



GOBIERNO
DE ESPAÑA

MINISTERIO
DE CIENCIA
E INNOVACIÓN

MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

SECRETARÍA DE ESTADO
DE TELECOMUNICACIONES
Y PARA LA SOCIEDAD DE
LA INFORMACIÓN



Red
IRIS

SIR

¿Cuánto más vas a esperar?

Cándido Rodríguez

candido.rodriguez@rediris.es

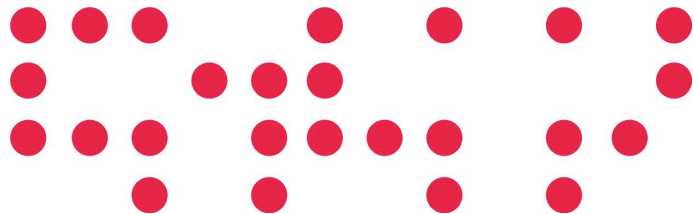
1. ¿Qué es el SIR?

2. ¿Cómo unirse?

3. Novedades

4. Estadísticas

5. Futuro



¿Qué es el SIR?

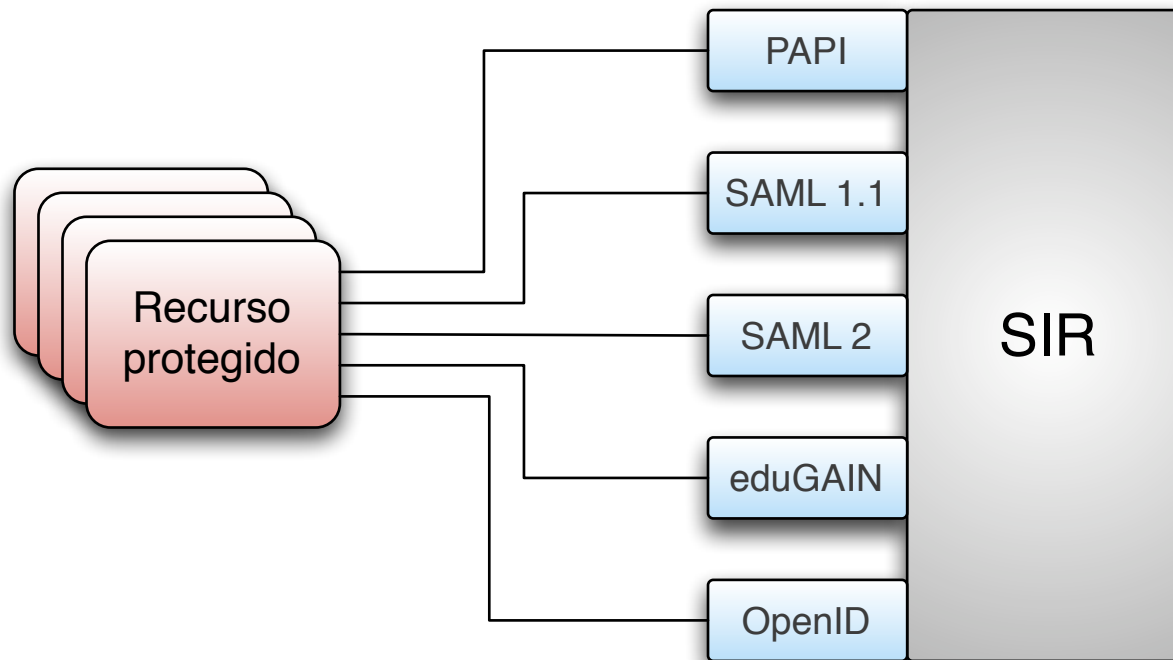


Red IRIS

- Es un hub de interconexión entre proveedores de identidad y de servicio
 - Instituciones dando acceso a sus usuarios
 - Recursos protegidos potencialmente disponibles a todas las instituciones
- Bases de una federación
 - Proveedor de identidad
 - Realiza la autenticación del usuario y emite los atributos del usuario
 - Proveedor de servicio
 - Comprueba las credenciales del usuario para realizar la autorización en el acceso al servicio
- Papel de RedIRIS en esta federación
 - Actúa de intermediario de confianza

¿Qué es el SIR?

- La federación SIR soporta los siguientes protocolos:



¿Qué es el SIR?



GOBIERNO DE ESPAÑA

MINISTERIO DE CIENCIA E INNOVACIÓN

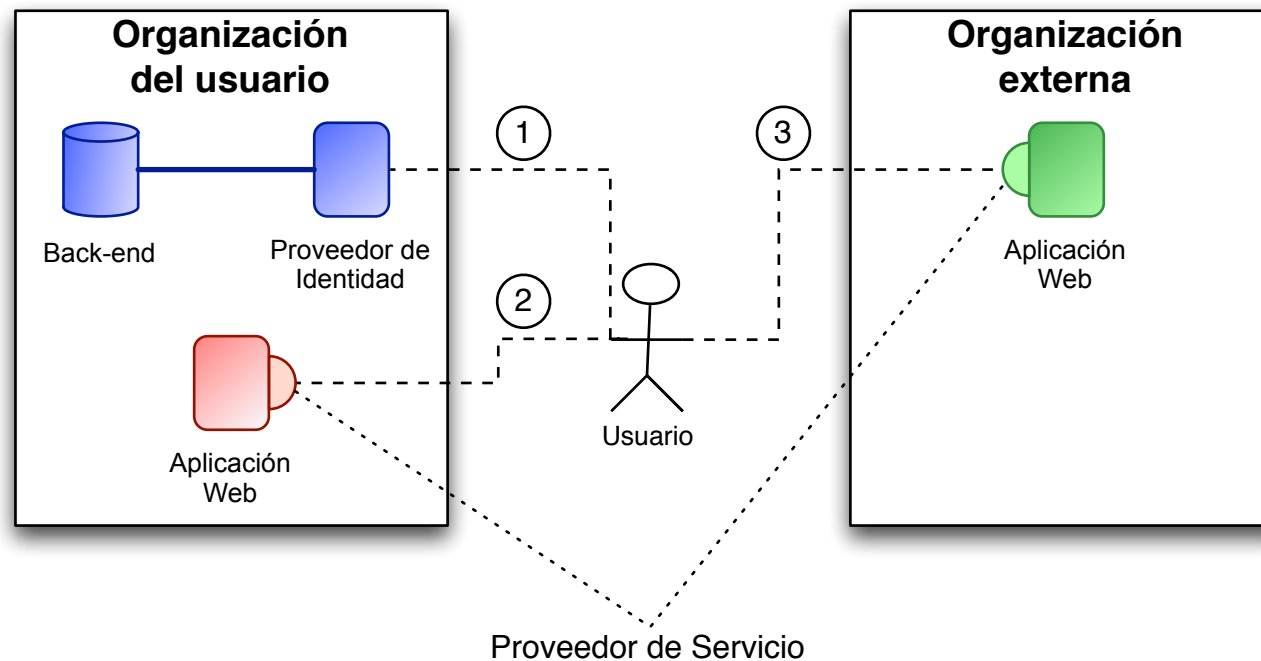
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

SECRETARÍA DE ESTADO DE TELECOMUNICACIONES Y PARA LA SOCIEDAD DE LA INFORMACIÓN



Red IRIS

- El funcionamiento del SIR se basa en tecnologías de federación de identidades



- **Ventajas de una federación**
 - No se gestionan las cuentas de usuario de instituciones externas
 - Reducimos costes en la gestión de nuestra infraestructura
 - Baja la complejidad de las políticas de seguridad
 - Cumplimos con la LOPD
 - Los usuarios sólo tienen que recordar un par usuario/contraseña
 - Menos post-it → más seguridad
 - El usuario no tiene que solicitar uno a uno acceso a los proveedores de servicio
 - Una vez que añadimos un recurso a la federación, queda potencialmente disponible para el usuario

- **Ventajas para una institución**
 - Acceso a los recursos protegidos ofrecidos en el SIR
 - Aunque algunos requieren contrato previo
 - Infraestructura federada de autenticación y autorización
 - Incluso si no tiene un software de IAA
 - Conectores para LDAP, BBDD, ...
 - Uso de los protocolos de IAA en SIR
 - Metadatos por institución
 - Proveedor de identidad para uso interno
 - <http://yo.rediris.es/>
 - Estadísticas

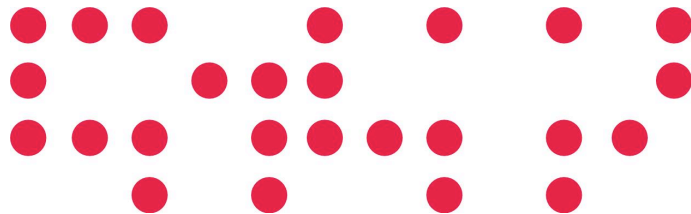
1. Estado actual del SIR

2. ¿Cómo unirse?

3. Novedades

4. Estadísticas

5. Futuro



¿Cómo unirse?



Red IRIS

- Único requerimiento técnico
 - Tener usuarios
- Contactar con sir@rediris.es
 - Analizar caso
 - Conectar software de SSO o despliegue de conector
 - Añadir institución en la federación de pruebas
 - No hay ningún tipo de compromiso
 - Validar capacidad técnica
- Enviar documento de condiciones de uso firmado

- Más información en
 - <http://www.rediris.es/sir/howto-idp.html>

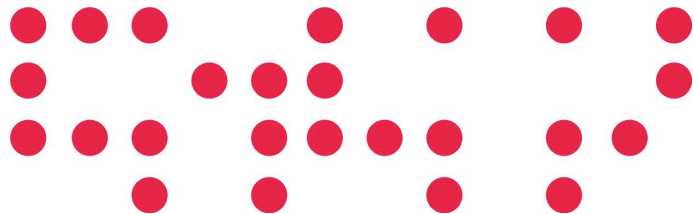
1. Estado actual del SIR

2. ¿Cómo unirse?

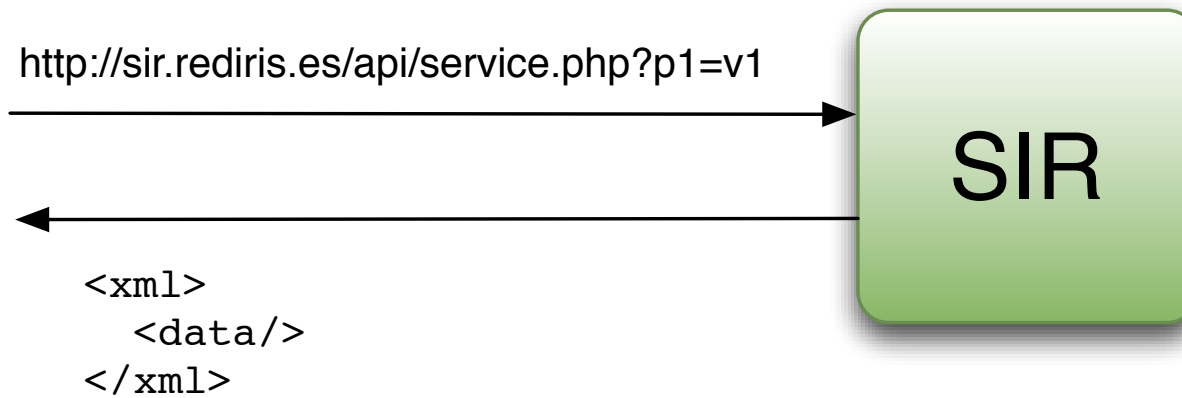
3. Novedades

4. Estadísticas

5. Futuro



- Creación de una API tipo REST para SIR
 - Acceso WAYFless
 - Lista de SPs para un IdP
 - Lista de IdPs



- Acceso WAYFless
 - Acceder al recurso sin preguntar la institución del usuario
- No es posible con todos los SPs
- URL de acceso
 - Parámetros de entrada
 - spid
 - idpid
 - <http://sir.rediris.es/idpfirst/?idpid=xxx&spid=yyy>
- Ejemplo
 - <http://sir.rediris.es/idpfirst/?idpid=us&spid=sciencedirect>

- Lista de proveedores de servicio para una institución
 - Información en XML
- Muchos SPs no están abiertos a todo el SIR
 - Hay que incluir manualmente la disponibilidad
- URL de acceso
 - Parámetros de entrada
 - **ididp**: ID proveedor identidad en SIR
 - lang: idioma, es o en.
 - idsp: ID proveedor de servicio en SIR
 - prot: protocolo de conexión
 - category: categoría a la que pertenece
 - http://www.rediris.es/sir/api/sps_available.php
- http://www.rediris.es/sir/devel/api-sps_available.html

- Lista de proveedores de identidad en SIR
 - schachHomeOrganization
 - IDs de sus conectores de Shibboleth / SAML
 - Información en XML
- http://www.rediris.es/sir/api/idps_available.php

- Proveedor de identidad que cubre los casos:
 - La institución del usuario no está en SIR
 - La institución del usuario no le añade un entitlement
 - ... y no se crea automáticamente la cuenta
- ¿Es el inicio del fin de la federación?
 - ¡¡NO!!



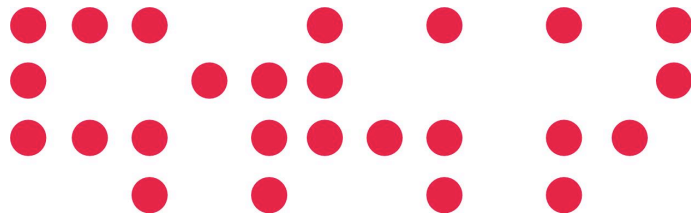
- **Pocos proveedores de servicio funcionan con SIR**
 - Proveedores de servicio de RedIRIS: IRISRBL, Wikis, ...
 - ... por ahora ...
- **Alta de usuario**
 - <http://www.rediris.es/sir/aesir/>
 - Usuario solicita alta de usuario
 - ID usuario debe ser un correo electrónico
 - Comentario ayuda a aceptar alta
 - Validamos datos de usuario
 - Validamos cumple requisitos
 - Envío de contraseña aleatoria por email

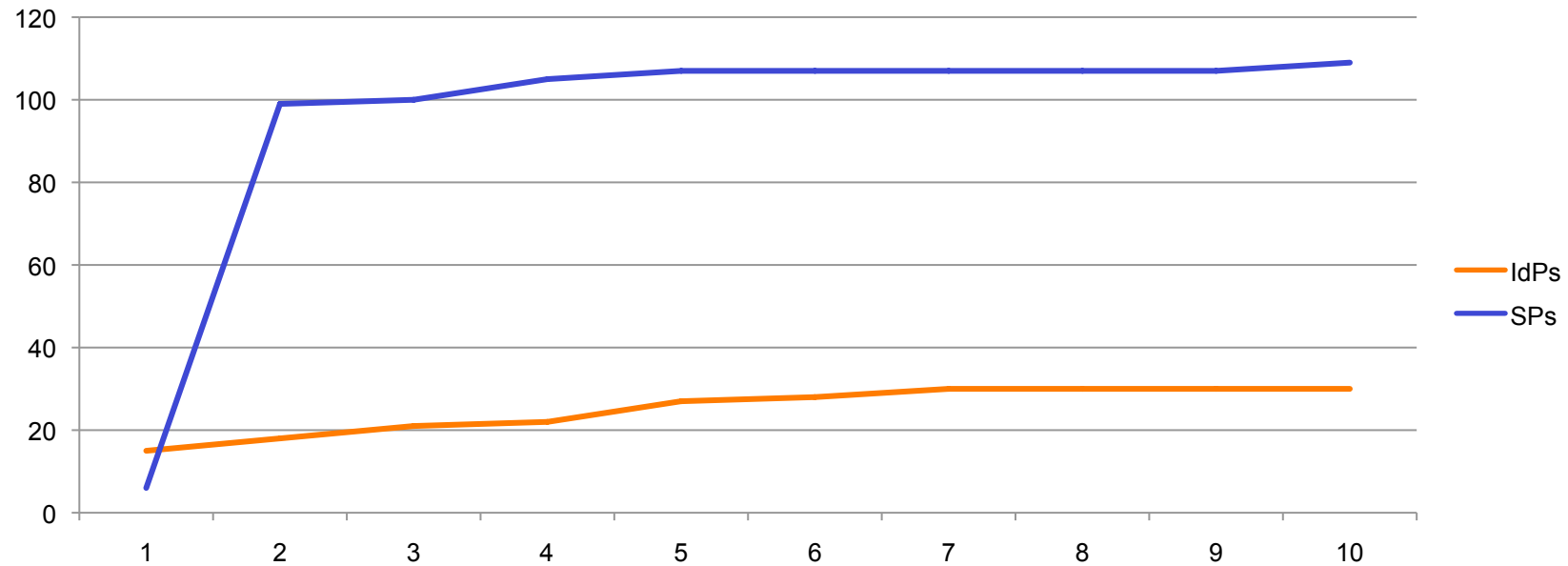




- **WAYF**
 - Muestra instituciones disponibles en SIR
- **WAYF a la carta**
 - Muestra las instituciones válidas para el proveedor de servicio
 - Look & feel personalizado
 - Por el SP al que se accede
 - Por los IdPs disponibles para dicho SP
- **Base para nuevas federaciones basadas en SIR**
 - Federación catalana
 - Federación gallega

1. Estado actual del SIR
2. ¿Cómo unirse?
3. Novedades
4. Estadísticas
5. Futuro

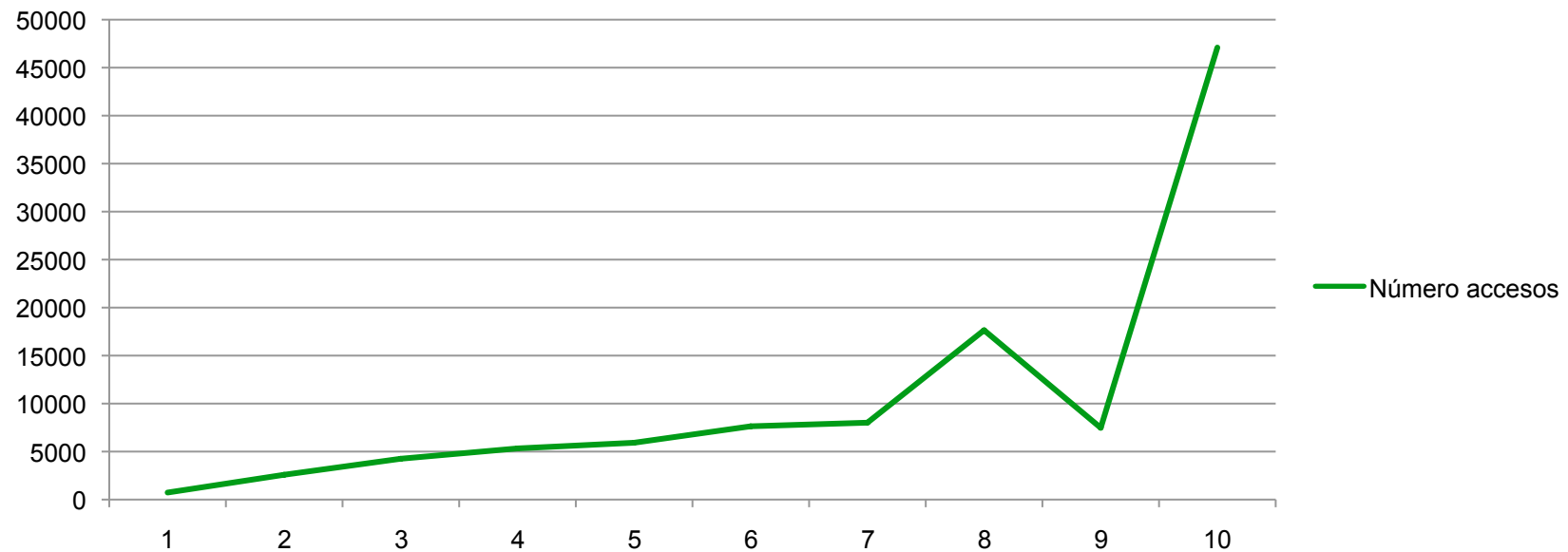




- Proveedores de identidad
 - 30
- Proveedores de servicio
 - 109

- Evolución del uso del servicio

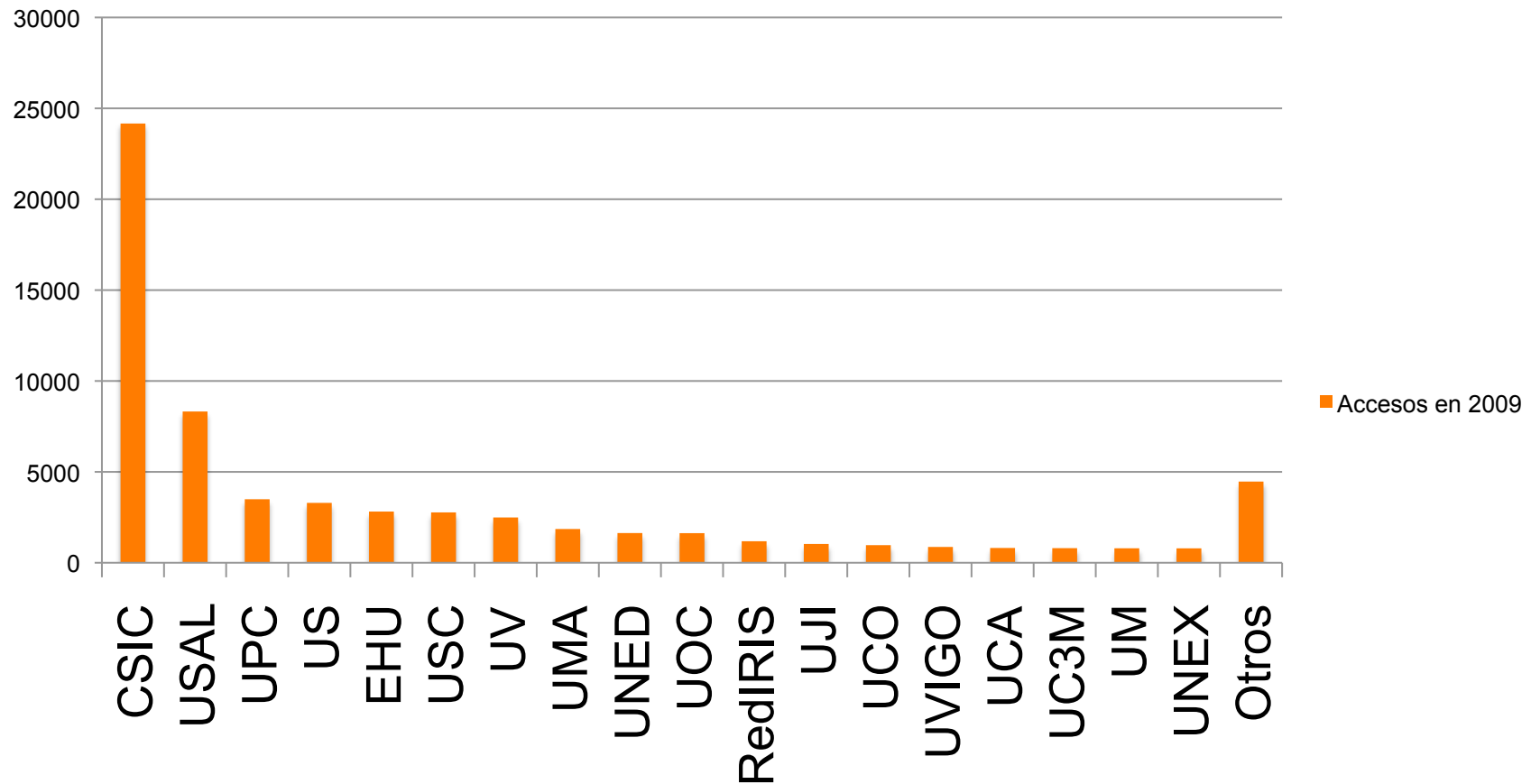
Número accesos





- Instituciones más activas en accesos

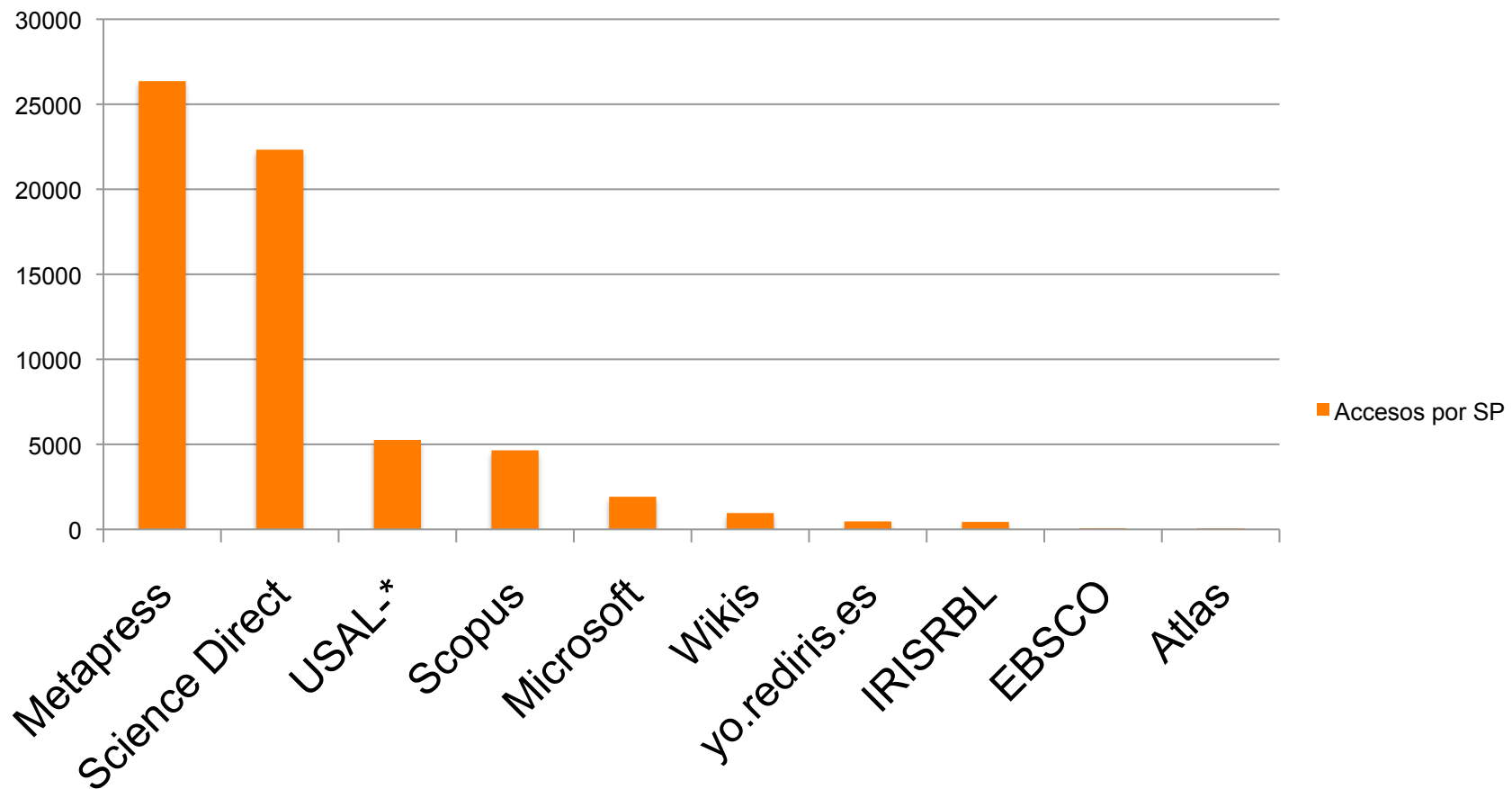
Accesos en 2009





- SPs más activos en accesos

Accesos por SP



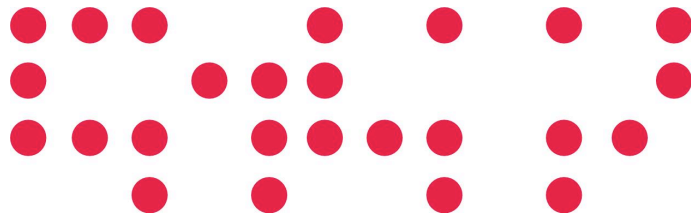
1. Estado actual del SIR

2. ¿Cómo unirse?

3. Novedades

4. Estadísticas

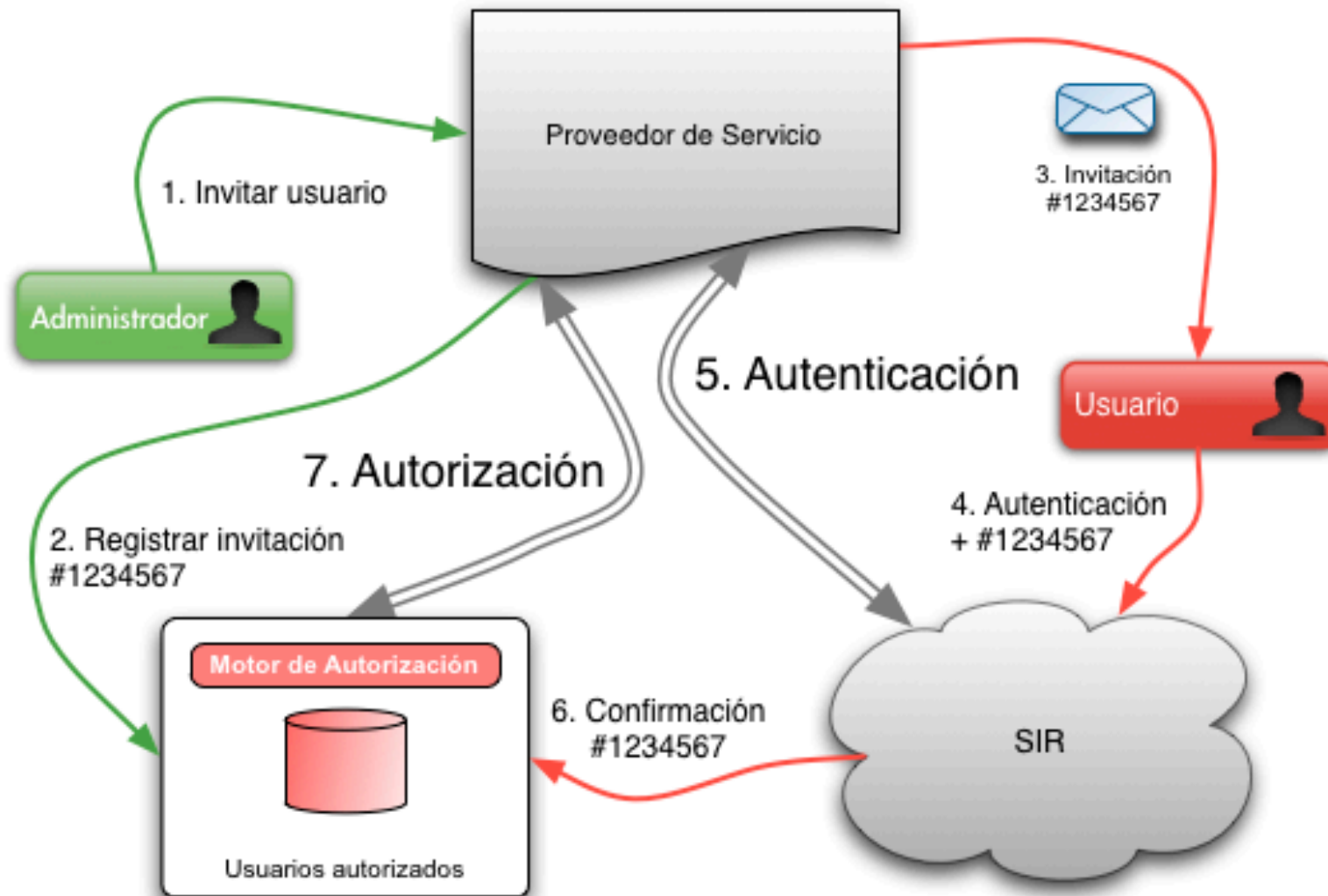
5. Futuro





- **Autorización basada en invitaciones**
 - Proceso sencillo basado en correo electrónico.
 - Más sencillo que los *entitlements*.
 - Válido para cualquier aplicación dentro de la federación.
 - Se recomienda encarecidamente el envío del atributo **schacPersonalUniqueCode** por parte de todos los proveedores de identidad.

Autorización en SIR

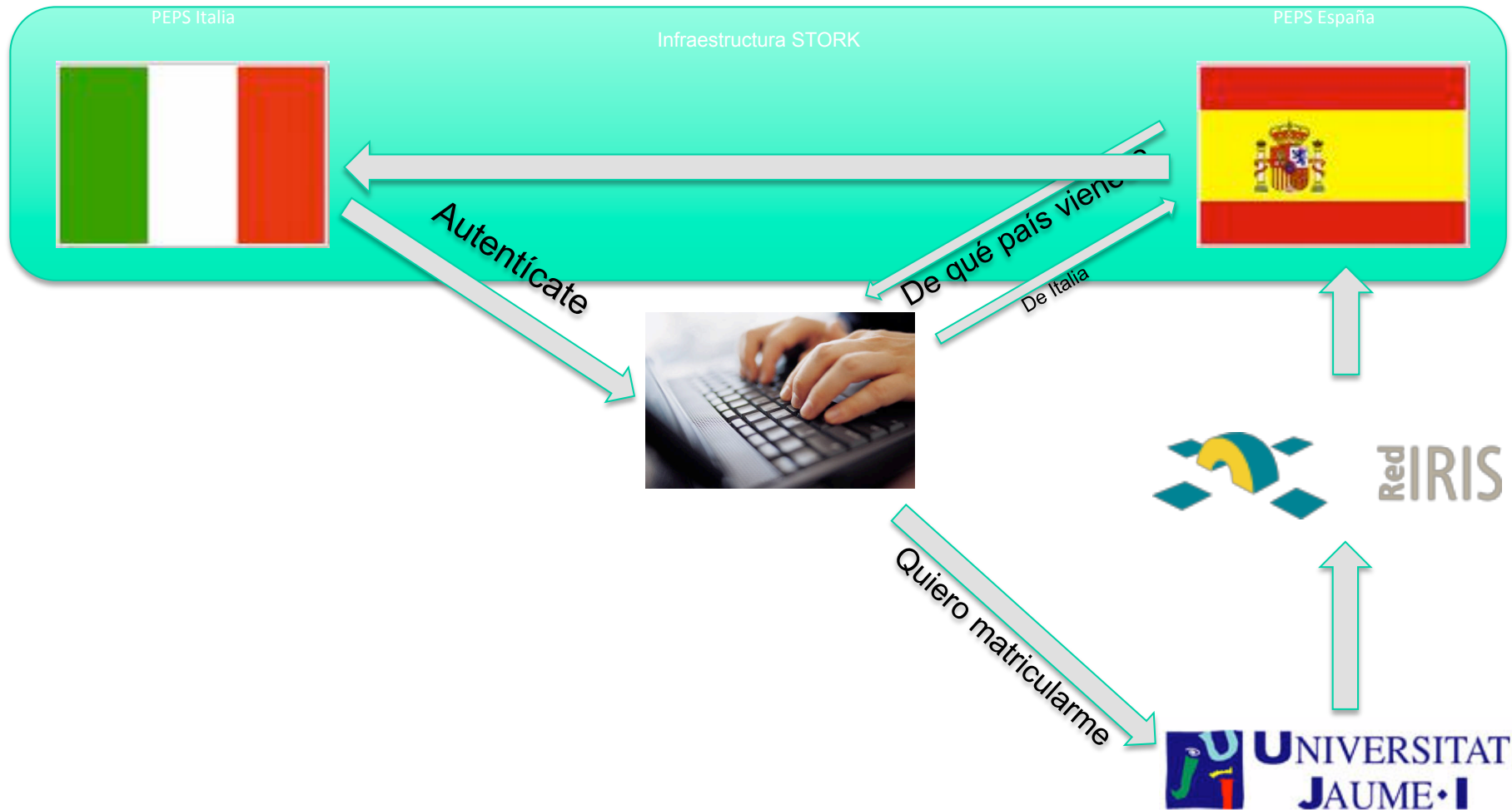




- **schacPersonalUniqueCode (sPUC)**
 - **Único y persistente** en toda la federación.
 - Basado en URNs:
 - `urn:mace:terena.org:schac:personalUniqueCode:es:rediris:sir:mbid:{md5}6fa359e1e4efc46166`
 - *Digest* del correo electrónico del usuario.
 - Garantiza la **privacidad**
 - No reversible
 - Garantiza la **identidad**
 - Permite corroborar una identidad SIR con un correo electrónico

- <http://www.eid-stork.eu>
 - Interoperabilidad de identificadores electrónicos entre los Estados Miembros de la UE
 - El resultado del proyecto será una infraestructura común, demostrada en base a distintos pilotos STORK
- **Piloto 3 – Movilidad de estudiantes**
 - Por ejemplo, permitirá a los estudiantes españoles acceder a servicios administrativos en universidades extranjeras usando el DNle

STORK: piloto



- 7 de las 10 universidades del piloto ya están en SIR
 - A las restantes se les ayudará a conectarse
- La conexión SIR – PEPS está en camino
 - Adaptación al perfil SAML2-STORK
 - Petición de atributos desde el SP
 - Nivel de calidad de autenticación requerida (QAA)
 - Interconexión RedIRIS - Red SARA (MPR)
- Piloto operativo para Junio 2010

- Recursos bibliotecarios son los más usados
- Alta de acceso mediante SIR no es trivial
 - Contrato previo entre institución y proveedor
 - Gestión económica
 - Acuerdo previo entre SIR y proveedor
 - Gestión técnica
 - Asociar ID de institución en SIR con lista de contratos en proveedor
 - Gestión administrativa
- Contacto técnico en SIR no es el enlace adecuado
 - Contacto directo con biblioteca

- Nueva persona de contacto
 - Contacto de biblioteca
 - **Sólo han comunicado 10 de 30**
- Lista de correo SIR-BIBS
 - Lista de contactos de biblioteca
 - Alta de la lista en Diciembre
- ¿Futura sesión de SIR-BIBS?

- Portal de usuario de SIR
 - Gestionar sus atributos
 - Consentimiento de atributos
 - Información para no técnicos
 - Lista de proveedores disponibles
 - Bookmarks
 - Novedades
 - Sistema de log-out centralizado
 - Elige log-out para la aplicación o en el SIR

<http://www.rediris.es/sir/>



www.red.es

Edificio CICA, Campus Universitario
Avenida Reina Mercedes s/n
41012 Sevilla. España

Tel.: 95 505 66 00
Fax: 95 505 66 27
www.red.es
www.rediris.es