

Actualidad Servicios RedIRIS

Grupos de Trabajo

Madrid, 29 de Noviembre de 2017





Conectividad RedIRIS

Catálogo de servicios

Conectividad

Por defecto
al conectar

Intranet académica y de la investigación
Acceso a la Internet Global
Gestión de incidencias de Red (IRIS-NOC)

Análisis de rendimiento
Informes y Control
Looking glass
Test velocidad



OPS (24x7) NOC (8x5)



IRIS-IP
IRIS-TICKETS
IRIS-DNS



Servicio IPv6
Servicio de distribución de contenidos Multicast
Servicio de sincronización horario de equipos

Bajo demanda

Servicio de direccionamiento IP
Servicio DNS

IPv4 – IPv6

Hosting - delegación - secundario

Redes Privadas

VPN L2
VPN L2 Múltiple

Circuitos virtuales
Circuitos ópticos

Circuitos ópticos 10G

Novedades Servicio DNS

- Nuevo Servicio “Hosting DNS” (<http://www.rediris.es/dns/hosting-dns.html>)
 - Permite la creación, mantenimiento y publicación de zonas DNS en los servidores de RedIRIS
 - A través de IRISDNS, las instituciones podrán dar de alta nuevas zonas, editarlas o darlas de baja
 - El contenido de la zona es exclusivamente responsabilidad de la institución, y aunque las zonas se crean con unos registros por defecto, es posible dar de alta y modificar cualquier de ellos.
- Herramienta de gestión de servicio IRISDNS (<http://www.rediris.es/dns/irisdns.html>)
 - Herramienta web. Autenticación y autorización mediante SIR.
 - Permite a las instituciones autogestionar los servicios DNS proporcionados por RedIRIS
 - Hosting – Secundario – Delegación
 - Altas, bajas, modificaciones.
 - Publicación de nuevos dominios
 - Cambios implementados inmediatamente.
 - Mantiene un registro de las operaciones realizadas.
 - Permite ejecutar cambios individuales o masivos.



Géant Cloud IaaS Framework

“TOWARDS THE CLOUDS TOGETHER”

Antonio Saravia

antonio.saravia@rediris.es

@asaraviag

- **Contrato marco** disponible y en uso en toda Europa
 - “Towards Pan-European Cloud Services” (<https://www.youtube.com/watch?v=wujP8WFKXlo>)
- **Múltiples beneficios:**
 - Ahorro de costes (descuentos y reducción significativa de los costes de tráfico)
 - Agilidad (licitación conjunta ya realizada por GÉANT)
 - Cumplimiento de la normativa europea sobre seguridad y protección de datos
 - Inicio de sesión único (SSO) con las credenciales propias de cada institución a través del servicio de Federación de identidades de RedIRIS (SIR - eduGAIN)
 - Conexiones optimizadas (Direct peering) con los proveedores cloud
- **Ya en uso en España:** 16 instituciones, principalmente privadas, ya se están beneficiando. Situación de “stand-by” en las instituciones **públicas**
 - Contrato Marco apoyado en la Directiva europea 2014/24/UE sobre contratación pública.
Por fin se aprobó en el Congreso la nueva LCSP donde **se transpone esta Directiva**.

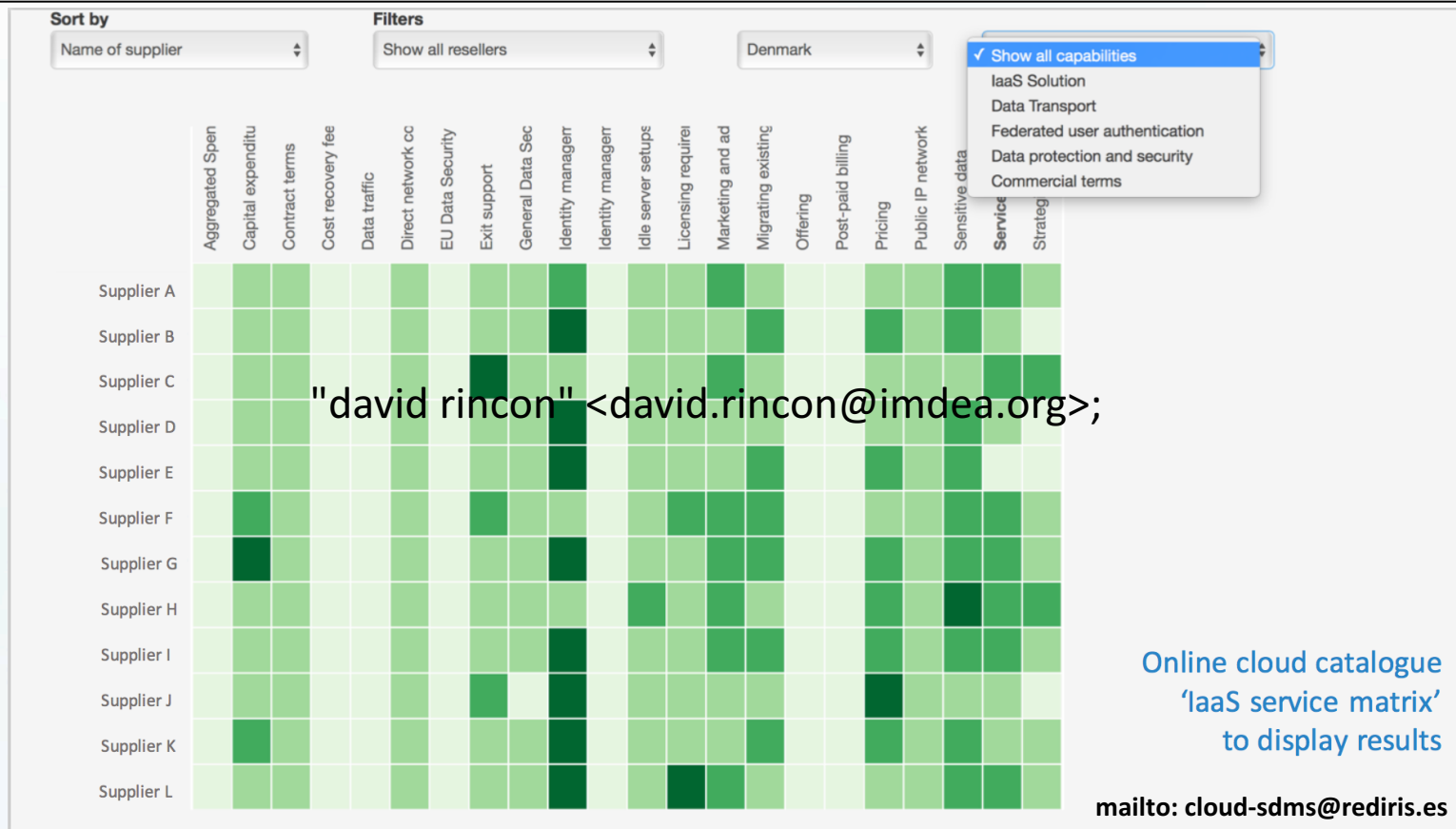
Proveedores Cloud para España



OIPs



Online Cloud Catalogue: IaaS service matrix (<https://catalogue.geant.org/reports/>)



Servicios middleware



GOBIERNO
DE ESPAÑA

MINISTERIO
DE ECONOMÍA, INDUSTRIA
Y COMPETITIVIDAD

MINISTERIO
DE ENERGÍA, TURISMO
Y AGENDA DIGITAL

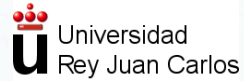


Infraestructuras
Científicas y Técnicas
Singulares

- SIR
 - SIR-CL@ve
 - O365
- Eduroam
- TCS
- AE:
 - IRIS-SARA
 - NISUE
- Monitorización
- Herramientas adicionales:
 - **RID:** Registro de identificadores digitales
 - **FTP:** Repositorio de réplicas

Servicio *SIR*: Federación de identidades

Usuario

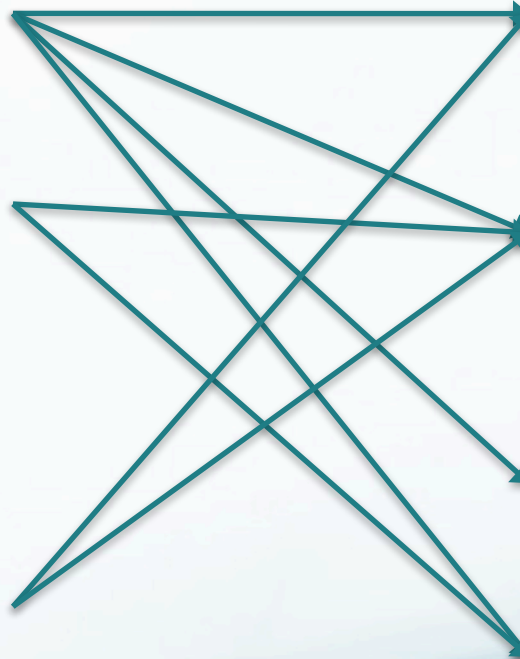


CONSEJO SUPERIOR
DE INVESTIGACIONES
CIENTÍFICAS

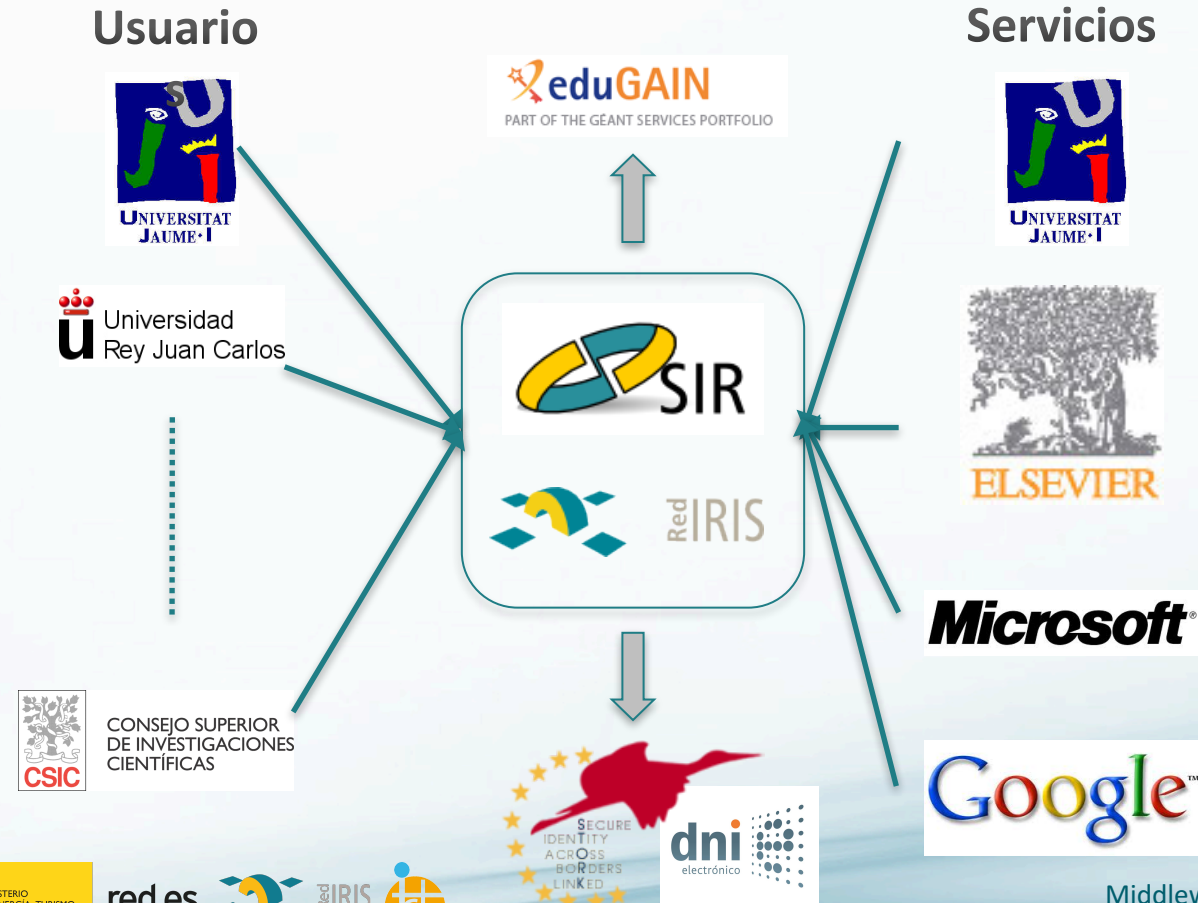
Servicios



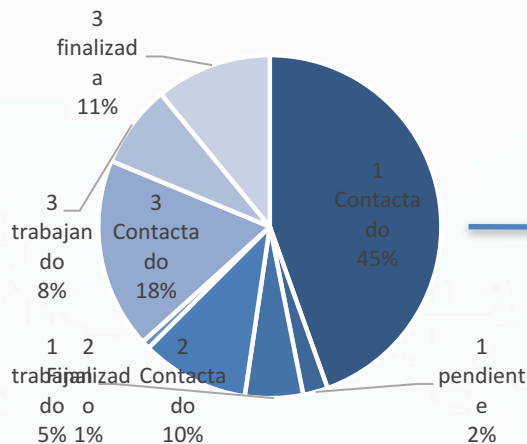
Microsoft®



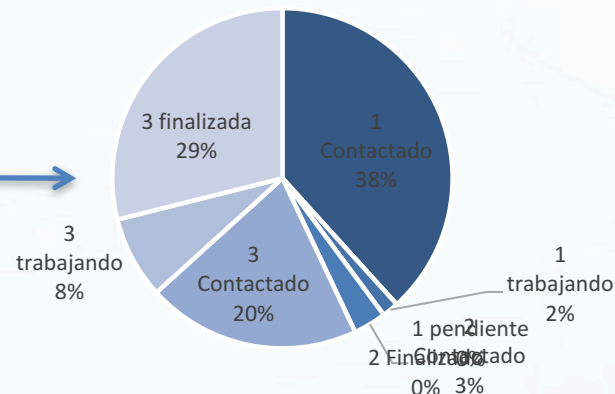
Servicio *SIR*: Federación de identidades



Migración SIR -> SIR2



Junio 2017



Noviembre 2017

Nuevo apoyo para acelerar este proceso

- Integración con cl@ve
 - Permite que los proveedores de servicio SIR puedan usar cl@ve como IdP
 - En pro 7, en pre 19
- Integración O365
 - Permite utilizar SIR como mecanismo para autenticar contra o365
 - Desarrollado por Microsoft con el soporte de RedIRIS
 - US y UPM

“Abre tu portátil, y estás conectado”

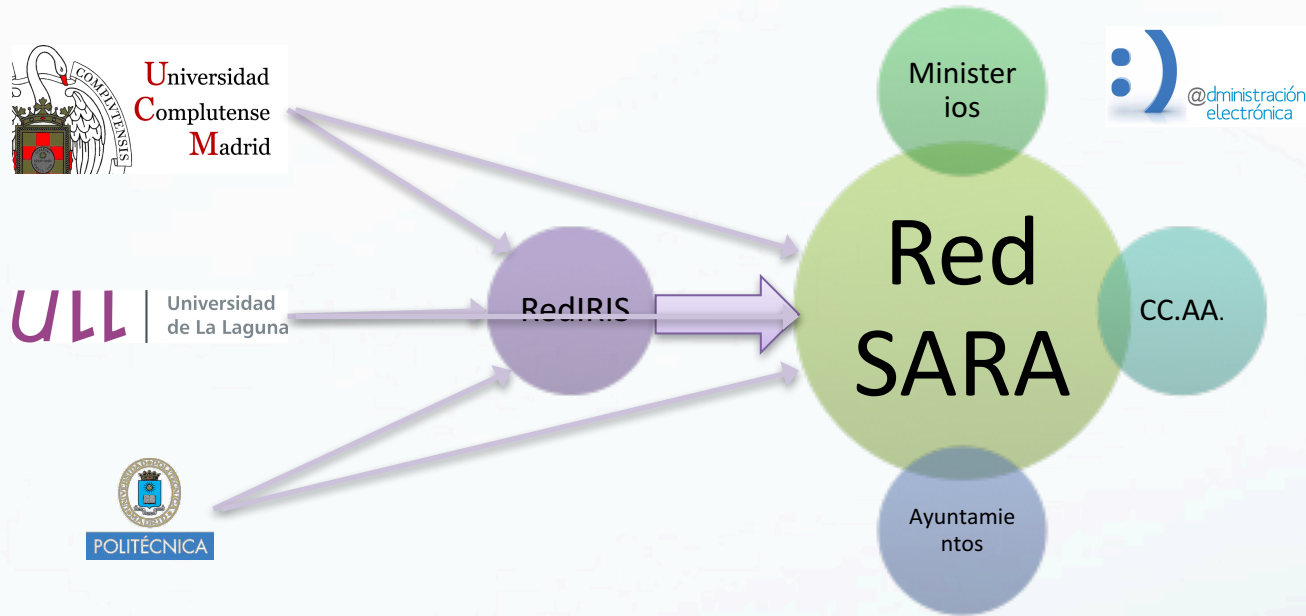


- Servicio global de roaming para instituciones académicas y científicas
- Despliegue en 37 países de la UE, además de EEUU, Canadá y Asia-Pacífico
- En España, desplegado masivamente gracias al programa Campus en Red de red.es
- Estadísticas (2017):
 - 141 instituciones conectadas en España
 - > 25 millones de autenticaciones procesadas al mes



- Vídeo divulgativo de *eduroam*
 - Más de 47.000 visitas en youtube
 - Coste < 1.000€ (desarrollo internacional, adaptado a España)





- RedIRIS como Proveedor de Acceso a SARA para universidades, OPIS e ICTSs
- Racionalización de infraestructuras y gestión de accesos

Sobre el servicio de certificados digitales

*Desde el año 2006, RedIRIS proporciona a sus instituciones afiliadas un servicio gracias al cual pueden solicitar, sin coste para ellas, múltiples tipos de **certificados digitales** (de servidor, personales, de firma de código, de e-Ciencia, ...) emitidos por entidades reconocidas a escala global*

RedIRIS - la red académica y de investigación española

- pkIRISGrid (finalización)
 - 12 años de existencia (2005-2017)
 - 50 autoridades de registro (RAs)
 - 180 operadores de RAs
 - Casi 10.000 certificados emitidos
- TCS
 - Desde mitad de 2015
 - 170 instituciones participantes
 - Más de 11.000 certificados emitidos
 - Más de 800 son de perfiles Grid (e-Ciencia)



RedIRIS - la red académica y de investigación española

- pkIRISGrid (finalización)
- TCS
 - <https://www.rediris.es/tcs>
 - Soporte
 - tcs@rediris.es
 - Lista de administradores del servicio en las instituciones
 - tcs-user@listserv.rediris.es

RedIRIS - la red académica y de investigación española



Servicio de
Monitorización
de RedIRIS

Monitorización de servicios



GOBIERNO
DE ESPAÑA

MINISTERIO
ECONOMÍA, INDUSTRIA
Y COMPETITIVIDAD

MINISTERIO
DE ENERGÍA, TURISMO
Y AGENDA DIGITAL



Infraestructuras
Científicas y Técnicas
Singulares

Sobre el servicio de monitorización...



Servicio de
Monitorización
de RedIRIS

El Servicio de Monitorización de RedIRIS ofrece a las instituciones afiliadas la posibilidad de analizar y diagnosticar el estado de sus servicios, desde un punto neutro situado fuera de su red corporativa, ofreciendo la visión de un observador externo.

Algunas cifras (del servicio que desaparece)

- Lanzado en 2012
- 82 instituciones usando el servicio
- 258 hosts monitorizados
- 305 servicios
- 375 direcciones de contacto
- Más de 50000 chequeos al día
- 1231 *tickets* válidos (peticiones de soporte) desde el comienzo
- Listado de servicios monitorizados:
 - <https://www.rediris.es/monitor/docs/servicios.html>

Sobre la actualización del servicio

- La nueva plataforma recibe el nombre «avizor»
- Finalizando el ajuste de la plataforma, y replicando las monitorizaciones existentes
- Nueva terminología:
 - Un agente \approx una máquina a monitorizar
 - Un grupo de agentes \approx un *tenant* \approx una institución
 - Un módulo \approx un servicio a monitorizar
 - Una métrica \approx cada dato o característica de un agente
- Plataforma escalable, inicialmente parametrizada para:
 - 2000 agentes
 - 50000 monitores (chequeos, con intervalos 5-10

Piloto del nuevo servicio

- Ha estado funcionando durante un año aproximadamente
- Principales conclusiones:
 - La plataforma es potente, aunque por ello puede resultar compleja
 - Valoración positiva de las nuevas capacidades de informes y alertas
 - Vemos necesario hacer una migración inicial de los chequeos en la monitorización anterior como punto de partida
 - Se ve necesaria también formación para exprimir las posibilidades al máximo
- Se ha estado probando la nueva plataforma también para monitorización de NISUE y SIR2

Plan de migración

- Replicación de chequeos en nueva plataforma (en curso)
- Replicación de contactos genéricos (en curso)
 - los contactos individuales podrán establecerse por las personas con acceso a la plataforma
- Petición de firma de nuevo CUSO
 - Recopilación de contactos *de servicio* actualizados
- Creación del *tenant*, asignación de chequeos y contactos de la anterior plataforma, creación de alertas e informes mensuales
- Envío de instrucciones de acceso al *tenant*, vía SIR2
- Eliminación de la monitorización anterior

Elementos de coordinación

- Misma dirección de soporte:
sysmon@rediris.es
- Misma lista de coordinación:
IRIS-MONITOR@LISTSERV.REDIRIS.ES
- Nuevo wiki de documentación:
<https://wiki.rediris.es/Monitor>

Formación

- Prevista formación para primeros meses de 2018
- Se tratará de que conozcamos mejor las posibilidades de la nueva plataforma
- Se realizarán ejercicios prácticos, tanto de monitorización remota (desde la plataforma), como basada en agentes de software





Sistemas y Seguridad



GOBIERNO
DE ESPAÑA

MINISTERIO
DE ECONOMÍA, INDUSTRIA
Y COMPETITIVIDAD

MINISTERIO
DE ENERGÍA, TURISMO
Y AGENDA DIGITAL



Colaboración	
IRISList	Listas de distribución individuales, para cualquier usuario científico
AutoList	Un servicio de listas de distribución para cada institución
FileSender	Intercambio de ficheros pesados entre usuarios
Seguridad	
Lavadora	Correo limpio en los buzones de las instituciones
DDoS – Autofiltrado	Descarte de tráfico hacia servidores no críticos de la institución.
DDoS – Trafico limpio	Red de limpieza de tráfico hacia servidores críticos de la institución
Sistemas	
NTP	Servicio de hora de RedIRIS

EVOLUCIÓN

- **Autolist.** Autoservicio personalizado de listas de distribución.
- **Filesender.** Servicio de intercambio de ficheros/archivos.
- **DDoS.** Servicio de mitigación de ataques de denegación de servicio.

EN DESARROLLO PARA 2018

- **NTP autenticado y filtrado.**
- **Servicio de transferencia de volúmenes de datos.**

Autolist – <http://rediris.es/autolist>

- AutoList es una espacio que permite a una institución crear su propio servicio de listas de distribución autogestionado, con su propio dominio e identidad
 - Panel de administrador y de usuario
 - Formulario para creación de listas por parte de usuarios
 - Estadísticas globales
- Todo el acceso a AutoList es vía SIR y si todavía no se se dispone de SIR dispone de alternativas en bbdd local
- Las credenciales de acceso a LISTSERV también serán vía SIR y via clasica
- Estadísticas AutoList
 - Instituciones: 20
 - Listas creadas: 139
 - Suscriptores: 35.000
- Próximamente: API para cargar usuarios desde bbdd/LDAP de la institución

NEW

NEW

Filesender – <http://rediris.es/filesender>

- Completo servicio para transferir ficheros de hasta 10GB
- Permite enviar ficheros a usuarios SIR
- Permite enviar invitaciones temporales a usuario anónimos para transferir ficheros
- Cada usuario dispondrá de una panel de administración de transferencias e invitaciones
- Ventajas de sobre servicios similares como CONSIGNA
 - Paneles individuales
 - Tamaño cuasi ilimitado de ficheros
 - Mas sencillo e intuitivo
- ¿ Se puede sustituir FileSender por Consigna ? ¿Cómo?

Filesender <http://rediris.es/filesender>

¿qué es?

Plataforma de intercambio de ficheros o archivos.

¿quién lo puede
usar?

Disponible para toda la comunidad RedIRIS

¿requisitos para
usarlo?

Las instituciones deben disponer de SIR para usarlo
Los usuarios externos (no SIR) por invitación.

¿limitaciones?

Solo en el tamaño de los archivos, que debe ser
inferior a **100gigas**.

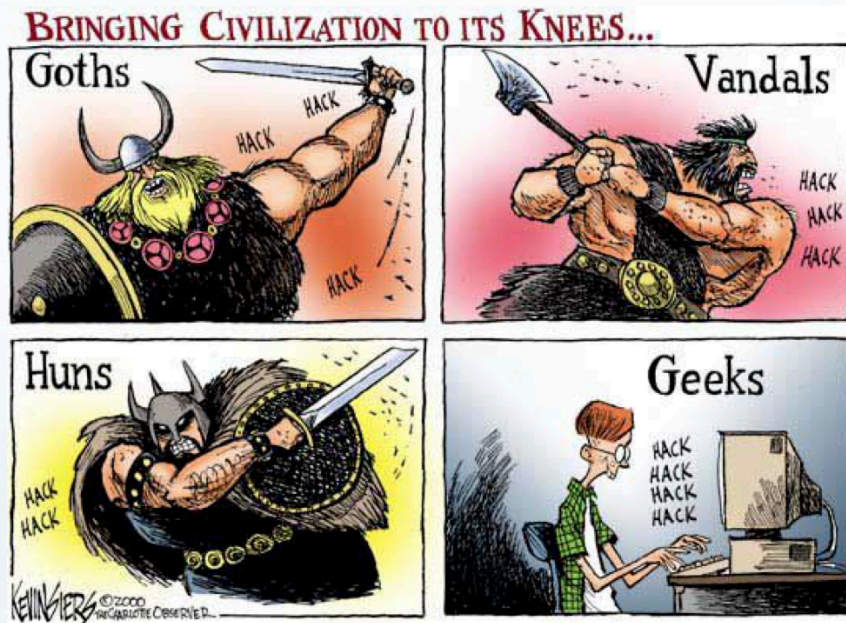
¿como accedo?

<https://filesender.rediris.es>

- NTP autenticado y filtrado del protocolo
 - Más información en : iris-ntp@listserv.rediris.es
- Servicio optimizado transferencia de volúmenes de datos científicos para las instituciones afiliadas.



Actualización de los servicios para mitigación de DDOS



DDOS

Conseguir por diversas formas que un servicio no este operativo, por lo general por saturación de alguno de los elementos que permiten dar este servicio.

-
- PREGUNTA para animar a la gente a conectarse

¿Qué tipo de ataques observáis ?

- Saturación de enlace de red troncal
- Saturación del Firewall / router de acceso
- Saturación del Servidor
- Saturación de la aplicación

Servicios para la Mitigación en RedIRIS

- Visibilidad
- Autofiltrado
- Limpieza de trafico

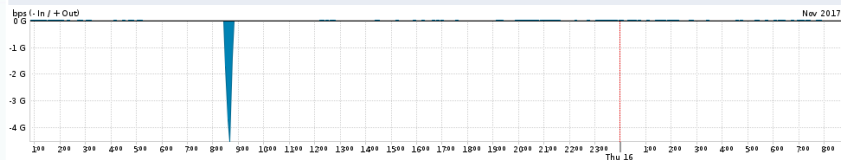
Visibilidad

- Complementa a nivel de seguridad la información de NetFlow que proporciona el servicio de informes de conexión proporcionado por el área de Red.
- En proceso de despliegue y ajustes finales de configuración (acceso federado)
- Debe complementarse con herramientas propias de la institución

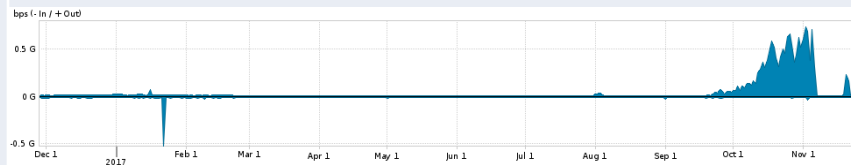
¿Qué se usa en ataques de amplificación ?

- Protocolos basados en UDP
- Falsificación de trafico origen (IP de la victima) a servidores mal configurados.
- La respuesta (en paquetes/bytes) suele ser mayor que la consulta.

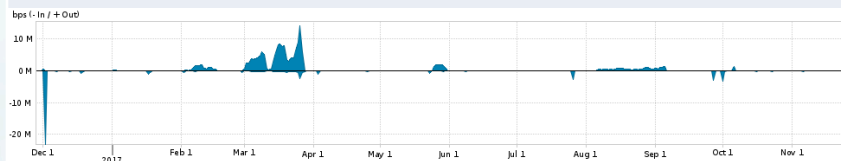
LDAP



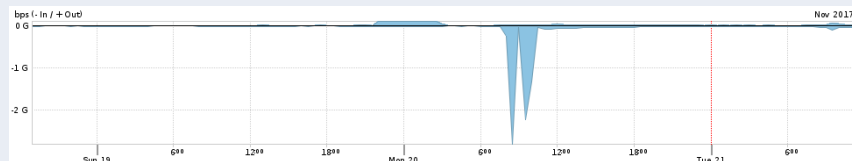
NTP



CHARGEN



DNS



Autofiltrado

- Permite a una institución bloquear tráfico con destino IP propias.
- Posibilidad de filtrar “aguas arriba” de RedIRIS , permitiendo el tráfico dentro de RedIRIS.
- Autoservicio: La institución decide cuando aplicar el bloqueo y cuando volver a permitir el tráfico
- Evolución futura a filtros más específicos ([FoD, de GEANT](#))
- 7 instituciones están usando el servicio ahora mismo
- ~80 rutas filtradas

Limpieza de tráfico

- Actuación bajo demanda una vez configurado el servicio.
- Medidas activas y pasivas para evitar el trafico
- Coordinado con la institución que esta siendo víctima del ataque
- Algunas contramedidas tienen efectos colaterales.

Limpieza de tráfico

Evolución a un sistema de limpieza transparente para las instituciones.

- ~80 % de las instituciones se les puede aplicar limpieza de forma transparente
- Necesidad de solicitar el servicio para tener una mejor visibilidad del tráfico con destino los servicios a proteger.
- Previsto el funcionamiento en modo autoservicio en 2018
- 22 instituciones tienen activado el servicio