

Desarrollo y evolución de la plataforma de autenticación y autorización (A&A) para el PIC

Marc Santamaria, Pau Tallada, Esther Acción, Alex Luelmo, *et al.*

Jornadas Tecnicas Rediris 2026
La Coruña (España) | 23-25 Jun 2026

Índice

1. Port d'Informació Científica (PIC)
2. Visión general
3. Registro
4. Privilegios
5. Control de acceso
6. Trazabilidad
7. Retos, configuración actual, y próximos pasos



Alcance de la infraestructura

Cómputo + Almacenamiento + Facilidades físicas

~80%

Recursos Tier-1

~10%

ATLAS Tier-2/3

Requisito estratégico

~10% Otros proyectos con requerimientos variables

⇒ Sistema de A&A adaptable



Objetivos

 **Autorregistro**

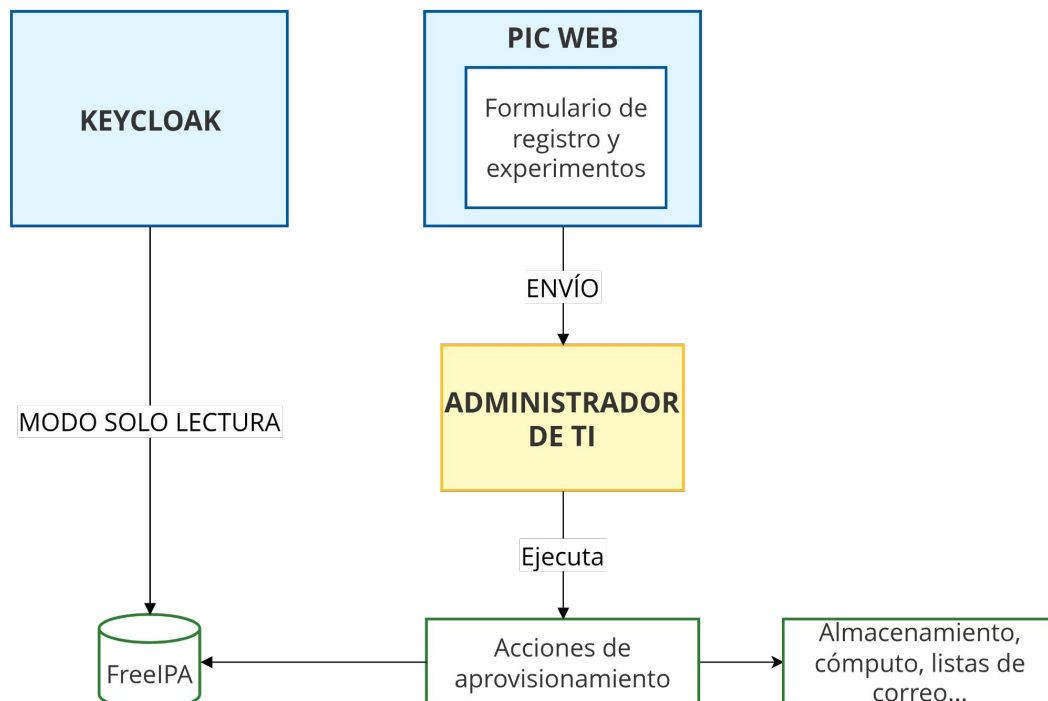
 **Aprovisionamiento automático**

 **Aprobación por patrocinador**

 **Mejoras en la seguridad**



Arquitectura legada y limitaciones

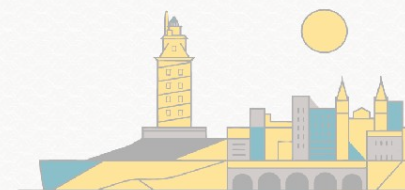


 Keycloak federado a FreeIPA

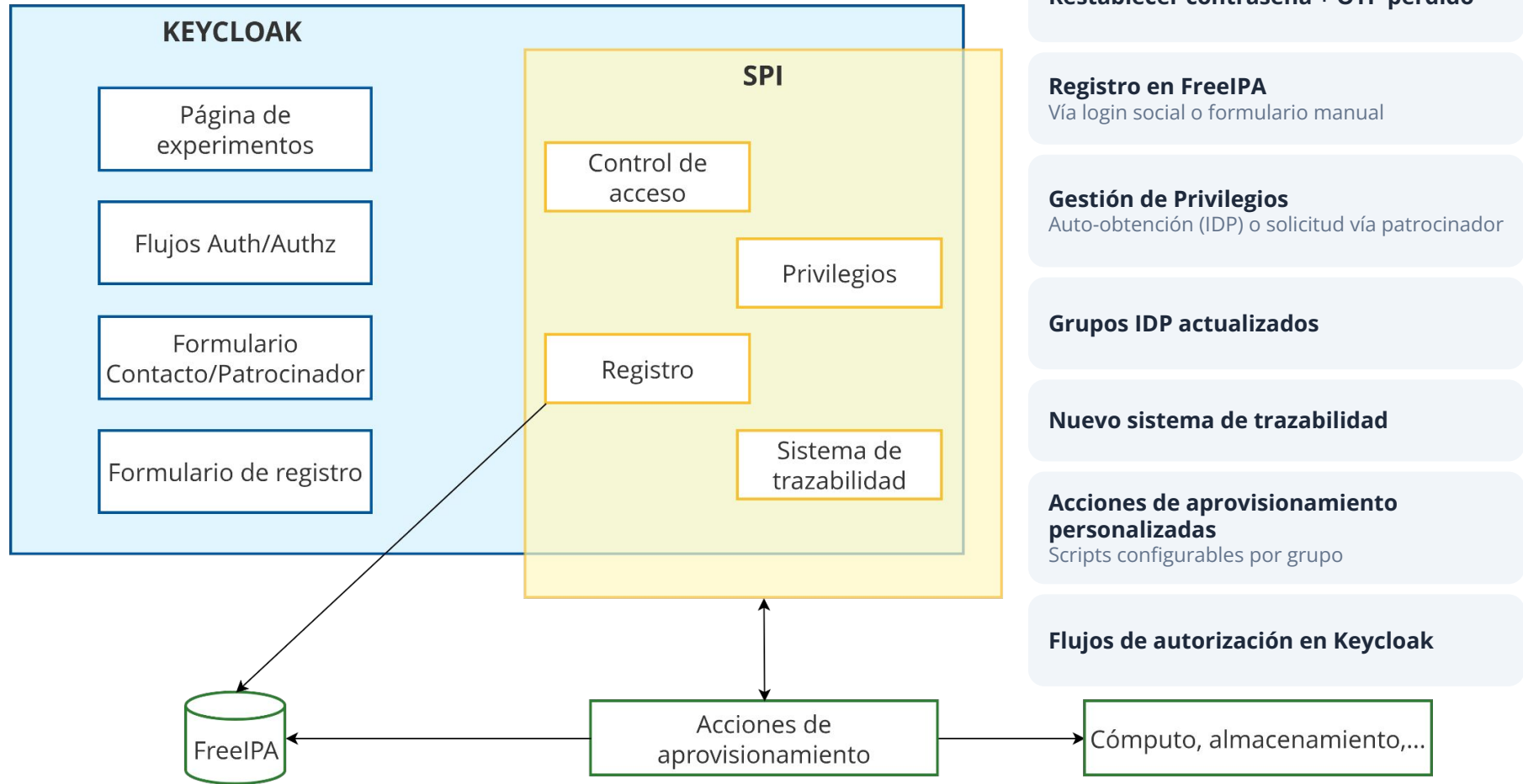
 Registros a traves de IPA

 Contacto/Patrocinador

 Autorización a traves de Keycloak



Nueva arquitectura



REGISTRO



Objetivos del Registro



Autorregistro

- Introducción manual de los detalles de perfil
- Soporte para proveedores de identidad (IdP) sociales



Integración Transparente

Sincronización completamente invisible con FreeIPA desde la perspectiva del usuario



Aprovisionamiento POSIX

Configuración automatizada de entornos de usuario y atributos POSIX estándar



Máxima Flexibilidad

Entorno altamente personalizable y genérico, diseñado para futuras extensiones



Arquitectura de Registro

PIC FreelPA Federated User Create config x

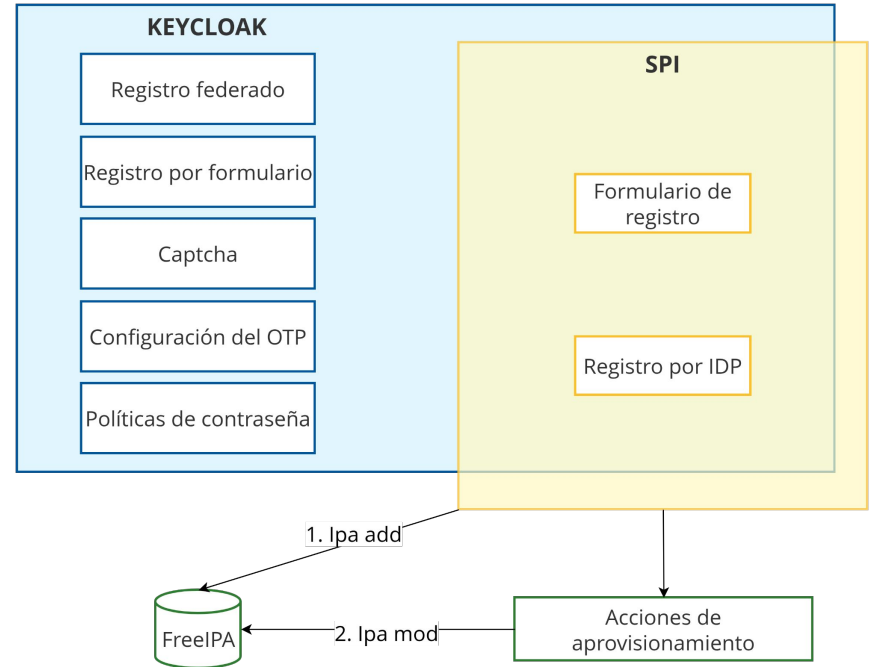
Alias * ⓘ
Users group first broker

Authenticator Reference ⓘ

Authenticator Reference Max Age ⓘ

Enter GID Number ⓘ
50108

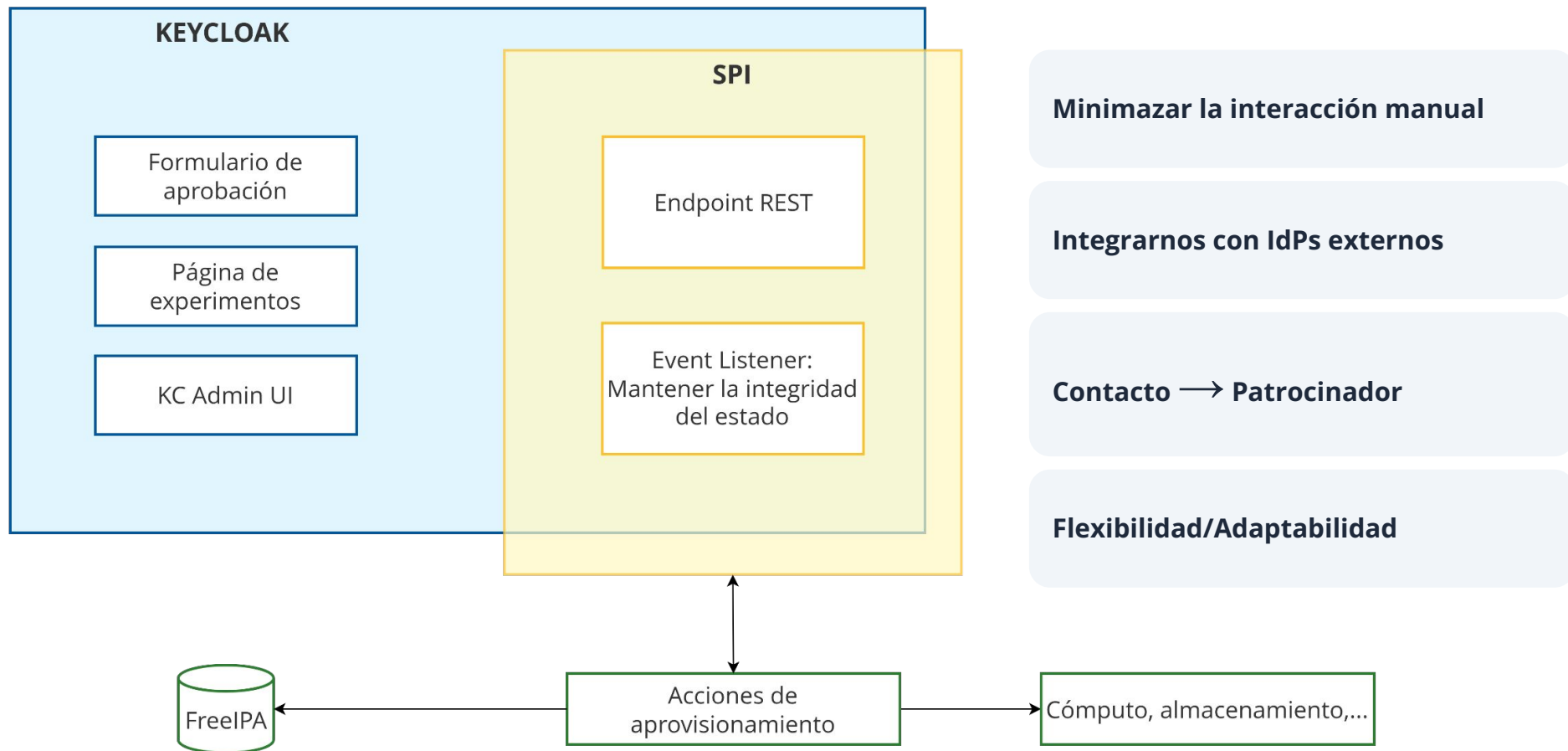
Save Cancel Clear



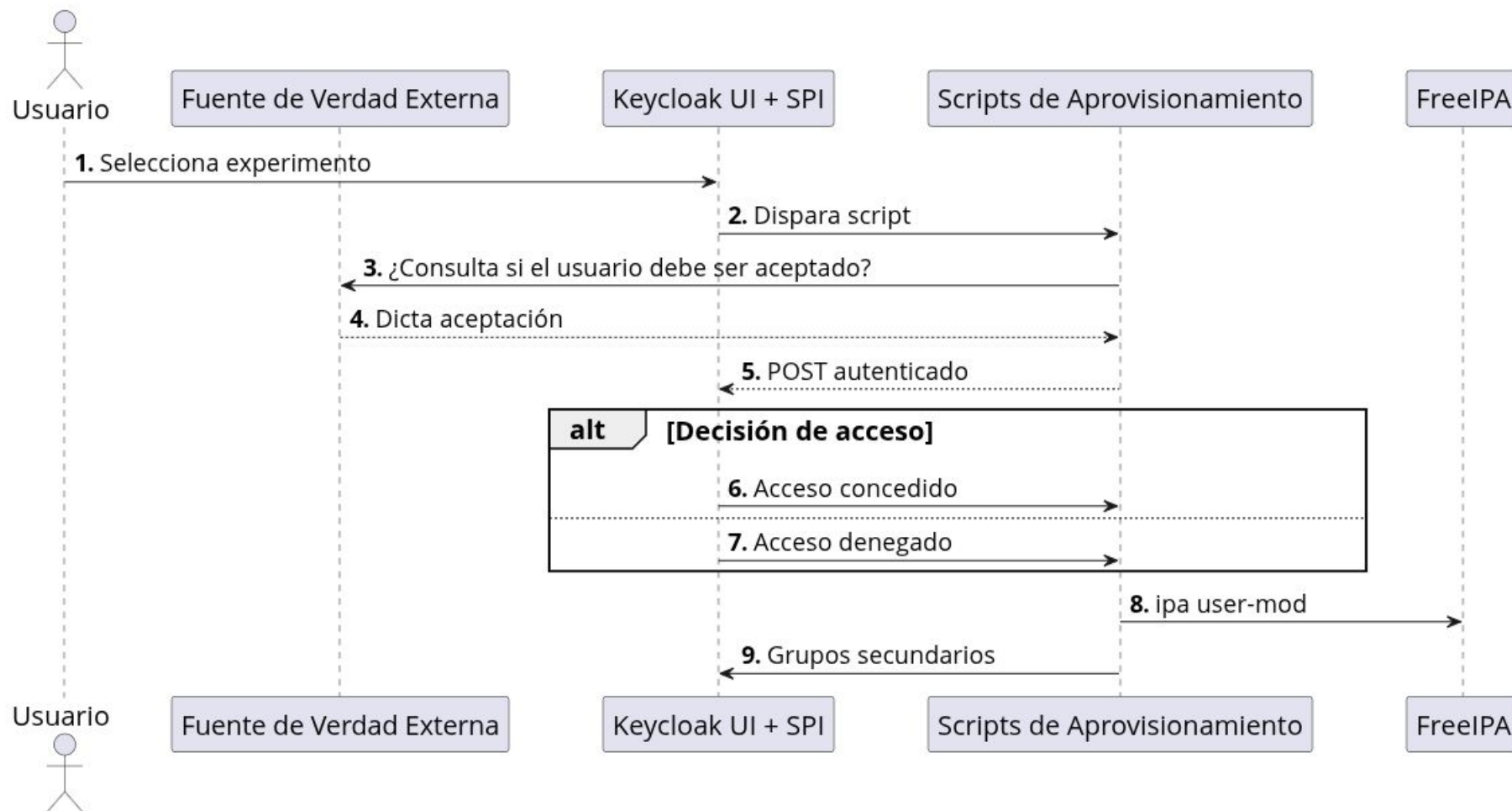
PRIVILEGIOS



Arquitectura de privilegios



Privilegios: Flujo Genérico



CONTROL DE ACCESO



Objetivos del Control de Acceso



Protección de los servicios

Se prohíbe estrictamente el acceso de usuarios sin privilegios a servicios privilegiados.



Configuración centralizada

Totalmente configurable a través de la interfaz de Keycloak para una gestión simplificada.



Sincronización con el IdP

Sincronización continua en segundo plano de experimentos con IdP externo.

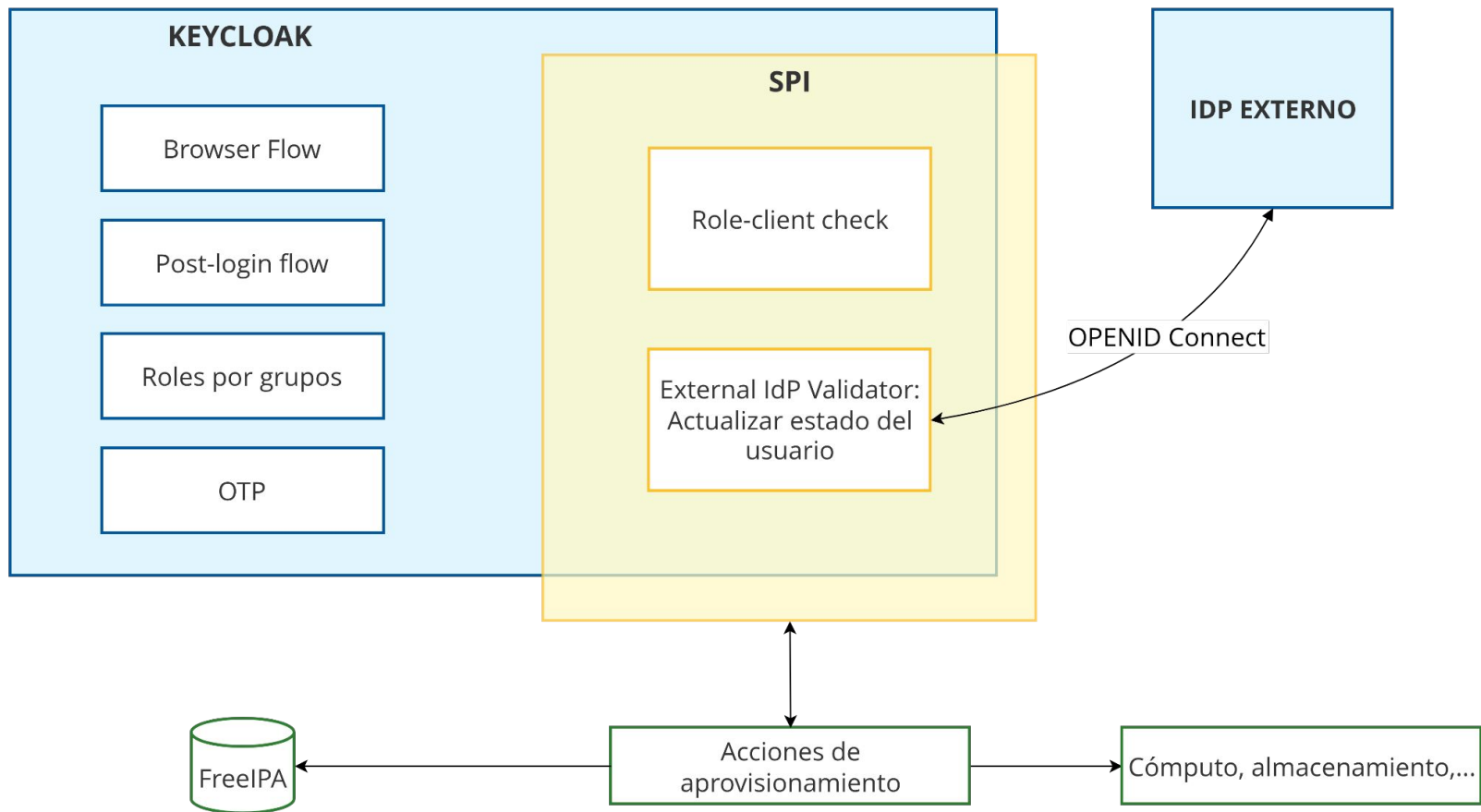


Periodo de gracia

Implementación de un periodo de gracia para experimentos que no proporcionan un token offline.



Arquitectura del Control de Acceso



Arquitectura del Control de Acceso

⋮	▼	flow	Browser ?	Required ▼
⋮		step	Cookie ?	Alternative ▼
⋮		step	Identity Provider Redirector ?	Alternative ▼
⋮	▼	flow	Browser Form ?	Alternative ▼
⋮		step	Username Form ?	Required
⋮	>	flow	Check account lock ?	Conditional ▼
⋮		step	Username Password Form ?	Required
⋮		step	OTP Form ?	Required ▼
⋮	>	flow	Refresh Token ?	Conditional ▼
⋮		execution	Role Client Check ?	Required ▼

Vista del administrador de keycloak del flujo de browser



Arquitectura del Control de Acceso

Role Client Check config

Alias ?

Roles

Authenticator Reference ?

Authenticator Reference Max Age ?

Clients Roles List ?

Key	Value	
jupyter	jupyter-user	⊖
gitlab	gitlab-user	⊖
login	ssh-user	⊖
grafana	grafana-user	⊖

+ Add Clients Roles List

Error Message ?

privilegedAccessNoticeText

Save

Cancel

Clear



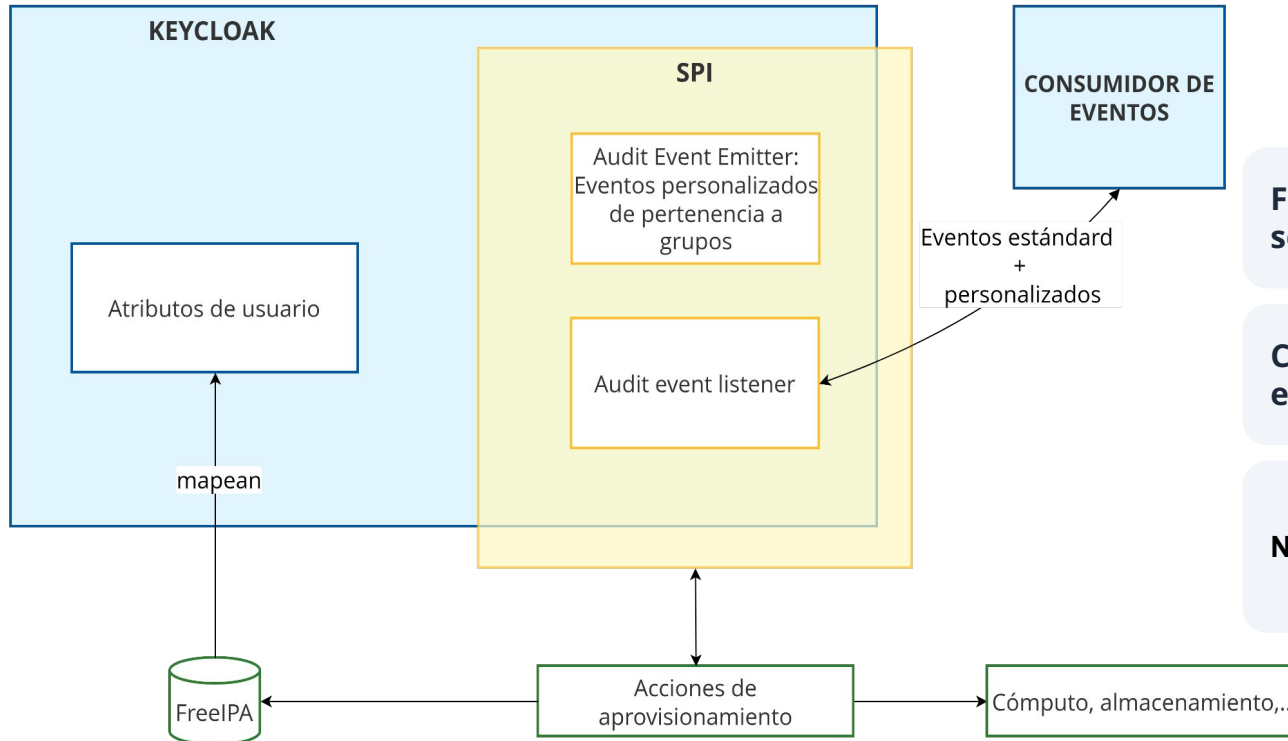
Flujo de Renovación de estado



EVENTOS



Arquitectura de eventos



Flexibilidad para enviar eventos a servicios de streaming

Correos personalizados para el equipo de TI

Nuevo diseño de trazas



Arquitectura de eventos

Dear all,

A user has been added to the group test.

- **Username** msantama
- **Full name** Marc Santamaria
- **User email** msantama@pic.es
- **Group** test

Group contacts:

- **Pau Tallada Crespi** (tallada): test@pic.es

Added by:

- **Keycloak Admin** (admin): admin@pic.es

Accepted at: 2026-06-19 10:31:24

Best regards,

PIC Services team

groupSponsorPerson

cms,Pepe Flix,pepe@pic.es

astro,Keycloak Admin,admin@pic.es

incaem,Francesc Torradeflot,francesc@pic.es

materialscommons,Marc Santamaria,msantama@pic.es

[+ Add groupSponsorPerson](#)

Implementación y retos



UI/UX



First broker login



Periodo de gracia



Grupo primario



Fallos en flujo renovación



AuthZ sin privilegios

English

Provide your account details

* Required fields

If you need to link your existing account to this identity provider, just add your username / email

Username *

Email *

First name *

Last name *

Gender

Submit



Estado actual y próximos pasos

✓ En Producción

- **Registro:** Formulario manual e IdP Social → Passwordless
- 2FA y PAM-auth delegados vía OpenID
- Nuevo diseño de auditoría y separación de responsabilidades
- Autorización basada en roles en Keycloak
- Nuevo sistema de privilegios flexible
- Cambio de grupo primario (Perfil de Usuario)
- LSST-IdP Flujo Completo
- EduGAIN como Social IdP

↗ Próximos Pasos

- Control de versiones de la configuración de Keycloak
- Refinamientos en los flujos
- Refinamientos en UI/UX



Gracias por su atención

¿Preguntas?



Agradecimientos

This work is co-funded by the Recovery and Resilience Facility (Spain) with funding from the European Union NextGenerationEU (PRTR-C17.I1).



SLIDES DE BACK UP



REGISTRO DE NUEVO



PROCESO DE REGISTRO

PIC
port d'informació
científica

English

[Back to login](#)

Sign up with

Google

or complete your profile

* Required fields

Username +
We recommend first letter of the name + surname all lowercase

Password +

Confirm password +

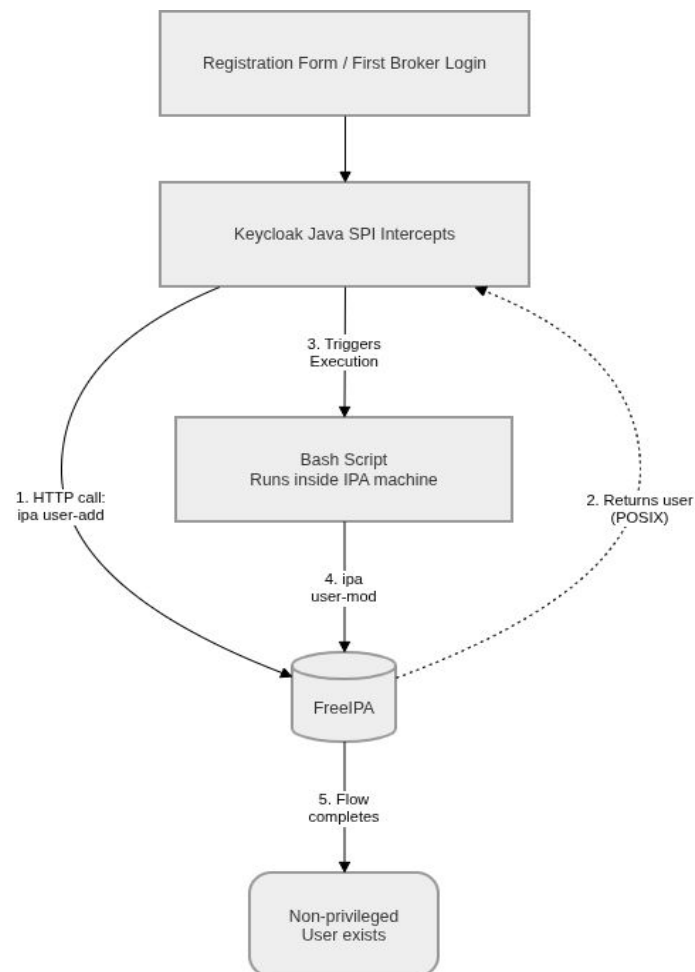
Email +

First name +

Last name +

Gender +

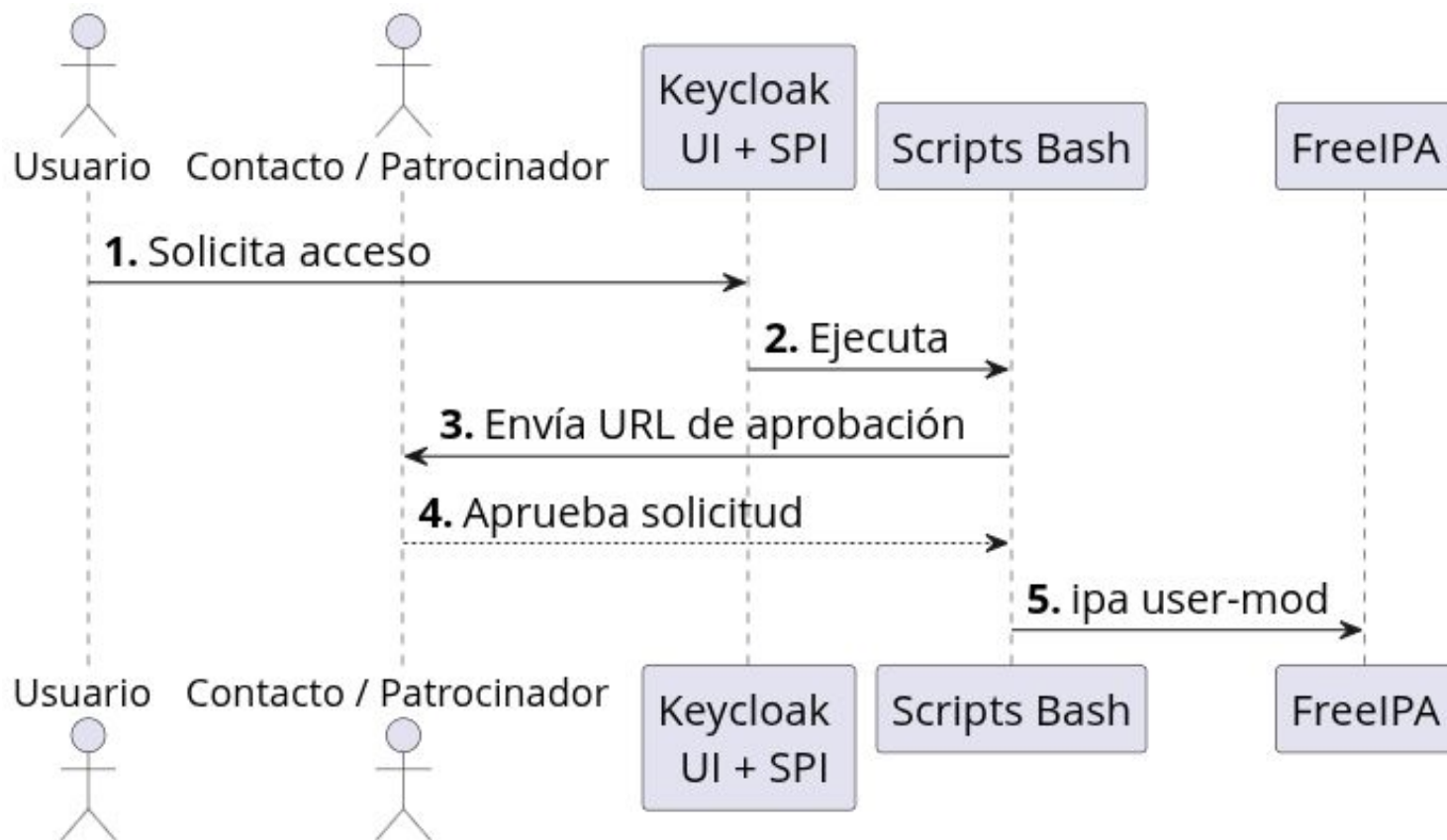
Register



PRIVILEGIOS DE NUEVO



Privilegios: Flujo Manual

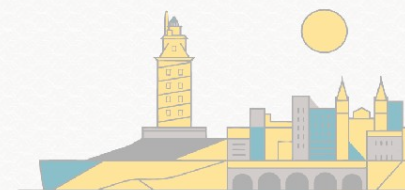


Privilegios: Flujo Manual

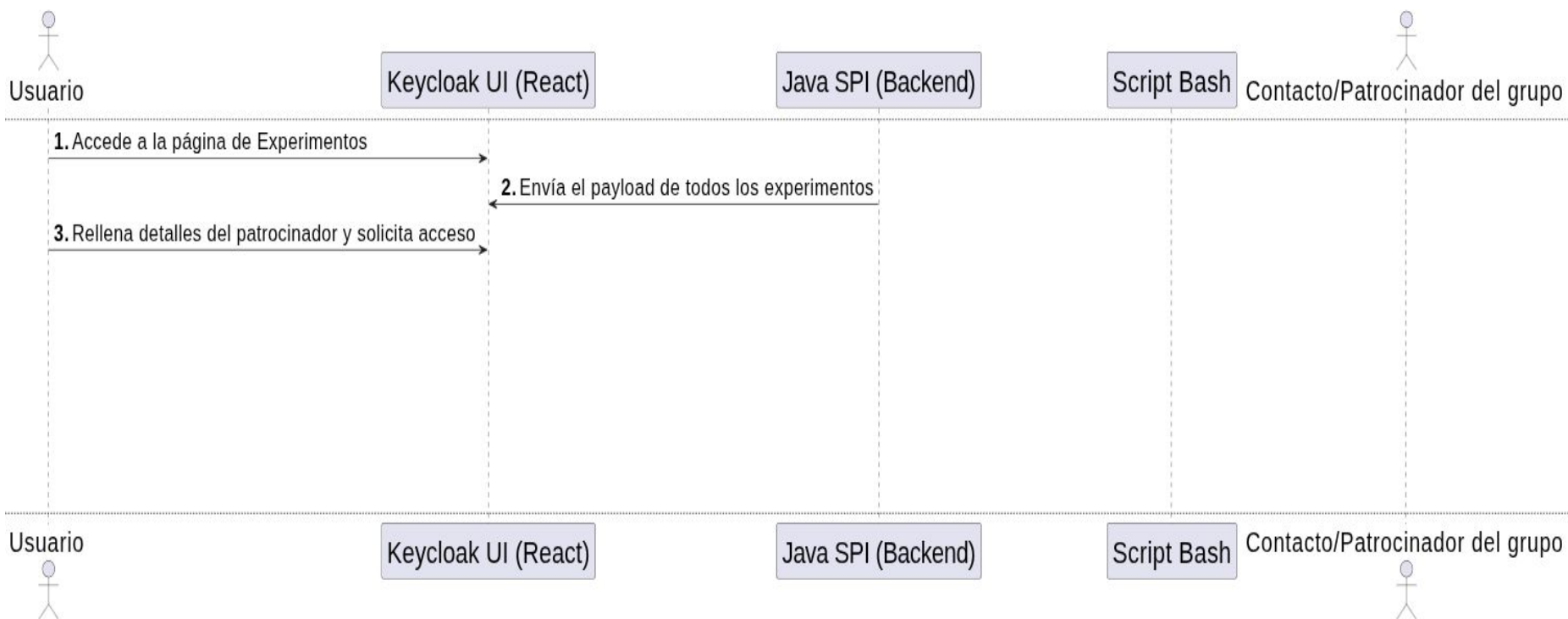


Experiments

Experiment	Description	Action
agn	AGN	Request Access
ai	PIC Applied AI	Request Access
aicourse	PIC Deep Learning Course	Request Access
at3	Atlas Tier-3	Request Access
at3-pixels	Atlas Tier-3 Pixels	Request Access
atlas	ATLAS	Request Access



Privilegios: Flujo Manual



Privilegios: Flujo Manual

Select a Sponsor ×

Who is your sponsor for the project?

☐ Pilar Casado

☐ Thorsten Lux

☒ Other

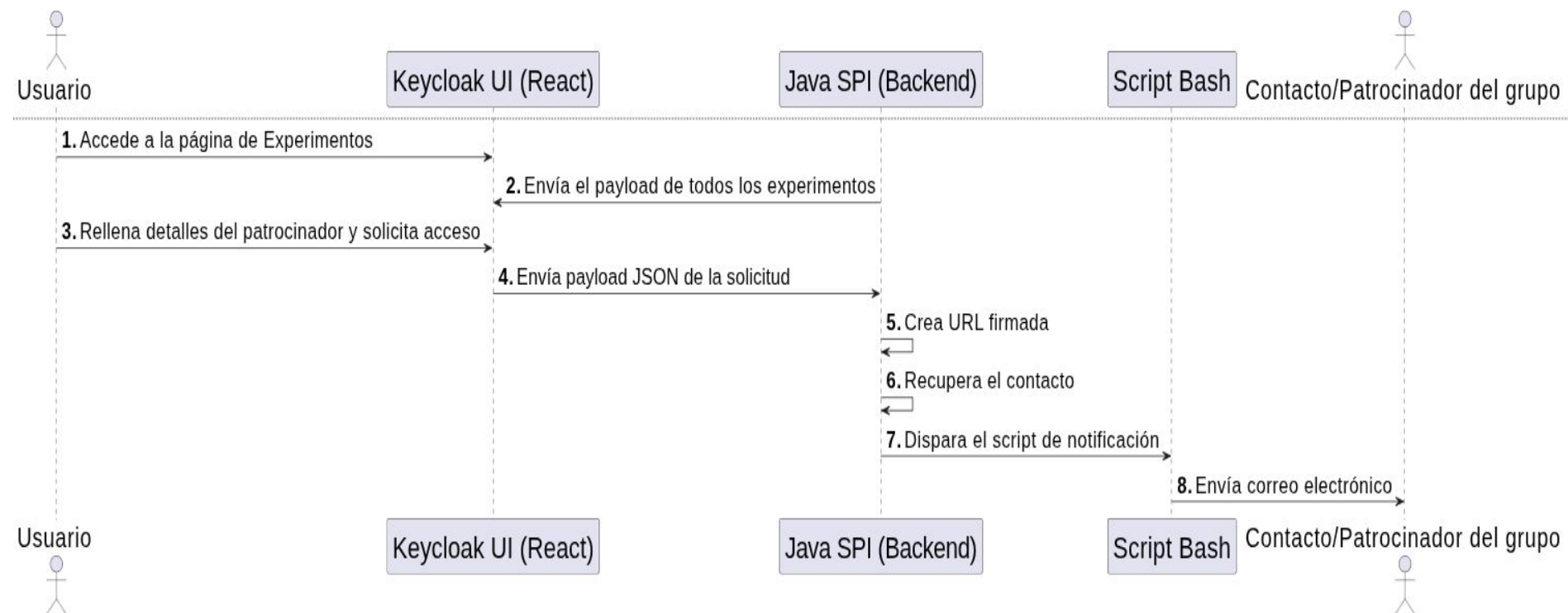
Sponsor name *

Sponsor email *

[Cancel](#)



Privilegios: Flujo Manual



Privilegios: Flujo Manual

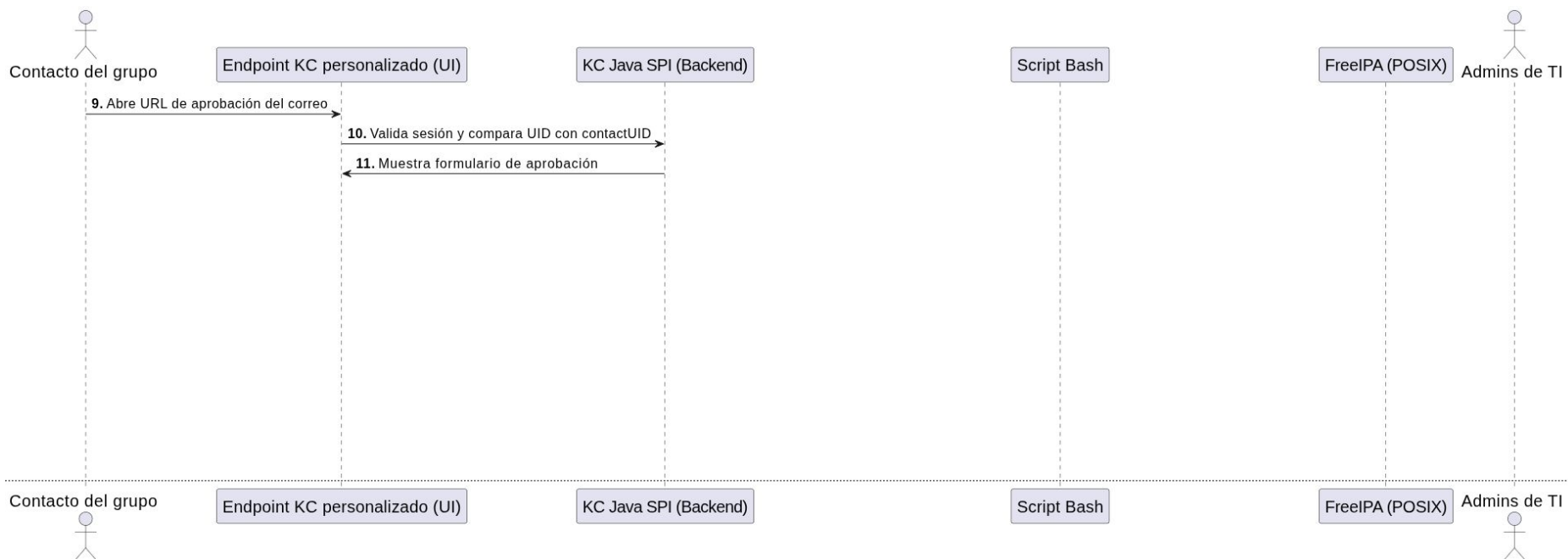
The user msantam2 with email msantama+contact2@pic.es has requested access to the group **test_group_marc2**.

To review the request, please visit: [See Request](#)

Warning: You must be logged in to your account associated with this email to see the request.



Privilegios: Flujo Manual



Privilegios: Flujo Manual



Català

Group access request

You are about to make an important decision regarding user access. Please review the information below carefully before proceeding.

User
msantama

Email
msantama@pic.es

Group
test

Sponsor name
My Sponsor fullname

Sponsor email
mysponsoremail@pic.es

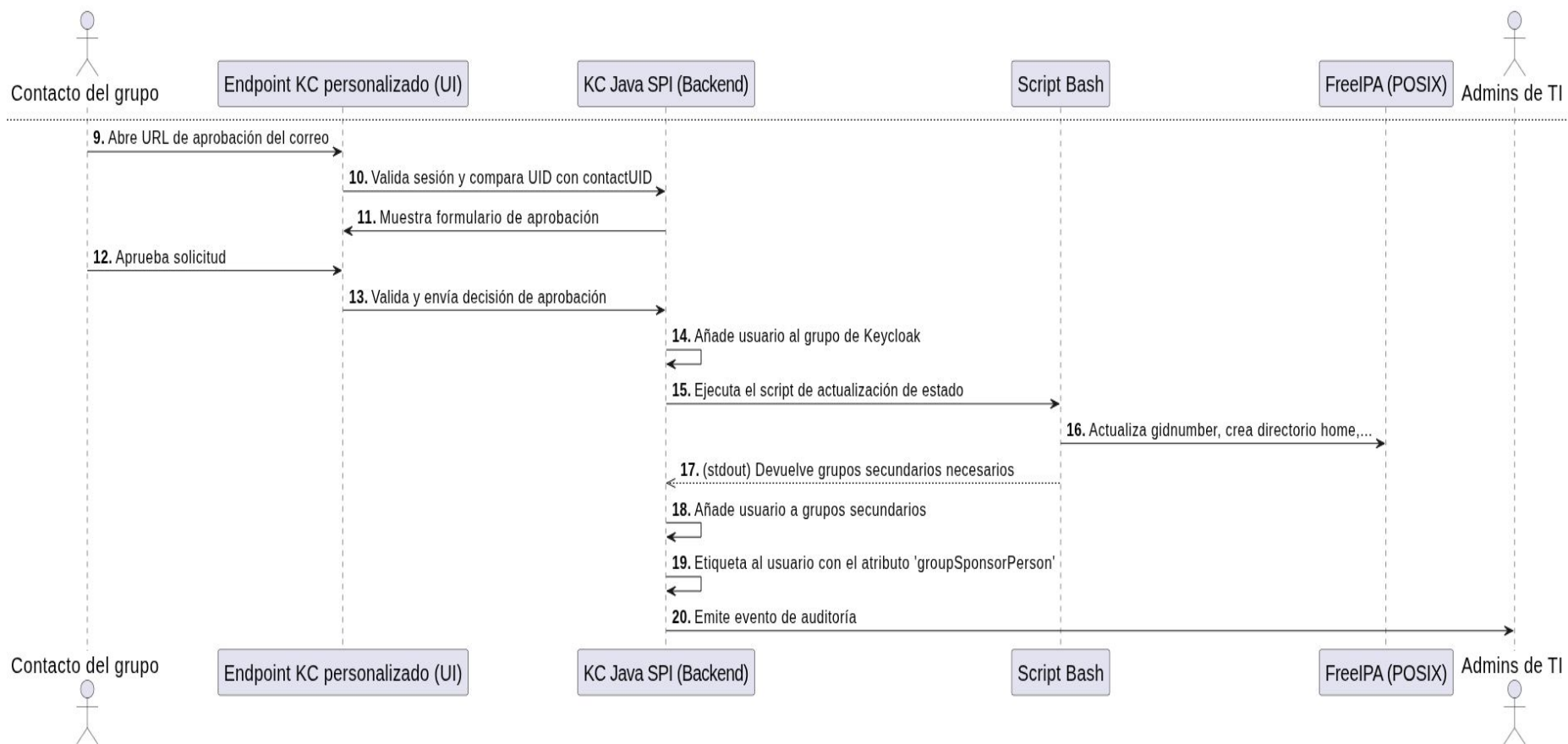
Deny User

Accept User

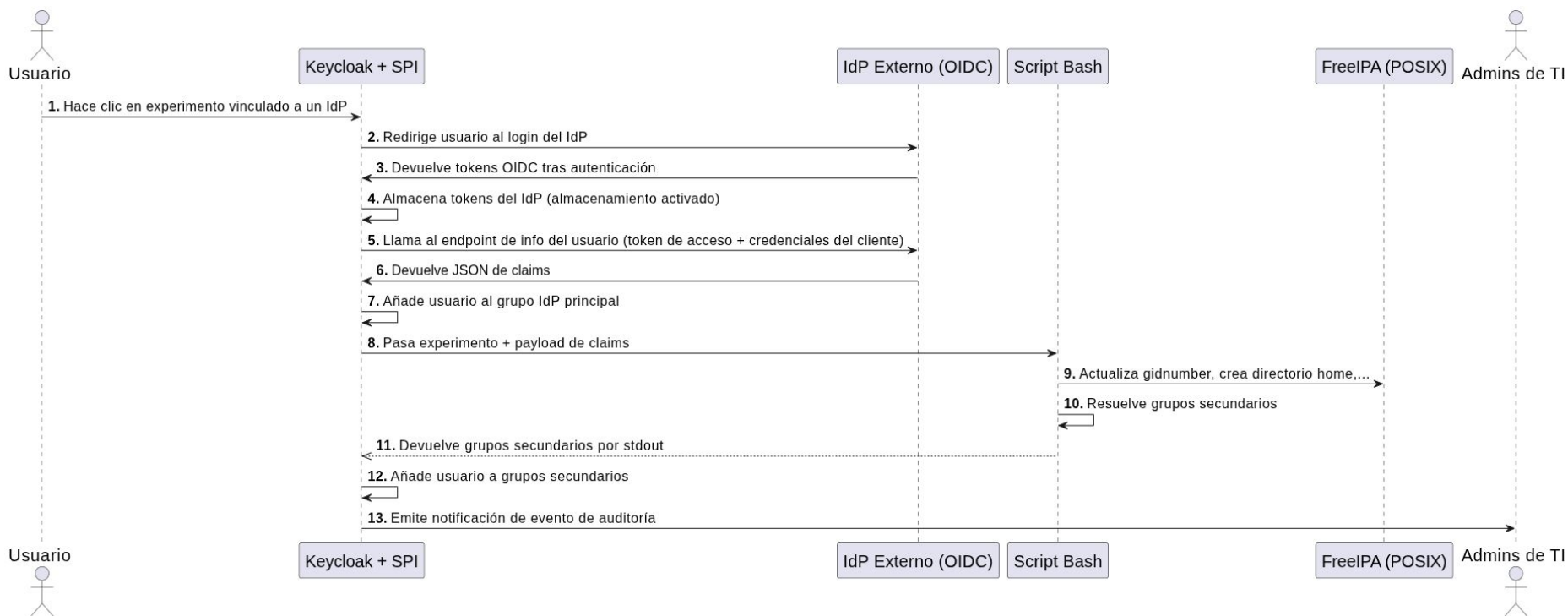
If you are here by mistake or unsure about the action to take, please close this page.



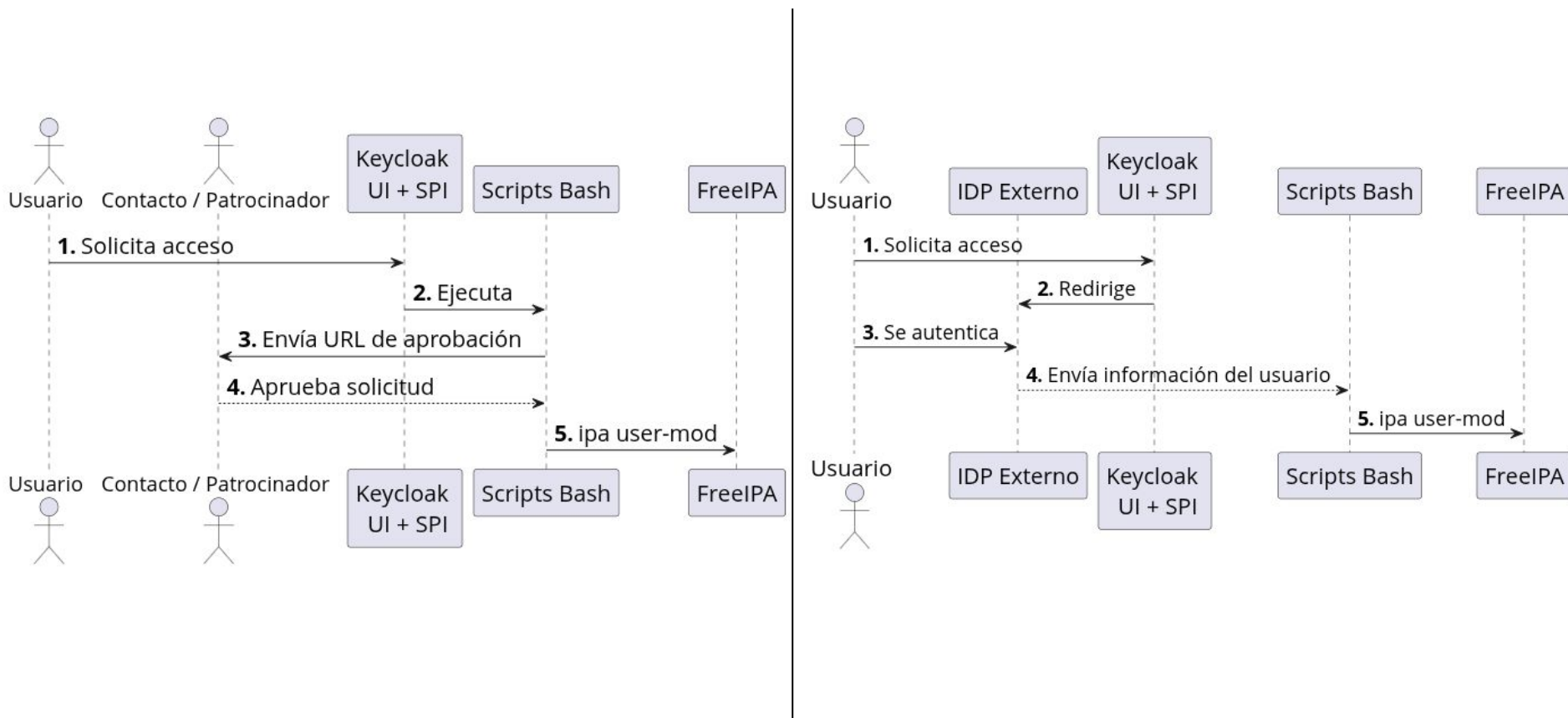
Privilegios: Flujo Manual



Privilegios: Flujo IDP



Privilegios: Comparativa Flujos



PERIODO DE GRACIA AL DETALLE



