an object. Each name is one value of this multi-valued attribute. If the object corresponds to a person, it is typically the person's full name."

# Definición del esquema

- Personalizaciones del eduPerson
  - brEduPerson (Brasil)
  - swissEduPerson (Suiza)
  - auEduPerson (Australia)
  - ... y otras
  
- Existen también las federaciones que utilizan solo esquemas ya definidos, sin personalizaciones
- Esta es una de las definiciones a se hacer en el proyecto de la federación

# Definición del esquema

- Esquemas más usados:
  - **person**: <http://schema.org/Person>
  - **eduPerson**:  
<http://middleware.internet2.edu/eduperson/docs/internet2-mace-dir-eduperson-201203.html>
  - **inetOrgPerson**: <http://www.ietf.org/rfc/rfc2798.txt>
  - **SCHAC**: <http://www.terena.org/activities/tf-emc2/docs/schac/schac-20061212-1.3.0.schema.txt>
- Utilización de esquemas por federación:
  - <https://refeds.terena.org/index.php/FederationSchema>



# Provedores de identidade y de servicio

# Proveedores de identidad y de servicio

- **Proveedores de servicio:** entidades que prestan algún tipo de servicio para algunos o todos los miembros de una federación
- Después de la autenticación de un usuario, puede definir diferentes perfiles de acceso, que cambian de acuerdo con las informaciones recibidas sobre el usuario
  - Un sistema de atribución y visualización de calificaciones de alumnos en una universidad
  - Un portal de publicaciones en que diferentes instituciones pueden tener diferentes acuerdos de permisos para sus miembros

# Proveedores de identidad y de servicio

- **Proveedores de identidad:** entidades dónde están almacenadas las informaciones de acceso de un usuario a la federación y sus atributos
- Es a quien el proveedor de servicios envía las credenciales digitadas por el usuario que intenta hacer una autenticación
- Es también quién realiza la autenticación del usuario
- Si la autenticación es bien sucedida, envía el *token* de autenticación y los atributos del usuario al proveedor de servicios

# Proveedores de identidad y de servicio

- Los proveedores de identidad y de servicios son definidos en la federación por medio de los metadatos, un archivo XML que contiene las informaciones que posibilitan la autenticación y el cambio de atributos

# Proveedores de identidad y de servicio

- Ejemplo: cafe-metadata.xml

```
▼<EntitiesDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:shibmd="urn:mace:shibboleth:metadata:1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" Name="urn:mace:shibboleth:cafe:chimarrao">
  ▶<!--...-->
  ▶<!--...-->
  ▶<!--...-->
  ▶<!--...-->
  ▶<!--...-->
  ▶<!--...-->
  ▶<!-- SHIBBOLETH 2.X -->
  ▶<!--...-->
  ▼<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:shibmd="urn:mace:shibboleth:metadata:1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" entityID="https://cafe.ufpa.br/idp/shibboleth">
  ▼<IDPSSODescriptor protocolSupportEnumeration="urn:mace:shibboleth:1.0 urn:oasis:names:tc:SAML:1.1:protocol urn:oasis:names:tc:SAML:2.0:protocol">
    ▼<Extensions>
      <shibmd:Scope regexp="false">ufpa.br</shibmd:Scope>
    </Extensions>
    ▼<KeyDescriptor>
      ▼<ds:KeyInfo>
        ▼<ds:X509Data>
          ▶<ds:X509Certificate>...</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>
    <ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding"
Location="https://cafe.ufpa.br:8443/idp/profile/SAML1/SOAP/ArtifactResolution" index="1"/>
    <ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="https://cafe.ufpa.br:8443/idp/profile/SAML2/SOAP/ArtifactResolution"
index="2"/>
    <NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</NameIDFormat>
    ▼<NameIDFormat>
      urn:oasis:names:tc:SAML:2.0:nameid-format:transient
    </NameIDFormat>
    <SingleSignOnService Binding="urn:mace:shibboleth:1.0:profiles:AuthnRequest" Location="https://cafe.ufpa.br/idp/profile/Shibboleth/SSO"/>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://cafe.ufpa.br/idp/profile/SAML2/POST/SSO"/>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign" Location="https://cafe.ufpa.br/idp/profile/SAML2/POST-SimpleSign/SSO"/>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://cafe.ufpa.br/idp/profile/SAML2/Redirect/SSO"/>
  </IDPSSODescriptor>
  ▼<AttributeAuthorityDescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol urn:oasis:names:tc:SAML:2.0:protocol">
```



# Proveedores de identidad y de servicio

- Estructuras principales en el archivo de metadatos (Shibboleth 2.X):
  - *EntitiesDescriptor*: es el descriptor de una entidad o de un grupo de entidades. Ejemplo: un archivo de metadatos, un SP o un IdP
  - *Role descriptors*: describen el rol de la entidad que está siendo descrita. Roles importantes son `<md:IDPSSODescriptor>` y `<md:AttributeAuthorityDescriptor>` cuándo la entidad en cuestión es un IdP, y `<md:SPSSODescriptor>` para un SP
  - *Contact person*: describe las informaciones de contacto del responsable por una entidad. Esta es la persona que debe ser contactada en caso de problemas de autenticación a un servicio específico



# *Discovery Service*

Ministério da  
Cultura

Ministério da  
Saúde

Ministério da  
Educação

Ministério da  
Ciência, Tecnologia  
e Inovação

GOVERNO FEDERAL  
**BRASIL**  
PAÍS RICO É PAÍS SEM POBREZA

# *Discovery Service*

- Tiene por objetivo posibilitar que el usuario informe al proveedor de servicios su institución de origen

# Discovery Service

- DS centralizado
  - Está en el centro de la federación, generalmente en el mismo servidor que el archivo central de metadatos
  - Busca informaciones sobre las instituciones en el archivo central de la federación y ofrece las opciones de institución a el usuario

# Discovery Service

- DS a partir del SP
  - Está en cada uno de los SPs de la federación. El SP busca en su instancia de el archivo de metadatos las opciones posibles de IdPs y las presenta al usuario
  - El modelo utilizado para el *Discovery Service* puede ser una escoja de la federación o del proveedor de servicio



# Certificados

Ministério da  
Cultura

Ministério da  
Saúde

Ministério da  
Educação

Ministério da  
Ciência, Tecnologia  
e Inovação

GOVERNO FEDERAL  
**BRASIL**  
PAÍS RICO É PAÍS SEM POBREZA

# Certificados

- Para garantizar la confiabilidad y permitir la identificación de entidades, se puede utilizar la criptografía de llave pública para firmar los metadatos
- Así, los certificados utilizados en las entidades debe ser lo mismo que aquél presente en sus metadatos

# Certificados

- El Shibboleth recomienda la utilización del certificado todo en los metadatos en vez de utilizar nombres y llaves públicas
- Este nivel de seguridad y confiabilidad es también parte de las definiciones a se hacer para la federación
- <https://wiki.shibboleth.net/confluence/display/SHIB2/BuildAFederation>





## Índice – Parte 3

- Archivo central de metadatos
- Confederaciones
- Gestión de identidad
- Configuración de proveedores de identidad
- Configuración de proveedores de servicios



# Archivo central de metadatos

# Archivo central de metadatos

- Lo que define una federación es el archivo central de metadatos
- Este archivo contiene todas las entidades de la federación, o sea, todos los SPs y IdPs
- Cada entidad de la federación debe mantener una instancia local actualizada del archivo central
- En este archivo, el DS buscará todos os proveedores de identidad federados donde un usuario podrá autenticarse

# Archivo central de metadatos

- El archivo central de metadatos puede ser construido de dos modos
  - Archivo único: todos los metadatos están concentrados en un único archivo, que debe ser editado manualmente siempre que un nuevo IdP o SP adherir a la federación
  - Archivos múltiples: cada bloco de metadatos está en un archivo, dentro o fuera del dominio de la federación. En este caso, se debe utilizar un agregador de metadatos para construir el archivo central
- El modo de manutención de los metadatos de las entidades es también una opción que se puede hacer en el proyecto de la federación

# Archivo central de metadatos

- Ejemplos de agregadores de metadatos
  - Shibboleth Metadata Aggregator
  - RepoX
  - OAICat
  - ... y otros



# Confederaciones

# Confederaciones

- Federaciones pueden tener recursos que sean útiles a otras federaciones
- Las confederaciones permiten que usuarios de una federación se autentiquen en servicios de otra
- Hecho con cambios de archivos de metadatos y acuerdos bilaterales

# Confederaciones

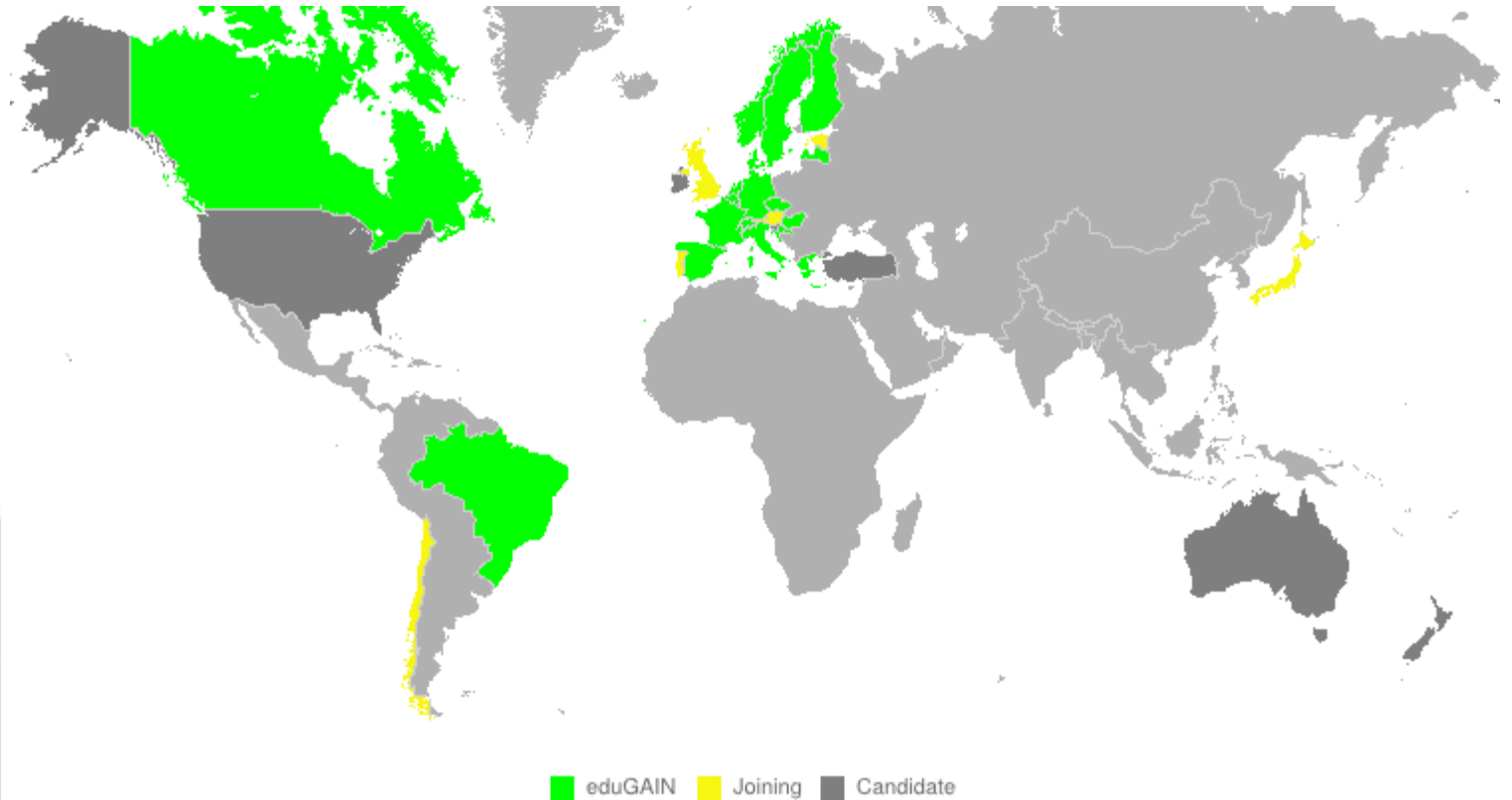
- eduGAIN: Iniciativa
  - Empezó como una confederación de países europeos
  - Su cantidad de servicios y usuarios conectados era también interesante para federaciones fuera de Europa





# Confederaciones

- eduGAIN: Mapa de federaciones



# Confederaciones

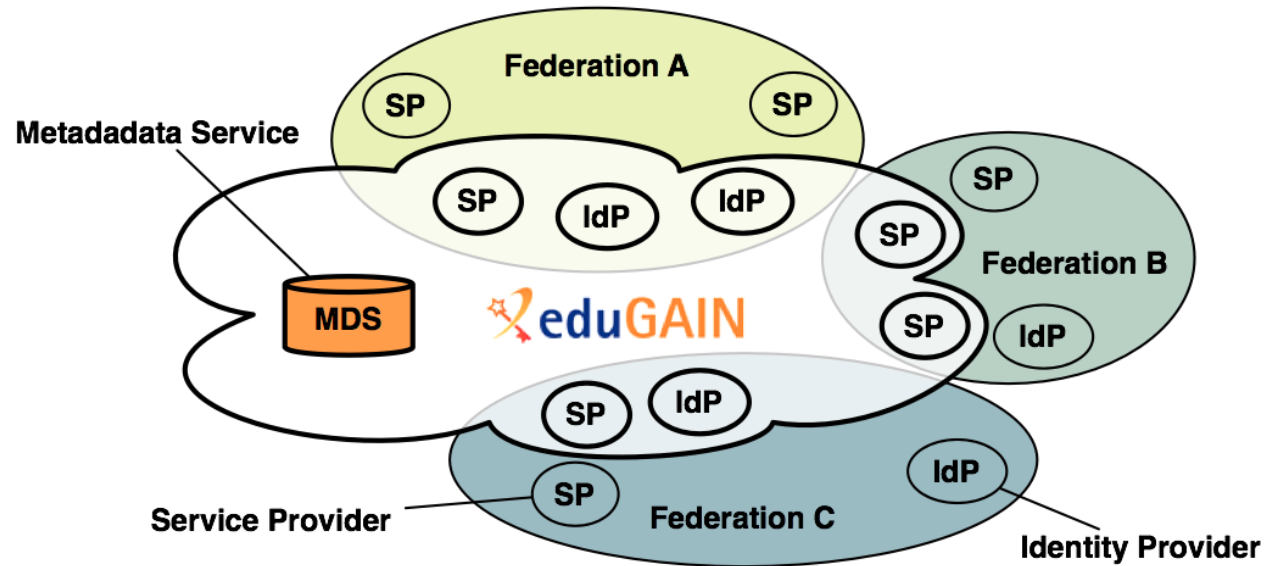
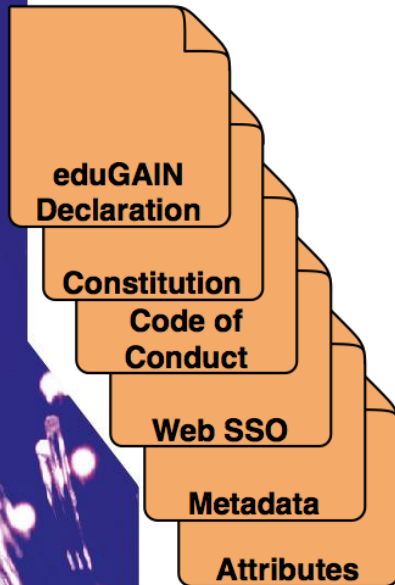
- eduGAIN: Proveedores
  - 122 proveedores de identidad
  - 55 proveedores de servicio

<http://www.terena.org/~schofield/servicecatalogue/>



# Confederaciones

- eduGAIN: estructura



# Confederaciones

- eduGAIN: miembros

- ▶ **Belgium - Belnet Federation**
- ▶ **Brazil - CaFe**
- ▶ **Canada - Canadian Access Federation**
- ▶ **Croatia - AAI@EduHr (production - information missing)**
- ▶ **Czech Republic - eduID.cz**
- ▶ **Denmark - WAYF**
- ▶ **Finland - HAKA**
- ▶ **France - Fédération Éducation-Recherche**
- ▶ **Germany - DFN**
- ▶ **Greece - GRNET (production - information missing)**
- ▶ **Hungary - eduId.hu**
- ▶ **Italy - IDEM**
- ▶ **Latvia - LAIFE**
- ▶ **Norway - FEIDE**
- ▶ **Spain - SIR**
- ▶ **Sweden - SWAMID**
- ▶ **Switzerland - SWITCHaai**
- ▶ **The Netherlands - SURFfederatie**

# Confederaciones

- eduGAIN: cómo adherir

▶ Contact email

▶ Signing declaration

▶ Metadata source and signing certificate

▶ TSG delegate and deputy

▶ Federation page

▶ Policy

▶ Registration practice statement

[http://www.edugain.org/technical/joining\\_checklist.php](http://www.edugain.org/technical/joining_checklist.php)





# Gestión de identidad

# Gestión de identidad

- Una das etapas principales para asegurar que el concepto de federación sea siempre mantenido es la gestión de identidad
- Esta es la garantía de que los miembros de una federación son únicos y que corresponden a una persona que tiene un vínculo con la institución

# Gestión de identidad

- Desafíos
  - Impedir el acceso de identidades artificiales en la federación: admin, cuentas de departamento, cuentas de grupos, etc.
  - Garantir que todos los usuarios sean únicos: cuentas duplicadas, nombres errados, usuarios de más de una institución, registros duplicados en bases distintas...
  - Garantir que todos los usuarios tengan un vínculo válido con la institución



# Gestión de identidad

- Como hacemos en CAFe
  - Es parte del proceso de adhesión de los IdPs a realización de adecuación de las bases
  - Utilización del software EID (Export Import Directory Tool): unificación de bases, conciliación de registros, sincronización agentada de todas las fuentes de datos
  - Herramienta desarrollada por la UFMG
  - Disponible en sourceforge, solo en portugués



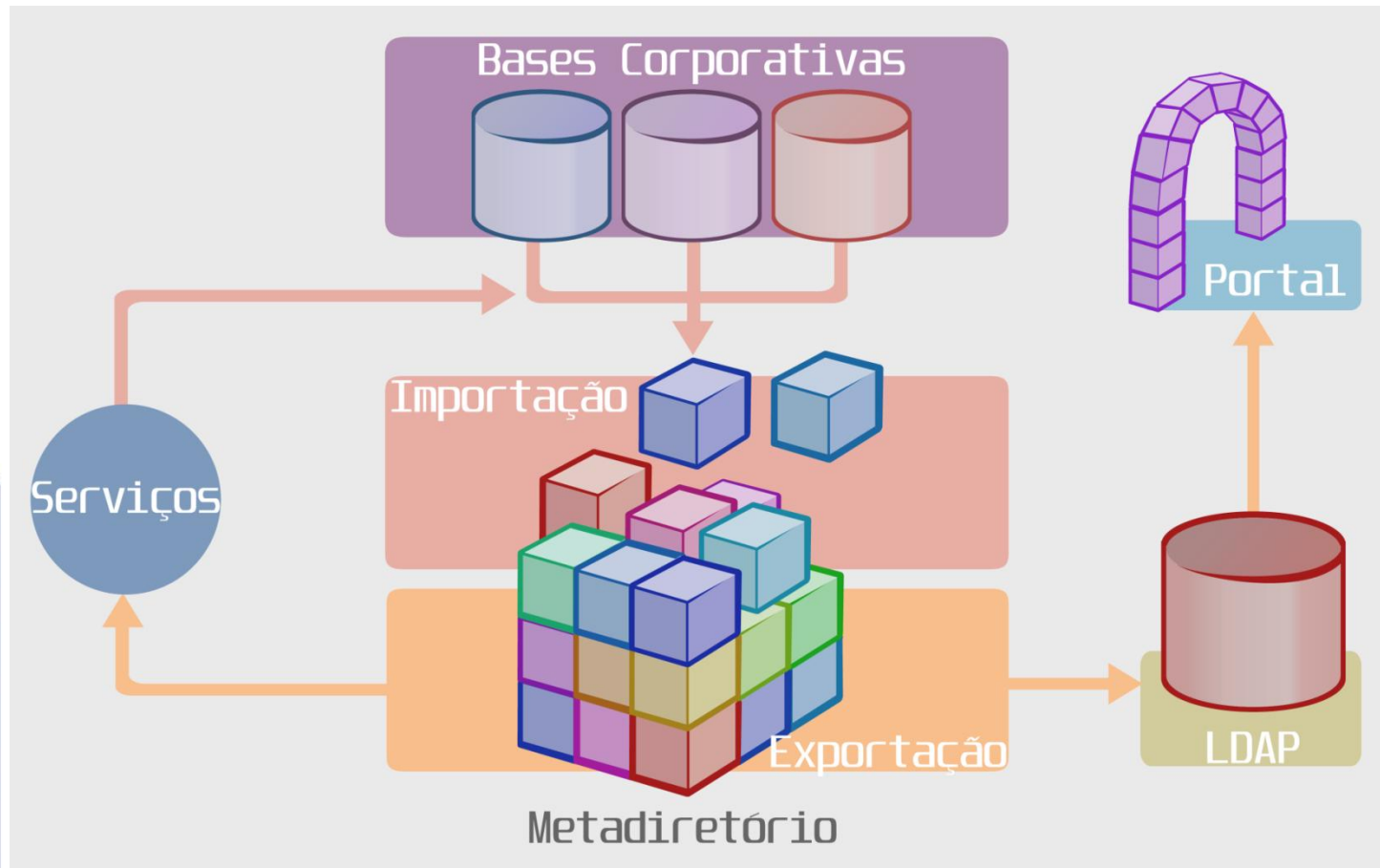
# Gestión de identidad

- Como hacemos en CAFe
  - La herramienta construye un metadirectorio a partir de diferentes bases de datos: relacional, textual, CSV, Excel...
  - Con el metadirectorio, es posible hacer la conciliación de registros aparentemente duplicados. Ellos ya son detectados por la herramienta, pero el administrador debe decidir si son registros parecidos o los mismos registros. Ejemplo: homónimos, gemelos, nombres parecidos



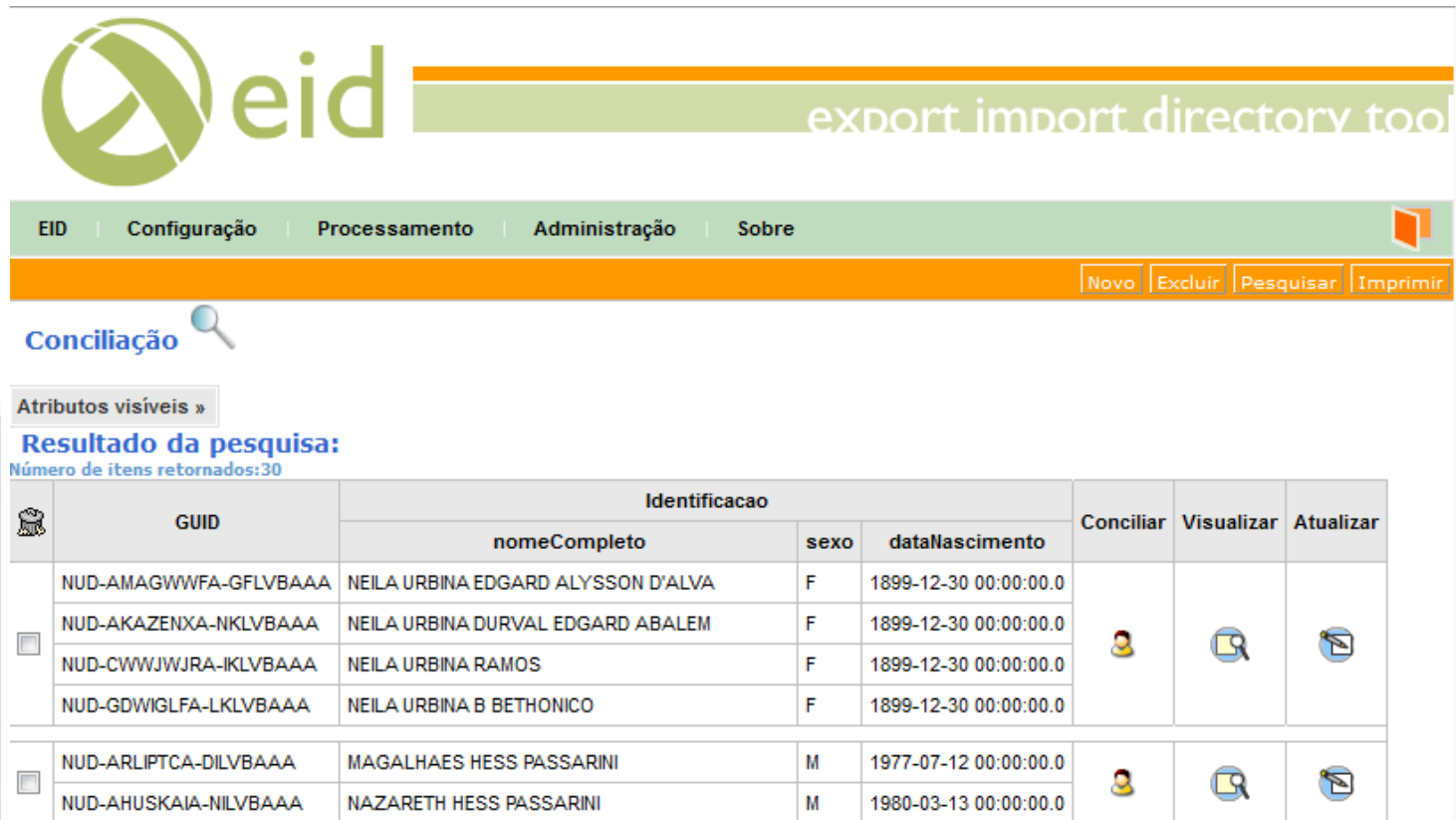
# Gestión de identidad

- EID: como funciona



# Gestión de identidad

- EID: registros para conciliación



The screenshot displays the EID web application interface. At the top, there is a logo for 'eid' and the text 'export import directory tool'. Below this is a navigation menu with options: EID, Configuração, Processamento, Administração, and Sobre. A secondary menu contains buttons for 'Novo', 'Excluir', 'Pesquisar', and 'Imprimir'. The main content area is titled 'Conciliação' with a magnifying glass icon. Below this, there is a section for 'Atributos visíveis »' and 'Resultado da pesquisa:'. The search results are displayed in a table with 30 items returned. The table has columns for GUID, Identificação (nomeCompleto, sexo, dataNascimento), and actions (Conciliar, Visualizar, Atualizar).

	GUID	Identificação			Conciliar	Visualizar	Atualizar
		nomeCompleto	sexo	dataNascimento			
<input type="checkbox"/>	NUD-AMAGWWFA-GFLVBAAA	NEILA URBINA EDGARD ALYSSON D'ALVA	F	1899-12-30 00:00:00.0			
<input type="checkbox"/>	NUD-AKAZENXA-NKLVBAAA	NEILA URBINA DURVAL EDGARD ABALEM	F	1899-12-30 00:00:00.0			
	NUD-CWWJWJRA-IKLVBAAA	NEILA URBINA RAMOS	F	1899-12-30 00:00:00.0			
	NUD-GDWIGLFA-LKLVBAAA	NEILA URBINA B BETHONICO	F	1899-12-30 00:00:00.0			
<input type="checkbox"/>	NUD-ARLIPTCA-DILVBAAA	MAGALHAES HESS PASSARINI	M	1977-07-12 00:00:00.0			
	NUD-AHUSKAIA-NILVBAAA	NAZARETH HESS PASSARINI	M	1980-03-13 00:00:00.0			

# Gestión de identidad

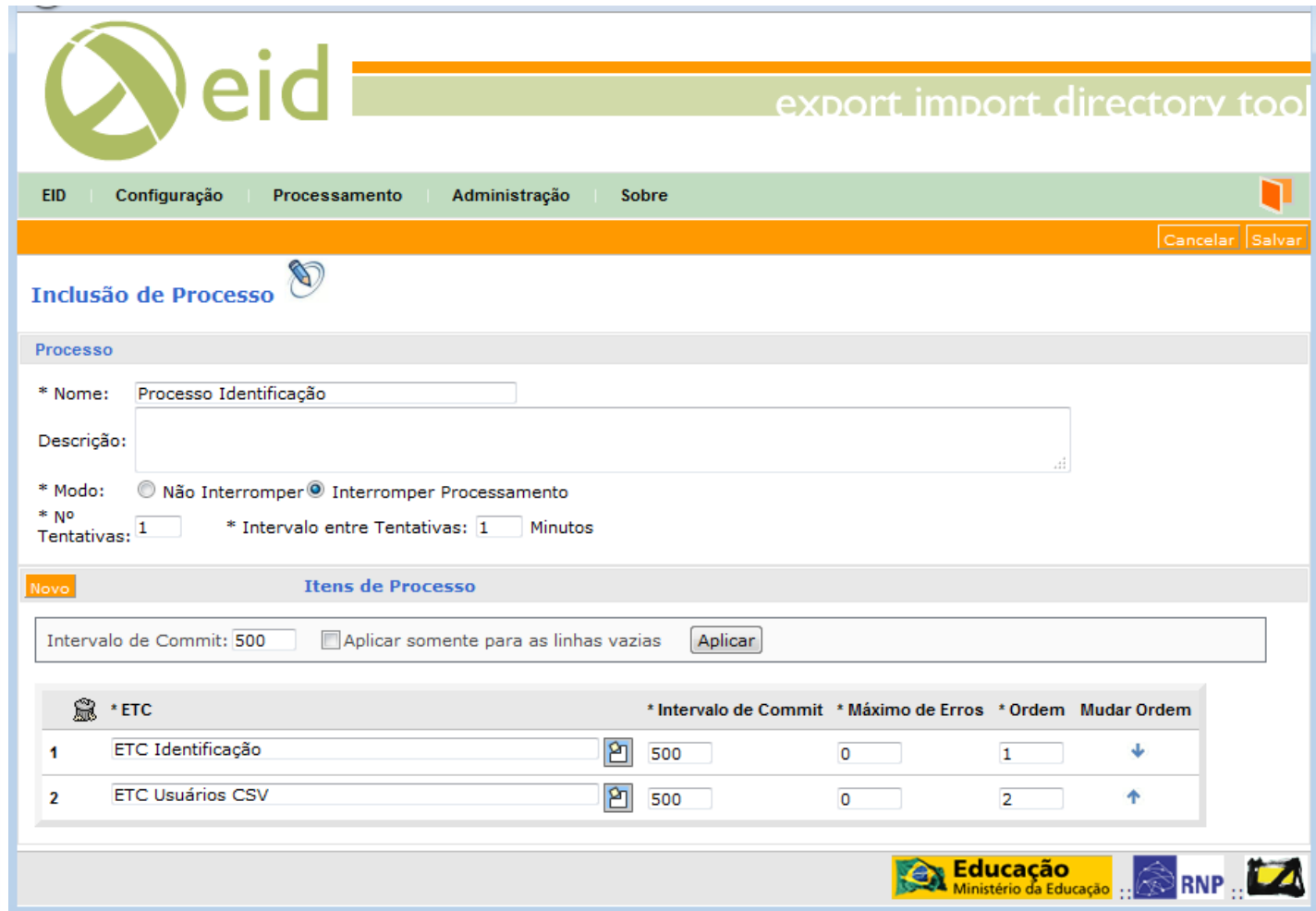
- EID: definición de archivo CSV como fuente de datos



The screenshot displays the EID web application interface. At the top, there is a logo for 'eid' and the text 'export import directory tool'. Below this is a navigation menu with options: 'EID', 'Configuração', 'Processamento', 'Administração', and 'Sobre'. A 'Cancelar' button and a 'Salvar' button are visible on the right side of the menu. The main content area is titled 'Inclusão de Arquivo CSV' and contains a form for adding a CSV file. The form has a section for 'Repositório de Dados' with a dropdown menu set to 'Arquivo CSV'. Below this is a section for 'Arquivo CSV' with three input fields: '\* Nome:', 'Descrição:', and '\* Diretório:'. At the bottom of the page, there are logos for 'Educação Ministério da Educação', 'RNP', and another logo.

# Gestão de identidade

- EID: configuração de procesamento de extracção



The screenshot displays the EID web interface. At the top, there is a logo for 'eid' and the text 'export import directory tool'. Below this is a navigation menu with options: 'EID', 'Configuração', 'Processamento', 'Administração', and 'Sobre'. A 'Cancelar' button and a 'Salvar' button are visible in the top right corner.

The main section is titled 'Inclusão de Processo' and contains the following configuration fields:

- Processo**
  - \* Nome:
  - Descrição:
  - \* Modo:  Não Interromper  Interromper Processamento
  - \* Nº Tentativas:  \* Intervalo entre Tentativas:  Minutos
- Itens de Processo**
  - Intervalo de Commit:   Aplicar somente para as linhas vazias

* ETC	* Intervalo de Commit	* Máximo de Erros	* Ordem	Mudar Ordem
1 ETC Identificação	<input type="text" value="500"/>	<input type="text" value="0"/>	<input type="text" value="1"/>	↓
2 ETC Usuários CSV	<input type="text" value="500"/>	<input type="text" value="0"/>	<input type="text" value="2"/>	↑

At the bottom of the interface, there are logos for 'Educação Ministério da Educação', 'RNP', and another logo.

# Gestión de identidad

- EID: agentamiento de procesamiento



The screenshot displays the EID web application interface. At the top, there is a logo for 'eid' and the text 'export import directory tool'. Below this is a navigation menu with options: EID, Configuração, Processamento, Administração, and Sobre. A secondary bar contains 'Cancelar' and 'Salvar' buttons. The main section is titled 'Inclusão de Agendamento' with a pencil icon. Under the 'Agendamento' heading, there are several form fields: '\*Processo' (Processo Eid), '\*Tipo de Repetição' (Não repetir), '\*Item de Início' (1 - ETC Identificação), '\*Finalizar no Item' (3 - ETC Usuários CSV), 'Próxima Execução:' (12/05/2011), and a checked 'Processar Agora' checkbox. Below this is a section for 'Horários permitidos para processamento' (Allowed processing times) with a 'Novo' button. It contains a table with columns for 'Horário de Início' and 'Horário de Término' and three rows for scheduling entries.

**Agendamento**

\*Processo: Processo Eid  
\*Tipo de Repetição: Não repetir  
\*Item de Início: 1 - ETC Identificação  
\*Finalizar no Item: 3 - ETC Usuários CSV  
Próxima Execução: 12/05/2011  Processar Agora  
Resultado de Processamento:

**Novo** Horários permitidos para processamento

	Horário de Início	Horário de Término
1	12:00	06:00
2		
3		

# Gestión de identidad

- Como hacemos en CAFe
  - Después de la creación del metadirectorio, se puede crear un nuevo directorio LDAP unificado utilizando el EID2LDAP
  - La sincronización entre las bases antiguas y la nueva se hace por medio del sistema





# Gestión de identidad

- Como hacemos en los casos no contemplados por el EID
  - Filtros para identidades artificiales
  - Definición de reglas para evitar la duplicación de usuarios en diferentes instituciones
  - ... y así damos el soporte para que nuestros IdPs hagan la gestión de identidad

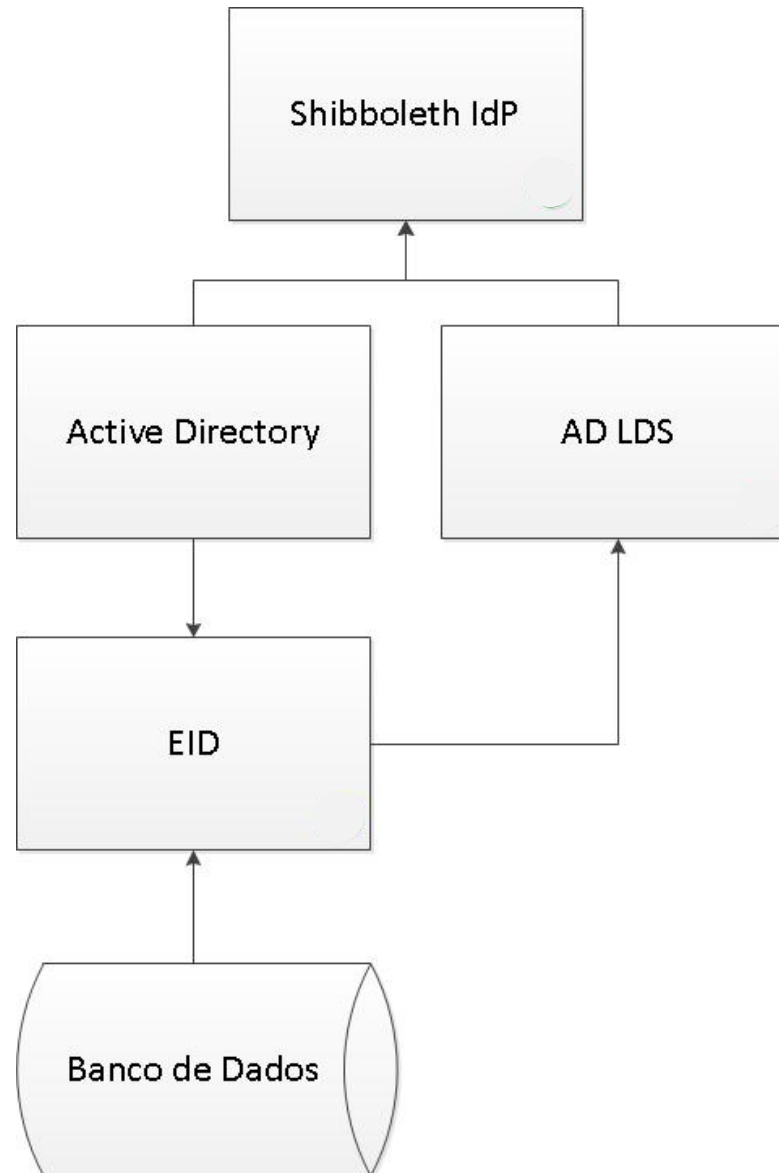
# Gestión de identidad

- Utilización del AD
  - Una das herramientas de directorio utilizadas por las instituciones es el AD
  - Problema: no es posible extraer directamente el vínculo de un usuario con la institución. Sería necesario hacer una personalización de los atributos o utilizar un script para extraer el vínculo de otra fuente
  - Ni siempre los responsables por los IdPs poseen este conocimiento del directorio

# Gestión de identidad

- AD: Como hicimos en CAFe
  - Muchas instituciones nos pedían ayuda sobre como liberar el atributo de vínculo, y no se tenía soporte oficial a directorios AD dentro de la federación
  - Solución: creación de un directorio paralelo utilizando AD LDS y utilización de un atributo adicional apenas para comunicación entre AD y Shibboleth, conteniendo las informaciones de parentesco
  - En esta solución, la verificación de las credenciales ocurren en el AD. Si fueron validadas, los atributos del usuario son enviados al SP por el AD LDS
  - El EID es también compatible con esa solución

# Gestión de identidad





# Configuração del proveedor de identidad



# Configuración del proveedor de servicio



## Índice – Parte 4

- Páginas úteis

# Páginas útiles

- Informaciones útiles sobre federaciones:

<https://wiki.shibboleth.net/confluence/display/SHIB2/Home>

- Guías de instalación

<http://www.switch.ch/aai/support/identityproviders/>

<http://www.switch.ch/aai/support/serviceproviders/>



Muchas gracias!

## Camila Santos

Analista de Operaciones  
<camila.santos@rnp.br>

Directoría Adjunta de Gestión de Servicios  
(DAGSer)  
Rede Nacional de Ensino e Pesquisa (RNP)