



## European Union's FP7 Programme

### DG Connect

Directorate C: Excellence in Science

Unit C1: e-Infrastructure



## Deliverable D2.2

# On line Training Material on AAI development for Staff training



A project of the Seventh Framework Programme  
(FP7)



This project is funded by the European Commission



A project implemented by RedCLARA

## Periodical Progress Report

### *ELCIRA Deliverable: D2.2 – On line Training Material on AAI development for Staff training*

Document Full Name	<b>On line Training Material on AAI development for Staff training</b>
Date	<b>March, 2013</b>
Activity	<b>WP2 (Coordinated Actions for AAI between EU and LA)</b>
Lead Partner	<b>RNP</b>
Document status	<b>Draft Version</b>
Classification Attribute	
Document link	

**Abstract:** This document describes and shows how the on line training material on AAI was developed and organized. This training was developed to be used on technical staff training. The material will be development to be used on line only; there will be no printed material. Provide technical training to at least 2 people from NRENs that will join the project. This course will be on line using the virtual training platform “RedCLARA Aprende”.



A project of the Seventh Framework Programme (FP7)



This project is funded by the European Commission



A project implemented by RedCLARA

## COPYRIGHT NOTICE

Copyright © Members of the ELCIRA Project, March 2013.

ELCIRA (Europe Latin America Collaborative e-Infrastructure for Research Activities – Call (part) identifier: FP7-INFRASTRUCTURES-2012-1 – Project number: 313180) is a project co-funded by the European Commission within the Seventh Framework Programme (FP7), Infrastructures (DG Connect, Directorate C: Excellence in Science, Unit C1: e-Infrastructure). ELCIRA began on 1<sup>st</sup> June 2012 and will run for 24 months.

For more information on ELCIRA, its partners and contributors please see <http://elcira.redclara.net> (this website will be available in October 1<sup>st</sup> 2012).

You are permitted to copy and distribute, for non-profit purposes, verbatim copies of this document containing this copyright notice. This includes the right to copy this document in whole or in part, but without modification, into other documents if you attach the following reference to the copied elements: “Copyright © Members of the ELCIRA Project, 2012”.

Using this document in a way and/or for purposes not foreseen in the paragraph above, requires the prior written permission of the copyright holders.

The information contained in this document represents the views of the copyright holders as of the date such views were published.

THE INFORMATION CONTAINED IN THIS DOCUMENT IS PROVIDED BY THE COPYRIGHT HOLDERS “AS IT IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE MEMBERS OF THE ELCIRA COLLABORATION, INCLUDING THE COPYRIGHT HOLDERS, OR THE EUROPEAN COMMISSION BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THE INFORMATION CONTAINED IN THIS DOCUMENT, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.



A project of the Seventh Framework  
Programme (FP7)



This project is funded by the European  
Commission



A project implemented by RedCLARA

## DELIVERABLE ROUTE

	Name	Member/Activity	Date	Responsible
<b>From</b>	Leandro Guimarães	WP2	March, 2013	RNP
<b>Approved by</b>	Antônio Carlos Fernandes Nunes	WP2	March, 2013	RNP



A project of the Seventh Framework  
Programme (FP7)



This project is funded by the European  
Commission



A project implemented by RedCLARA

## TABLE OF CONTENTS

COPYRIGHT NOTICE .....	2
DELIVERABLE ROUTE .....	3
1.- TRAINING structure .....	5
2.- TRAINING topics .....	6
2.1 Module 1:.....	9
2.2 Exercise Module 1 .....	10
2.3 Module 2:.....	11
2.4 Exercise Module 2 .....	12
2.5 Module 3.....	13
2.6 Exercise Module 3 .....	14
2.7 Module 4.....	15
2.8 Module 5.....	16
2.9 Module 6.....	17
2.10 Module 7.....	18
2.11 Module 8.....	19
2.12 Module 9.....	20
2.13 Module 10.....	21



A project of the Seventh Framework  
Programme (FP7)



This project is funded by the European  
Commission

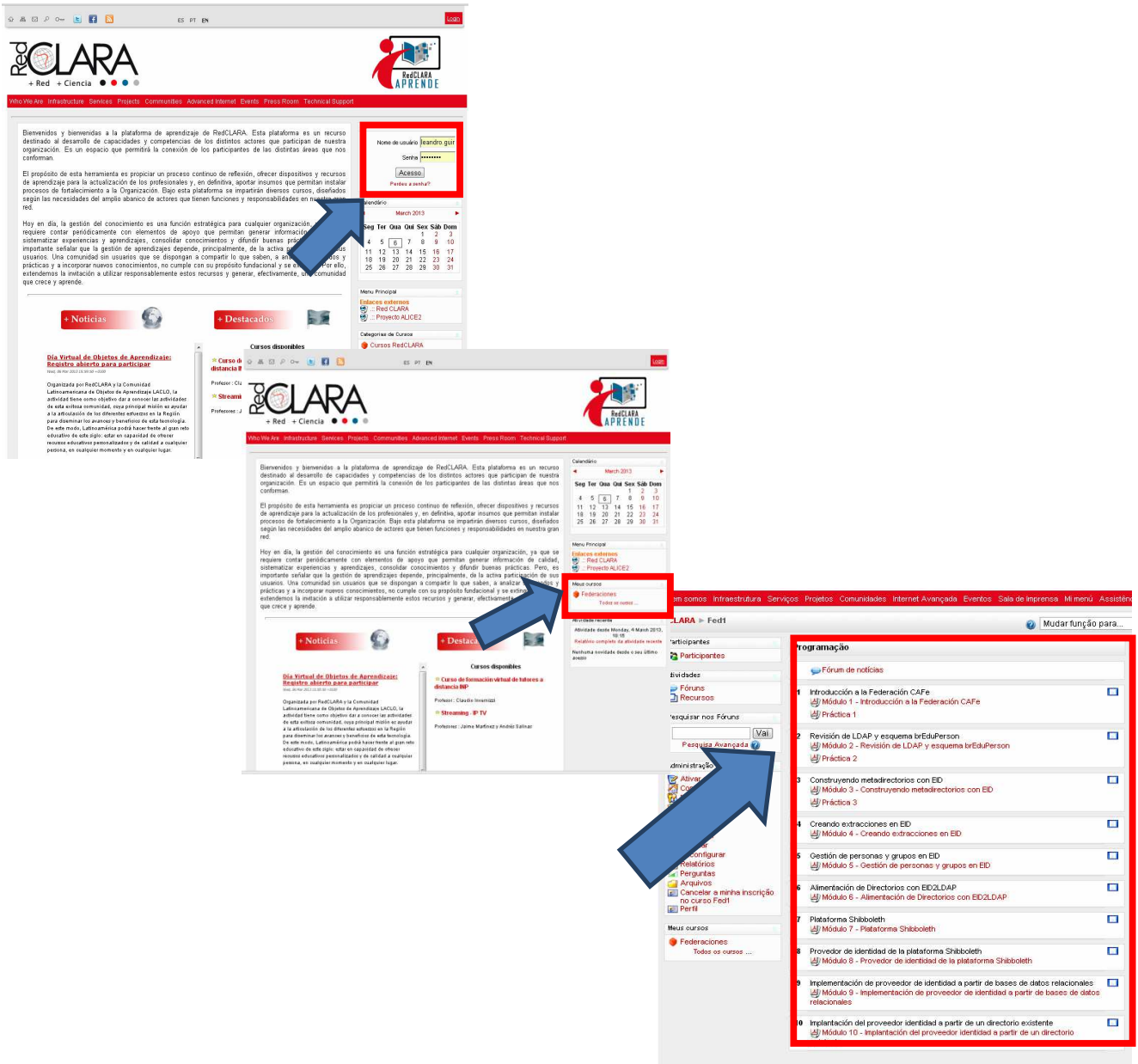


A project implemented by RedCLARA

## 1.- TRAINING STRUCTURE

The training was published in virtual training platform “RedCLARA Aprende” at:

- [http://www.redclara.net/index.php?option=com\\_wrapper&view=wrapper&Itemid=573&lang=en](http://www.redclara.net/index.php?option=com_wrapper&view=wrapper&Itemid=573&lang=en)



The screenshot displays the RedCLARA Aprende platform interface. At the top, there is a navigation menu with options like 'Inicio', 'Infraestructura', 'Servicios', 'Proyectos', 'Comunidades', 'Internet Avanzada', 'Eventos', 'Sala de Impresión', 'Mi menú', and 'Asistencia'. Below the navigation, there is a login form with fields for 'Nombre de usuario' and 'Contraseña', and a 'Acceso' button. A calendar for March 2013 is visible, showing the current date as the 4th. The main content area features a 'Bienvenidos y bienvenidas' message and a 'Curso disponible' section. On the right side, there is a 'Programación' section with a list of 10 modules, each with a checkbox and a link to the module content.



A project of the Seventh Framework Programme (FP7)



This project is funded by the European Commission



A project implemented by RedCLARA

## 2.- TRAINING TOPICS

### Module 1: Introduction to federation

- Infrastructure of a federated authentication and authorization;
- Federation elements
- Interaction between federation's elements
- Academic federation examples
- Brazilian federation (CAFe)
- Course Overview

### Module 2 – LDAP revision and brEduPerson schema

- LDAP revision
  - Directory services LDAP and OpenLDAP
  - LDAP models
  - LDIF representation
  - Shell commands and Grafic interface
- brEduPerson Squema
  - Information models and example names to be used in brEduPerson squema

### Module 3 – Building metadata with EID

- Overview of EID
  - Motivation
  - Metadirectories
  - Export and Import Directory (EID)
  - EID and brEduPerson
- Extraction configuration
  - Definición de repositorio
  - Definición extracciones
  - Definición de procesos
  - Agendamientos

### Module 4 – Extracting data with EID

- Removing text files
- Resolution object EID
- Global Parameters
- Incremental import
- Conversion Scripts



A project of the Seventh Framework  
Programme (FP7)



This project is funded by the European  
Commission



A project implemented by RedCLARA

- unification algorithms
- Web Services
- Common Problems

### Module 5: Identity and groups management with EID

- Manual management of people
  - Reconciliation of records
  - Insertion of new people
  - Alteration of data via interface
- Group Management
  - Insert and update groups
  - Removal of groups

### Module 6: Directories populating with EID2LDAP

- Introduction
  - EID2LDAP
  - Features
- Architecture
  - XML EID
  - XSLT
  - Processing LDIF
- Configure and use
- Common Problems

### Module 7: Shibboleth platform

- Introduction
- Identity Provider (IdP)
- Service Provider (SP)
- WAYF (Where Are You From?) / DS (Discovery Service)
- Metadata
- Operation
- Activities

### Module 8: Identity Provider Shibboleth platform

- Apache
- Tomcat
- CAS
- Shibboleth IdP

### Module 9: Implementing identity provider from relational databases



A project of the Seventh Framework  
Programme (FP7)



This project is funded by the European  
Commission



A project implemented by RedCLARA



- Deployment path of an identity provider
- Methodology adopted or
- activities or Route

### Module 10: Identity provider implementation from an existing directory

- Introduction to Shibboleth-IdP
  - Shibboleth-IdP
  - Data source
- Scenario Analysis
- Attributes required by federation
  - Attributes of original scheme
- Mapping definitions
  - Rename attributes
  - Change the attribute value
  - Modify sequence of attributes



A project of the Seventh Framework  
Programme (FP7)

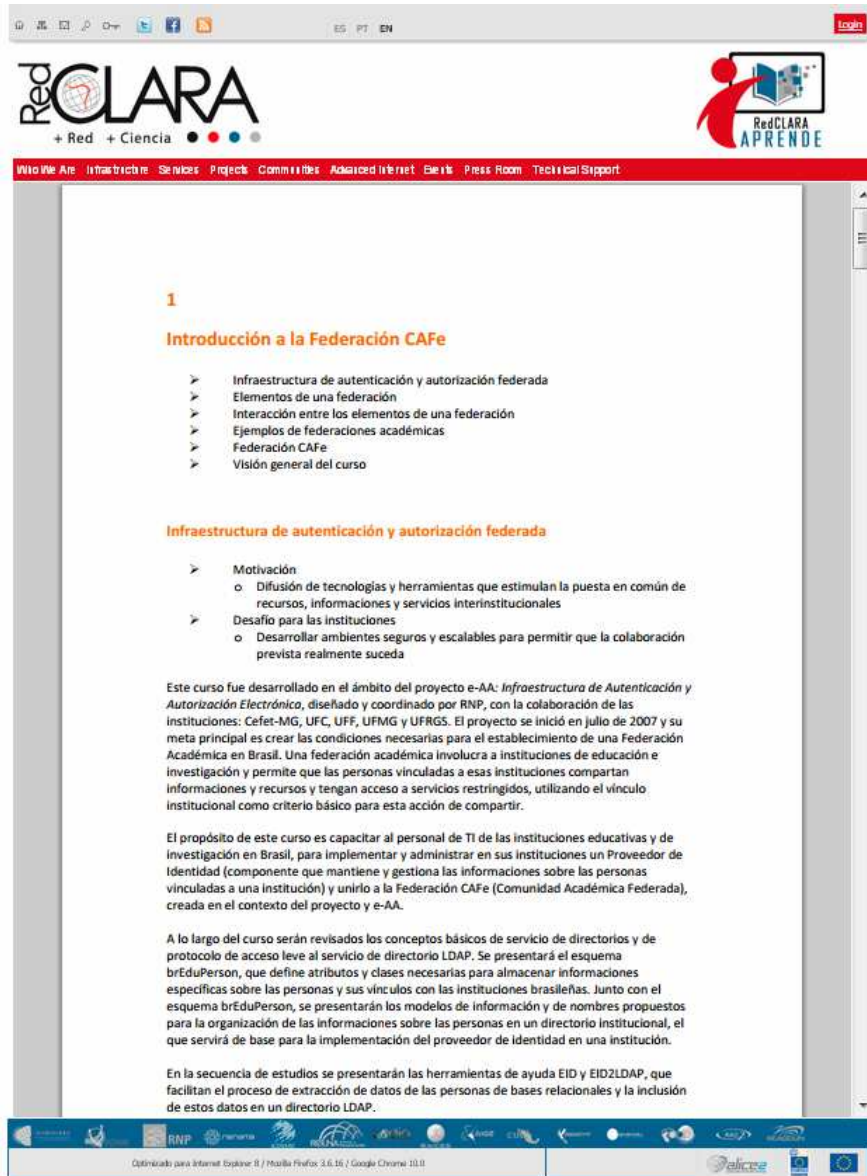


This project is funded by the European  
Commission



A project implemented by RedCLARA

## 2.1 MODULE 1:



The screenshot shows a web browser window displaying the RedCLARA website. The page title is "1 Introducción a la Federación CAFe". The navigation menu includes: Who We Are, Infrastructure, Services, Projects, Committees, Advanced Internet, Events, Press Room, Technical Support. The main content area lists the following topics:

- Infraestructura de autenticación y autorización federada
- Elementos de una federación
- Interacción entre los elementos de una federación
- Ejemplos de federaciones académicas
- Federación CAFe
- Visión general del curso

Below this list, there is a section titled "Infraestructura de autenticación y autorización federada" with sub-points:

- Motivación
  - Difusión de tecnologías y herramientas que estimulan la puesta en común de recursos, informaciones y servicios interinstitucionales
- Desafío para las instituciones
  - Desarrollar ambientes seguros y escalables para permitir que la colaboración prevista realmente suceda

The page also contains several paragraphs of text explaining the course's development, objectives, and the role of the CAFe Federation.



A project of the Seventh Framework Programme (FP7)

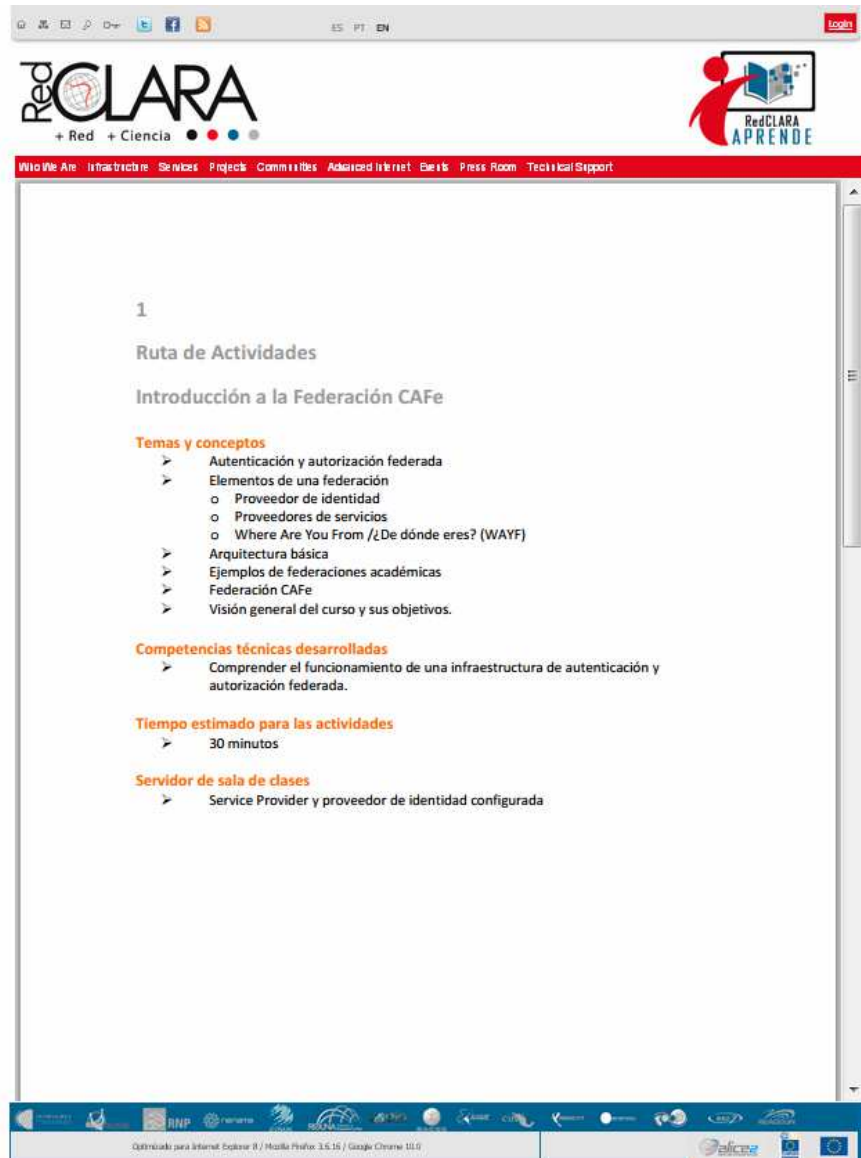


This project is funded by the European Commission



A project implemented by RedCLARA

## 2.2 EXERCISE MODULE 1



The screenshot shows a web browser window displaying the RedCLARA website. The page title is "1 Ruta de Actividades" and the main heading is "Introducción a la Federación CAFe". The content is organized into several sections:

- Temas y conceptos**
  - > Autenticación y autorización federada
  - > Elementos de una federación
    - o Proveedor de identidad
    - o Proveedores de servicios
    - o Where Are You From /¿De dónde eres? (WAYF)
  - > Arquitectura básica
  - > Ejemplos de federaciones académicas
  - > Federación CAFe
  - > Visión general del curso y sus objetivos.
- Competencias técnicas desarrolladas**
  - > Comprender el funcionamiento de una infraestructura de autenticación y autorización federada.
- Tiempo estimado para las actividades**
  - > 30 minutos
- Servidor de sala de clases**
  - > Service Provider y proveedor de identidad configurada

The browser's address bar shows the URL "http://www.redclara.net/". The page footer includes the text "Optimizado para Internet Explorer 8 / Mozilla Firefox 3.5.10 / Google Chrome 10.0" and logos for RNP, RedCLARA, and ELCIRA.



A project of the Seventh Framework  
Programme (FP7)

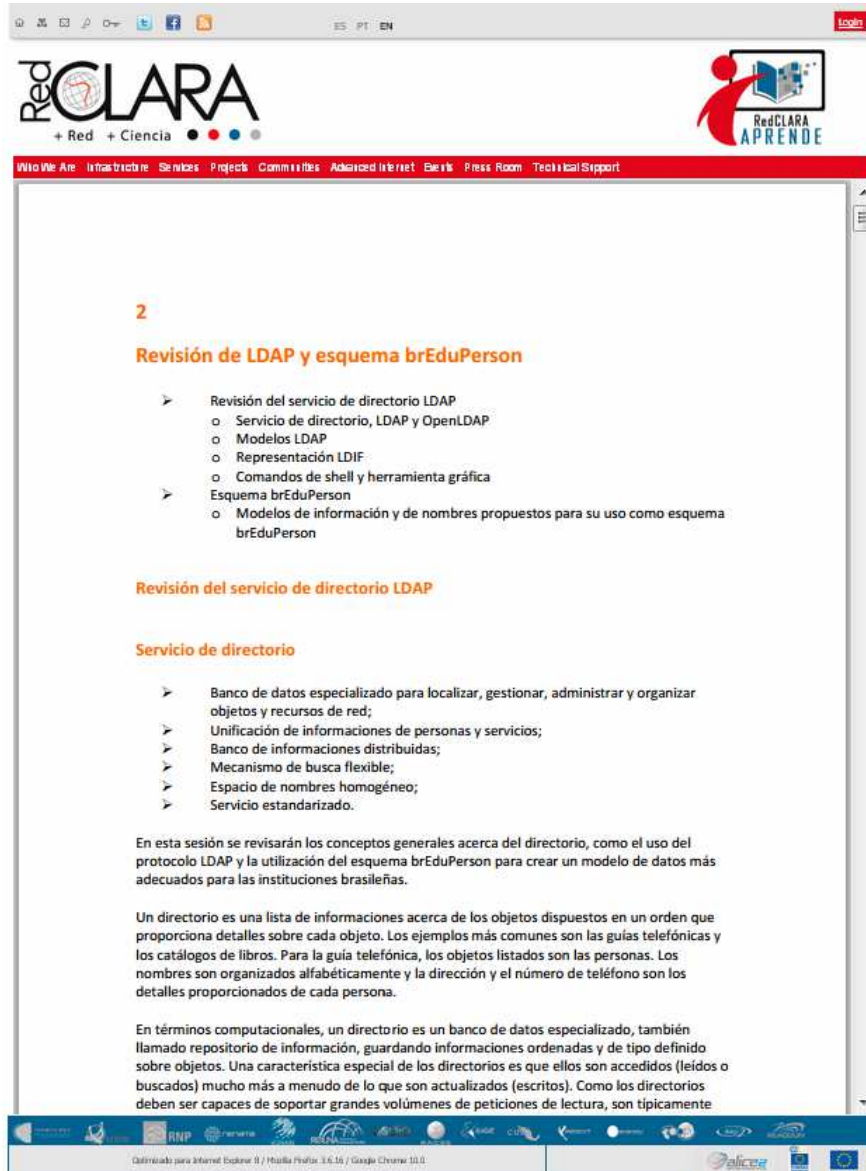


This project is funded by the European  
Commission



A project implemented by RedCLARA

## 2.3 MODULE 2:



The screenshot shows a web browser window displaying the RedCLARA website. The page title is "2 Revisión de LDAP y esquema brEduPerson". The content includes a list of topics to be covered in the session, such as "Revisión del servicio de directorio LDAP" and "Revisión del servicio de directorio LDAP". The page also contains introductory text about directories and LDAP protocols.

### 2

#### Revisión de LDAP y esquema brEduPerson

- Revisión del servicio de directorio LDAP
  - Servicio de directorio, LDAP y OpenLDAP
  - Modelos LDAP
  - Representación LDIF
  - Comandos de shell y herramienta gráfica
- Esquema brEduPerson
  - Modelos de información y de nombres propuestos para su uso como esquema brEduPerson

#### Revisión del servicio de directorio LDAP

#### Servicio de directorio

- Banco de datos especializado para localizar, gestionar, administrar y organizar objetos y recursos de red;
- Unificación de informaciones de personas y servicios;
- Banco de informaciones distribuidas;
- Mecanismo de busca flexible;
- Espacio de nombres homogéneo;
- Servicio estandarizado.

En esta sesión se revisarán los conceptos generales acerca del directorio, como el uso del protocolo LDAP y la utilización del esquema brEduPerson para crear un modelo de datos más adecuados para las instituciones brasileñas.

Un directorio es una lista de informaciones acerca de los objetos dispuestos en un orden que proporciona detalles sobre cada objeto. Los ejemplos más comunes son las guías telefónicas y los catálogos de libros. Para la guía telefónica, los objetos listados son las personas. Los nombres son organizados alfabéticamente y la dirección y el número de teléfono son los detalles proporcionados de cada persona.

En términos computacionales, un directorio es un banco de datos especializado, también llamado repositorio de información, guardando informaciones ordenadas y de tipo definido sobre objetos. Una característica especial de los directorios es que ellos son accedidos (leídos o buscados) mucho más a menudo de lo que son actualizados (escritos). Como los directorios deben ser capaces de soportar grandes volúmenes de peticiones de lectura, son típicamente



A project of the Seventh Framework Programme (FP7)

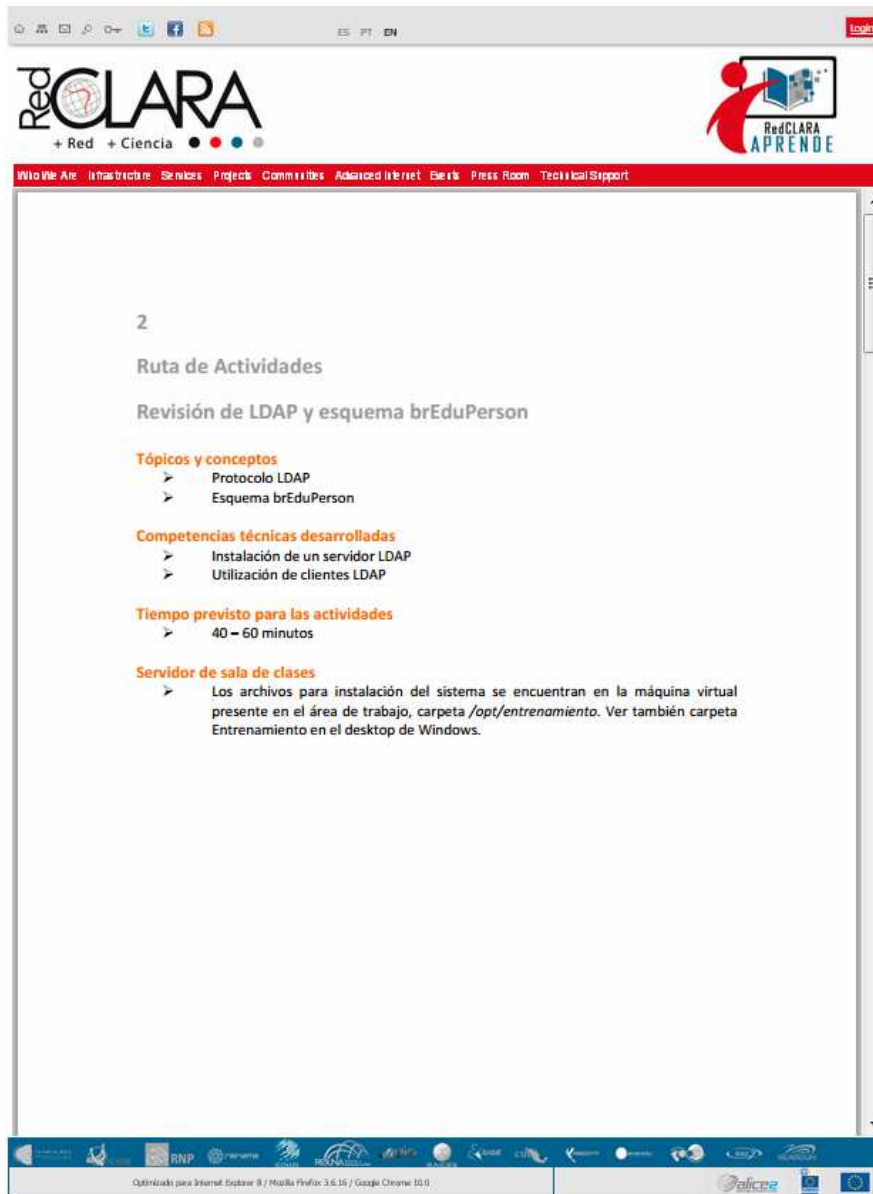


This project is funded by the European Commission



A project implemented by RedCLARA

## 2.4 EXERCISE MODULE 2



The screenshot shows a web browser window displaying the RedCLARA website. The page title is "2 Ruta de Actividades" and the main heading is "Revisión de LDAP y esquema brEduPerson". The content is organized into several sections:

- Tópicos y conceptos**
  - Protocolo LDAP
  - Esquema brEduPerson
- Competencias técnicas desarrolladas**
  - Instalación de un servidor LDAP
  - Utilización de clientes LDAP
- Tiempo previsto para las actividades**
  - 40 - 60 minutos
- Servidor de sala de clases**
  - Los archivos para instalación del sistema se encuentran en la máquina virtual presente en el área de trabajo, carpeta */opt/entrenamiento*. Ver también carpeta Entrenamiento en el desktop de Windows.

The browser's address bar shows the URL <http://www.redclara.net>. The footer of the page contains logos for the Seventh Framework Programme, the European Commission, and RedCLARA.



A project of the Seventh Framework Programme (FP7)

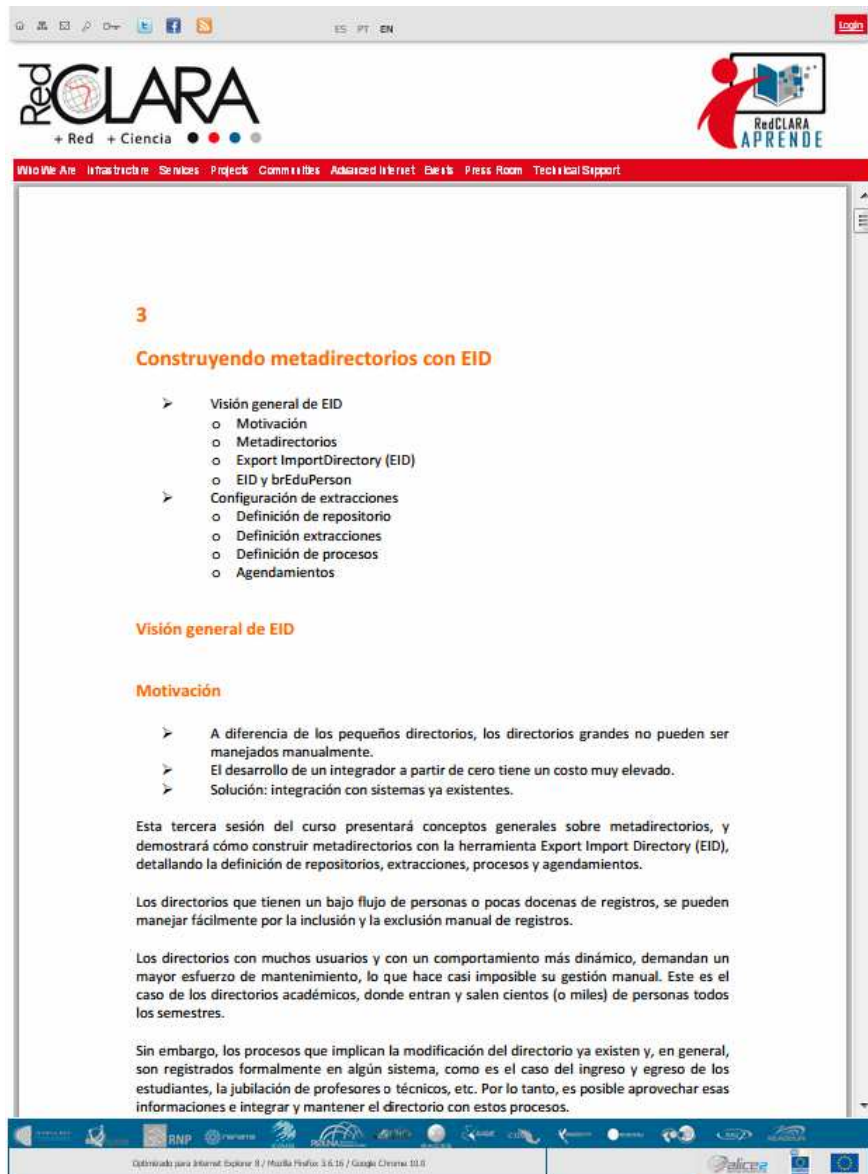


This project is funded by the European Commission



A project implemented by RedCLARA

## 2.5 MODULE 3



**3**

### Construyendo metadirectorios con EID

- Visión general de EID
  - Motivación
  - Metadirectorios
  - Export Import Directory (EID)
  - EID y brEduPerson
- Configuración de extracciones
  - Definición de repositorio
  - Definición extracciones
  - Definición de procesos
  - Agendamientos

#### Visión general de EID

#### Motivación

- A diferencia de los pequeños directorios, los directorios grandes no pueden ser manejados manualmente.
- El desarrollo de un integrador a partir de cero tiene un costo muy elevado.
- Solución: integración con sistemas ya existentes.

Esta tercera sesión del curso presentará conceptos generales sobre metadirectorios, y demostrará cómo construir metadirectorios con la herramienta Export Import Directory (EID), detallando la definición de repositorios, extracciones, procesos y agendamientos.

Los directorios que tienen un bajo flujo de personas o pocas docenas de registros, se pueden manejar fácilmente por la inclusión y la exclusión manual de registros.

Los directorios con muchos usuarios y con un comportamiento más dinámico, demandan un mayor esfuerzo de mantenimiento, lo que hace casi imposible su gestión manual. Este es el caso de los directorios académicos, donde entran y salen cientos (o miles) de personas todos los semestres.

Sin embargo, los procesos que implican la modificación del directorio ya existen y, en general, son registrados formalmente en algún sistema, como es el caso del ingreso y egreso de los estudiantes, la jubilación de profesores o técnicos, etc. Por lo tanto, es posible aprovechar esas informaciones e integrar y mantener el directorio con estos procesos.



A project of the Seventh Framework Programme (FP7)

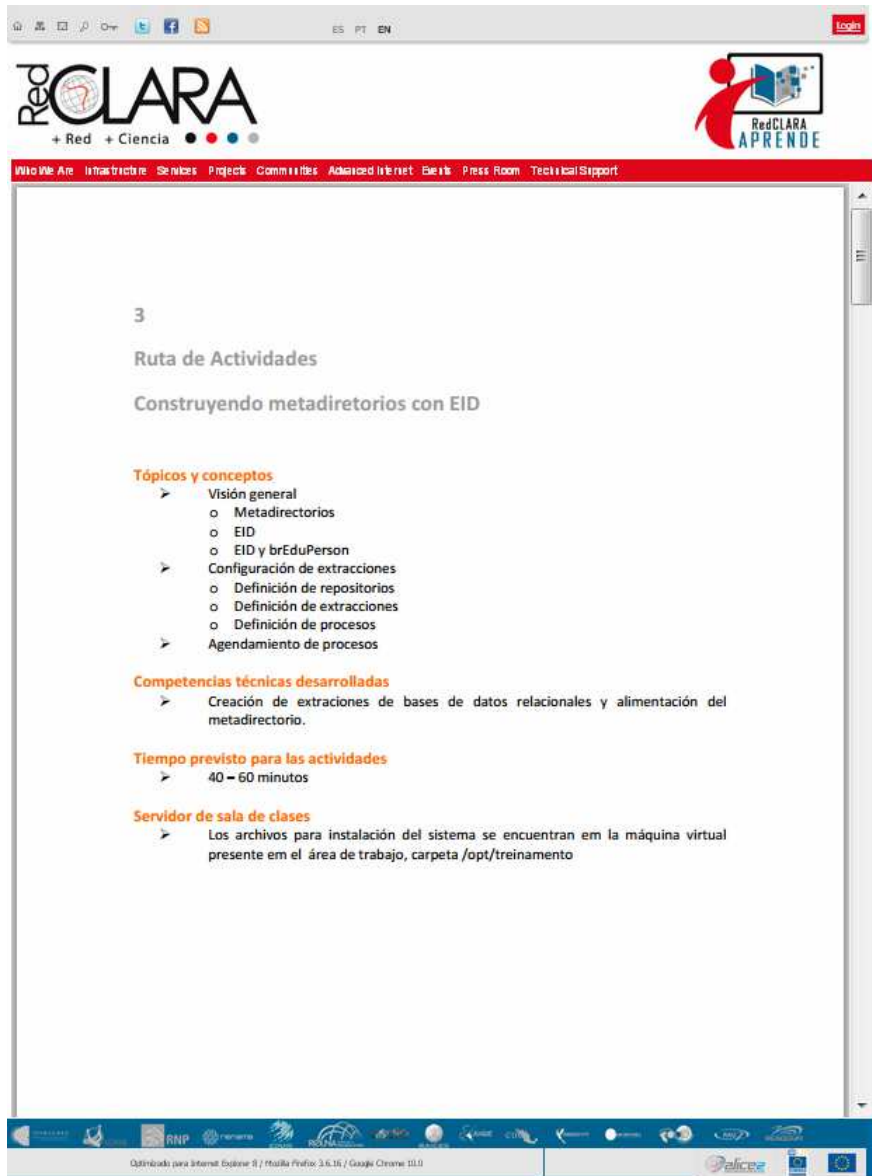


This project is funded by the European Commission



A project implemented by RedCLARA

## 2.6 EXERCISE MODULE 3



The screenshot shows a web browser window displaying the RedCLARA website. The page title is '3 Ruta de Actividades' and the main heading is 'Construyendo metadirectorios con EID'. The content is organized into several sections:

- Tópicos y conceptos**
  - **Visión general**
    - Metadirectorios
    - EID
    - EID y brEduPerson
  - **Configuración de extracciones**
    - Definición de repositorios
    - Definición de extracciones
    - Definición de procesos
  - **Agendamiento de procesos**
- Competencias técnicas desarrolladas**
  - Creación de extracciones de bases de datos relacionales y alimentación del metadirectorio.
- Tiempo previsto para las actividades**
  - 40 – 60 minutos
- Servidor de sala de clases**
  - Los archivos para instalación del sistema se encuentran en la máquina virtual presente en el área de trabajo, carpeta /opt/treinamento

The browser's address bar shows the URL 'http://www.redclara.europa.eu/...'. The website header includes the RedCLARA logo and navigation links like 'Who We Are', 'Infrastructure', 'Services', 'Projects', 'Committees', 'Advanced Internet', 'Events', 'Press Room', and 'Technical Support'. The footer contains logos for the Seventh Framework Programme, the European Commission, and RedCLARA.



A project of the Seventh Framework Programme (FP7)

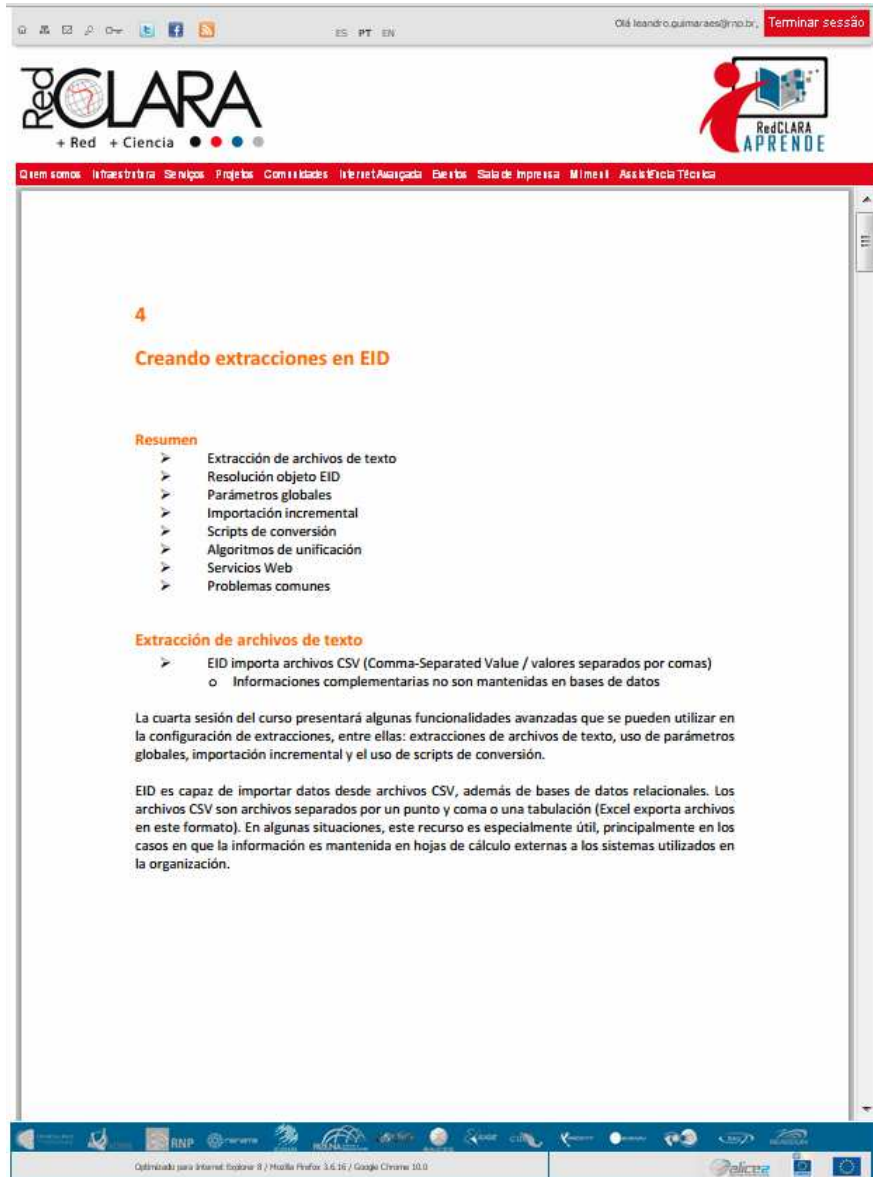


This project is funded by the European Commission



A project implemented by RedCLARA

## 2.7 MODULE 4



4

### Creando extracciones en EID

**Resumen**

- Extracción de archivos de texto
- Resolución objeto EID
- Parámetros globales
- Importación incremental
- Scripts de conversión
- Algoritmos de unificación
- Servicios Web
- Problemas comunes

**Extracción de archivos de texto**

- EID importa archivos CSV (Comma-Separated Value / valores separados por comas)
  - Informaciones complementarias no son mantenidas en bases de datos

La cuarta sesión del curso presentará algunas funcionalidades avanzadas que se pueden utilizar en la configuración de extracciones, entre ellas: extracciones de archivos de texto, uso de parámetros globales, importación incremental y el uso de scripts de conversión.

EID es capaz de importar datos desde archivos CSV, además de bases de datos relacionales. Los archivos CSV son archivos separados por un punto y coma o una tabulación (Excel exporta archivos en este formato). En algunas situaciones, este recurso es especialmente útil, principalmente en los casos en que la información es mantenida en hojas de cálculo externas a los sistemas utilizados en la organización.



A project of the Seventh Framework Programme (FP7)



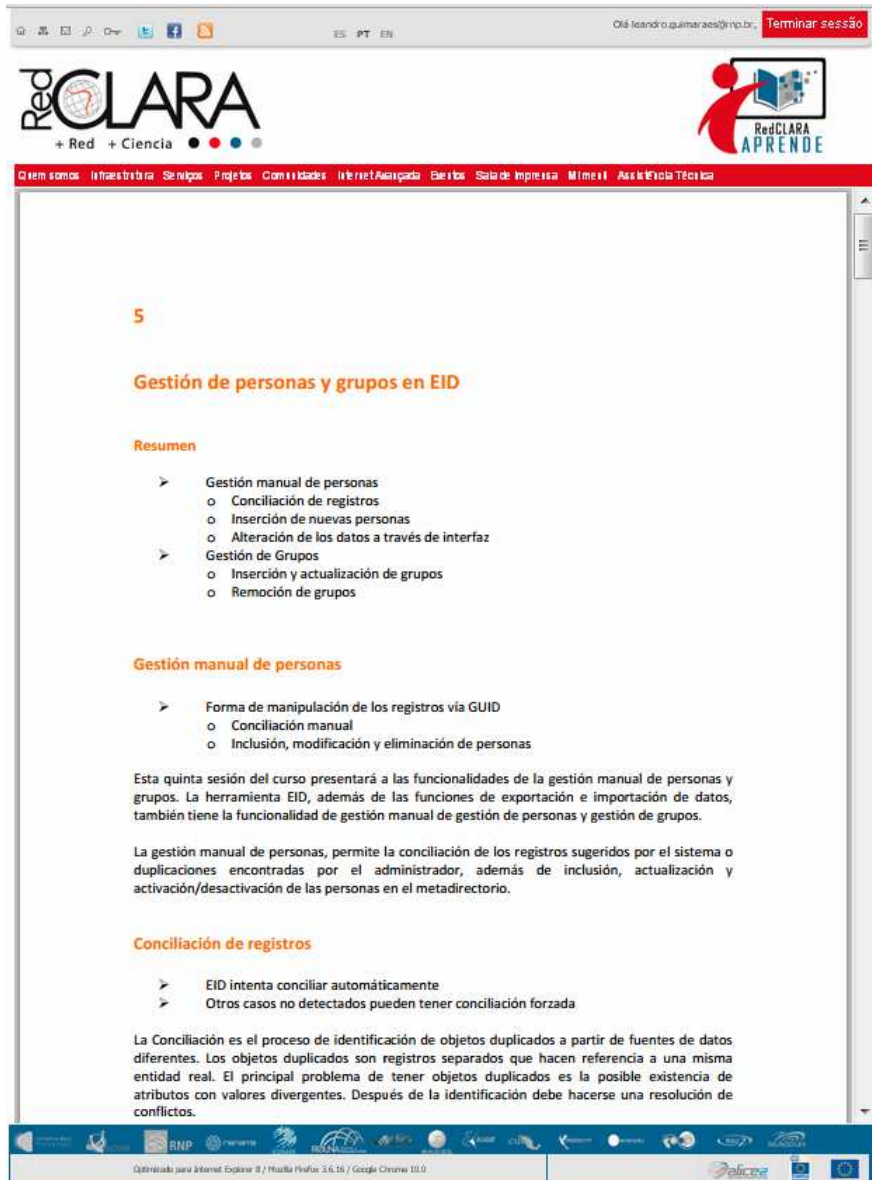
This project is funded by the European Commission



A project implemented by RedCLARA



## 2.8 MODULE 5



**5**

### Gestión de personas y grupos en EID

**Resumen**

- Gestión manual de personas
  - Conciliación de registros
  - Inserción de nuevas personas
  - Alteración de los datos a través de interfaz
- Gestión de Grupos
  - Inserción y actualización de grupos
  - Remoción de grupos

**Gestión manual de personas**

- Forma de manipulación de los registros vía GUID
  - Conciliación manual
  - Inclusión, modificación y eliminación de personas

Esta quinta sesión del curso presentará a las funcionalidades de la gestión manual de personas y grupos. La herramienta EID, además de las funciones de exportación e importación de datos, también tiene la funcionalidad de gestión manual de gestión de personas y gestión de grupos.

La gestión manual de personas, permite la conciliación de los registros sugeridos por el sistema o duplicaciones encontradas por el administrador, además de inclusión, actualización y activación/desactivación de las personas en el metadirectorio.

**Conciliación de registros**

- EID intenta conciliar automáticamente
- Otros casos no detectados pueden tener conciliación forzada

La Conciliación es el proceso de identificación de objetos duplicados a partir de fuentes de datos diferentes. Los objetos duplicados son registros separados que hacen referencia a una misma entidad real. El principal problema de tener objetos duplicados es la posible existencia de atributos con valores divergentes. Después de la identificación debe hacerse una resolución de conflictos.



A project of the Seventh Framework Programme (FP7)



This project is funded by the European Commission



A project implemented by RedCLARA

## 2.9 MODULE 6



**6**

### Alimentación de directorios con EID2LDAP

**Resumen**

- Introducción
  - EID2LDAP
  - Características
- Arquitectura
  - XML de EID
  - XSLT
  - Procesamiento de LDIF
- Configuración y uso
- Problemas comunes

**Introducción**

#### EID2LDAP

- Busca informaciones del directorio almacenadas en un servidor EID y los transfiere a los servidores LDAP.

La sexta sesión del curso presentará la herramienta EID2LDAP. La introducción se refiere a sus características y su arquitectura (XML de EID, XSLT y procesamiento LDIF); son vistas las configuraciones y algunos ejemplos de uso de la herramienta, incluyendo los problemas comunes.

El EID2LDAP es una herramienta que tiene acceso al servidor EID a través de servicios web, transforma los registros al formato LDIF compatible con el servidor LDAP de destino y transfiere las informaciones.

#### Características

- Permite el agendamiento periódico de exportación
  - En cada exportación, se actualizan sólo los registros modificados/insertados/suprimidos desde la última exportación
- Acceda a EID vía servicios Web



A project of the Seventh Framework Programme (FP7)

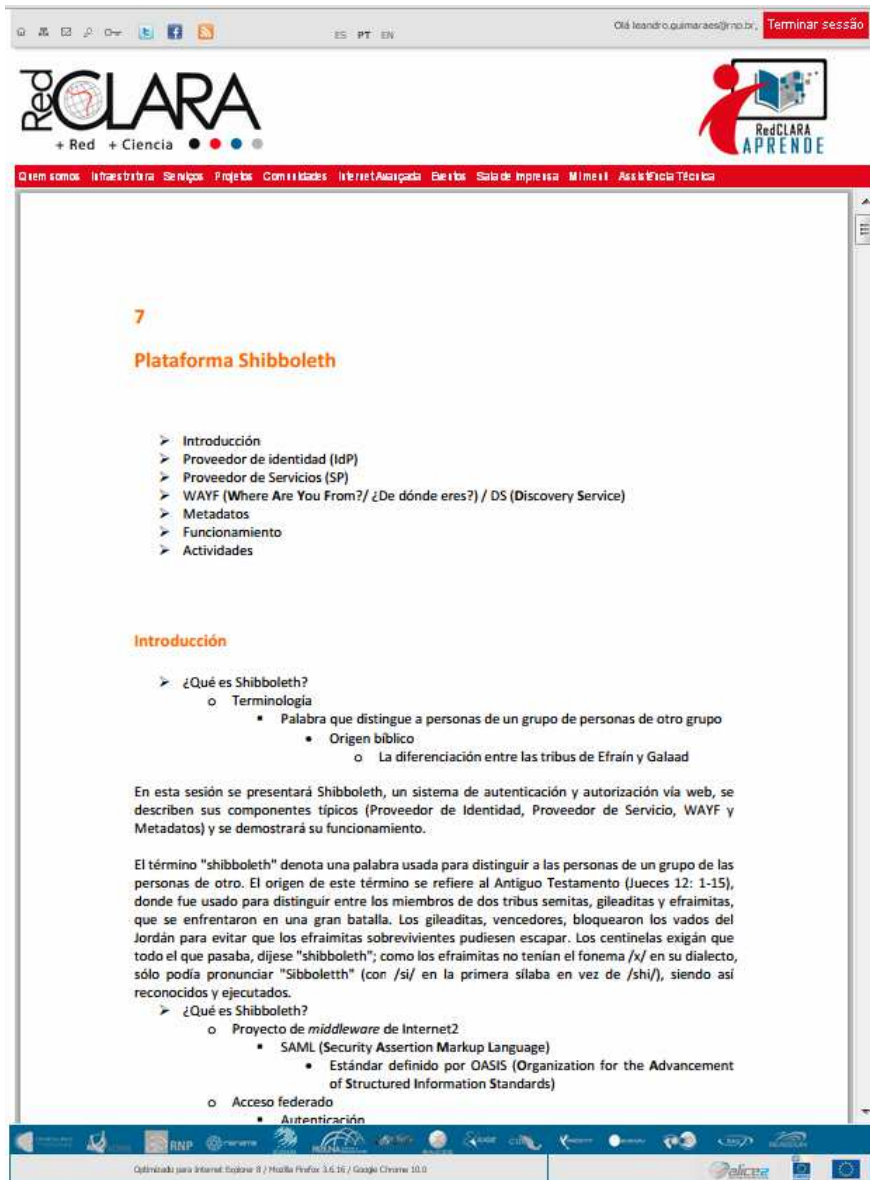


This project is funded by the European Commission



A project implemented by RedCLARA

## 2.10 MODULE 7



7

### Plataforma Shibboleth

- Introducción
- Proveedor de identidad (IdP)
- Proveedor de Servicios (SP)
- WAYF (Where Are You From? / ¿De dónde eres?) / DS (Discovery Service)
- Metadatos
- Funcionamiento
- Actividades

#### Introducción

- ¿Qué es Shibboleth?
  - Terminología
    - Palabra que distingue a personas de un grupo de personas de otro grupo
      - Origen bíblico
        - La diferenciación entre las tribus de Efraim y Galaad

En esta sesión se presentará Shibboleth, un sistema de autenticación y autorización vía web, se describen sus componentes típicos (Proveedor de Identidad, Proveedor de Servicio, WAYF y Metadatos) y se demostrará su funcionamiento.

El término "shibboleth" denota una palabra usada para distinguir a las personas de un grupo de las personas de otro. El origen de este término se refiere al Antiguo Testamento (Jueces 12: 1-15), donde fue usado para distinguir entre los miembros de dos tribus semitas, gileaditas y efraimitas, que se enfrentaron en una gran batalla. Los gileaditas, vencedores, bloquearon los vados del Jordán para evitar que los efraimitas sobrevivientes pudiesen escapar. Los centinelas exigían que todo el que pasaba, dijese "shibboleth"; como los efraimitas no tenían el fonema /x/ en su dialecto, sólo podía pronunciar "Sibboleth" (con /s/ en la primera sílaba en vez de /sh/), siendo así reconocidos y ejecutados.

- ¿Qué es Shibboleth?
  - Proyecto de *middleware* de Internet2
    - SAML (Security Assertion Markup Language)
      - Estándar definido por OASIS (Organization for the Advancement of Structured Information Standards)
  - Acceso federado
    - Autenticación

Optimizado para Internet Explorer 8 / Mozilla Firefox 3.6.16 / Google Chrome 10.0



A project of the Seventh Framework Programme (FP7)

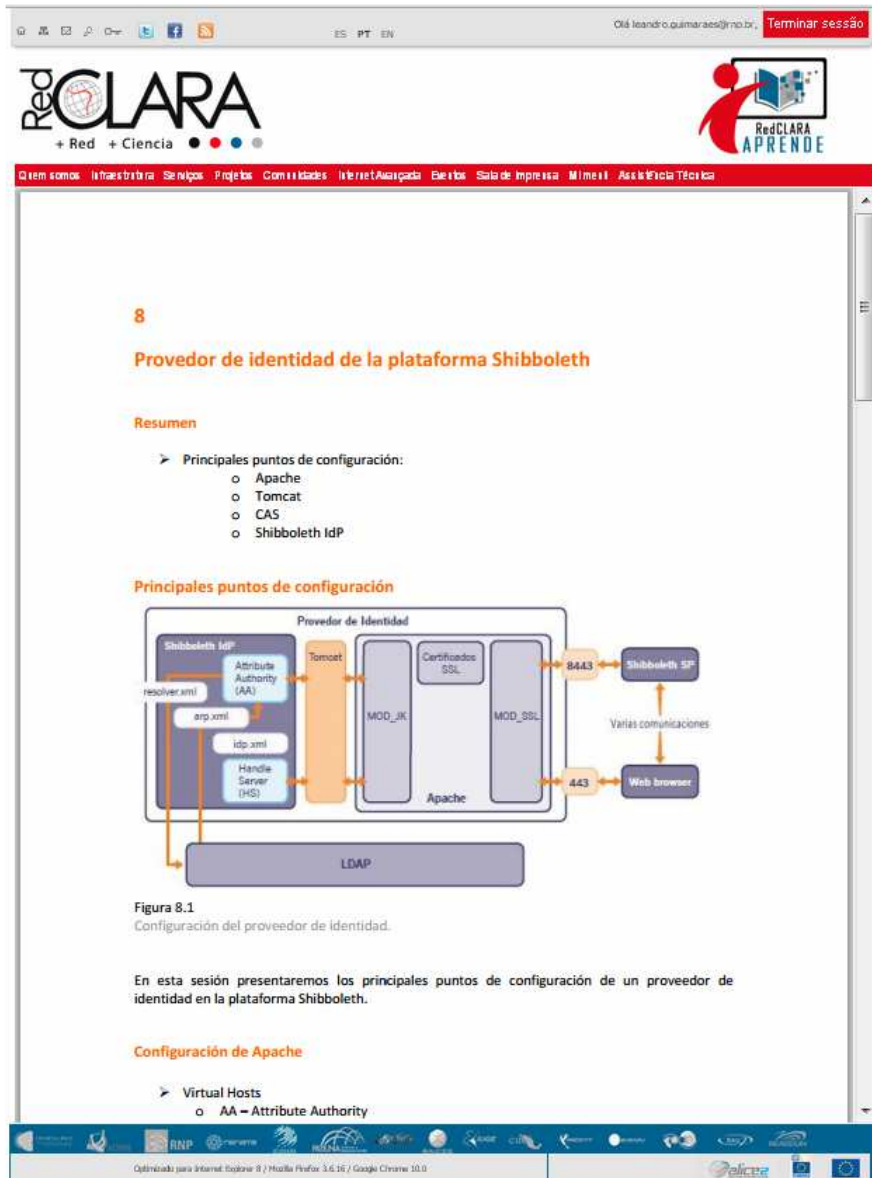


This project is funded by the European Commission



A project implemented by RedCLARA

## 2.11 MODULE 8



The screenshot shows a web browser window displaying a training module page. The page title is "8 Proveedor de identidad de la plataforma Shibboleth". The page content includes a "Resumen" section with a list of configuration points: Apache, Tomcat, CAS, and Shibboleth IdP. Below this is a diagram titled "Principales puntos de configuración" showing the architecture of the Shibboleth IdP. The diagram includes components like Shibboleth IdP, Tomcat, Apache, and LDAP. The Apache component is further detailed with sub-components: MOD\_JK, Certificados SSL, and MOD\_SSL. The diagram also shows connections to Shibboleth SP and a Web browser. The page footer includes a navigation bar with various links and a footer with logos for the Seventh Framework Programme, European Commission, and RedCLARA.

### 8 Proveedor de identidad de la plataforma Shibboleth

**Resumen**

- Principales puntos de configuración:
  - o Apache
  - o Tomcat
  - o CAS
  - o Shibboleth IdP

**Principales puntos de configuración**

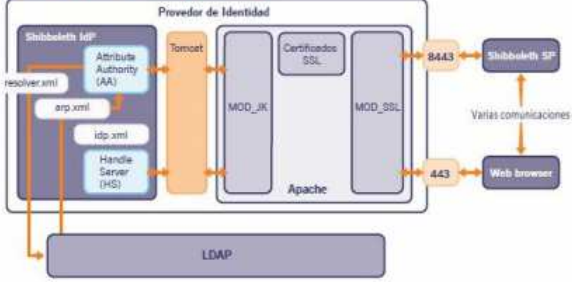


Figura 8.1  
Configuración del proveedor de identidad.

En esta sesión presentaremos los principales puntos de configuración de un proveedor de identidad en la plataforma Shibboleth.

**Configuración de Apache**

- Virtual Hosts
  - o AA – Attribute Authority



A project of the Seventh Framework  
Programme (FP7)

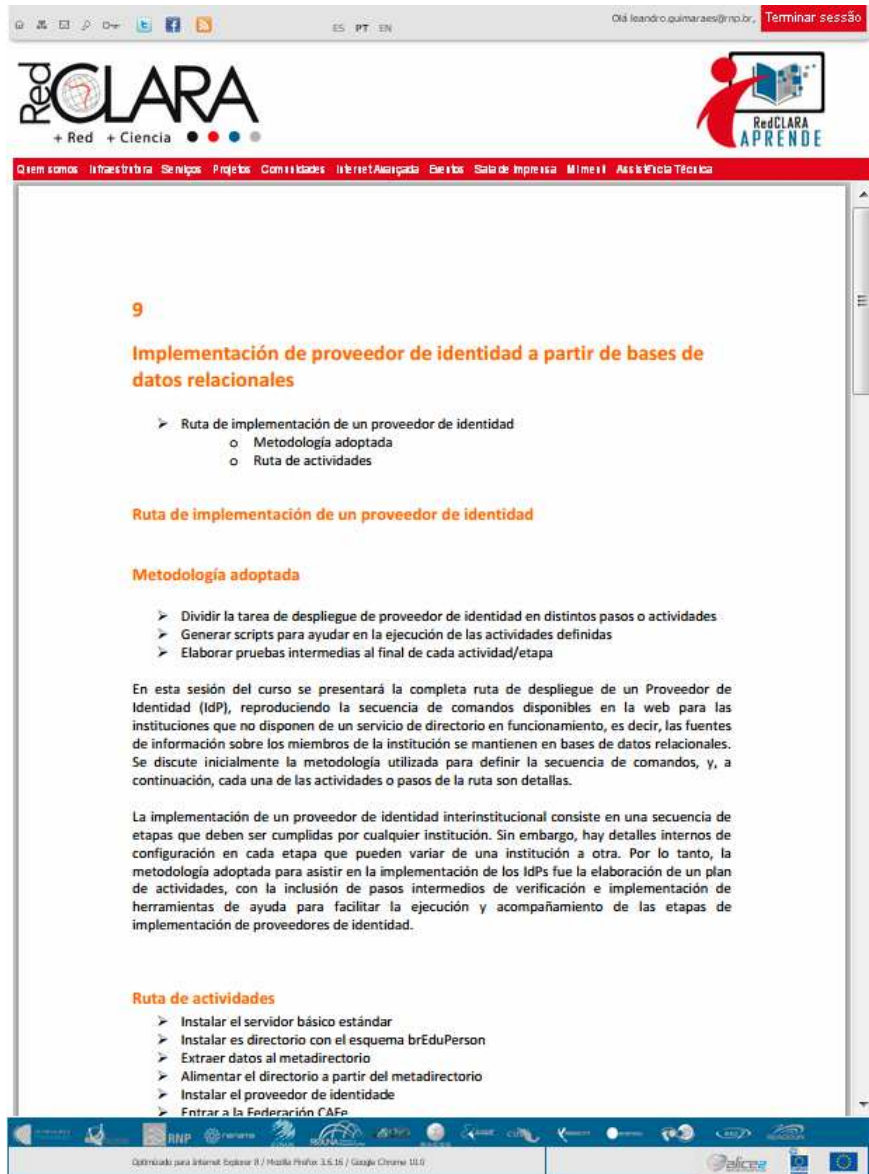


This project is funded by the European  
Commission



A project implemented by RedCLARA

## 2.12 MODULE 9



9

### Implementación de proveedor de identidad a partir de bases de datos relacionales

- Ruta de implementación de un proveedor de identidad
  - Metodología adoptada
  - Ruta de actividades

#### Ruta de implementación de un proveedor de identidad

#### Metodología adoptada

- Dividir la tarea de despliegue de proveedor de identidad en distintos pasos o actividades
- Generar scripts para ayudar en la ejecución de las actividades definidas
- Elaborar pruebas intermedias al final de cada actividad/etapa

En esta sesión del curso se presentará la completa ruta de despliegue de un Proveedor de Identidad (IdP), reproduciendo la secuencia de comandos disponibles en la web para las instituciones que no disponen de un servicio de directorio en funcionamiento, es decir, las fuentes de información sobre los miembros de la institución se mantienen en bases de datos relacionales. Se discute inicialmente la metodología utilizada para definir la secuencia de comandos, y, a continuación, cada una de las actividades o pasos de la ruta son detalladas.

La implementación de un proveedor de identidad interinstitucional consiste en una secuencia de etapas que deben ser cumplidas por cualquier institución. Sin embargo, hay detalles internos de configuración en cada etapa que pueden variar de una institución a otra. Por lo tanto, la metodología adoptada para asistir en la implementación de los IdPs fue la elaboración de un plan de actividades, con la inclusión de pasos intermedios de verificación e implementación de herramientas de ayuda para facilitar la ejecución y acompañamiento de las etapas de implementación de proveedores de identidad.

#### Ruta de actividades

- Instalar el servidor básico estándar
- Instalar es directorio con el esquema brEduPerson
- Extraer datos al metadirectorio
- Alimentar el directorio a partir del metadirectorio
- Instalar el proveedor de identidad
- Entrar a la Federación CAFE



A project of the Seventh Framework Programme (FP7)

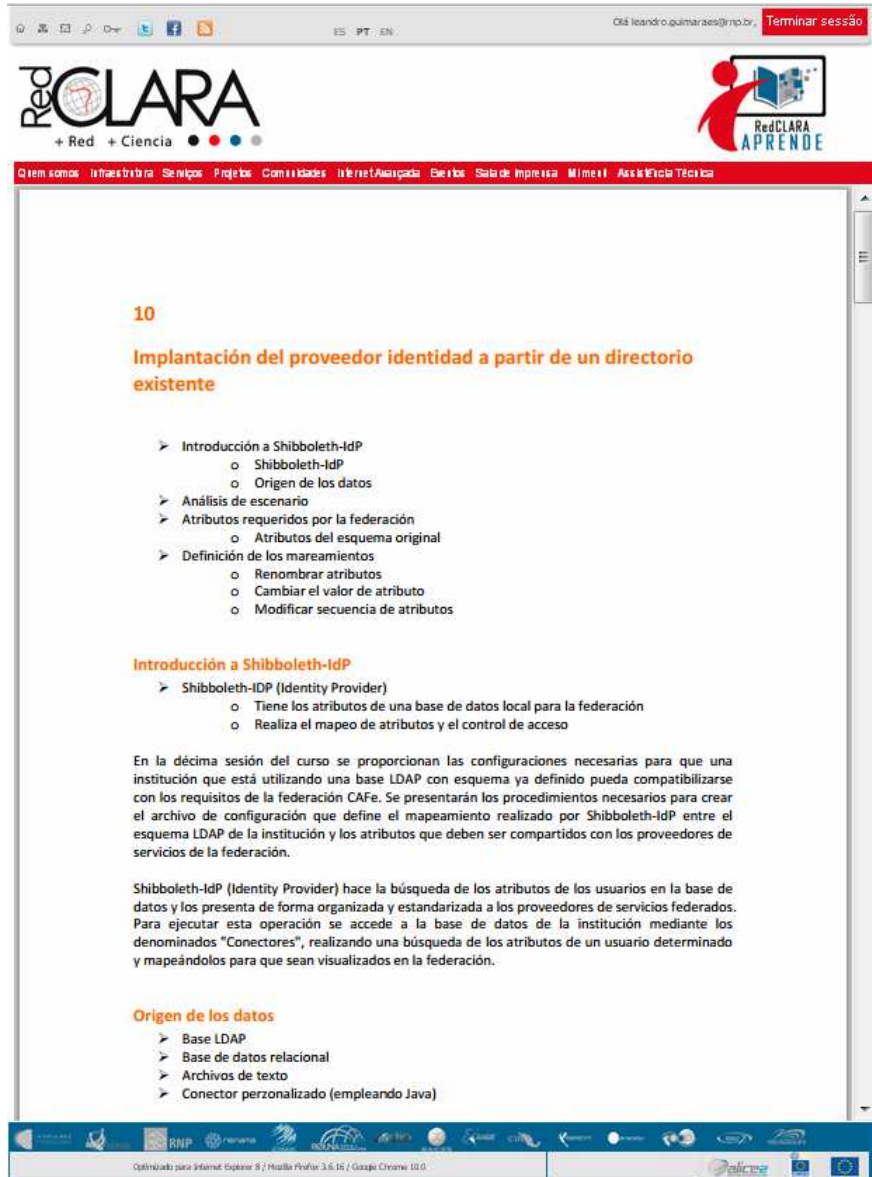


This project is funded by the European Commission



A project implemented by RedCLARA

## 2.13 MODULE 10



**10**

### Implantación del proveedor identidad a partir de un directorio existente

- Introducción a Shibboleth-IdP
  - Shibboleth-IdP
  - Origen de los datos
- Análisis de escenario
- Atributos requeridos por la federación
  - Atributos del esquema original
- Definición de los mapeamientos
  - Renombrar atributos
  - Cambiar el valor de atributo
  - Modificar secuencia de atributos

#### Introducción a Shibboleth-IdP

- Shibboleth-IDP (Identity Provider)
  - Tiene los atributos de una base de datos local para la federación
  - Realiza el mapeo de atributos y el control de acceso

En la décima sesión del curso se proporcionan las configuraciones necesarias para que una institución que está utilizando una base LDAP con esquema ya definido pueda compatibilizarse con los requisitos de la federación CAFe. Se presentarán los procedimientos necesarios para crear el archivo de configuración que define el mapeamiento realizado por Shibboleth-IdP entre el esquema LDAP de la institución y los atributos que deben ser compartidos con los proveedores de servicios de la federación.

Shibboleth-IdP (Identity Provider) hace la búsqueda de los atributos de los usuarios en la base de datos y los presenta de forma organizada y estandarizada a los proveedores de servicios federados. Para ejecutar esta operación se accede a la base de datos de la institución mediante los denominados "Conectores", realizando una búsqueda de los atributos de un usuario determinado y mapeándolos para que sean visualizados en la federación.

#### Origen de los datos

- Base LDAP
- Base de datos relacional
- Archivos de texto
- Conector personalizado (empleando Java)



A project of the Seventh Framework Programme (FP7)



This project is funded by the European Commission



A project implemented by RedCLARA