

Actualidad

SIR2 /

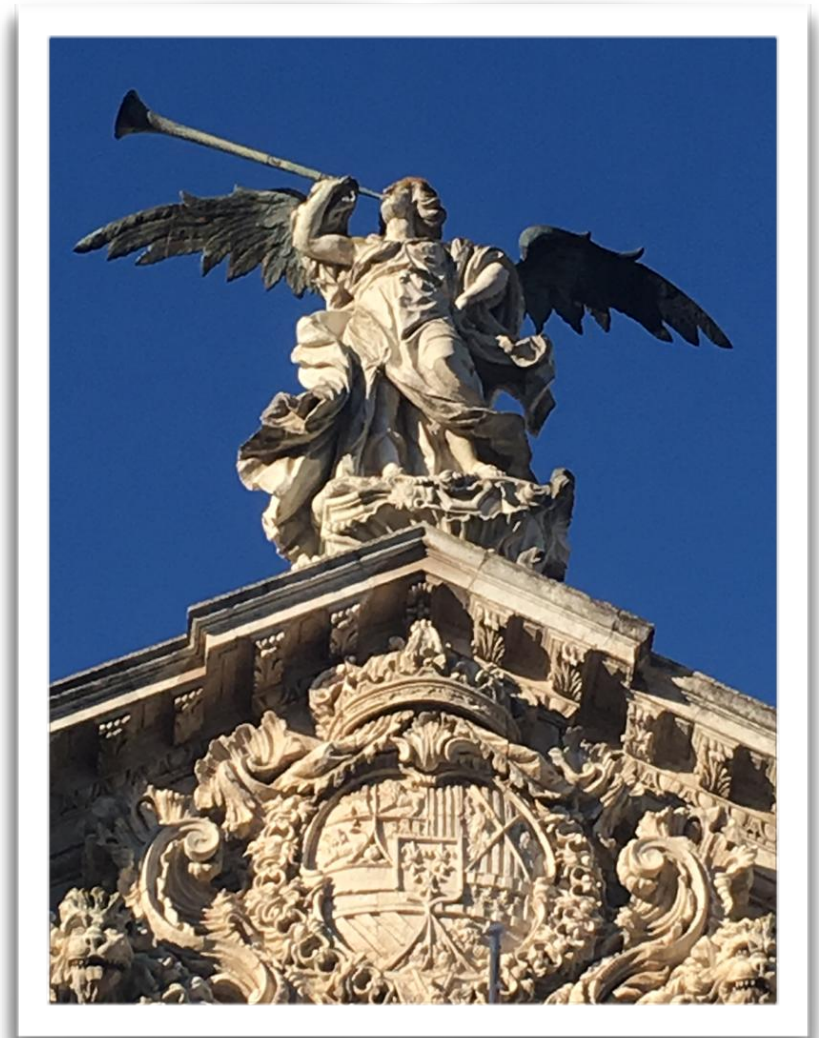
eduroam

José Manuel Macías Luna

🐦 @lonoak

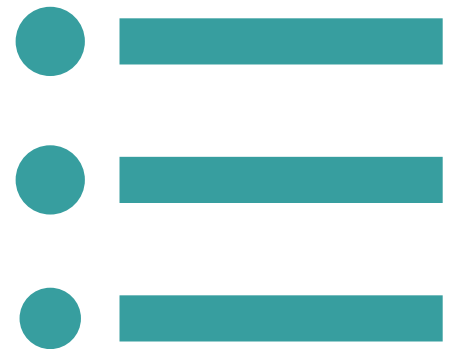
✉️ jmanuel.macias@rediris.es

Sevilla, 28 de mayo de 2019

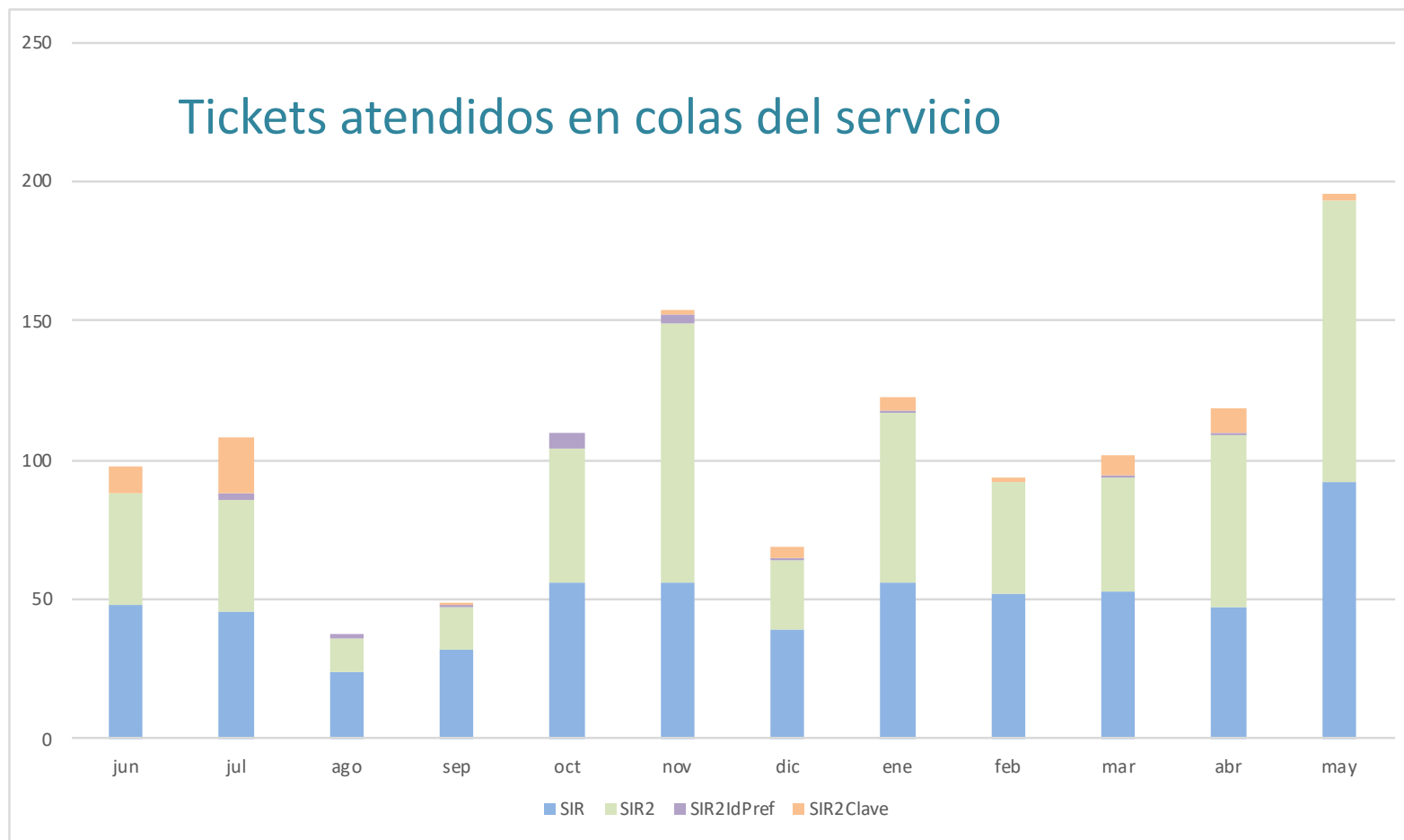


Agenda

- Actualidad federación de identidades
 - Operación del servicio / migración
 - Cl@ve / Cl@ve 2
 - eduGAIN
 - IdP en la nube
- Actualidad eduroam
 - eduroam Managed IdP
 - piloto eduroam Visitor Access



Operación del servicio de federación de identidad






1260 tickets válidos atendidos en el último año


Operación del servicio de federación de identidad


- Menos tickets de migración de IdPs PAPI a SAML2
 - la mayoría ha concluido la migración
- Pasarela SAML de salida (de SIR) ha ocupado buena parte de nuestro tiempo
 - Actualización del software
 - Preparación para “migración de SPs”
- Puesta en marcha paulatina de SIRRR
 - SIRRR = SIR Resource Registry





SIR Resource Registry

 Federations Identity Providers Service Providers Register Administration EN   0

Identity Provider: RedIRIS - Spanish Research and Academic Network 

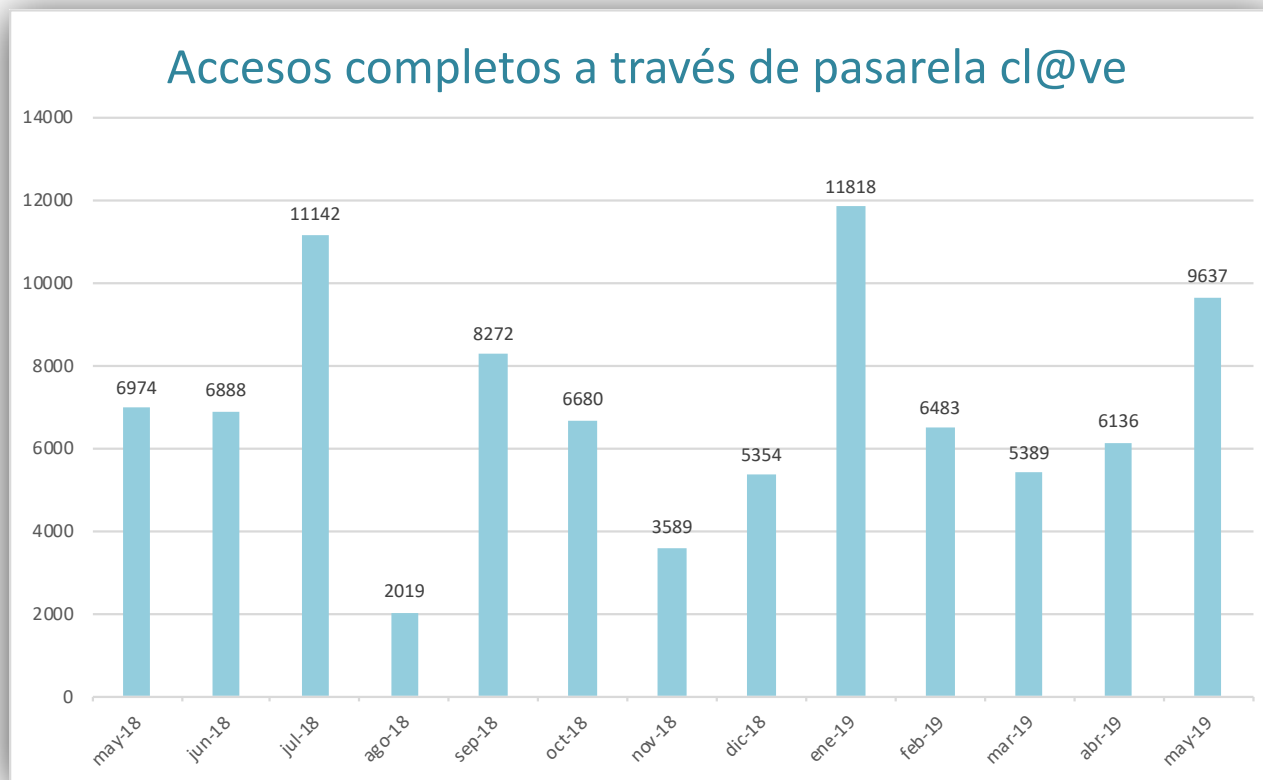
DASHBOARD / IDENTITY PROVIDERS / REDIRIS - SPANISH RESEARCH AND ACADEMIC NETWORK 

 General Membership Metadata Management Logs/Stats

Status 	Enabled Managed locally
Last modification	2019-05-26 22:42:45
EntityID	https://www.rediris.es/sir/redirisidp
Name of organization	es: RedIRIS - Red Académica y de Investigación de España en: RedIRIS - Spanish Academic and Research Network
Displayname of organization	es: RedIRIS en: RedIRIS
URL to information about organization	es: http://www.rediris.es/ en: http://www.rediris.es/index.php.en
Registration Authority	http://www.rediris.es/
Registration Date	2017-12-12 01:29:00
Registration Policy	en: SIR2 MRPS
Entity Attribute	Research and Scholarship Entity Category Security Incident Response Trust Framework for Federated Identity (SIRTFI)
Valid From/Until	unlimited -- unlimited

Registro de Recursos SIR - © 2019 Powered by Jagger

- Algunos datos de pasarela cl@ve(producción):
 - Proveedores de servicio: 34
 - Instituciones: 18



Cl@ve / Cl@ve 2

- Cl@ve 2 ya funcionando en pre-producción y producción
- Todo listo para comenzar la transición a cl@ve2:
 - Para SPs SAML2 WebSSO, solamente cambiar end-point y tener en cuenta el nuevo perfil de atributos
 - Para SPs Cl@ve, deberán transicionar a medio plazo (desaparecerá la infraestructura del lado del ministerio) a Cl@ve 2:
 - la pasarela ofrece una interfaz cl@ve a cl@ve2
 - no recomendable: los kits están sin soporte
 - Para SPs Cl@ve2 ofrecemos soporte, pero recomendamos WebSSO
 - Inminentemente se lanzará el nuevo entorno de producción de la pasarela, así como documentación con detalles sobre estos cambios
 - Actualmente podéis ya solicitarlo en el entorno de pre-producción de la pasarela
 - Para niveles de confianza sustancial o alto, es requisito usar Cl@ve 2 en servicios públicos

Cambios en eduGAIN

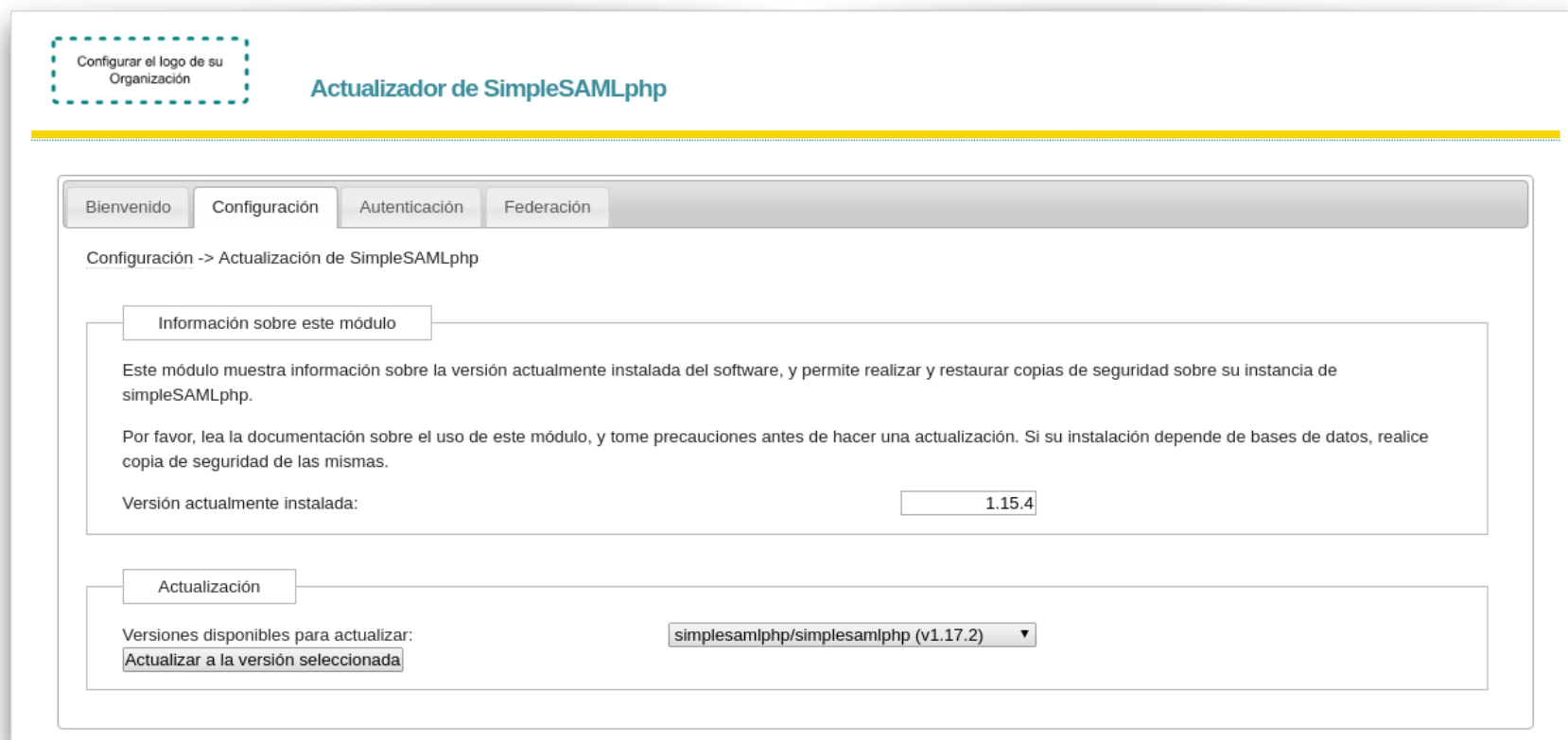
- Actualmente ya hay 77 proveedores de identidad de nuestra federación en eduGAIN
- Se están introduciendo algunos cambios en los metadatos que exportamos:
 - “Research & Scholarship” y “SIRTFI” serán Opt-out
 - Opt-In “CoCo v.1”, pendiente “CoCo v.2”
 - Se incluyen mejoras en extensiones de metadatos de interfaz de usuario
- Cada vez más servicios disponibles a través de eduGAIN
 - Incorporación de servicios InAcademia y eduTeams

Más sobre eduGAIN

- Documentación útil:
 - Herramientas de eduGAIN (wiki de SIR2):
 - <https://redir.is/GJAXV>
 - Kit de desarrollo de políticas de AARC (Authentication and Authorization for Research and Collaboration):
 - Orientado a infraestructuras científicas que deseen desplegar servicios que necesiten soportar autenticación y autorización
 - Plantillas de políticas, guías de uso, vídeos explicativos, y glosario disponibles
 - <https://aarc-project.eu/policies/policy-development-kit/>

Soporte IdP de referencia

- Nuevo pre-instalador, basado en composer:
 - <https://redir.is/JEDMX>
- Nuevo módulo de actualización: <https://redir.is/PVTJA>



The screenshot shows the 'Actualizador de SimpleSAMLphp' (SimpleSAMLphp Updater) web interface. At the top left, there is a dashed box with the text 'Configurar el logo de su Organización'. The main title is 'Actualizador de SimpleSAMLphp'. Below the title is a navigation bar with four tabs: 'Bienvenido', 'Configuración', 'Autenticación', and 'Federación'. The 'Configuración' tab is selected, and the page content is titled 'Configuración -> Actualización de SimpleSAMLphp'. There are two main sections: 'Información sobre este módulo' and 'Actualización'. The 'Información' section contains text about the module's purpose and a warning to read documentation before updating. It also shows the 'Versión actualmente instalada:' as '1.15.4'. The 'Actualización' section shows 'Versiones disponibles para actualizar:' with a dropdown menu set to 'simplesamlphp/simplesamlphp (v1.17.2)'. Below the dropdown is a button labeled 'Actualizar a la versión seleccionada'.

Piloto IdP en la nube

- Retrasos en el comienzo del piloto
 - previsión de comenzar en junio
- Se ha estado trabajando en:
 - Despliegue del *cluster* k8s de producción
 - CVE-2018-1002105 (kube-apiserver) y CVE-2019-5736 (runc)
 - Finalización entorno de integración continua
 - Almacenamiento seguro de contraseñas (Argon2)
 - Funcionalidad de cambio de contraseñas
 - Requisito de acceso con doble factor al panel de administración



eduroam Managed IdP

- “IdP eduroam para instituciones pequeñas”
- Gestión de usuarios + Instancia de eduroam CAT
- EAP-TLS como método de autenticación
 - no se utilizan el usuario y contraseña de la institución
- Invitación a los usuarios mediante correo electrónico
- Lo que es:
 - un IdP en eduroam para instituciones de tamaño pequeño
 - una solución cómoda para el administrador
- Lo que **no** es:
 - una solución que escale bien
 - una solución para visitantes



eduroam Managed IdP

The screenshot shows the eduroam Managed IdP administration page. At the top left, it says "eduroam Managed IdP" and "View this page in English(GB)". Below this is a URL: "https://hosted.eduroam.org/?idp=19". A map of Madrid, Spain, is displayed in the center, with several locations marked: Alvarado, AZCA, Cuatro Caminos, Nuevos Ministerios, República Argentina, and Ríos Rosas. Below the map are three buttons: "Edit general Identity Provider details", "Delete Identity Provider", and "Reset all Identity Provider settings".

Available Support actions

Check National Roaming Operator server status [Go!](#)

Profiles for this Identity Provider

Managed IdP

You can create up to 200 users. Their credentials will carry the name `opauehash@19-18.es.hosted.eduroam.org`.

[Manage User Base](#)

User Downloads

At the bottom, there is a footer with the following text: "eduroam Managed IdP - Release CAT-2.0.1 © 2011-2019 GÉANT Association on behalf of the GÉANT Projects funded by EU; and others Full Copyright and Licenses". There are also logos for "eduroam® Privacy Notice" and "European Commission Communications Networks, Content and Technology".



eduroam Managed IdP

View this page in English(GB)

<https://hosted.eduroam.org/?idp=19>

[Edit general Identity Provider details](#) [Delete Identity Provider](#) [Reset all Identity Provider settings](#)

Available Support actions

[Check National Roaming Operator server status](#) [Go!](#)

Profiles for this Identity Provider

Managed IdP

You can create up to 200 users. Their credentials will carry the name `opaquehash@19-18.es.hosted.eduroam.org`.

[Manage User Base](#)

eduroam Managed IdP - Release CAT-2.0.1 on behalf of the GEANT Projects funded by EU GEANT Association Full Copyright and Licenses eduroam® Privacy Notice European Commission Communications Networks, Content and Technology

[Add new user](#) [Import users from CSV file](#)

Please enter a username of your choice and user expiry date to create a new user: (UTC)

[Add new user](#)



eduroam Managed IdP

View this page in English (GB)

https://hosted.eduroam.org/?idp=19

[Edit general Identity Provider details](#) [Delete Identity Provider](#) [Reset all Identity Provider settings](#)

Available Support actions

Check National Roaming Operator server status [Go!](#)

Profiles for this Identity Provider

Managed IdP

You can create up to 200 users. Their credentials will carry the name `opauehash@19-18.es.hosted.eduroam.org`.

[Manage User Base](#)

eduroam Managed IdP - Release CAT-2.0.1 on behalf of the GEANT Projects funded by EU

GEANT Association Full Copyright and Licenses

eduroam® Privacy Notice

European Commission Communications Networks, Content and Technology

Your eduroam® access is ready

eduroam CAT Invitation System <cat-invite@eduroam.pl> para jmanuel.macias

Hello!

A new eduroam® access credential has been created for you by your network administrator. Please follow the following link with the device you want to enable for eduroam® to get a custom eduroam® installation program just for you. You can click on the link, copy and paste it into a browser or scan the attached QR code.

<https://cat-pilot.eduroam.org/accountstatus/accountstatus.php?token=a85a267eb9482614c58b6748375104f2e354ff29a722e>

Please keep this email or bookmark this link for future use. After picking up your eduroam® installation program, you can use the same link to get status information about your eduroam® account.

Regards,
eduroam Configuration Assistant Tool

[Add new user](#) [Import users from CSV file](#)

Please enter a username of your choice and user expiry date to create a new user:

[Add new user](#)



eduroam Visitor Access

- Piloto de eduroam para acceso de visitantes
- Una solución para la gestión de credenciales
- Utiliza una instancia proporcionada a través de acuerdo con eduroam NL (SURFnet)
- Algunas características
 - gestión delegada de invitaciones
 - configuración de la duración de las invitaciones
 - invitaciones por correo y SMS
 - renovación/revocación de invitaciones
 - carga de invitaciones en bloque



eduroam Visitor Access

The screenshot shows the 'Insert visitors - batch upload' page. At the top, there is a dark blue header with the eduroam logo, a language selector set to 'EN', and the user name 'Jose Manuel Macias'. Below the header is a navigation bar with links for Home, My eVA, Admin, Environment admin, and Settings. The main content area has a light blue background and contains a 'Note' box with instructions on how to upload a CSV file. Below the note is a form titled 'INSERT VISITORS - BATCH UPLOAD' with fields for Name, File (with a file explorer icon), and a comment box. There are also time selection fields for 'From (00:00)' and 'Till (23:59)', and checkboxes for 'Notification by Email' and 'Notification by SMS'. At the bottom of the form are 'Cancel' and 'Submit' buttons. The footer features the Red IRIS logo.

The screenshot shows the 'Create visitor' page. It has the same header and navigation as the previous page. The main content area is titled 'Create visitor' and contains a form titled 'CREATE VISITOR'. The form is divided into two sections: 'Visitor' and 'Notify visitor'. The 'Visitor' section has fields for First name, Insertion, Surname, Email address, Mobile number (with a dropdown for country code), and Communication language. The 'Notify visitor' section has checkboxes for 'Notification by Email' and 'Notification by SMS'. Below this is a 'Date' section with a text prompt and two time selection fields for 'From (00:00)' and 'Till (23:59)'. At the bottom is a 'Comments about this author' section with a text area and 'Cancel' and 'Submit' buttons. The footer features the Red IRIS logo.

