Traslado del nodo de Madrid

- Ahora toca el traslado del nodo regional al centro de *housing*

Durante el verano del año pasado, RedIRIS trasladó el nodo nacional de Serrano 142 al centro de *housing* Carrier House 2 de Telvent, en Alcobendas. Tras este traslado, es el turno de mover el nodo regional de Madrid.

El reto principal es coordinar a todos los centros y operadoras con las que trabajan dichos centros. Para facilitar el traslado, RedIRIS ha ampliado sus instalaciones en Telvent. Los centros tienen la posibilidad de trasladar su enlace con la configuración actual en Serrano 142, o bien aprovechar para ampliarlo. Esta opción la están eligiendo bastantes centros, pasando a enlaces basados en tecnología ethernet.

Actualmente estamos trabajando con Telvent, los centros de Madrid y las distintas Operadoras para realizar el traslado lo antes posible.

Miguel Ángel Sotos
(miguel.sotos@rediris.es)
Área de red

Donación de un router CRS de CISCO

- Router de última generación donado a la red académica

CISCO ha donado a RedIRIS un CRS (Carrier Routing System). Se trata de un router de última generación y gran capacidad de proceso, preparado para enlaces de 40Gbps.

ACTO PROTOCOLARIO DE ENTREGA DEL CRS

El pasado mes de diciembre con la asistencia del Ministro de Industria, del Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información y del Secretario General de Política Científica y Tecnológica del Ministerio de Educación se realizó un acto protocolario junto con una rueda de prensa para hacer la presentación de la máquina y sus utilidades a los medios (*www.rediris.es/anuncios/20061220.es.html*).

RedIRIS ha elaborado un plan de pruebas con el router, para poder analizarlo y estudiar todas sus características y funcionalidades. En una primera fase, las pruebas con el router se realizarán en un entorno controlado, en los laboratorios de RedIRIS en el Edificio Bronce y en la siguiente fase, el router se trasladará a Telvent donde se instalará junto al nodo nacional. En ese entorno, se realizarán pruebas de servicios y funcionalidades avanzadas del router.

Miguel Ángel Sotos
(miguel.sotos@rediris.es)
Área de red

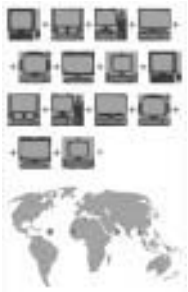
Lanzamiento del VII Programa Marco

- Principal mecanismo de financiación de I+D+i

El día 6 de febrero, representantes de RedIRIS acudieron a la Jornada que organizó en Bruselas la Comisión Europea *(http://cordis.europa.eu/ist/rn/ri-cnd/fp7info-day.htm),* en la que se explicaron a los investigadores que trabajan en el área de las e-infraestructuras cuáles son las principales novedades que incorpora el VII Programa Marco, y qué previsiones de ayudas y convocatorias existen para ese área de las e-infraestructuras.

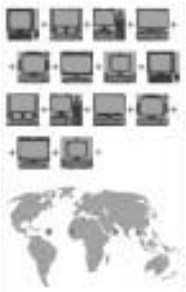
El VII Programa Marco es el principal mecanismo de financiación de I+D+i a escala comunitaria para el periodo comprendido entre 2007 y 2013. Durante esos años, está previsto que las autoridades comunitarias inviertan más de 50 billones de euros.

Las principales áreas cubiertas por este Programa Marco son "Cooperación" (32 billones de euros – investigación en temas de salud, biotecnología, alimentación, TIC, energía, medio ambiente, etc.); "Ideas" (7 billones de euros – Consejo de Investigación Europeo);



Para facilitar el traslado del nodo de Madrid, RedIRIS ha ampliado sus instalaciones

CISCO ha donado a RedIRIS un CRS (router de última generación)



RedIRIS prevé participar en los nuevos proyectos del VII Programa Marco en materia de redes académicas y Grid

El PERT ya es un servicio en producción que se encarga de resolver las incidencias relacionadas con problemas de rendimiento en red

"Gente" (4,7 billones de euros – formación); y "Capacidades" (4,2 billones de euros –"infraestructuras de primer nivel para una investigación de primer nivel").

Dentro del programa "Capacidades" están incluidas las e-infraestructuras necesarias para la e-ciencia, entre las que se encuentran varias directamente relacionadas con la actividad de RedIRIS, como las redes académicas y de investigación o el desarrollo de sistemas de computación en Grid.

Para los años 2007 y 2008, el VII Programa Marco contempla proyectos relacionados con e-infraestructuras por valor de 200 millones de euros. Una parte considerable de ese presupuesto estará destinada a dar continuidad a proyectos clave del VI Programa Marco en esta área. Así, se han presupuestado 95 millones de euros de ayudas para el proyecto GN3, que permitirá mantener el despliegue de la red académica y de investigación paneuropea GÉANT2, y se prevé que se destinen unos 35 millones de euros a EGEE3, el sucesor del principal proyecto de Grid europeo, EGEE-II.

RedIRIS tiene previsto participar en esos nuevos proyectos del VII Programa Marco en materia de redes académicas (GN3) y Grid (EGEE3). RedIRIS se plantea además seguir colaborando en proyectos de extensión del Grid a otras zonas (EELA2, para Latinoamérica) o en proyectos, con otras fuentes de financiación comunitaria, para la extensión de las redes académicas de alta velocidad a Latinoamérica (ALICE) o a la cuenca del Mediterráneo (EUMEDCONNECT). Desde RedIRIS se están analizando también nuevas propuestas relacionadas con su ámbito de actividad, a las que ha sido invitada a participar.

Alberto Pérez
(alberto.perez@red.es)
Subdirector de RedIRIS

GÉANT2

- Actualidad sobre la red paneuropea de redes académicas y de investigación

El pasado mes de enero tuvo lugar en Cambridge (Reino Unido) el Technical Workshop de GÈANT2, en cuyo contexto se celebraron distintas reuniones sobre la actividad de investigación en marcha y a las que asistieron varios representantes de la red académica española.

• Actividad SA3: *Perfomance Response Team*

- Actividad para desarrollar el servicio de Premium IP y el PERT *(Performance Response Team).*

La actividad de servicio SA3 (Service Activity 3) consiste entre otras tareas en desarrollar el servicio de Premium IP y el PERT *(Performance Response Team).* El PERT ya es un servicio en producción en GÉANT2 y consiste en un equipo formado por varias redes académicas nacionales (entre ellas RedIRIS) que mediante turnos rotatorios (uno por semana), se encarga de resolver las incidencias relacionadas con problemas de rendimiento en red.

El PERT atiende problemas de todas las NREN (y sus centros conectados) con conexiones a GÉANT2. Por ahora, tiene una estructura centralizada, y se ha empezado a trabajar en una propuesta para descentralizar el PERT (formando una estructura similar a la de los CERT actuales). Desde que comenzó el PERT, se ha ido creando una base de datos de conocimientos relacionados con temas de rendimiento de aplicaciones y red, y actualmente se ha convertido en una herramienta de obligada consulta para cuestiones de este tipo.

La base de datos se puede consultar en: *http://lkb.pert.geant2.net/ PERTKB/WebHome.*

• Actividad JRA1: *Performance Monitoring and Measurement*

- Actividad dentro del servicio de información de topología de red

RedIRIS está involucrada en esta actividad dentro del servicio de información de topología de red, un servicio que ofrece información topológica multi-dominio intercambiando la información con tecnología Web Services *(http://en.wikipedia.org/wiki/Web_services).* El servicio almacena tanto información del pasado como del presente o del futuro.

Este servicio permite intercambiar la topología de red de las diferentes NREN y por lo tanto tener una visión global de la misma. Posibles usos incluyen proveer información de la topología a herramientas de monitorización como "weather maps" o seguir los cambios que

se produzcan en la topología, tanto para planificación de red como para la localización y resolución de problemas.

El pasado 11 de enero, se presentó la primera implementación del servicio. Actualmente varias NREN están en fase de prueba y RedIRIS está instalando un servidor para facilitar a los desarrolladores que incorporen en sus aplicaciones las funcionalidades ofrecidas por el *Topology Service*.

- **Actividad JRA2: Security**

  - Actividad para la dotación de un marco de seguridad a GÉANT2

Los aspectos más interesantes tratados durante esta reunión fueron los siguientes:

- Transición a Servicio. Como comentamos en el boletín anterior sobre este tema, para aumentar su cobertura, las actividades que se están diseñando en el contexto del JRA2 relacionadas con la promoción en la creación de nuevos equipos de seguridad en aquellas NREN dentro de GÉANT2 que no dispongan de dicha funcionalidad se van a trasladar a un servicio en operación. Actualmente se sigue trabajando en este plan de transición a servicio, concretamente en los temas relacionados con el diseño y participación en un sistema de *mentoring*, el diseño de un portal para CERT en GÉANT2 (*www.geant2.net/cert*) y el de material de formación sobre el conjunto integrado de herramientas de monitorización de tráfico (nfsen, *http://sourceforge.net/projects/nfsen* y Flow Moon, *www.flowmoon.org*), a incluir dentro de los cursos de formación TRANSIT *(www.ist-transits.org/)*.

- Protección de elementos y servicios de red de GN2. Los documentos de recomendaciones y políticas de seguridad para el equipamiento de red y servicios de GÉANT2 redactados durante los años anteriores deben ser revisados y enriquecidos por los APM (GN2 Access Port Managers), lo que servirá también para publicitar el trabajo realizado a sus partners.

- Creación de servicios de seguridad. Durante el presente año, el trabajo en este Work Item se está centrando en la detección de anomalías avanzadas, donde se incluyen el módulo de predicción de anomalías para nfsen basado en el algoritmo Holt-Winters desarrollado por Hungarnet (*http://bakacsin.ki.iff.hu/~kissg/project/ nfsen-hwl*), BICHOS desarrollado por RedIRIS (*www.rediris.es/cert/proyectos/bichos*) y DDoSVax desarrollado por SWITCH (*www.tik.ee.ethz.ch/~ddosvax/*). Además, se está haciendo un seguimiento del trabajo realizado por Anukool Lakhina de la Universidad de Boston (Network -Wide Anomaly Diagnosis with NetReflexSystem, *http://cspeople.bu.edu /anukoll/pubs.html*).

- Diseño y establecimiento de una infraestructura de coordinación de incidentes de seguridad. Centrado en estos momentos en la difusión de información sobre la operativa de la infraestructura de coordinación en todo el GN2, y donde también se incluyen el desarrollo del material de formación, el esquema de *mentoring* y el diseño de un *roadmap* para el servicio de seguridad que se implemente para la red paneuropea Geant2 de los que hemos hablado anteriormente.

- **Actividad JRA3: AutoBAHN**

  - Actividad de asignación automática de ancho de banda en redes heterogéneas

La implementación de la Fase 1 del Inter-Domain Manager (IDM) se ha completado con éxito, incluyendo un módulo funcional de la herramienta Pathfinder que incorpora un motor de *routing* (OSPF-TE) basado en Quagga. A su vez, se han desarrollado los primeros componentes del Domain Manager (DM) y se han iniciado las pruebas de la Fase 1 del IDM con actualizaciones de la versión actual que incorporan resultados de dichas pruebas.

Se está comenzando a planificar un escenario de pruebas real para el IDM en forma de demo que será presentado proximamente.

Se han finalizado y entregado a revisión interna los documentos: DJ3.3.3 (Informe sobre la monitorización del servicio de Ancho de Banda Bajo Demanda) y el DJ3.5.3 (Informe de pruebas de unión de diferentes tecnologías) y a su vez se ha realizado la validación del esquema de bases de datos (cNIS) propuesto por SA3, en función de la aportación realizada por JRA3 en su actividad de WI-05. Como resultado de la misma, se realizarán diversas revisiones y se añadirán elementos a dicho esquema.

Se ha iniciado también el Documento DJ3.4.1,2 (Especificación Técnica del Inter-Domain

Durante este año, el trabajo en la creación de servicios de seguridad se centra en la detección de anomalías avanzadas

Se está comenzando a planificar un escenario de pruebas real para el IDM *(Inter-Domain Manager)*

Manager) y próximamente será entregado a revisión interna.

En JRA3 se han finalizado y entregado dos colaboraciones para la conferencia TCN'07 que contemplan resultados del trabajo que se viene realizando en la actividad:

- *Stitching of technology domains in GN"-JRA3*, V. Reijs y colaboradores.
- *A Bandwidth-on-Demand System Case-study Based on GN2 Project Experiences*, M. Campanella y colaboradores.

Algunos otros puntos tratados fueron:

- El estado de implementación del IDM, planes de pruebas e integración con cNIS.
- Plan de implementación del Pathfinder.
- Diseño y planificación de la implementación del módulo de AAI.
- Marco de trabajo de la actividad Technology Stitching).
- Diseño del módulo de monitorización de JRA3, integración de los scripts actuales con la herramienta de monitorización desarrollada en el marco de otras actividades (JRA1-JRA4).
- Diseño del Domain Manager.

Durante el Workshop también tuvo lugar una reunión entre JRA3 y JRA5 donde se discutieron diferentes aspectos sobre la interoperabilidad del módulo IDM AAI con eduGAIN y se participó en una reunión conjunta con representantes de Internet2-ESnet-CANARIE para tratar temas relativos al plano de control de las diferentes tecnologías utilizadas en la actualidad. Los resultados fueron presentados al 'GLIF working meeting', que tuvo lugar en Estados Unidos los días 14 y 15 de febrero.

Se cambiado el nombre de esta actividad que anteriormente se llamaba (Ancho de Banda Bajo Demanda) habiéndose elegido finalmente AutoBAHN (Automated Bandwidth Allocation over Heterogeneus Networks).

• Actividad JRA5: *Roaming and Authorisation*

- Actividad relacionada con los servicios de movilidad e identidad digital

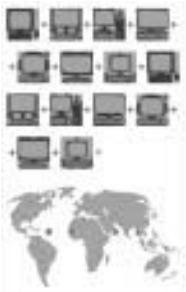
A lo largo de los últimos meses, las actividades dentro de la JRA5 *(www.geant2.net /server/show/nav.758)* se han concentrado, por un lado, en la formalización de eduroam como servicio de la red GÉANT y, por otro, en el desarrollo de la infraestructura de autenticación y autorización eduGAIN.

La formalización de eduroam ha supuesto la constitución de un comité encargado de velar por las condiciones en las que se presta el servicio y definir las vías para su evolución futura. También se ha preparado un documento definiendo la política de uso de eduroam, que ha sido remitido a cada una de las redes académicas participantes para ser ratificado. Este documento, entre otras cosas, especifica las tecnologías que se consideran válidas para que una infraestructura de acceso a la red forme parte de eduroam, así como el conjunto de servicios mínimos que deben prestarse a través de ella.

Dentro de eduGAIN se han realizado demostraciones de interoperabilidad entre las infraestructuras de autenticación y autorización de RedIRIS (PAPI), SWITCH (Shibboleth) y UNINETT (Sun Federation Manager), con lo que la posibilidad de acceso entre recursos web protegidos con cualquiera de estos productos es ya una realidad. Como demostrador permanente se está utilizando el Wiki de la JRA5, hospedado en RedIRIS (*www. redirirs.es/jra5wiki/*). Ha comenzado el trabajo para el uso de la tecnología eduGAIN en los entornos de perfSONAR (monitorización de la red) y AutoBAHN (ancho de banda bajo demanda), lo que supone la aplicación por primera vez de este tipo de control de acceso federado en estos entornos, más allá del acceso web.

También ha arrancado el proyecto DAMe (*http://dame.inf.um.es/*), iniciado bajo los auspicios de la JRA5 de GN2 y con el objetivo de explorar el uso de atributos para realizar un control de acceso más inteligente en infraestructuras de acceso a la red como eduroam, así como el empleo de la identidad del usuario de manera consistente en cualquier servicio: desde el propio acceso a la red hasta a cualquier aplicación, incluyendo web y Grids. Este proyecto está liderado por la Universidad de Murcia.

Miguel Ángel Sotos
(miguel.sotos@rediris.es)
Área de red
Ulisses Alonso
(ulisses.alonso@rediris.es)
Área de red



La formalización de eduroam ha supuesto la constitución de un comité encargado de velar por las condiciones en las que se presta el servicio

El Wiki de la JRA5 está hospedado en RedIRIS

Chelo Malagón
(chelo.malagon@rediris.es)
Equipo de Seguridad IRIS-CERT
Alberto Escolano
(alberto.escolano@rediris.es)
Área de red
Diego Lopez
(diego.lopez@rediris.es)
Coordinador del Área de Middleware

Proyecto EELA

- Proyecto sobre e-infraestructuras entre Europa y América Latina

Entramos en el segundo año del proyecto y ya se ha hecho la primera revisión del mismo, que ha sido muy satisfactoria *(www.eu-eela.org)*. Se espera que el informe oficial de la Comunidad Europea sea igualmente positivo.

Dentro de las tareas de difusión y formación, desde enero de 2006, 930 personas han asistido a tutoriales y escuelas de grids. En cuanto a conferencias, ya se ha organizado el cuarto Workshop con una gran aceptación.

Respecto a entidades participantes, en la actualidad hay 36 conectadas a la red de pruebas de los tres proyectos existentes: aplicaciones biomédicas, aplicaciones de físicas de altas energías y educación en el entorno grid.

La participación del área de red se centra en el paquete de trabajo 2, cuyo objetivo es montar tanto una infraestructura de red de pruebas con los servicios de red necesarios para garantizar el correcto funcionamiento del proyecto como las aplicaciones necesarias para monitorizar esta infraestructura.

Después de la optimización de las transacciones TCP y de la mejora de la velocidad de transferencia de datos, necesarios para ejecutar las aplicaciones de forma eficiente, se ha diseñado un completo sistema de monitorización basado en las herramientas de EGEE GridICE, GStat y SAM.

Durante 2007 se pondrá en marcha un piloto de centro de operación de red (NOC) que utilizará entre otras una herramienta de monitorización extremo a extremo que ya se está desarrollando en GÈANT2, perfSONAR y un sistema de gestión de incidencias.

Ya hay conectados a ella 7 centros de recursos en Europa y 7 en Latinoamérica, sumando entre todos 734 CPU y más de 60 terabytes de almacenamiento.

Cada centro de recursos tiene un responsable y un contacto de seguridad que tienen el respaldo de técnicos con experiencia. El objetivo para el año 2007 es que estos centros alcancen un estado de calidad una vez que el proceso de certificación esté consolidado.

Para tener el reconocimiento internacional de infraestructura de grid se han desarrollado autoridades de certificación y dos oficinas virtuales, una para soporte de grid y otra dedicada a aplicaciones.

Finalmente, respecto a la continuidad del proyecto se está preparando la documentación necesaria para proponer a la Comisión Europea en un par de meses la segunda parte del proyecto, EELA2, que tendría cabida dentro del VII Programa Marco de la Unión Europea.

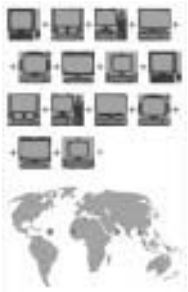
Maribel Cosín
(maribel.cosin@rediris.es)
Área de red

Proyecto DIOR

- Proyecto para el dimensionamiento de redes IP y ópticas

El 1 de octubre de 2006 iniciamos un proyecto llamado DIOR (Dimensionado de redes IP y redes ópticas: aplicación a los accesos de la red académica y de investigación española RedIRIS) en colaboración con la Universidad Autónoma de Madrid.

En términos generales el proyecto se centra en la búsqueda de estrategias de manejo eficiente de la información que a día de hoy proporcionan los sistemas de gestión. El proyecto tiene dos objetivos; primero caracterizar cuál es la evolución previsible del tráfico en los accesos a RedIRIS, y en segundo lugar adecuar las reglas de dimensionado a la tecnología IP sobre WDM. En este sentido, uno de los objetivos del proyecto es analizar cómo es posible llevar el tráfico de RedIRIS a través de circuitos ópticos conmutados y eventualmente, con tecnología de conmutación óptica de ráfagas y paquetes.



En la actualidad hay 36 entidades conectadas a la red de pruebas de los tres proyectos existentes en EELA

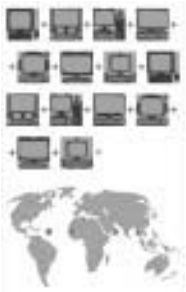
El proyecto DIOR trata sobre el dimensionamiento de redes IP y ópticas

Se analizarán los tráficos agregados de la red en estudio en escalas de tiempo grandes y a partir de ahí se tratará de encontrar reglas de dimensionado aceptables y prácticas que traten de basarse en parámetros simples.

Esther Robles
(esther.robles@rediris.es)
Coordinadora del Área de Red

Proyecto MUPBED

- Proyecto para implantación de nuevas tecnologías de red



El Proyecto MUPBED trata de implantar nuevas tecnologías de red

RedIRIS participa en el proyecto MUPBED de la Comisión Europea *(www.ist-mupbed.org),* junto con otras NREN como GARR y DFN (italiana y alemana), fabricantes como Marconi y Telecos, como Telefónica o T-Systems. En el proyecto se está realizando una serie de pruebas en varios *testbeds* desplegados, interconectando dos tipos de dominios: con ASON/GMPLS e IP/MPLS, todo ello sobre un plano de control unificado. Los *testbeds* se interconectan con una red de nivel 2 que se ha construido con L2VPN sobre GÉANT2 y las NREN.

Actualmente, el proyecto se encuentra en su último año, participando activamente en diferentes eventos con TERENA, donde se muestran los resultados obtenidos.

Miguel Ángel Sotos
(miguel.sotos@rediris.es)
Área de red

EGEE-II

- Actualidad sobre la monitorización de red en el proyecto

El proyecto OSIRIS entra en su segunda mitad

Dentro de este proyecto se incluye la monitorización del rendimiento de la red. Para ello RedIRIS está colaborando con el Edinburgh Parallel Computing Centre (EPCC) de la Universidad de Edimburgo *(www.epcc.ed.ac.uk)* para el despliege del servicio e2emonit *(www.egee-npm.org/e2emonit)*. Este servicio ofrece medidas obtenidas a partir de herramientas de monitorización activas como PingER, UDPmon e IPERF que ofrecen métricas de RTT, tasa de transferencia de UDP y TCP así como medidas de pérdida de paquetes UDP e ICMP entre diferentes puntos de la topología de EGEE-II. Los resultados de estas medidas se exportan al centro de operaciones de grid (GOC) que monitoriza la red EGEE-II y hace de intermediario entre las diferentes NREN involucradas dentro del proyecto y los usuarios del grid.

Ulisses Alonso
(ulisses.alonso@rediris.es)
Área de red

OSIRIS

- Proyecto europeo para la integración de servicios en tiempo real

El proyecto OSIRIS (Open Source Infrastructure for Run-time Integration of Services) entra en su segunda mitad. En el último plenario que tuvo lugar a comienzos de diciembre de 2006 en Málaga se destacaron los siguientes avances:

- La revisión del proyecto por parte de la oficina ITEA (Information Technology for European Advancement) fue superada satisfactoriamente.
- El documento de arquitectura ha sido mejorado y completado; asimismo, se ha seleccionado OSGi como plataforma de despliegue de los servicios.
- Se han dado pasos muy importantes en la integración de los servicios de autenticación y autorización con OSGi.
- Preparación del deliverable Services Layer v1 (abril 2007).

Como hitos a medio plazo, podemos reseñar el desarrollo de un documento sobre seguridad en OSIRIS y la implementación del protocolo PAPI basado en Web Services.

Para más información se puede acudir tanto a la la página web del proyecto (*www.itea-osiris.org*, como a la de ITEA (*www.itea-office.org*).

Ajay Daryanani
(ajay.daryanani@rediris.es)
Área de Middleware

Resultados de la encuesta realizada en las últimas Jornadas Técnicas de RedIRIS

- Valoración de los usuarios a los servicios ofrecidos por RedIRIS

Una vez procesados los resultados de las encuestas que invitamos a cumplimentar a los asistentes de las últimas Jornadas Técnicas celebradas en Granada, algunas de las lecturas que hemos sacado de ellas son las siguientes:

- Aunque el número de respuestas recogidas fue aceptable, nos gustaría en ediciones posteriores simplificar el procedimiento de cumplimentación, para poder obtener una opinión global aún más significativa, y con la buena disposición y ayuda de los asistentes, poder mejorar el servicio.

  El propósito de estas encuestas no es otro que el de conocer la opinión de RedIRIS y sus servicios entre sus organizaciones usuarias. Es la única forma de que disponemos en la actualidad para poder valorar de una forma directa la percepción que tienen los usuarios de los servicios que se ofrecen o su nivel de uso en la comunidad académica. También nos ayuda a detectar necesidades de servicio no cubiertas por nuestra parte, o a constatar que determinados servicios pueden continuar prestándose cuando en realidad ya apenas son demandados.

- Los resultados globales obtenidos en la encuesta son claramente positivos. La mayoría de los que opinan consideran que los servicios ofrecidos son buenos, siendo en general pocos los que creen que son regular, y muy pocos los que los valoran de forma negativa. El servicio que tiene una peor valoración en la actualidad es el portal web. Cabe indicar al respecto que dicho portal está ya en proceso de renovación y actualización.

- Aparecen como servicios muy bien valorados en la comunidad RedIRIS el servicio de movilidad eduroam y el de seguridad IRIS-CERT, al igual que algunos servicios específicos de red como el noc, el servicio de IPv4, el de DNS, el de direcciones IP o el NTP. A la vista de los resultados, la actividad del área de difusión y organización de eventos es otra de las que hn recibido una valoración positiva.

- Hay algún tipo de servicio que se refleja como claramente desconocido, y aunque no se pretende que todo el mundo utilice todos los servicios, sí se busca por parte de RedIRIS que por lo menos se tenga un conocimiento global de ellos, ya que si bien ahora pueden no resultar necesarios a una institución, podrían serlo en otro momento.

Agradecemos mucho vuestra participación, y os animamos a que sigáis enviándonos vuestras opiniones.

María Bolado
(maria.bolado@rediris.es)
Coordinadora de Relaciones Externas

Jornadas de e-Ciencia

- Conferencias para promover el uso de la tecnología Grid

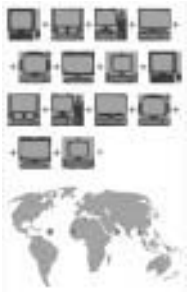
Coincidiendo con la revisión de los proyectos europeos EELA, EuChinaGrid y EuMedGrid en Madrid, el Ciemat organizó un congreso de e-Ciencia (*http://webrt.ciemat.es:8000/e-science/index.html*) los pasados días 1 y 2 de marzo durante el cual se ofreció una serie de conferencias destinadas a promover el uso de la tecnología Grid, visualizando diferentes experiencias que se están desarrollando a nivel internacional así como plataformas Grid en producción existentes. RedIRIS contribuyó en este congreso con la ponencia "Building Global Services for Supporting the e-Science Initiatives" en la que se ofreció una visión global sobre el trabajo que se ha desarrollado y se desarrolla actualmente en el marco de la e-Ciencia y los servicios de RedIRIS focalizados en el soporte y desarrollo de infraestructuras Grid.

Antonio Fuentes
(antonio.fuentes@rediris.es)
Àrea de Sistemas y Tecnología Grid

6º Tutorial sobre Grid - EGEE/EELA/EuMedGrid

- Curso de Grid para usuarios y administradores

RedIRIS, en colaboración con la Facultad de Informática de la Universidad Complutense de Madrid, organizó el pasado mes de octubre un



Aparecen como servicios muy bien valorados en la comunidad el de movilidad eduroam y el de seguridad IRIS-CERT

Las jornadas de e-ciencia estaban destinadas a promover el uso de la tecnología Grid

curso de formación en tecnología Grid destinado tanto a administradores como a usuarios de la comunidad académica y científica española. Este curso se desarrolló en el contexto de las actividades NA3 (Formación) de EGEE (*www.eu-egee.org*), WP4 (Difusión) de EELA *(www.eu-eela.org)* y WP5 de EuMedGrid *(www.eumedgrid.org).*

El curso contó con la participación de alumnos tanto españoles como extranjeros, todos de habla hispana, pertenecientes a distintas universidades y centros y distintas áreas de conocimiento; el profesorado provenía de la UCM, el CIEMAT, RedIRIS y del Instituto de Física de Catania en Italia

El tutorial contó además con una charla invitada de expertos en *middleware* Grid del grupo de investigación en Arquitectura de Sistemas Distribuidos de la Facultad de Informática de la Universidad Complutense de Madrid, que describieron cómo el metaplanificador GridWay, desarrollado por este grupo de investigación, puede usarse para la distribución, control y ejecución de tareas en el Grid.

Desde Latinoamérica, también asistieron personas que actualmente están participando en el proyecto EELA. El curso estaba restringido a un máximo de 40 alumnos y, como la demanda fue muy superior, está en preparación un segundo que tendrá lugar el próximo mes de mayo.

Antonio Fuentes
(antonio.fuentes@rediris.es)
Área de Sistemas y Tecnología Grid

Ataques más inteligentes y más difíciles de detectar en 2006

Durante 2006 se ha confirmado un nuevo cambio en el patrón de ataques, pasando de los famosos ataques masivos de gusanos y similares, a ataques más silenciosos, inteligentes y dirigidos, y por tanto más difíciles de detectar. Los ataques más frecuentes han seguido siendo los ataques de fuerza bruta SSH, junto a los problemas relacionados con la inyección de código HTML, debido a las vulnerabilidades conocidas en sistemas PHP, siendo las máquinas zombies el origen de la gran mayoría de los ataques de los que tenemos constancia. La proliferación de los 0-day-exploits y el constante aumento del *phishing* y los troyanos bancarios han tenido un gran impacto social y mediático.

Para finalizar, 2007 se presenta como un año bastante parecido al pasado. La prolifereción de sitios web, *blogs, wikis,* etc., hará del web el mecanismos favorito para la distribución de *malware* utilizando ataques CSS (Cross Site Scripting) o aprovechando tecnologías emergentes como el Ajax o la Web 2.0. Todo hace pensar que el uso de *rootkits* y *malware* con fines lucrativos, el desarrollo de troyanos incrustados en imágenes y películas para evitar filtros y antivirus, el decremento del *phishing* a favor de técnicas de ingeniería social más novedosas, el uso de vulnerabilidades en redes sociales tipo You Tube o MySpace para distribuir de forma masiva *malware* y, sobre todo, las redes de *bots* nos mantendrán ocupados durante el próximo año.

Chelo Malagón
(chelo.malagon@rediris.es)
Equipo de Seguridad IRIS-CERT

Informe de incidentes de seguridad 2006

- Informe sobre la situación de la seguridad en la red académica

Un año más, IRIS-CERT ha publicado en su página web el informe anual de incidentes correspondiente al pasado año 2006 (*www.rediris.es/cert/doc/informes/2006/*).

Se trata del quinto informe anual que publicamos y cuyo objetivo es el de dar a conocer los problemas de seguridad que protagonizaron el año 2006, su incidencia en la red académica y una predicción de las tendencias en el futuro próximo.

Cese de actividades de RedIRIS-PKI

- La iniciativa de dotar a la comunidad RedIRIS de una infraestructura de certificación pública ya se ha convertido en un servicio estable

Se ha convertido en servicio estable la infraestructura de certificación pública

En 1997 comenzó en RedIRIS una nueva iniciativa a modo de Grupo de Trabajo (GTI-PCA, *www.reddiris.es/pkiliris-pca/gti-pca/index.es.html*) cuyo objetivo era el de dotar a la comunidad RedIRIS de una infraestructura de certificación de claves públicas, basada en X509, con unos requisitos y políticas de certificación homogéneas, como paso inicial para la implantación de servicios avanzados de seguridad en nuestra comunidad. Este grupo de trabajo culminó en el 2000 con el

establecimiento de una infraestructura de certificación para la comunidad (RedIRIS-PKI, *www.rediris.es/pki/iris-pca*) como servicio estable. Desde entonces hasta ahora distintas universidades han participado de diferentes maneras en dicha infraestructura, acercando así una tecnología, por entonces emergente, a nuestras instituciones, y permitiendo alumbrar servicios más avanzados basados en esta tecnología como el SCS (*www.rediris.es/cert/scs*) y la PKI de IRISGrid (*http://pki.irisgrid.es*).

Con la sensación de haber cumplido nuestra misión, es necesario cerrar un ciclo que nos ha permitido avanzar en el entendimiento y despliegue de este tipo de infraestructuras y por eso queremos anunciar el cese de actividades de la infraestructura de clave pública RedIRIS-PKI.

Hasta la fecha de expiración del actual certificado raíz en noviembre de 2007, y cumpliendo con lo especificado en nuestra política de Certificación (*www.rediris.es/pki/iris-pca/docs/politica.html*), seguiremos firmando y publicando CRL, pero ya no se aceptan nuevas inscripciones.

Muchas gracias a todos los que habéis participado en este proyecto a lo largo de los años por vuestra colaboración.

Chelo Malagón
(chelo.malagon@rediris.es)
Equipo de Seguridad IRIS-CERT

Grupo de Trabajo RTIR

- Herramienta de gestión de incidentes de seguridad

Como ya se ha comentado en números anteriores del boletín, RTIR (Request Tracker for Incident Response, *www.bestpractical.com/rtir*) es la herramienta de libre distribución, actualmente utilizada por IRIS-CERT al igual que por otros equipos de seguridad en Europa y el resto del mundo, para realizar la tarea de atención y gestión de incidentes.

Desde la última referencia hecha en el boletín número 76 de RedIRIS, el grupo de trabajo (*www.terena.org/activities/tf-csirt/rtir.html*) ha seguido avanzando y trabajando a fin de que el desarrollo de la nueva versión mejore la herramienta actual. Durante este periodo de tiempo, tenemos que destacar algunos de los sucesos más importantes del proyecto, como la finalización de la primera y segunda fase en marzo y octubre de 2006, respectivamente, que han producido las primeras versiones estables del RTIR v.2. Estas versiones incorporan prácticamente la mayoría de las nuevas especificaciones diseñadas por el grupo de trabajo, como la mejora de la generación de informes y estadísticas; la mejora en el rendimiento de la herramienta; la integración con RT y RTFM... Además desde IRIS-CERT y como parte de los compromisos adquiridos como responsables técnicos del proyecto, se ha elaborado un documento de migración, que tiene como destinatarios a los usuarios actuales y futuros de RTIR. Añadir también que todas las versiones estables del *software*, así como el documento de migración están disponibles a través de *ftp://sunsite.rediris.es/rediris/cert/rtir*.

Hay que destacar el interés del grupo de trabajo en la difusión de sus resultados, de forma que sean lo más útiles posible para los equipos de seguridad que los utilizan en la actualidad; para ello, durante las distintas reuniones que se han mantenido de coordinación del proyecto, se ha pensado en la posibilidad de crear un web *(rtir.org);* que sirva como nexo de unión para toda la comunidad de usuarios de RTIR, y donde estén disponibles las versiones estables, la documentación sobre su utilización e instalación y los nuevos desarrollos que quieran ser compartidos con la comunidad.

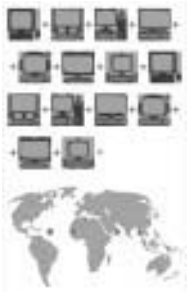
Actualmente nos encontramos en el desarrollo de la tercera y última fase del proyecto, que concluirá entre mediados de mayo y principios de junio, dependiendo de los resultados de las pruebas a las que será sometida la última versión del RTIR.

Carlos Fuentes
(Carlos.Fuentes@RedIRIS.es)
Equipo de seguridad IRIS-CERT

Racionalización del servicio de news

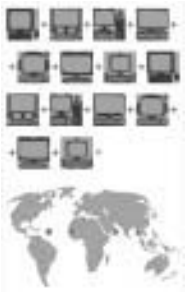
- Evolución del servicio de distribución de news de RedIRIS

El servicio de distribución de News de Usenet IRIS-NEWS viene funcionando en RedIRIS desde 1993, y ha sido un servicio de carácter colaborativo y de consulta muy ampliamente utilizado. Debido a su concepción, las News fue



Desde IRIS-CERT se ha elaborado un documento de migración, que tiene como destinatarios a los usuarios actuales y futuros de RTIR

El servicio de distribución de News de Usenet IRIS-NEWS viene funcionando en RedIRIS desde 1993



El volumen de información de las News era considerable comparado con los anchos de banda de las líneas de comunicación de RedIRIS

El Foro Abuses agrupa a los principales operadores españoles

el primer canal de Internet que de forma abierta y sin moderar transportaba y distribuía grandes volúmenes de información que atravesaban fronteras. Esta distribución se aprovechó para el intercambio de contenidos en muchos casos ilícitos o no académicos, provocando enconados debates en el seno de la comunidad RedIRIS.

El volumen de información de las News era considerable comparado con los anchos de banda de las líneas de comunicación que RedIRIS tenía en esos momentos y esto obligó a ajustar la topología de IRIS-NEWS a la de la red, centralizando todo el servicio en el servidor de RedIRIS que hacía de único intercambiador de News entre sus clientes y los proveedores nacionales e internacionales. Ha venido siendo un servicio que requería pocos recursos, sencillo de gestionar y con buenos rendimientos.

Tanto el aumento del ancho de banda como la aparición de nuevas tecnologías y otros servicios han provocado una disminución lenta pero continuada del uso del Servicio IRIS-NEWS. Las encuestas pasadas a las instituciones afiliadas a RedIRIS nos indican que el servicio ha entrado en declive y que su uso empieza a ser residual.

Por este motivo, RedIRIS está evaluando el futuro del Servicio definiendo un plan de actuación para cerrar el ciclo de vida de IRIS-NEWS. Entre las primeras medidas que se han adoptado figura la *liberación* del puerto 119/NNTP del *backbone* de RedIRIS que ha estado filtrado desde sus orígenes. Esto implica que las instituciones que deseen mantener el servicio puedan buscar y llegar a acuerdos con otros operadores que hagan de intercambiadores de grupos de News. RedIRIS también está evaluando la posibilidad de ofrecer durante un periodo de tiempo limitado un servidor de acceso de lectura de News para aquellas instituciones que tienen pocos usuarios y que no pueden mantener su propio servidor.

En las reuniones de los próximos grupos de trabajo se espera tomar una decisión al respecto, que será oportunamente difundida entre todas las partes afectadas.

Jesús Sanz de las Heras
(jesus.heras@rediris.es)
Servicio de correo electrónico

Resumen del IV Foro Abuses

• Foro de lucha contra el *spam*

El Foro Abuses (*www.rediris.es/abuses/*) es una plataforma coordinada por RedIRIS desde hace ya siete años, que agrupa a los principales operadores españoles (el 90 por ciento de la Internet española, según AIMC- *www.aimc.es*). Los objetivos del Foro son coordinar las acciones técnicas entre operadores en la lucha contra las amenazas como el *spam,* las escaneos, estafas, etc., y la mejora continua en la defensa de la Red. Desde el punto de vista de RedIRIS, consideramos útil este foro como canal de transmisión entre los ISP españoles y las instituciones de nuestra Comunidad.

La última reunión de este foro que constituye la IV edición se celebró el 1 de marzo, y en ella se trataron temas de interés ya conocidos entre la Comunidad RedIRIS. Destacamos las principales acciones de esta reunión:

- Se aprobó la incorporación al Foro Abuse como miembros especiales del Centro Criptológico Nacional (CCN-CERT). Cert de la administración española y responsable de sus incidentes de seguridad y del CATA (INTECO). Cert para Pymes y responsable de los temas de seguridad en esta área.

- Lista Blanca española, iniciativa coordinada por RedIRIS en el Foro Abuse (*www.rediris.es/abuses/eswl*).

  - Se comentó la necesidad de mejorar el formato de los registros.
  - La Lista Blanca está siendo utilizada por los *relays* de: ARRAKIS, IBERCOM, MENTA, ONO, Telefónica, Terra, Telecable, etc., y por unas veinte universidades. El CCN-CERT se comprometió a recolectar las IP de *relays* de las Administraciones Públicas.
  - Hubo varias propuestas para hacer de secundarios de las actuales zonas de la Lista Blanca

- Se adoptó la decisión de que todos los *relays* de miembros del Foro implementaran SPF en un plazo por determinar, se hiciera difusión de SPF y se extrajerán estadísticas.

- Listas Negras. Dado que las Listas Negras se utilizan, se propuso hacer unas recomendaciones de las más valoradas y de los criterios de selección más importantes para tener en cuenta a la hora elegir estas listas, ya que existen cientos de ellas y muchas con dudosas políticas.

- Se consensuó el documento "Buenas prácticas para operadores de correo" (*www.rediris.es/ abuses/docus/BCP.pdf*) y se debatió el documento "Cualificación de incidentes graves para actuaciones globales" (*www.rediris.es/abuses/docus/LT6-CMP.pdf*)

Jesús Sanz de las Heras
(jesus.heras@rediris.es)
Servicio de Correo electrónico

Lista Blanca de servidores de correo de RedIRIS

- Lista de recopilación de servidores de correo salientes que cumplen una serie de criterios *anti-spam* para evitar los problemas ocasionados por las listas negras

El uso de Listas Negras vía DNS, al ser más económica que analizar contenidos, es uno de los mecanismos más utilizados como primer nivel de defensa frente al *spam,* permitiendo interrumpir las transacciones SMTP desde IP comprometidas. El uso de esta tecnología ha crecido exponencialmente a raíz del incremento de IP comprometidas que actúan como emisores de *spam (zombies/bot),* aunque a veces es posible que algún dominio/IP bien gestionado sea incluido automáticamente en alguna de estas Listas Negras provocando que correos buenos no lleguen a sus destinatarios. Las políticas de alta y baja en las Listas Negras dependen mucho de sus gestores y salir de algunas de ellas puede ser un proceso complejo por lo que es necesario que antes de hacer uso de una Lista Negra se lea y entienda su política de gestión.

Para evitar estos trastornos, RedIRIS junto con otros operadores españoles mediante el Foro Abuses (*www.rediris.es/abuses/*) ha puesto en marcha una Lista Blanca española cuyos objetivos son: evitar el impacto negativo de las medidas *anti-spam,* especialmente los bloqueos por el uso de Listas Negras e intentar garantizar la entrega de correo a nivel nacional.

La Lista Blanca de RedIRIS (*www.rediris.es/abuses/eswl/*) es una base de datos de IP de servidores de correo legítimos con el objeto de reducir los falsos en los filtros *anti-spam*. Ofrece dos zonas:

- **ESwl** es la zona oro. Formada por operadores españoles Foros e instituciones de RedIRIS. Todas las IP de esta zona disponen de puntos de contactos contrastados para resolver cualquier problema. Están incluidos los *relays* de correo: Telefónica, Telecable, Terra, Euskaltel, Hostalia, Sarenet, Interhost, Orange, Arrakis, ONO, YA.COM y unas 200 instituciones de RedIRIS

- **MTAwl** es la zona plata y está formada por empresas, proveedores internacionales, ministerios, etc. No se dispone de contactos contrastados y sus posibles niveles de spam son muy aceptables.

Se puede utilizar en varios formatos

- Consultas al DNS. Mecanismos similares a las habituales de consultas en listas negras. Se ofrecen dos zonas: *eswl.dnsbl.rediris.es* y *mtawl.dnsbl.rediris.es*

- Consultas http. Posibilidad de descargarse periódicamente las zonas vía http para uso local. Se ofrecen formatos para Postfix, Sendmail y Greylist.

La Lista Blanca de RedIRIS intercambia información con otras iniciativas europeas similares como *dnswl.org* (*www.dnswl.org*) y actualmente la chequean los más importantes ISP españoles y unas 40 instituciones de la Comunidad de RedIRIS.

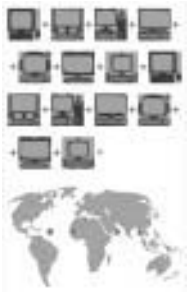
Utilizar y darse de alta en la Lista Blanca es gratuito y sencillo, por lo que recomendamos que se den de alta las IP de los servidores de correo de vuestras instituciones.

Jesús Sanz de las Heras
(jesus.heras@rediris.es)
Servicio de Correo electrónico
Francisco Monserrat
(francisco.monserrat@rediris.es)
Equipo de Seguridad IRIS-CERT

Proyecto para la creación de una red de *spamtraps*

- Red para la captura de correo basura

Desde RedIRIS, hace aproximadamente un año, se empezó a trabajar en un proyecto para desplegar una red de *spamtraps*. Este es un término utilizado para designar las trampas de captura de *spam;* estas trampas son direcciones de correo electrónico reales, asociadas a uno o



La lista blanca española pretente evitar el impacto negativo de las medidas *antispam*

Spamtraps es un término utilizado para designar las trampas de captura de *spam*

El objetivo final del proyecto es procesar y analizar la información recibida en las trampas de *spam*

Aprobación de una norma para incorporar el Lenguaje de Signos Español en redes informáticas

varios buzones, pero que no son utilizadas por personas o procesos, por lo que nunca podrán enviar correo, simplemente recibirlo. Esto nos permite garantizar que todo el correo que reciban los buzones de *spamtraps* será 100 por cien *spam*. No obstante para recibirlo estas direcciones deben ser conocidas, por eso el segundo objetivo de una red de spamtraps es definir mecanismos para que estas direcciones sean capturadas por los sistemas automáticos de recolección de direcciones y empiecen a recibir *spam, phishing, malware*, etc. Para facilitar la recogida de direcciones de *spamtraps* generamos paginas html que se reparten entre diferentes servidores web de instituciones colaboradoras; todas las direcciones trampa son almacenadas en un único servidor y en un único buzón que evidentemente no dispone de ningún tipo de filtro *antispam*.

El objetivo final del proyecto es procesar y analizar la información recibida en las trampas de *spam*. Actualmente la red de *spamtraps* dispone de unas 5.000 direcciones y recibe una media de 6.000 mensajes diarios. De esta información recibida extraemos:

- Direcciones IP enviando spam para:
  - Crear una Lista Negra.
  - Comprobar qué IP de la Lista Blanca (*www.rediris.es/abuses/eswl*) envía *spam*.
  - Analizar la efectividad de las Listas Negras.
  - Mapa *on line* de orígenes de emisores de *spam* y recolectores de direcciones.
- Patrones de comportamiento del *spam*
  - Ataques de *malware* y *phishing*.
  - Contrastar y clasificarlo según *Spamassassin*.
  - Extraer posibles nuevos virus.
  - Analizar los url y clasificarlos.

Otro tipo de información es conocer el tiempo que se tarda en recibir *spam* desde que se coloca el *spamtraps*. La idea es que estos resultados beneficien principalmente a las instituciones que colaboran en el proyecto.

Actualmente el proyecto ha generado unas 20 páginas html con unas 3.000 direcciones repartidas en diferentes instituciones (*www.rediris.es/mail/spamtoso/*), aunque se trata de un número muy bajo, dado los pocos recursos necesarios para participar en este proyecto.

La forma más sencilla de participar es ofreciendo al Proyecto un subdominio de la institución, escogiendo un nombre que no exista y que no se vaya a utilizar nunca, por ejemplo *xyz* del dominio *rediris.net*. Una vez seleccionado el nombre basta con crear en el servidor de vuestra zona DNS una entrada como esta: xyz.rediris.net MX 10 aaa.rediris.es; es decir, que todo el correo *@xyz.rediris.net* sea recogido por el servidor *aaa.rediris.es*. En caso de estar interesados en participar en este proyecto contactar con: *eswl@rediris.es* para recibir más detalles.

Jesús Sanz de las Heras
(jesus.heras@rediris.es)
Servicio de Correo electrónico

Francisco Monserrat
(francisco.monserrat@rediris.es)
Equipo de seguridad IRIS-CERT

Aprobación de la norma AENOR 139804

- Esta norma proporciona los requisitos básicos para incorporar el Lenguaje de Signos Español (LSE) en redes informáticas

El pasado 9 de febrero fue publicada en el BOE la Resolución de 16 de enero de 2007, de la Dirección General de Desarrollo Industrial, por la que se someten a información pública los proyectos de normas UNE que AENOR tiene en tramitación y entre los que consta el proyecto de norma PNE 139804. Al escribir esta nota la fase de información pública ya ha finalizado y en un periodo breve de tiempo, una vez han sido considerados los comentarios aportados a la norma, ésta se hará oficial después de su publicación en el BOE.

Desde RedIRIS hemos participado en el proceso de redacción de dicha norma como miembros del Subcomité 8 del Comité Técnico AEN/CTN 139 de AENOR.

Entre el más de millón de personas con algún grado de discapacidad auditiva que existe en nuestro país, un amplio grupo de ellos se comunica mediante el lenguaje de signos (LS).

El LS es considerado por muchas de estas personas como la forma más natural de comunicación, por encima de la información transmitida de forma escrita. En contra de lo que pudiera pensarse, no existe un LS universal, al igual que sucede con el lenguaje escrito y hablado que en cada región existe una modalidad con algunas variantes. De esta forma, dentro de España tenemos el LSE (Lenguaje de

Signos Español) y el LSC (Lenguaje de Signos Catalán) y esta norma puede aplicarse a ambos.

La norma PNE 139804 proporciona los requisitos básicos para incorporar el Lenguaje de Signos Español (LSE) en redes informáticas, con el objetivo de que los contenidos lleguen al usuario en buenas condiciones de comprensión.

Entre los campos cubiertos por la norma PNE 139804 están las características de la puesta en escena (encuadre, colores, iluminación, etc.), las características técnicas de la reproducción de LSE (como por ejemplo, las imágenes por segundo y el tamaño de imagen), la forma de indicar a los usuarios la presencia de este tipo de contenidos en sitios web, etc..

Esta norma no se aplica a la videoconferencia, aunque sí existen requisitos y recomendaciones recogidas en ella que podrían ser aplicables a este campo. Está destinada a los siguientes grupos de personas:

- Creadores de contenidos para redes informáticas.
- Diseñadores de web.
- Desarrolladores de aplicaciones basadas en redes informáticas.
- Responsables de los servidores informáticos de contenidos.
- Evaluadores de la accesibilidad de productos y servicios basados en redes informáticas.
- Responsables de la adquisición y compra de bienes y servicios accesibles por parte de la Administración Pública.

Esta Norma complementa la UNE 139803:2004 sobre accesibilidad a los contenidos web, definiendo requisitos adicionales para el caso de que esos contenidos incorporen LSE. También complementa la Norma UNE 139802:2003 sobre accesibilidad al *software*, cuando las aplicaciones hagan uso de LSE.

José Mª Fontanillo
(jmaria.fontanillo@rediris.es)
Servicios multimedia

Proyecto ARCA

- Sindicación de los contenidos multimedia

La producción y transmisión de contenidos multimedia por parte de las universidades a través de las redes informáticas es habitual desde hace años. En muchos casos es notable la profesionalización que se está produciendo en la elaboración de dichos contenidos que abarcan cursos, charlas, conferencias, etc. Estos contenidos son emitidos en directo y/o grabados para su posterior visionado como vídeo bajo demanda (VoD) (*www.rediris.es/pruebas/arca/*).

En muchos casos se han detectado dificultades para que los usuarios encuentren los contenidos, debido en parte a que los buscadores sólo indexan la información de las páginas web que contienen los elementos multimedia. Por otro lado, esta dificultad se acrecienta ya que estas páginas se generan de forma dinámica.

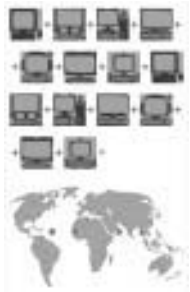
La utilización de motores específicos en cada portal que tengan en cuenta la metainformación del contenido no es una solución adecuada ya que el usuario tiene que conocer y buscar el contenido por distintos portales y algunos portales como *youtube* sólo indexan los contenidos albergados en ellos mismos.

Estos problemas se agravan cuando se trata de contenidos en directo, puesto que es muy difícil saber qué emisiones hay en directo en un momento dado en la red y cuáles va a haber en un futuro que nos puedan interesar.

ARCA viene a mejorar la situación mediante la sindicación de contenidos multimedia. El principal objetivo es mejorar la visibilidad de estos contenidos facilitando el acceso a los usuarios y partiendo de las siguientes premisas:

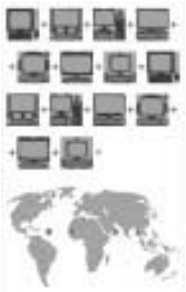
- Federación de la publicación de contenidos.
- Facilidad de uso.
- Mínimo esfuerzo de administración y mantenimiento.

El proyecto ARCA se inicia como parte de un desarrollo interno de gestión integral de servicios y contenidos multimedia en la Universidad Carlos III de Madrid (*http://arca.uc3m.es/arca/*), aunque en la actualidad está



Es notable la profesionalización que se está produciendo en la elaboración de contenidos

ARCA viene a mejorar la situación actual mediante la sindicación de contenidos multimedia



Creación de un nuevo grupo de trabajo de voz sobre IP

Nuevo grupo de trabajo sobre herramientas de colaboración multimedia avanzadas

abierto a la comunidad y en otras universidades se están desarrollando módulos para ARCA, como por ejemplo el de estadísticas en la Universidad Rey Juan Carlos.

La interfaz de los usuarios es un portal web donde se pueden efectuar búsquedas o ver la información organizada según diversos criterios: eventos en directo organizados en un calendario con distintas vistas, búsqueda por filtros, categorización según códigos UNESCO para ciencia y tecnología, etc.

Se utiliza el formato RSS como protocolo de intercambio de información. Los *feeds* de ARCA emplean espacios de nombres de RSS 2.0: *itunes rss, yahoo media rss* y *google media base.* El motivo para añadir espacios de nombres es que las etiquetas de RSS 2.0 se quedan cortas a la hora de sindicar contenidos multimedia. Sin estos sería imposible ubicar un ítem de rss en el tiempo (anunciar un evento) o indicar información multimedia del ítem (bitrate, duración, codec...).

El funcionamiento de ARCA se basa en la generación por parte de cada institución de un archivo RSS con información de los contenidos en directo, como VoD y *podcast/videocast* que desea publicar. Desde el portal web se actualiza cada cierto tiempo la información y se almacena en una BBDD para su posterior procesamiento.

ARCA pretende ser ser el embrión para la creación de un portal del tipo "research channel" en la comunidad académica.

José Mª Fontanillo
(jmaria.fontanillo@rediris.es)
Servicios multimedia

Grupo de Trabajo de VoIP

- Creación de un nuevo grupo de trabajo en la comunidad académica sobre servicios avanzados de voz sobre IP

A finales de 2006, y motivado por el interés mostrado por diversas instituciones en servicios avanzados de voz sobre IP, creamos un nuevo grupo de trabajo cuya coordinación se lleva a cabo mediante la lista *gt-voip@listserv.rediris.es.*

Los objetivos de dicho grupo son los siguientes:

- Intercambio de experiencias y conocimiento en esta área.
- Fomentar los beneficios que se obtienen por el uso de la tecnología VoIP y ayudar a desarrollar servicios de comunicación avanzados.
- Coordinar las distintas actividades que se están desarrollando en las instituciones en VoIP (conectar islas SIP).
- Generar documentación para el despliegue de VoIP dentro de la red académica.
- La presentación de un proyecto para el despliegue de VoIP.

Hasta la fecha han tenido lugar dos reuniones no presenciales, en las que se ha fijado una serie de actividades que se encuentran en fase de desarrollo.

José Mª Fontanillo
(jmaria.fontanillo@rediris.es)
Servicios multimedia

TF- ECS

- Grupo de trabajo sobre herramientas de colaboración multimedia avanzadas

El pasado día 21 de febrero se realizó una reunión del grupo de trabajo TF-ECS (Task Force Enhanced Communication Services). Este grupo de trabajo está explorando herramientas de colaboración que van más allá de la conferencia simple con voz y vídeo. Se trata de coordinar las iniciativas en este terreno que se realizan a nivel nacional y asistir en el despliegue de servicios de colaboración de próxima generación. El grupo investiga cuál es el impacto de los desarrollos futuros en las comunicaciones en tiempo real y se define la arquitectura y el modelo de confianza que permitirá la interoperabilidad con los desarrollos nacionales.

Dentro de este grupo se está llevando a cabo una experiencia piloto de ENUM *(www.nrenum.net)* bajo una raíz no oficial, con el objetivo de permitir que los países que no tengan acceso al árbol oficial puedan realizar sus *testbed* bajo esta raíz que es temporal y está albergada en la red suiza SWITH.

Además se está elaborando una actualización del *cookbook* que TERENA editó en marzo de 2004 *(www.terena.org/activities/iptel/chapters/IPTELEPHONYCOOKBOOK.pdf)* abordando temas que no se trataban en éste.

Por otra parte, en la próxima conferencia de TERENA *(http://tnc2007.terena.org/)* miembros

de este grupo realizarán un workshop práctico sobre la arquitectura del servicio e implementación práctica.

José Mª Fontanillo
(jmaria.fontanillo@rediris.es)
Servicios multimedia

PAPI y Shibboleth

- Infraestructuras de autenticación y autorización

RedIRIS ha completado la fase final de pruebas de la interconexión entre PAPI y Shibboleth. Éste es un *software* desarrollado por Internet2 para crear infraestructuras de autenticación y autorización (IAA) y que cumple el estándar SAML, lenguaje para el intercambio de mensajes entre los diferentes componentes de IAA, que ha sido publicado por OASIS y que la industria y los proveedores de servicio están comenzando a aceptar.

Cabe destacar que, para la comprobación de esta integración, se ha añadido un servidor de autenticación (AS) de PAPI en las federaciones TestShib y Switch AAItest, basadas ambas en Shibboleth. TestShib es una federación creada por Internet2 para que proveedores de identidad y de servicio puedan realizar las comprobaciones necesarias de que sus componentes son compatibles con los perfiles Shibboleth. Por otro lado, Switch ha implantado en Suiza una federación para las organizaciones académicas y científicas de dicho país, proveyendo además de otra federación de prueba, llamada AAItest, para que sus organizaciones preparen su *software* compatible con los perfiles Shibboleth.

De esta forma, si una organización tiene un servidor de autenticación de PAPI podrá añadir a aquellos proveedores de servicio, como Elsevier o JSTOR, que hayan elegido un *software* compatible con los perfiles Shibboleth para proteger sus recursos. Además, en el caso contrario de que una organización disponga de Shibboleth, podrá comunicarse correctamente con cualquier recurso protegido por PAPI, aprovechando así las características avanzadas que ofrece este último como el proxy con reescritura.

Cándido Rodríguez
(candido.rodriguez@rediris.es)
Área de Middleware

TF-MOBILITY

- Grupo de trabajo sobre movilidad de Terena

El pasado enero se celebró en Cambridge la 14ª reunión del grupo de trabajo de Terena sobre movilidad (*www.terena.org/activities/tf-mobility*). El principal punto de la agenda fue la discusión sobre la constitución dentro del ámbito de GÉANT2 de una actividad de servicio específica para eduroam (*www.eduroam.org*), con todo lo que ello conlleva (acuerdos de servicio, monitorización y soporte a usuarios). Este es sólo el primer paso, iremos dando más detalles de lo que se vaya acordando.

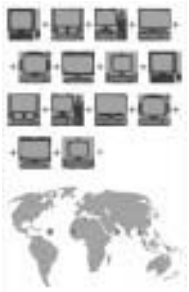
Se informó en la reunión sobre el estado actual de la aplicación Secure W2. La compañía holandesa que lo desarrollaba, Alfa&Aris, se ha dividido y ha surgido la empresa Secure W2 (*www.securew2.org*), que continuará con el desarrollo; realizando mejoras y terminando la versión de la aplicación para Vista, actualmente en desarrollo y seguirá siendo de código abierto. Se solicitó la colaboración de características deseables para discutirlas con los desarrolladores.

También se repasó el estado del internet *draft* sobre RadSec, además de informarse sobre el inicio de pruebas con *radsec* en breve. Otra noticia respecto a *radsec* es la creación de un proxy que está actualmente siendo desarrollado. Este proxy convierte peticiones RADIUS (UDP) en protocolo RadSec (TLS/IPv6).

Se trataron tanto los distintos problemas que tiene ahora eduroam (derivados en gran parte de la utilización de RADIUS), como sus posibles soluciones de cara al futuro (construcción de un modelo de confianza más sólido, una estructura de enrutamiento basada en DNS en lugar de la jerarquía actual, cambiar el protocolo de transporte de las credenciales). El escenario propuesto hacía uso extensivo de PKI o del modelo de confianza propuesto para eduGAIN.

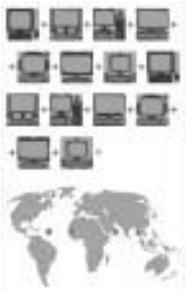
Otros temas tratados fueron la monitorización y estadísticas, sobre las que se está trabajando, recopilando las herramientas utilizadas por las distintas NREN, el estudio de nuevas tecnologías (mobileIP, IPv6), la inclusión de nuevos países en eduroam, y la revisión del sitio web que se está llevando a cabo.

José Manuel Macías
(jmanuel.macias@rediris.es)
Área de Middleware



Se ha completado la fase final de pruebas de la interconexión entre PAPI y Shibboleth

Siguen sumándose países en la iniciativa eduroam



Se continúa con la consolidación de servicios y propuestas tales como TACAR, SCHAC o SCS

Las instituciones que tengan ya instalado Sun Access Manager podrán usar PAPI

TF-EMC2

- Grupo de trabajo sobre infraestructuras *middleware*

El grupo TF-EMC2 (*www.terena.org/activities/tf-emc2/meetings/7/*), que se reunió en Málaga los pasados 16 y 17 de octubre, continúa con la consolidación de los servicios y propuestas que han nacido en su seno (como TACAR, SCHAC o SCS, de los que se habla en otras reseñas) y explorando nuevas líneas de actividad para asentar el desarrollo de infraestructuras middleware interoperables en las redes académicas europeas.

Dentro de estas nuevas actividades, resulta obligado señalar la constitución de ECAM (European Council for Academic Middleware-*www.terena.org/activities/tf-emc2/ecam/*), con participación de expertos de las redes académicas europeas, norteamericana y australiana. Presidido por RedIRIS, el objetivo del ECAM es definir las líneas estratégicas de las actividades en middleware de TERENA, dar soporte a estas actividades y asesorar a las organizaciones miembros de la asociación en sus iniciativas nacionales.

El grupo ha puesto en marcha también un estudio de las condiciones en las que se prestan servicios de identidad digital en las diferentes redes académicas (REFEDS), así como los esfuerzos de coordinación con las actividades relacionadas con sus áreas de interés en el IETF (*www.rediris.es/wiki/tf-emc2/index.php/Federations*).

Mención especial merece la atención que el grupo TF-EMC2 viene prestando a los llamados sistemas de identidad "centrados en el usuario", de los que el nuevo sistema CardSpace incorporado en el Windows Vista es el ejemplo paradigmático (*http://cardspace.netfx3.com/*).

Se pretende con ello aprovechar las nuevas oportunidades ofrecidas por estos sistemas (en especial en cuanto a su difusión entre los usuarios), así como hacer converger propuestas comerciales, como las de OpenID *(www.openid.net/),* difundidas en ciertos entornos (*blogs,* sitios de publicación de contenidos como Flickr), con las infraestructuras de gestión de identidad operadas por las redes académicas.

Diego López
(diego.lopez@rediris.es)
Coordinador del Área de Middleware

Conexión PAPI-Sun Access Manager

- Intercambio de información sobre identidades de usuarios entre ambos sistemas

Fruto de las conversaciones que se iniciaron durante las pasadas Jornadas, el proyecto de interconexión entre PAPI (*http://papi.rediris.es/*) y Sun Access Manager (*www.sun.com/software/products/access_mgr/*) ha comenzado. En el grupo de trabajo participa el equipo de desarrollo de PAPI en RedIRIS, expertos en identidad digital de Sun y desarrolladores del JavaCenter ubicado en el CICA.

El objetivo es que ambos sistemas puedan intercambiar información sobre las identidades de los usuarios, de manera que pueda combinarse su uso dentro de cualquier entorno. De esta manera, las instituciones que tengan ya instalado Sun Access Manager podrán usar PAPI para realizar conexiones en modo proxy a recursos remotos con control de acceso por IP o aprovechar las facilidades de integración de PAPI con lenguajes como Perl o PHP. Por su parte, las organizaciones que tengan desplegados servicios de identidad basados en PAPI podrán aprovechar las facilidades de gestión y provisión que ofrece la suite de identidad de Sun, así como su integración directa con otros productos del mismo fabricante.

Diego López
(diego.lopez@rediris.es)
Coordinador del Área de Middleware

SCHAC y esquemas IRIS

- Esquema orientado a facilitar el intercambio de datos entre instituciones académicas.

En la reunión del TF-EMC2 de Málaga se realizó una revisión del esquema SCHAC (*www.terena.nl/activities/tf-emc2/schac.html*) y algunos de los puntos tratados fueron:

- Evolución de SCHAC desde sus primeras versiones: el uso de la rama de OID: 1.3.6.1.4.1.25178.1 y el del espacio de nombres: *urn:mace:terena.org:schac*
- Cambios de nombre y sintaxis de varios atributos.
- Uso de URN en los atributos: schacHome Organization Type, schacPersonal Position, schacPersonalUniqueCode,schac Personal UniqueID y schacUserStatus.

- Creación de un registro de URN para describir los atributos anteriores. Será gestionado por TERENA y delegará subespacios de nombre a las NREN *(www.terena.nl/registry/terena.org/schac/).*
- Aceptación de la propuesta de uso de los identificadores homeOrganizationType, personalPosition,personalUniqueCode, personalUniqueID y userStatus como componentes de los espacios de nombre de los URN.
- Vocabulario común para los atributos de tipo URN donde se definen identificadores comunes y extensiones nacionales.

  - Para el espacio común se usan los identificadores :eu: e :int:, por ejemplo: *urn:mace:terena.org:schac:homeOrganizationType:eu:NRENAffiliate*
  - Para el espacio de extensiones nacionales se usa el TLD, por ejemplo: *urn:mace:terena.org:schac:homeOrganizationType:es:universidad*

- Eliminación del atributo schacUUID.

Desde aquella reunión hemos seguido trabajando para obtener la versión 1.3.0 del esquema SCHAC que fue liberada el 12 de diciembre de 2006.

Varias organizaciones en el ámbito internacional han adoptado este esquema y han añadido sus atributos a sus esquemas locales. RedIRIS también está incorporando algunos de los atributos de SCHAC a sus esquemas y recomienda su uso a todas las instituciones afiliadas.

Javier Masa
(Javier.masa@rediris.es)
Área de Middleware

IRIS-CERT miembro del AntiPhising Working Group

- La red académica miembro del grupo internacional contra el fraude a través de Internet

Tras la firma de un acuerdo con el AntiPhising Working Group *(www.antiphising.org),* el grupo de seguridad de RedIRIS, IRIS-CERT se ha convertido en miembro investigador de este grupo internacional centrado en la prevención del fraude por Internet, famoso en los últimos tiempos por la recepción de correos que simulan la identidad de una institución financiera e inducen a los usuarios a proporcionar sus datos personales *(phising).*

El Antiphising Working group (APWG) es un foro que agrupa tanto a fabricantes de productos de seguridad, como a agencias de gobierno y grupos de seguridad con el objetivo común de mitigar el fraude en Internet, cuenta con más de de 2.500 miembros y sus principales áreas de trabajo son la elaboración de códigos de buenas prácticas, educación de los usuarios, evaluación de soluciones y la recogida de información sobre la incidencia del *phising* y la coordinación con los cuerpos policiales .

Francisco Monserrat
(francisco.monserrat@rediris.es)
Equipo de seguridad IRIS-CERT

Próxima reunión del FIRST

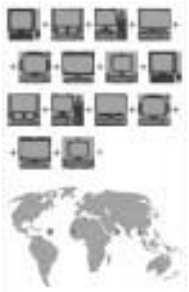
- La conferencia anual de seguridad internacional se celebrará este año en Sevilla

La conferencia anual de Seguridad FIRST que se va a a celebrar el próximo mes de junio en Sevilla *(www.first.org/conference/2007/),* es una ocasión única para asistir a un gran foro en la materia donde van a participar ponentes de reconocido prestigio mundial.

La conferencia de este año está centrada en la identidad digital y cuenta con la participación de ponentes de la talla de Francisco García Morán (Dirección General de Informática de la Comisión Europea), Mary Ann Davidson, (Jefa de Seguridad de Oracle) o George Stathakopoulos (Director General de Seguridad de productos de Microsoft).

A nivel técnico la conferencia también contará con la asistencia de personas de reconocido prestigio, como Wietse Venema, autor entre otros de los conocidos programas *TCPWrappers, Satan, postfix y TCT*; Joanna Rutkowska, autora de los programas *red pill* y *blue pill*, de detección de entornos virtuales, Peter G. Allot de ISS y otros muchos expertos de seguridad.

Paralelamente a la conferencia se celebrará una serie de actividades tales como la segunda reunión conjunta de equipos de seguridad y



A nivel internacional también se está implantando el esquema SCHAC

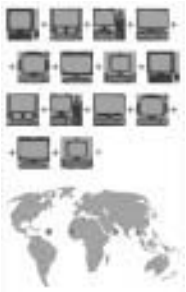
La próxima reunión del First tendrá lugar en Sevilla

cuerpos de seguridad del estado, (2nd Joint CSIRT and Law Enforcement Half Workshop), demostraciones de productos de seguridad y otras actividades.

Francisco Monserrat
(francisco.monserrat@rediris.es)
Equipo de seguridad IRIS-CERT

pkIRISGrid CA y EUGridPMA

- Autoridades de certificación en entornos Grid



PkIRISGrid CA es la infraestructura de clave pública IRISGrid

PkIRISGrid CA, es la infraestructura de clave pública IRISGrid. Desde su acreditación por la EUGridPMA (www.eugridpma.org/), el 25 de enero de 2006, se han creado 20 autoridades de registro que han recibido más de 550 solicitudes de certificados. La CA ha emitido más de 300 certificados de servidor y 200 de usuario.

A mediados del pasado mes de enero se celebró la novena reunión de la EUGridPMA en Abingdon (Reino Unido) y entre los temas tratados destacan:

- El último informe de la Russian DataGrid CA (RDID) antes de su finalización. La CA dejó de emitir nuevos certificados a finales de 2005 y el último válido expiró a finales de septiembre de 2006. Sigue emitiendo CRL pero se cuestiona la necesidad de seguir haciéndolo puesto que ya no existen certificados válidos.

  Esta CA ha sido reemplazada por la Russian Data-Intensive Grid CA (RDIG CA) y se han eliminado las referencias a la antigua CA en las distribuciones que emite la EUGridPMA.

- Reunión del grupo OGF-CAOPS. Revisión del documento Grid Certificate Profile con objeto de poder llevar una versión casi definitiva a la reunión de febrero del OGF en Chapel Hill

- Actualidad sobre TACAR. En la nueva versión 1.4.3 de su política aparece la figura del *trusted introducer*, que realiza la labor de intermediario entre TERENA y los responsables de las CA que forman el repositorio, así como aquellas que desean formar parte del mismo

- Presentación de la nueva CA SWITCHslcs basada en un servicio de credenciales de validez muy corta, lo que permite que casi no sean necesarias las revocaciones. Los certificados son generados usando un sistema de gestión de identidad en lugar de la tradicional autoridad de registro.

- PGP party entre todos los asistentes y sesión de firmas con notarios de Thawte, cuya finalidad es ampliar las relaciones de confianza entre los miembros de la EUGridPMA.

- Revisión de los requisitos mínimos para los perfiles SLCS y MICS incidiendo en los problemas de la identificación de los ususarios.

- Visita a las instalaciones del Rutherford Appleton Laboratory donde está situada la autoridad de certificación de la UK e-Science CA.

- Presentación de las últimas novedades en el servicio de certificados de servidor SCS, donde se planteó la posibilidad de que la Educational CA de GlobalSign sea acreditada por la EUGridPMA.

- Revisión en profundidad de varias CA acreditadas entre las que se encuentran la SlovakGrid Certification Authority (Eslovaquia) y la LIP-CA (Portugal).

- Presentación de nuevas CA para su acreditación: BG-ACAD (Bulgarian Grid CA), MaGrid (Moroccan Grid CA), Romanian GRID CA y AEGIS (Serbia).

Javier Masa
(Javier.masa@rediris.es)
Área de Middleware

El *software* pkIRIS gestiona la PKI de eduGAIN

- El *software* de certificación de RedIRIS elegido para gestionar la arquitectura de autenticación y autorización de GÉANT2.

El *software* de RedIRIS ha sido elegido para gestionar la PKI de eduGAIN

El *software* ha sido elegido para gestionar la PKI de eduGAIN. Esta PKI tiene como objetivo generar certificados que permitan comprobar la identidad de los componentes eduGAIN entre sí.

La arquitectura de la PKI de eduGAIN es jerárquica y con profundidad 2 en la cadena de certificación. La CA raíz (eduGAINCA) sólo emite certificados para otras CA hijas (sólo una de momento, eduGAINSCA); siendo éstas la que emiten los certificados para los componentes eduGAIN.

El *software* pkIRIS da soporte a ésta arquitectura mediante la gestión de la eduGAINSCA quedando oculta la CA raíz a los solicitantes de certificados. pkIRIS ofrece a los usuarios una interfaz web de solicitud de certificados ágil que evita al usuario generar la clave privada y la CSR a "mano"; siendo el navegador web quien las genera y almacena. Cuando las solicitudes han sido procesadas y emitidos los certificados, notifica a los solicitantes de este hecho vía e-mail; remitiendo a estos a la interfaz de descargas de certificados, desde la cual se puede instalar el certificado solicitado en el navegador web.

Ya se han emitido certificados para componentes eduGAIN para diversas NREN como RESTENA, PIONIER, UNINETT y RedIRIS.

Javier Masa
(Javier.masa@rediris.es)
Área de Middleware

SCS: Servicio de Certificados de Servidor

- Éxito del Servicio de Certificados de Servidor en la comunidad RedIRIS

El servicio ha tenido una gran aceptación por parte de las instituciones, lo que queda reflejado en el número de certificados solicitados, más de 450 en sólo 9 meses desde que se inició el servicio en junio del 2006.

El número de instituciones que han solicitado estos certificados ha ido creciendo hasta sobrepasar la cifra de 40. Inicialmente dichos certificados se usaban exclusivamente en los servidores institucionales de cada organización pero, poco a poco, se ha ido extendiendo el mensaje de que el servicio funciona, es gratuito y evita los *pop-ups,* por lo que estamos recibiendo una avalancha de solicitudes por parte de departamentos y otros pequeños centros.

Originalmente creímos que los certificados serían utilizados para asegurar conexiones http pero, con el tiempo se ha puesto de manifiesto que éstos se usan para asegurar muchos otros servicios como radius, smtp, pop, imap, ldap, etc.

Javier Masa
(Javier.masa@rediris.es)
Área de Middleware

Inauguración de la Red Española de Supercomputación

- Red que conectará varios supercomputadores a lo largo de la geografía española

El pasado 13 de marzo se inauguró la Red Española de Supercomputación (RES), en un acto presidido por la ministra de Educación y Ciencia, Mercedes Cabrera. RES se crea para conectar varios supercomputadores de toda España (Andalucía, Aragón, Canarias, Cantabria, Madrid y Valencia) con el Barcelona Supercomputing Center-Centro Nacional de Supercomputación (BSC-CNS) a través de RedIRIS, con el fin de dar respuesta a la creciente demanda de capacidad de cálculo de la comunidad científica española. Con la nueva red se espera multiplicar por tres la potencia de MareNortrum, que ahora es el quinto ordenador en potencia del mundo y el primero de Europa con sus 94,21 Teraflops.

RES se ha diseñado como una red virtual, conectando los centros participantes entre sí, a través de RedIRIS y de las respectivas redes autonómicas. En su primera fase, los centros que forman la red se conectarán a través de circuitos de hasta 1Gigabit por segundo. En la segunda fase está previsto aumentar la capacidad de los circuitos hasta los 10 Gigabits. La principal limitación en este momento es el supercomputador del Instituto Astrofísico de Canarias, para el que la conexión estará más limitada, ya que el enlace de RedIRIS con Canarias tiene una capacidad total de 622 Megabits.

Tomás de Miguel
(Tomas.demiguel@rediris.es)
Director

Ya se han emitido certificados para componentes eduGAIN para diversas NREN

Ya hay más de 40 instituciones con certificados SCS