

Servicios de RedIRIS Actualidad



Agenda

- Informe de Seguridad: Egida e incidentes (INCIBE)
- Actualidad en la red
- Novedades en el servicio IRIS-DNS
- Actualidad de servicios: Monitorización, Eduroam y SIR
- Actualidad de temas de administración electrónica
- Presentación nuevo servicio piloto: "SIR en la nube"

Servicios de seguridad EGIDA



GOBIERNO
DE ESPAÑA

MINISTERIO
DE CIENCIA, INNOVACION
Y UNIVERSIDADES

MINISTERIO
DE ECONOMÍA
Y EMPRESA

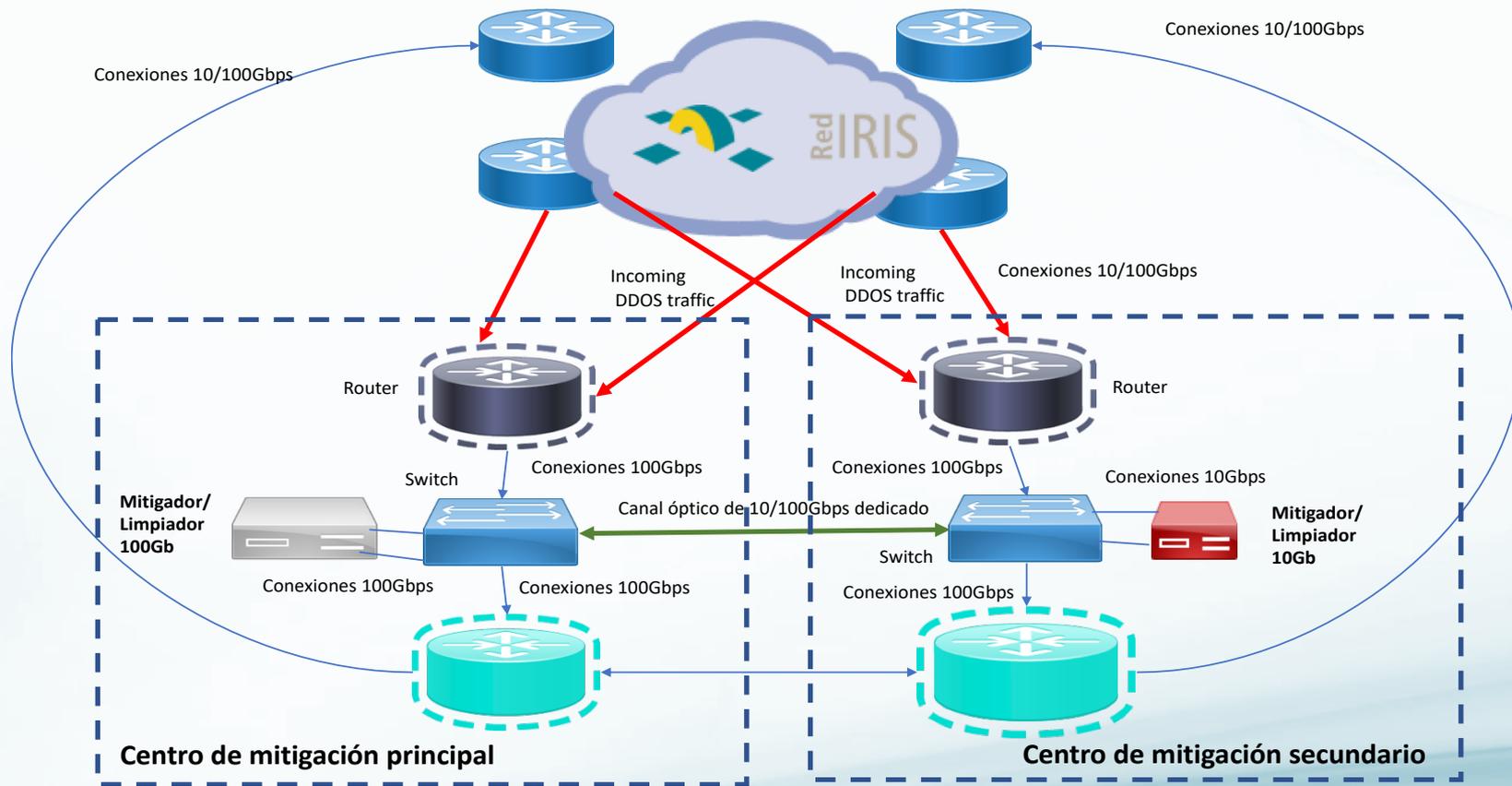


red
RIS

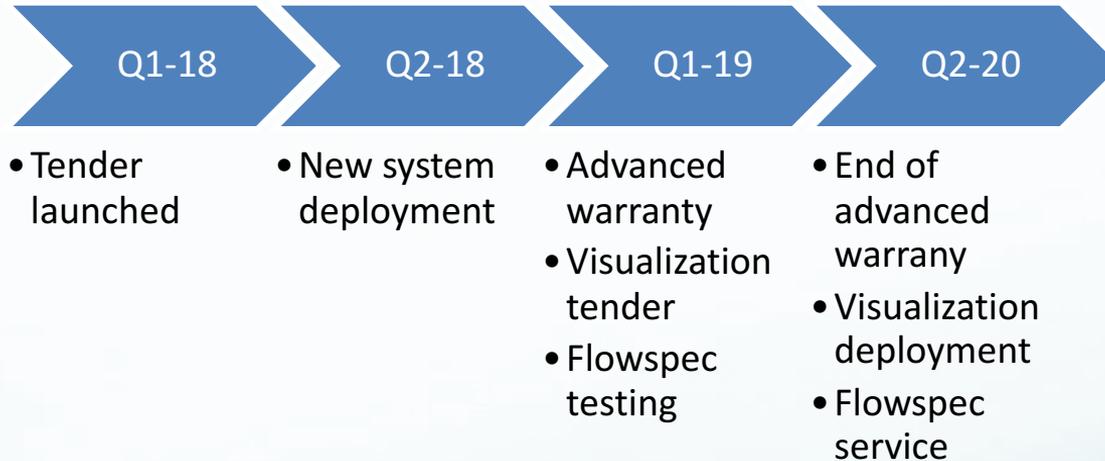


Infraestructuras
Científicas y Técnicas
Singulares

Egida v2. Scrubbing Center



Egida v.2 Timeline



Servicios de seguridad Incidentes



GOBIERNO
DE ESPAÑA

MINISTERIO
DE CIENCIA, INNOVACION
Y UNIVERSIDADES

MINISTERIO
DE ECONOMÍA
Y EMPRESA



red
RIS



Infraestructuras
Científicas y Técnicas
Singulares

 **incibe_**
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Novedades: Automatizaciones



PyRTIR: herramienta desarrollada en python que interactúa con la API REST 1.0 de RT

Basada en plugins por lo que facilita la extensión de la misma.



Objetivo:

Mejora de los procesos automatizando tareas de notificación y chequeo de fuentes y flujos de información de madurez alta.



Actualmente en producción:

- SSL FREAK
- Open-telnet
- VNC
- LDAP
- Portmapper

Futuro: otros servicios expuestos e infecciones con malware.

Incidencias destacadas: Servicios expuestos utilizados en DDoS

Notificaciones desde el CERT de servicios expuestos que podrían utilizarse para ataques DDoS por amplificación y que tras no corregirse han participado activamente en ataques de este tipo.

Varios casos, algunos de los ms destacados:

Notificación CERT DDoS	Servicio	Notificación
16/11/2018	Open Memcached	22/11/2018
29/01/2018	Open LDAP	28/09/2018
11/03/2018	Portmapper	
25/09/2018		
22/03/2018	Portmapper	
25/09/2018		
08/05/2018	DNS open resolver	25/09/2018

Incidencias destacadas: Intentos intrusión PSN

Notificaciones de PlayStation Network de intentos de acceso no autorizados.

Suele tratarse de equipos comprometidos.

215 incidentes gestionados.

En una primera notificación nos remiten el periodo de tiempo en el que se ha detectado el ataque y los dominios destino cuyas IP depende de la zona geográfica.

Se ha trabajado con Sony para disponer de mas detalle que permita a las instituciones identificar el equipo afectado en casos que hay NAT o direcciones IP pertenecientes a EDUROAM.

Gracias por su atención



Actualidad en la red



GOBIERNO
DE ESPAÑA

MINISTERIO
DE CIENCIA, INNOVACION
Y UNIVERSIDADES

MINISTERIO
DE ECONOMÍA
Y EMPRESA

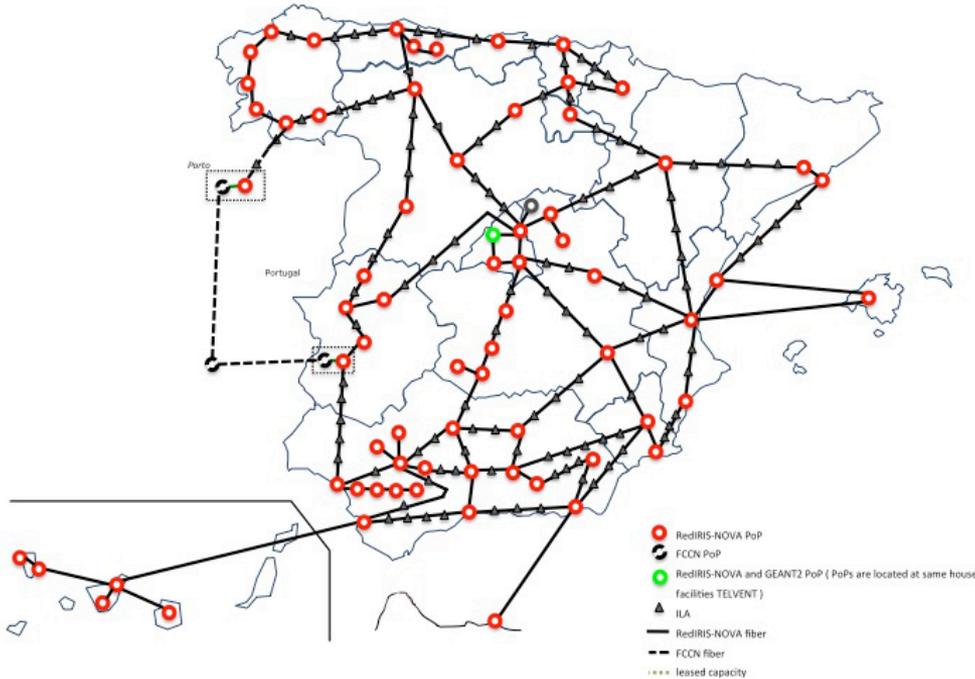


red
RIS



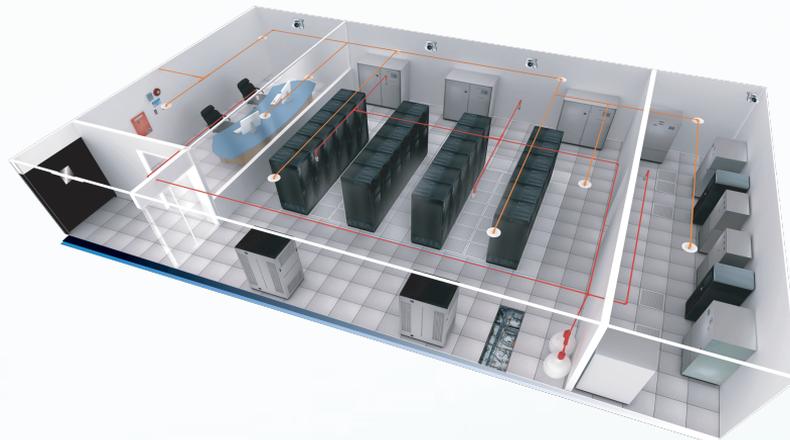
Infraestructuras
Científicas y Técnicas
Singulares

Diálogo competitivo: RedIRIS-NOVA 100



- Publicación 7 Ago 2018
- Presupuesto: 23M €
- Inicio fase diálogo

Auditoría de PdPs RedIRIS-NOVA



Servicio IRIS-DNS



GOBIERNO
DE ESPAÑA

MINISTERIO
DE CIENCIA, INNOVACION
Y UNIVERSIDADES

MINISTERIO
DE ECONOMÍA
Y EMPRESA



red IRIS



Infraestructuras
Científicas y Técnicas
Singulares

Novedades DNS 2017-2019

- 2017 - NOVIEMBRE → Arranque herramienta IRISDNS
- 2017 - NOVIEMBRE → Arranque servicio “HOSTING DNS”
- 2018 - MAYO → Servidores Anycast (PCH) para “HOSTING DNS”
- 2018 - MAYO → Perfiles de usuario para “HOSTING DNS”
- 2018 - MAYO → Estado de servicio para herramienta IRISDNS
- 2018 - NOVIEMBRE → Firmado DNSSEC para “HOSTING DNS”
- 2019 - ENERO → Firmado DNSSEC en REDIRIS
- 2019 - ENERO → Delegación DNSSEC en servicio DELEGACION
- 2019 - MAYO → Servidores Anycast para servicio SECUNDARIO

Mas info: iris-nic@rediris.es

<http://www.rediris.es/servicios/conectividad/dns/>

DNSSEC Y PERFILES EN HOSTING DNS

The screenshot shows the IRISDNS Hosting DNS management interface. The browser address bar displays <https://irisdns.rediris.es>. The navigation menu includes 'Hosting DNS', 'Secundario', 'Delegacion', 'Hosting DNS(Admin)', 'Secundario(Admin)', 'Delegacion(Admin)', 'Indicadores', 'Estado', 'Log', and 'Ayuda'. The 'Hosting DNS' menu item is circled in red. Below the navigation menu, there are several utility links: 'Refrescar', 'Descargar CSV', 'Cambios Masivos', 'Migrar desde secundario', and 'DNSSEC', with 'DNSSEC' also circled in red. The main content area displays a table of DNSSEC records. The table has columns for 'ZONA', 'TIPO', 'PRIMARIO', 'INSTITUCION', 'SECUNDARIOS', 'TTL', 'PERFIL', and 'SERVICIO'. The 'PERFIL' column is circled in red. The table contains four rows of data:

ZONA	TIPO	PRIMARIO	INSTITUCION	SECUNDARIOS	TTL	PERFIL	SERVICIO
ch23dnssec.secrediris.es	directa	130.206.3.37	RedIRIS	sun.rediris.es, chico.rediris.es, pch.anycast.rediris.es.	7200	user	HOSTING
ch24dnssec.secrediris.es	directa	130.206.3.37	RedIRIS	sun.rediris.es, chico.rediris.es, pch.anycast.rediris.es.	7200	user	HOSTING
sir2nube.rediris.es	directa	130.206.3.37	RedIRIS	sun.rediris.es, chico.rediris.es, pch.anycast.rediris.es.	7200	middleware	HOSTING
TEST-perfiles05.test.rediris.es	directa	130.206.3.37	RedIRIS	sun.rediris.es, chico.rediris.es, pch.anycast.rediris.es.	7200	user dnssec	HOSTING

DNSSEC EN HOSTING DNS

The screenshot shows the IRISDNS web interface. The browser address bar displays 'https://irisdns.rediris.es'. The page header includes the RedIRIS logo and 'IRISDNS HOSTING DNS'. A navigation menu contains 'Hosting DNS', 'Secundario', 'Delegacion', 'Hosting DNS(Admin)', 'Secundario(Admin)', 'Delegacion(Admin)', 'Indicadores', 'Estado', 'Log', and 'Ayuda'. The user 'jcarlos (RedIRIS)' is logged in. The main content area shows a table of DNSSEC records under the 'Hosting DNS > Dnssec' path.

ZONA	INSTITUCION	DNSSEC	KSK Rotación Activa	Claves ZSK	Estado ZSK	Claves KSK	Estado KSK	
ch23dnssec.secrediris.es	RedIRIS	SI	SI	(47790 Activate)	Sin rotación activa	(53317 Activate)	Sin rotación activa	
ch24dnssec.secrediris.es	RedIRIS	SI	SI	(16551 Activate)	Sin rotación activa	(49270 Activate)	Sin rotación activa	
sir2nube.rediris.es	RedIRIS	No	-	-	-	-	-	
TEST-perfiles05.test.rediris.es	RedIRIS	No	-	-	-	-	-	

ESTADO DE SERVICIO

IRISDNS HOSTING DNS

Hosting DNS Secundario Delegacion Hosting DNS(Admin) Secundario(Admin) Delegacion(Admin) Indicadores Estado Log Ayuda

Delegacion > Estado servicio

Rows: 1649

BLOQUE ^	ZONA	INSTITUCION	ESTADO	CONF. REDIRIS	CONF. INSTITUCION
	sim.rediris.es.aa2.secrediris.org.es	REDIRIS	OK	pch.anycast.rediris.es. chico.rediris.es. sun.rediris.es.	pch.anycast.rediris.es. chico.rediris.es. sun.rediris.es.
	255.206.130.in-addr.arpa.aa2.secrediris.org.es	REDIRIS	OK	pch.anycast.rediris.es. chico.rediris.es. sun.rediris.es.	sun.rediris.es. pch.anycast.rediris.es. chico.rediris.es.
	250.206.130.in-addr.arpa.aa2.secrediris.org.es	REDIRIS	OK	pch.anycast.rediris.es. chico.rediris.es. sun.rediris.es.	pch.anycast.rediris.es. chico.rediris.es. sun.rediris.es.
	245.206.130.in-addr.arpa.aa2.secrediris.org.es	REDIRIS	OK	pch.anycast.rediris.es. chico.rediris.es. sun.rediris.es.	sun.rediris.es. pch.anycast.rediris.es. chico.rediris.es.
	234.206.130.in-addr.arpa.aa2.secrediris.org.es	REDIRIS	OK	pch.anycast.rediris.es. chico.rediris.es. sun.rediris.es.	sun.rediris.es. chico.rediris.es. pch.anycast.rediris.es.
	229.206.130.in-addr.arpa.aa2.secrediris.org.es	REDIRIS	OK	pch.anycast.rediris.es. chico.rediris.es. sun.rediris.es.	pch.anycast.rediris.es. sun.rediris.es. chico.rediris.es.

eAdmon



GOBIERNO
DE ESPAÑA

MINISTERIO
DE CIENCIA, INNOVACION
Y UNIVERSIDADES

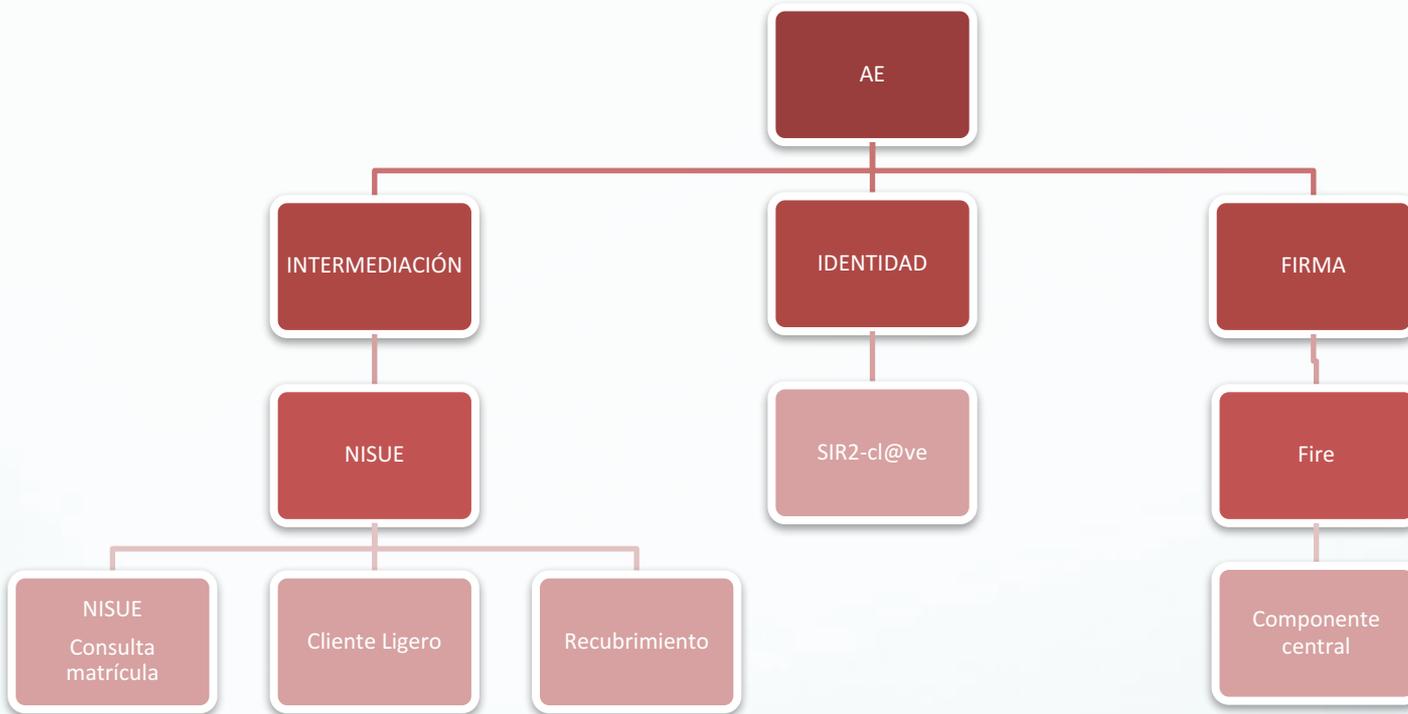
MINISTERIO
DE ECONOMÍA
Y EMPRESA



red
RIS



Infraestructuras
Científicas y Técnicas
Singulares



@FIRMA federado

IRIS-SARA



GOBIERNO DE ESPAÑA

MINISTERIO DE CIENCIA, INNOVACION Y UNIVERSIDADES

MINISTERIO DE ECONOMÍA Y EMPRESA



Actualidad de servicios eduroam, monitorización, identidad



GOBIERNO
DE ESPAÑA

MINISTERIO
ECONOMÍA, INDUSTRIA
Y COMPETITIVIDAD

MINISTERIO
DE ENERGÍA, TURISMO
Y AGENDA DIGITAL



Infraestructuras
Científicas y Técnicas
Singulares

Agenda

- Actualidad servicio de eduroam
- Actualidad servicio de monitorización
- Actualidad servicio de identidad



Servicio de
Monitorización
de RedIRIS



GOBIERNO
DE ESPAÑA

MINISTERIO
DE CIENCIA, INNOVACION
Y UNIVERSIDADES

MINISTERIO
DE ECONOMÍA
Y EMPRESA



Actualidad eduroam



- Entrada en funcionamiento de eduroam CAT 2.0
 - mejora interfaz de usuario
 - mejora en herramientas disponibles
 - próximamente, eduroam Managed IdP
- Encuesta redes de invitados Nicolás Velázquez
- ¿Interés en eduroam Visitor Access (EVA)?
 - Se pasará una encuesta por MovIRIS

Servicio de monitorización



Servicio de
Monitorización
de RedIRIS

- Migración en progreso
 - previsible que concluya a mediados de 2019
 - apagado de la plataforma anterior
- Recordatorio del proceso
 - Requisito estar en SIR2
 - Acceso inicial a la plataforma
 - Videoconferencia con la institución
- Formación para las ICTS

Servicio de monitorización (II)



Servicio de
Monitorización
de RedIRIS

- Datos sobre marcha:
 - 97 organizaciones añadidas
 - 286 agentes (hosts o equipos monitorizados)
 - 937 módulos (servicios o indicadores)
- ¿esto en qué se traduce?
 - $937 \times 5 \times 12 \times 24 \approx 1.349.280$ chequeos diarios
- En planes para 2019
 - Desarrollo de formación online

Servicio de federación de identidad

- Estado de la migración y próximos pasos
- Entidades en eduGAIN
- Soporte al IdP
- IdP en la nube
- Reto Conéctate con SIR2



Estado migración de SIR



- 70% al menos en fase 2 finalizada
- 29% no ha concluido fase 2
 - **si aún no estáis en fase 2, no deberíais demorarlo mucho más**
- Continuación de la migración de SPs a SIR2
 - se dejarán de ver en SIR1



GOBIERNO
DE ESPAÑA

MINISTERIO
DE CIENCIA, INNOVACION
Y UNIVERSIDADES

MINISTERIO
DE ECONOMÍA
Y EMPRESA



red.es



Infraestructuras
Científicas y Técnicas
Singulares

eduGAIN



- ya hay 69 IdPs en eduGAIN
 - idealmente, casi todos los IdPs deberían estar en eduGAIN
- **sólo** hay 3 SPs
 - recordad que os ofrecemos la posibilidad de utilizar un servicio de descubrimiento de eduGAIN, para servicios que queráis hacer visibles internacionalmente
- Estamos preparando un agregado de los SPs que importamos desde eduGAIN

Soporte al IdP de referencia



- Trabajando en varias líneas:
 - Mejora del instalador del IdP de referencia
 - Soporte de actualización vía web
 - Máquina virtual con IdP pre-instalado
 - vagrant → otros hipervisores, docker

Más actualidad SIR...

- IdP en la nube
- Reto Conéctate a SIR2



GOBIERNO
DE ESPAÑA

MINISTERIO
DE CIENCIA, INNOVACION
Y UNIVERSIDADES

MINISTERIO
DE ECONOMÍA
Y EMPRESA



red
IRIS



Infraestructuras
Científicas y Técnicas
Singulares

Servicio de identidad SIR2nube



GOBIERNO
DE ESPAÑA

MINISTERIO
DE CIENCIA, INNOVACION
Y UNIVERSIDADES

MINISTERIO
DE ECONOMÍA
Y EMPRESA



red
RIS



Infraestructuras
Científicas y Técnicas
Singulares

¿Qué vamos a ver?

- Qué es un IdP y su complejidad
- ¿Por qué decidimos realizar este proyecto?
- Ventajas y funcionalidades
- Tecnologías usadas
- Interfaces de usuario
- Calendario

Complejidad de un IdP

Almacenamiento
de logs

Repositorio
de datos

IdP eduroam

Estadísticas

IdP SIR2

IdM

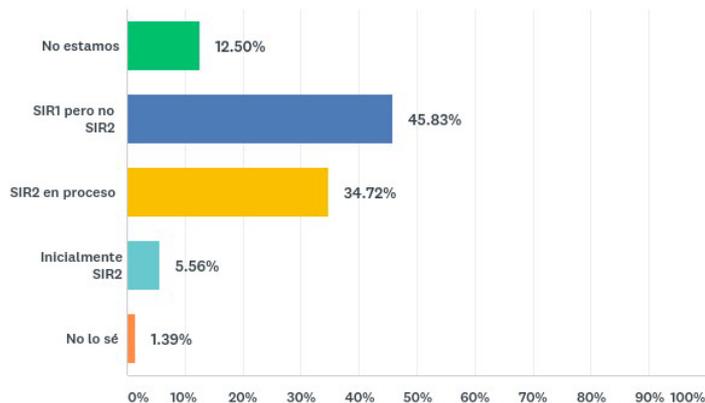
Dashboard
administración

Monitorización

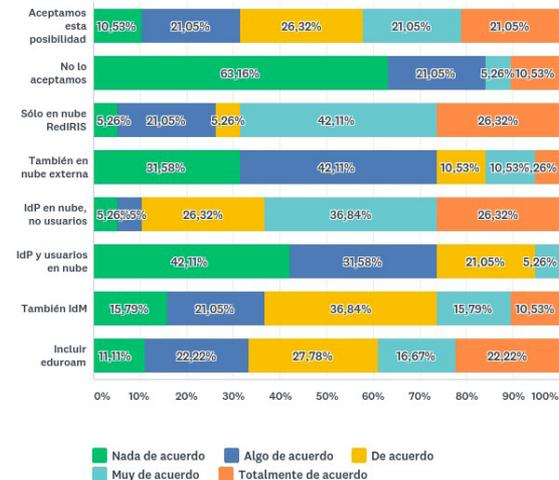
Backend de
sesiones

¿Por qué decidimos hacer este proyecto?

Q6 Situación actual en relación al servicio



Q12 Posibilidad de IdP en la nube - no universidades



Ventajas

- Solicitud de alta sencilla
- Posibilidad IdP eduroam
- Delegación del mantenimiento del IdP
 - Mantenimiento software del IdP, logs, sesiones, repositorio de datos.
- Incorporación continua de nuevas características
 - Adhesión de nuevos roles de usuarios o entitlements de acceso a servicios
- Panel centralizado de administración

Funcionalidades

- Gestión de usuarios (IDM)
 - Posibilidad de importar usuarios desde ficheros CSV
- Gestión de permisos de acceso por servicio (entitlements)
- Gestión de roles para usuarios
- Acceso a estadísticas de uso (SIR y eduroam)
- Acceso a logs generados por el IdP

Tecnologías usadas



GitHub



docker



kubernetes



Jenkins



vmware



IU: Interfaces de usuario

Petición de alta proveedor de identidad

Nombre del responsable

Email responsable

Nombre de la institución

Dominio de la institución

Logo institución

Seleccionar archivo | nada seleccionado

Más información

Enviar petición de alta del IdP en la nube

Validación proveedores de identidad

Institución	Dominio	Responsable	Email	Acción
UNIR	unir.net	Adolfo García	argarcianu@gmail.com	 
Institución X	instX.es	José Manuel Macías	macias@rediris.es	 

IU: Interfaces de usuario

Dar de alta un nuevo usuario

Nombre

Primer Apellido

Segundo Apellido

Mail

UID

Filiación:

Faculty Member

Student Affiliate

Staff Employee

Alum Library-walk-in

Entitlements:

Escoja Entitlements

Registrar

SIR2nube

Dashboard

IDM

Estadísticas

LOGS

Preferencias

Search for...

Crear Usuario

Exportar Usuarios

Importar Usuarios

Usuarios dados de alta

Muestra 10 entradas

Buscar:

Fecha creación	UID	Nombre	Primer apellido	Mail	Acción
2018-10-23	agarcia	Adolfo	Garcia	adolfo.garcia@externos.rediris.es	  
2018-10-24	camarillo	Cristian	Amarillo	camarillo@rediris.es	  
2018-10-25	bsc	BSC	BSC	bsc@bsc.es	  
2018-10-25	cenieh	CENIEH	CENIEH	cenieh@cenieh.es	  
2018-10-25	clpu	CLPU	CLPU	clpu@clpu.es	  

IU: Interfaces de usuario

SIR2nube Search for... [9] [7]

Dashboard
IDM
Estadísticas
LOGS
Preferencias

Logs / Overview

tail -f /var/log/system.log Filter

```
Nov 25 21:16:43 simplesamlphp WARNING [94c21c65ab] The 'userid.attribute' option has been deprecated.
Nov 25 21:16:43 simplesamlphp WARNING [94c21c65ab] The class or interface 'SimpleSAML_Logger' is now using namespaces, please use 'SimpleSAMLLogger'.
Nov 25 21:16:43 simplesamlphp NOTICE STAT [94c21c65ab] F-TICKS/sir.rediris.es/1.0#TS=1543177003#AP=https://www.rediris.es/sir/redirisidp#RP=https://monitor.eduroam.org/sp/module.php/saml/sp/metadata.php/default-sp#PN=db790e655fac551f533164a82e149ce089c4c17b625f983799b4781df66025b4#AM=urn:oasis:names:tc:SAML:2.0:ac:classes:Password#
Nov 25 21:16:43 simplesamlphp NOTICE STAT [94c21c65ab] saml20-ldap-SSO-first https://monitor.eduroam.org/sp/module.php/saml/sp/metadata.php/default-sp https://www.rediris.es/sir/redirisidp NA
Nov 25 21:16:43 simplesamlphp NOTICE STAT [94c21c65ab] saml20-ldap-SSO https://monitor.eduroam.org/sp/module.php/saml/sp/metadata.php/default-sp https://www.rediris.es/sir/redirisidp NA
Nov 26 12:01:40 simplesamlphp WARNING [3eef4875e5] The 'userid.attribute' option has been deprecated.
Nov 26 12:01:40 simplesamlphp WARNING [3eef4875e5] The class or interface 'SimpleSAML_Logger' is now using namespaces, please use 'SimpleSAMLLogger'.
Nov 26 12:01:40 simplesamlphp NOTICE STAT [3eef4875e5] F-TICKS/sir.rediris.es/1.0#TS=1543230100#AP=https://www.rediris.es/sir/redirisidp#RP=https://monitor.eduroam.org/sp/module.php/saml/sp/metadata.php/default-sp#PN=db790e655fac551f533164a82e149ce089c4c17b625f983799b4781df66025b4#AM=urn:oasis:names:tc:SAML:2.0:ac:classes:Password#
Nov 26 12:01:40 simplesamlphp NOTICE STAT [3eef4875e5] saml20-ldap-SSO-first https://monitor.eduroam.org/sp/module.php/saml/sp/metadata.php/default-sp https://www.rediris.es/sir/redirisidp NA
Nov 26 12:01:40 simplesamlphp NOTICE STAT [3eef4875e5] saml20-ldap-SSO https://monitor.eduroam.org/sp/module.php/saml/sp/metadata.php/default-sp https://www.rediris.es/sir/redirisidp NA
Nov 26 14:31:40 simplesamlphp WARNING [ecb396c6dc] The class or interface 'SimpleSAML_Logger' is now using namespaces, please use 'SimpleSAMLLogger'.
Nov 26 14:31:40 simplesamlphp NOTICE STAT [ecb396c6dc] F-TICKS/sir.rediris.es/1.0#TS=1543239100#AP=https://www.rediris.es/sir/redirisidp#RP=https://fpp.sir2.rediris.es/wayf/module.php/saml/sp/metadata.php/598558f78549c20d60e37ef986281e2bbf58ed70#PN=bccdc440c2e530681a47b66463fb35bb612548261bf21cf2ef60dcc515f930d8#AM=urn:oasis:names:tc:SAML:2.0:ac:classes:Password#
Nov 26 14:31:40 simplesamlphp NOTICE STAT [ecb396c6dc] saml20-ldap-SSO-first https://fpp.sir2.rediris.es/wayf/module.php/saml/sp/metadata.php/598558f78549c20d60e37ef986281e2bbf58ed70 https://www.rediris.es/sir/redirisidp NA
Nov 26 14:31:40 simplesamlphp NOTICE STAT [ecb396c6dc] saml20-ldap-SSO https://fpp.sir2.rediris.es/wayf/module.php/saml/sp/metadata.php/598558f78549c20d60e37ef986281e2bbf58ed70 https://www.rediris.es/sir/redirisidp NA
Nov 26 14:31:40 simplesamlphp ERROR [ecb396c6dc] Unable to generate NameID. Check the userid.attribute option.
Nov 26 14:31:40 simplesamlphp WARNING [ecb396c6dc] Falling back to transient NameID.
Nov 26 22:17:51 simplesamlphp WARNING [477db8f822] The 'userid.attribute' option has been deprecated.
```

Copyright © Your Website 2018

Calendario

	Requisitos	MVP	Piloto	Producción
mayo 2018	●			
junio 2018	●	●		
julio 2018	●	●		
agosto 2018		●		
septiembre 2018		●		
octubre 2018		●		
noviembre 2018		●		
diciembre 2018			○	
enero 2018			○	
febrero 2018			○	
marzo 2018				○
abril 2018				○