• RedIRIS2, migración

Como ya hemos venido anunciado, el pasado mes de junio hemos llevado a cabo la migración de los equipos que forman el nodo central de la red.

Las instalaciones de la empresa Carrier House 2, en Alcobendas, han sido seleccionadas para albergar el equipamiento del nodo central, formado por dos GigaRoutes que soportan los enlaces troncales y externos y un conjunto de servidores. Anteriormente este equipamiento estaba ubicado en las instalaciones del CSIC situadas en Madrid en la Calle Serrano, 142 y la topología era tal y como aparece reflejada en la figura 1.

FIGURA 1: TOPOLOGÍA INICIAL

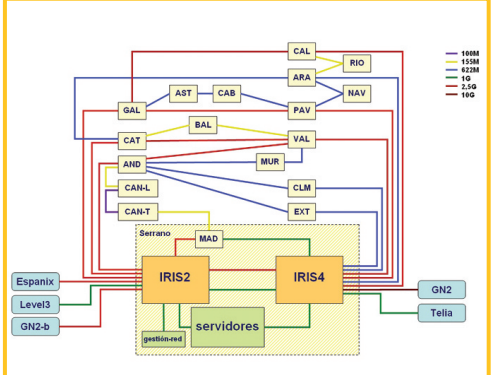
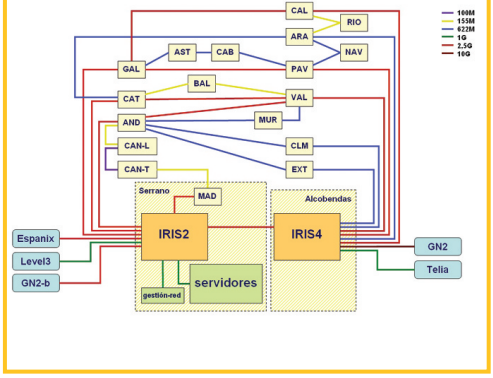


FIGURA 2: MIGRACIÓN DEL ROUTER IRIS4



La migración de los equipos de comunicaciones implica realizar también la de los enlaces que se conectan a ellos, por lo que la colaboración de los operadores que suministran dichos enlaces ha sido fundamental para el éxito de la migración. De entre todos ellos, Albura operador de la red nacional, por la cantidad de enlaces implicados, es el que más trabajo y recursos ha tenido que dedicar.

Gracias al mallado de la red nacional, el doble chasis en el nodo nacional y la diversificación de salidas externas, se pudo realizar una migración sin que se realizaran cortes en el servicio de comunicaciones. La migración se planificó en cuatro fases que se muestran a continuación.

- FASE I - 14 de junio
  Migración del router IRIS4 (figura 2)

- FASE II - 17 y 18 junio
  Migración de los servidores (figura 3)

  El cambio de ubicación de los servidores, dada la cantidad de máquinas implicadas se

FIGURA 3: MIGRACIÓN DE LOS SERVIDORES

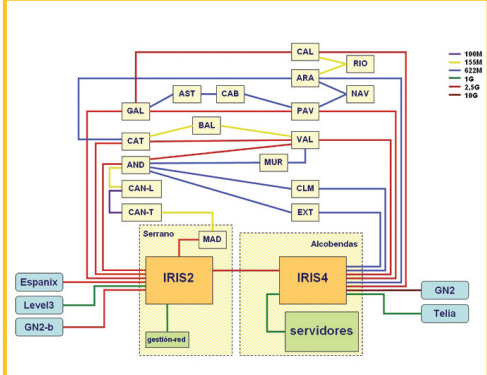
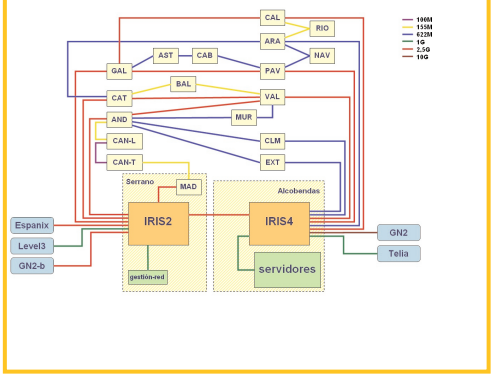


FIGURA 4: MIGRACIÓN DEL ROUTER IRIS2



realizó durante un fin de semana. Para minimizar el impacto en los servicios, se configuró una red de servicios mínimos en Serrano (DNS, web, correo, ...) que estuvo operativa durante este proceso de

Migración exitosa del nodo central de RedIRIS del CSIC a Carrier House 2

La migración de los equipos implica también la de los enlaces a los que se conectan

migración, eliminándose una vez finalizado con éxito este traslado.

- FASE III - 20 de junio
  Migración del router IRIS2 (figura 4)

RedIRIS EN CARRIER HOUSE 2

- FASE IV - En las instalaciones de RedIRIS de la calle Serrano aún quedan los equipos pertenecientes al nodo de Madrid. La cuarta y última fase finalizará una vez se realice la migración de este equipamiento y sus enlaces asociados. Sin embargo, dada la cantidad de enlaces que llegan a este nodo de todas las instituciones que en Madrid se conectan, esta fase tendrá una duración mayor.

Aún queda por completar la migración del nodo de Madrid

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

Herramienta de gestión de incidencias para el NOC

- **Mayor accesibilidad para los usuarios a la información de las incidencias que se reportan al área de red**

Utilizando el *software RT* de Best Practical, el área de red está poniendo en marcha una herramienta con objeto de llevar una gestión adecuada de los problemas o consultas que las instituciones reportan. De esta forma, tanto el personal de las instituciones como los técnicos del NOC tendrán fácilmente accesible toda la información relativa a una incidencia. Existirá un interfaz web, además de poderse utilizar mediante correo electrónico.

La herramienta estará en prueba durante los meses de verano y está previsto que para septiembre el *software* entre en producción a pleno rendimiento.

Se ha propuesto un marco común para la creación de una plataforma de monitorización multi-dominio

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

GÉANT2

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

Durante la pasada Reunión Técnica de GÉANT2 celebrada en Cambridge a primeros de junio *(www.geant2.net/)*, se llevó a cabo un seminario sobre la tecnología eduGAIN y sobre su aplicación dentro del proyecto tanto para la interconexión de infraestructuras de gestión de identidad como para su uso por otros servicios de GÉANT2, tales como el servicio de monitorización (JRA1) o el de Ancho de Banda Bajo Demanda (JRA3). EduGAIN, cuyo desarrollo está liderado por RedIRIS tiene previsto ofrecer un primer piloto a lo largo de este otoño.

Hay que destacar también la contribución de RedIRIS en otras actividades tal y como se describe a continuación:

• Actividad JRA1

- Actividad para el desarrollo de una plataforma de monitorización multi dominio

Se ha propuesto la utilización de un marco común para el desarrollo de los servicios que compondrán la plataforma, este marco se denomina perfSonar y está basado en tecnología WebServices *(http://en.wikipedia.org/wiki/Web_services)*.

Los principales servicios de la plataforma son:

- Servicios de mediciones. Se encargan de medir principalmente el retraso de la red, la pérdida de paquetes y de ancho de banda. Se pueden realizar bien mediciones bajo demanda o bien de carácter periódico para almacenarlas.
- Servicios de almacenamiento de mediciones. Estos servicios sirven como repositorio de información histórica del comportamiento de la red.

- Servicios de monitorización pasiva. Actualmente comprenden la monitorización de tráfico y la recolección de información de flujos exportados con Netflow.
- Servicio de información de topología de red. Cada dominio tendrá un servidor que almacenará la información actual e histórica sobre su topología de red en el que cada NREN puede definir la información que va a hacer pública al resto.
- Servicio de búsqueda. Actúa a modo de directorio de los servicios mencionados anteriormente (medición, almacenamiento, topología de red, etc.) que se registran en este servicio de búsqueda para que otros los localicen conociendo únicamente la ubicación del buscador de servicios.
- Servicios de visualización. Son las herramientas que utilizarán habitualmente las NRENs para las tareas de monitoriación en los NOC. Se conectan al servicio de búsqueda para conocer cómo acceder a los diferentes servicios de topología, almacenamiento y mediciones y finalmente ofrecer una interfaz que facilite el acceso a la información que proveen los diferentes servicios.

RedIRIS está involucrada en esta actividad dentro del servicio de información de topología de red. En la última reunión se decidió que se va a unificar el esquema con el que se guarda la información de la topología de la red en el JRA1 y el SA3.

• Actividad JRA2

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

JRA2 (Joint Research Activity) es la segunda, de las cinco actividades de investigación definidas en GÉANT2 enfocada a dotar de un marco de seguridad a la nueva red paneuropea, tanto en protección de equipos de red como en la cooperación entre las distintas redes para proporcionar una capacidad coordinada de respuestas ante incidentes *(www. geant2.net/)*.

Vamos a tratar dos aspectos en esta noticia: los progresos realizados en las distintas actividades en los últimos meses y el trabajo planificado para el tercer año de vida del JRA2, incluyendo los cambios de orientación y enfoque consensuados en cada *Work Item* para conseguir el mayor beneficio en los resultados del proyecto.

En el WI1 (protección de elementos y servicios de red de GN2), se presentó en mayo la revisión y actualización del documento de recomendaciones y políticas de seguridad para el equipamiento y servicios de la red GÉANT2. Esta nueva versión incluye novedades interesantes como son la división del texto en un parte dedicada exclusivamente a políticas y otra, más extensa y detallada orientada a técnicos, sobre BCPs *(Best Common Practices)*. Además, el nuevo documento incluye políticas específicas para servicios de nivel 1 y 2 no incluidas en su primera versión. Para el próximo año se quieren formalizar las relaciones con los ingenieros del *backbone* (por ejemplo APMs), cuya participación puede ser muy interesante y enriquecedora para el trabajo a llevar a cabo del que no parecen estar muy al tanto en este *Work Item*.

En el WI2 (creación de servicios de seguridad), se sigue trabajando en la definición de un conjunto integrado de herramientas, que podrán ser utilizadas por las distintas NRENs, para monitorizar el tráfico de la red de cara a detectar y diagnosticar anomalías y ataques de seguridad. Durante el presente año, se ha finalizado la definición de la arquitectura de la herramienta, y se ha redactado un documento sobre los requerimientos deseados. También está en proceso de estudio la estandarización del módulo de almacenamiento, que presumiblemente estará disponible en breve para los miembros del grupo. Para el próximo año del proyecto, los esfuerzos en este *Work Item* se van a centrar en la definición y especialización del módulo de anomalías, permitiendo una detección avanzada.

Se sigue trabajando en la definición de herramientas para la monitorización del tráfico de cara a la seguridad

Respecto al WI3 (diseño y establecimiento de una infraestructura de coordinación de incidentes de seguridad), en años pasados, el trabajo realizado en este ámbito se ha basado en dos máximas: aumentar la funcionalidad y la cobertura de la infraestructura. Para aumentar la cobertura, las actividades relacionadas con la promoción en la creación de nuevos equipos de seguridad en aquellas NRENs dentro de GÉANT2 que no dispongan de dicha funcionalidad se considera como un Servicio de Seguridad de GN2, y como tal se debe trasladar a un Servicio en Operación (SA). Las pruebas necesarias para definir los procedimientos y módulos de dicho servicio se van a llevar a cabo próximamente. En cuanto al aumento de las funcionalidades de la infraestructura de coordinación, los participantes en este *Work Item* no han mostrado, durante este año, mucho interés en el lanzamiento de nuevos

El trabajo del WI3 se ha enfocado a aumentar la funcionalidad y la cobertura de la infraestructura

servicios o actividades para hacer que la infraestructura de coordinación sea más sofisticada, con lo que no se van a continuar realizando esfuerzos en este sentido durante el próximo año. Por tanto el trabajo en este Work Item durante el tercer año se va a centrar en la difusión de información sobre la operativa de la infraestructura de coordinación en todo el GN2, no sólo entre los partners del WI3, para intentar así aumentar la seguridad de la red paneuropea en su conjunto.

• Actividad JRA3

- Actividad de Monitorización de Ancho de Banda Bajo Demanda

El objetivo de la actividad es determinar, cuando aparece un problema, qué dominio lo ha generado.

Los primeros resultados de la actividad han sido la implementación de la herramienta a lo largo de dos dominios, uno de ellos con tecnología Ethernet sobre MPLS y la otra SDH.

Los siguientes pasos irán destinados a conseguir los mismos resultados implicando nuevas tecnologías, aumentando el número de parámetros a tener en cuenta y utilizando métricas más complejas entre ellas.

- **Actividad *Pathfinder***

La principal tarea del módulo del *Pathfinder* en el *Inter-Domain Manager* (IDM) es la de proporcionar una lista de posibles caminos que cumplan una serie de requisitos en las peticiones de reserva de Ancho de Banda Bajo Demanda (BoD) y los primeros resultados de la actividad deberían estar disponibles para finales de agosto.

El módulo del *Pathfinder* trata de proporcionar una lista de posibles caminos que cumplan unos requisitos en las peticiones de reserva de Ancho de Banda Bajo Demanda

Se comenzará tomando como referencia la implementación de protocolo OSPFv2 existente en el *software* de encaminamiento Quagga.

- **Actividad de pruebas del prototipo de *Inter-Domain Manager* (IDM)**

El propósito del prototipo es dar soporte a futuros diseños o desarrollos aportando datos concretos sobre la arquitectura más idónea a utilizar y los diferentes problemas o cuellos de botella que puedan aparecer. A su vez se pretende controlar si el flujo del proceso de reserva de Ancho de Banda es aceptable y si existen aspectos que no se hayan tenido en cuenta en las fases previas del diseño.

El proceso de pruebas incluye seis casos, comenzando desde algunos muy simples hasta otros más complejos, que no hacen referencia a topologías del mundo real, pero que se han tenido en cuenta como posibles conexiones para realizar pruebas muy específicas.

Los informes de las pruebas realizadas proporcionarán las respuestas necesarias para continuar con una implementación adecuada del prototipo.

- **Actividad de pruebas y validación**

Esta actividad se divide en cuatro subactividades:

- Pruebas del prototipo de IDM. Se trata de comprobar si existe la posibilidad de realizar conexiones con la implicación de varios dominios.
- Pruebas de unión de diferentes tecnologías. Se han definido 14 escenarios de pruebas y los resultados de las mismas deberán reflejarse en el documento DJ 3.5.3.
- Definición de los recursos necesarios para el grupo de trabajo JRA4.
- Pruebas de herramientas de monitorización

- **Actividad de especificación del servicio de autorización y autenticación**

En esta actividad se desarrollará la interfaz necesaria para realizar la reserva de recursos necesarios para una conexión segura. Esta reserva se realizará según un modelo encadenado entre los diferentes dominios implicados en la conexión.

Se va a desarrollar la interfaz para realizar la reserva de recursos necesarios para una conexión segura

Los resultados previstos para la primera mitad del tercer año del proyecto en el grupo JRA3 serán los siguientes:

- Inicio del despliegue de la Fase 1 del *Inter Domain Manager*.
- Inicio del despliegue y de las pruebas de los nuevos componentes desarrollados: el *Pathfinder* y el esquema de representación de una topología abstracta.
- Diseño y puesta en funcionamiento de un módulo prototipo de *Inter-Domain Manager* incorporando dos tecnologías diferentes.
- Realización de pruebas en las interfaces con los sistemas de Ancho de Banda Bajo Demanda existentes (UCLP de CANARIE).
- Realización de avances en el interfaz con el Sistema de Provisión Multidominio Avanzado del grupo de trabajo SA3.
- Continuación del trabajo de monitorización para circuitos de BoD cooperando con los grupos de trabajo JRA1 y JRA4.

La mayoría de las tareas anteriormente citadas irán acompañadas de sus correspondientes actividades de pruebas con las diferentes tecnologías empleadas. Paralelamente se generará una versión actualizada del estado del arte de la tecnología.

Se ha considerado dedicar una tarea a establecer vías de comunicación con otros proyectos que estén trabajando en la misma línea.

• Actividad SA3

• Actividad dedicada al Sistema de Calidad de Servicio Extremo a Extremo

Dentro de la subactividad PERT *(Performance Enhacement Response Team)* tuvo lugar una discusión sobre los requerimientos de tener un sistema PERT descentralizado, teniendo en cuenta las diferentes responsabilidades en un entorno de gestión distribuido de la red, así como los procedimientos y las políticas necesarias para implementar el sistema en una red académica.

También se consideró la necesidad de encontrar las vías necesarias para una correcta difusión del sistema.

Se debe continuar trabajando para encontrar fondos para poder universalizar el sistema, debido a la multitud de lenguas existentes en las diferentes redes académicas de los distintos países de la Unión Europea.

Se están estudiando las diferentes posibilidades para comprobar el funcionamiento inicial del sistema, utilizando listas de correo, chat, jabber o algo ya existente que no suponga un consumo excesivo de los recursos existentes.

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

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

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

Alberto Escolano
(alberto.escolano@rediris.es)
Área de red

TERENA celebra su XX aniversario

• **La asociación europea de redes académicas y de investigación celebra su XX aniversario**

TERENA *(Trans-European Research and Education Networking Association)*, la asociación europea de redes académicas y de investigación, celebró el pasado 13 de junio su XX aniversario. El 13 de junio de 1986, la asociación comenzó su andadura bajo la denominación RARE *(Réseaux Asocies pour la Recherche Européenne),* cambiando su denominación a TERENA en 1994, cuando se fusionó con otra organización con fines similares, EARN *(European Academic & Research Network association).*

Con motivo de ese aniversario, TERENA *(www.terena.nl)* organizó una jornada en Ámsterdam a la que acudieron muchos de los pioneros en el desarrollo de redes académicas y de investigación a escala europea, que hicieron balance de la evolución experimentada en esta área y apuntaron tendencias para el futuro.

TERENA tiene hoy como miembros a 34 redes académicas y de investigación nacionales, a dos organismos internacionales y 10 miembros asociados. Gestiona siete grupos de trabajo (sobre redes de nueva generación, seguridad, autenticación, movilidad, videoconferencia, relaciones públicas y gestión de la cartera de servicios), coordina la prestación conjunta de servicios por redes académicas (p.ej., el servicio de certificados de servidores recientemente lanzado por RedIRIS), organiza jornadas y una conferencia anual y da soporte a distintas iniciativas.

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

TERENA lanza EARNEST

• Se trata de un estudio sobre el futuro de las redes académicas

Los pasados días 23 y 24 de mayo, TERENA (la asociación de redes académicas y de investigación europea) organizó en Berlín la reunión de lanzamiento de EARNEST (*Education And Research Networking Evolution*

La asociación europea de redes académicas y de investigación celebra su XX aniversario

TERENA lanza un estudio sobre el futuro de las redes académicas

Study), un estudio de prospectiva sobre el futuro de las redes académicas y de investigación NRENs *(National Research and Education Networks)*.

A esta reunión acudieron más de 80 personas, representando no sólo a NRENs como RedIRIS, sino también a otros colectivos interesados en esta materia, como asociaciones de universidades, institutos de investigación, representantes de la industria, miembros de la Comisión Europea y de algunos gobiernos nacionales, etc.

EARNEST supone una puesta al día del trabajo que se realizó en 2003 con su predecesor, el estudio SERENATE *(www.serenate.org)*, que intentaba determinar, en una perspectiva de 5-10 años, los aspectos estratégicos del desarrollo de las NRENs, analizados desde distintos puntos de vista (tecnológico, organizativo, financiero, legal...).

Ahora, TERENA, con la colaboración de todas las partes interesadas, coordinará la puesta al día de ese estudio, en un proceso que se espera que concluya a finales de agosto de 2007.

En esta reunión inicial de Berlín, a través de presentaciones y de grupos de trabajo, se intentaron identificar los temas más relevantes, entre los que destacaron la tendencia al despliegue de redes de fibra óptica, la extensión de los servicios de las redes académicas y de investigación a nuevos colectivos (p.ej., escuelas, hospitales, redes administrativas...), nuevas posibilidades de colaboración entre las NRENs y las universidades para mejorar las infraestructuras y servicios TIC dentro del campus, la necesidad de evitar la brecha digital en las redes académicas, el análisis de los mecanismos de financiación, etc.

Las presentaciones y conclusiones de esta reunión inicial están disponibles en el website de TERENA, en el que se irá añadiendo información a medida que avance el estudio *(www.terena.nl/activities/earnest/)*.

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

EARNEST supone una puesta al día del trabajo que se realizó en 2003 con su predecesor, el estudio SERENATE

Hay una gran preocupación en RIPE debido a los últimos ataques de DoS

LII reunión de RIPE

• LII reunión del foro abierto de colaboración sobre redes IP

Durante el pasado mes de abril se celebró la reunión número 52 de la comunidad RIPE en Estambul. El tema sobre el que más se incidió fue la seguridad en DNS. Hay una gran preocupación debido a los últimos ataques de DoS que se han producido y para evitarlo se recomienda tomar las siguientes medidas:

- Utilizar un primario oculto, de forma que el servidor visible de la organización sólo tendrá una copia de la zona de la misma. Los servidores que gestionen la zona realmente y den servicio a usuarios están en una red privada y sólo son accesibles por administradores y/o usuarios.
- Diferenciar los servidores que gestionan las zonas de aquellos que dan servicio a usuarios.
- Tratar de depender lo menos posible de máquinas externas que puedan estar comprometidas en un momento dado.
- Desactivar recursividad, activar RPF check en los interfaces y aplicar filtros para evitar spoofing.
- Implementar DNSSEC si es posible.
- Y por supuesto, tener instalada una versión no vulnerable.

Otros temas que se comentaron fueron la desactivación de la zona .ip6.int el 1 de junio, y la seguridad en BGP; hoy en día muchos de los fallos de routing que ocurren son debidos a errores humanos. En el IETF se está trabajando para desarrollar mecanismos de seguridad.

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

Proyecto EELA

• Proyecto sobre e-infraestructuras entre Europa y América latina

Desde el 1 de enero de 2006 y durante dos años se va a desarrollar el proyecto EELA *(E-Infrastructure shared between Europe and Latin-America)*, financiado por la Comunidad Europea.

De características similares al ya desarrollado en Europa, EGEE *(Enable Grids for E-SciencE),* el objetivo es montar una infraestructura de grid entre Europa y Latinoamérica basada en las redes IP académicas y de investigación nacionales y continentales ya existentes. Ésta será utilizada por aplicaciones de física de altas energías, biomedicina o medioambientales.

RedIRIS participa en diferentes grupos de trabajo de este proyecto. En concreto, desde el área de red, se está trabajando actualmente en la definición de los servicios que será necesario implementar, en base a las necesidades de los usuarios, y de las funciones del noc central que se creará específicamente para tener conocimiento de los problemas que existan en un momento dado en una NREN concreta y poder informar a los usuarios de este proyecto. Más adelante se trabajará en la realización de las pruebas necesarias para poner en producción lo que ahora se está definiendo.

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

EUGridPMA

- **Organización europea de coordinación de autoridades de certificación nacionales para infraestructura grid**

A primeros de junio se celebró la séptima reunión de la EUGridPMA en Budapest *(www.eugridpma.org/)*. Los temas más importantes tratados fueron:

- Propuesta de una segunda versión de TACAR que incluye procedimientos más ágiles a la hora de la incorporación de nuevas CAs de una manera más simple y cómoda.
- Actualización del documento de requisitos mínimos para la acreditación de una CA.
- Reunión del grupo CAOPS (grupo perteneciente al Global Grid Forum dedicado a explorar la evolución de las infraestructuras de clave pública y su aplicación en grids). Se realizó la revisión de varios de los documentos pendientes de actualización y se propuso su organización en diferentes grupos creando, a su vez, un glosario de términos común a todos ellos. Creación de un Wiki.
- Revisión de los perfiles de los certificados incidiendo en aquello que puede y no puede usarse en el subject DN. Propuesta de inclusión de estas pequeñas normas en el documento de requisitos mínimos para la acreditación de una CA.
- Presentación de dos CAs para su acreditación: CERN-IS y Croatian CA.
- Revision en profundidad de dos CAs ya acreditadas: UK e-Science CA y HellasGrid CA.
- Propuesta de inclusión de información adicional en los certificados (en forma de OIDs) de forma que se permita que un software determinado, pueda tomar decisiones de validación y autorización de forma automática.
- Presentación del servicio de certificados de servidor SCS.

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

III EuroCAMP

- **Tercera edición de la conferencia europea sobre tecnologías middleware**

La tercera edición del EuroCAMP *(European CAMPUS Architecture Middleware Planning)* se celebró en Ljubljana (Eslovenia) los días 3, 4 y 5 de abril de 2006, auspiciado por TERENA y organizado por ARNES, la red académica eslovena. El objetivo principal de estos grupos de trabajo consiste en desarrollar y compartir conocimiento en torno a tecnologías middleware.

Esta edición del EuroCAMP se centró en las experiencias de varias redes académicas europeas en gestión de identidad digital dentro y fuera del campus. Se trataron temas como interoperabilidad, federación y Single Sign-On, y su aplicación en proyectos como eduRoam o eduGAIN.

El programa y las presentaciones de este evento están disponibles en la página web de TERENA *(www.terena.nl/activities/eurocamp/april06/programme1.html)*.

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

En el área de red RedIRIS participa en EELA en la definición de los servicios a implementar en el noc central que se va a crear

El III EuroCAMP se centró en las experiencias de varias redes académicas europeas en gestión de identidad digital dentro y fuera del campus

III reunión del Foro ABUSES

- **Foro de equipos de respuesta de incidentes de seguridad en España**

El Foro ABUSES *(www.rediris.es/abuses)* es un grupo creado en 2002, liderado por RedIRIS desde sus orígenes, que ha ido sufriendo modificaciones en su formato hasta llegar al actual que se refundó en 2005. Constituye una plataforma que agrupa a los principales equipos de respuesta de incidentes *abuse@* de la Comunidad Internet española y cuyo objetivo es mejorar la eficacia en la resolución de incidentes y contribuir a la seguridad de Internet. Actualmente consta de unos 20 equipos de otros tantos operadores españoles.

En esta tercera reunión se presentó la dinámica de trabajo y las experiencias de los equipos de JAZZTEL y EUSKALTEL. Uno de los aspectos más importantes del Foro son los puntos de contacto de sus diferentes miembros y en este aspecto se afianzó el formato y el aumento del número de contactos. Se debatieron diferentes iniciativas y documentos, muchos de los cuales son prolongación de líneas de trabajo en la Comunidad RedIRIS. Entre las iniciativas debatidas se decidió habilitar un grupo de trabajo para definir el formato mínimo para el intercambio de incidentes, la creación de una *Whitelisting* de correo electrónico para el Foro ABUSES así como el intercambio de IPs maliciosas recogidas por los distintos operadores.

También podemos destacar la aprobación de documentos de referencia tales como: "Criterios para políticas de uso en las relaciones cliente-ISP e ISP-ISP" y "Recomendaciones para operadores de correo electrónico". Se propusieron otros nuevos documentos tales como el "Marco de referencia para la cualificación de incidentes graves para actuaciones globales".

Por último se decidió consolidar el Foro ABUSES y sentar las bases para dotarlo de unos estatutos que definan su estructura, mejoren la dinámica de trabajo, delimiten las condiciones para ser miembros del mismo y definan los recursos telemáticos necesarios, que hasta el momento han sido proporcionados por RedIRIS.

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

XVIII reunión del TF-CSIRT

- **Reunión del grupo de trabajo de TERENA sobre coordinación de equipos de respuesta de incidentes de seguridad europeos**

La XVIII reunión del TERENA TF-CSIRT *(CSIRT Coordination for Europe)* se celebró el pasado mayo en Vilnius, Lituania y estuvo organizada por LITNET CERT; el CERT de la red académica lituana.

En la reunión, además de las presentaciones generales del primer día *(www.terena.nl/tech/task-forces/tf-csirt)*, se hizo un recorrido por los diversos proyectos en los que el grupo de trabajo está inmerso. Entre ellos, lo más destacable es:

- Cursos TRANSITS *(www.ist-transits. org/).* En otoño se evaluará el MoU entre TERENA y el FIRST para el uso y mantenimiento del material, no siendo seguro que se mantenga dicho acuerdo, con lo que tendremos todavía que ver quién se hace cargo de estos cursos a partir del año próximo. A pesar de esto, está planeado impartir un nuevo curso a finales del 2006 en Europa, del que os informaremos en cuanto tengamos información.
- Objeto IRT. En las consultas simples del whois aparecerá en breve la información proporcionada por este objeto, que hasta ahora no aparecía, haciendo así más sencilla su utilización.
- CERTs & GRIDS *(www.terena.nl/activities/nrens-n-grids/)*. Se ha formado un nuevo grupo de trabajo dentro del TF-CSIRT cuyo objetivo es el de explorar las sinergias entre estas dos comunidades. Algunas actividades planeadas dentro del mismo engloban la creación de un metadirectorio, organización de reuniones que faciliten la definición de objetivos, problemática y posibles soluciones de los problemas de seguridad que afectan a esta comunidad, investigación de vulnerabilidad en el middleware utilizado por los Grids, etc..
- ENISA *(www.enisa.eu.int/)*. El TF-CSIRT está muy atento a las actividades que ENISA está llevando a cabo, buscando en todo momento colaboraciones y haciendo patente la representación del mundo de los CERTs en las actividades de la agencia. En su página web se han publicado diferentes informes de utilidad (inventario y checklist para nuevos

Reunión del Foro de equipos de respuesta de incidentes de seguridad en España

Se ha formado un nuevo grupo de trabajo dentro del TF-CSIRT cuyo objetivo es el de explorar las sinergias entre estas las comunidades CERT y GRID

equipos, inventario de legislación Europea relacionada con NIS (*Network Information Security*), *Informe del Review Board* sobre medidas de seguridad implantadas por los ISPs europeos, etc..). Por otro lado, ya está disponible el borrador del programa que regirá las actividades de ENISA durante el próximo año. Las áreas de interés, en este caso, son las siguientes: herramientas de seguridad, CSIRTs, *awareness raising,* gestión de riesgos, sistemas de autenticación, nuevas tecnologías. Este draft, pendiente de aprobación, está a la espera de recibir comentarios en los próximos meses.

Para concluir la reunión, repasamos los *Terms of References* del Task Force puesto que es necesario renovarlo durante dos años más a partir de mayo de 2006.

El nuevo documento estará disponible en breve en el web del Grupo de Trabajo con todas las modificaciones en los Grupos de Trabajo, Deliverables, etc. lógicas por la evolución y desarrollo de las distintas actividades que se llevan a cabo.

Las presentaciones, resúmenes y demás información acerca de esta reunión está disponible en la página web de TERENA: *www.terena.nl/activities/tf-csirt/meeting18/*

Para concluir, mencionar que también se celebró en Vilnius la reunión de Equipos Acreditados en el TI *(Trusted Introducer), www.trusted-introducer.nl/* en lo que respecta a información sobre estadísticas de incidentes e intercambio de tendencias.

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

Próximo FIRST en España

- **La conferencia anual sobre Seguridad por excelencia se celebrará el 2007 en España**

La conferencia anual de FIRST, organismo que agrupa a más de 180 grupos de Seguridad (CSIRT) se celebrará en Sevilla, a mediados del mes junio.

FIRST organiza todos los años una conferencia abierta en la que se dan cita miembros de los distintos grupos de seguridad a nivel mundial, el año que viene esta conferencia se celebrará en Sevilla y tiene como lema "Vida privada y riesgo corporativo: Privacidad digital, riesgos y responsabilidades", para poner mayor énfasis en cómo los problemas de seguridad pueden generar riegos en la información privada que mantienen los sistemas informáticos.

Alrededor de este tema central se desarrollarán una serie de reuniones paralelas sobre diversos aspectos, de forma similar a lo que ha ocurrido este año en Baltimore, donde hubo una reunión entre los denominados LEO, (*Law Enforcement Officer* o cuerpos de seguridad del estado) y los grupos de seguridad.

Esta conferencia es uno de los mayores eventos de seguridad que se realizan anualmente, iremos proporcionando más información al respecto a través de las listas de coordinación de RedIRIS no obstante también estará en constante actualización en la siguiente dirección: www.first.org/conference/2007. A día de hoy ya está publicada la petición de contribuciones y abierto el plazo para su presentación.

Esperamos que esta conferencia sea un éxito.

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

Reunión de CSIRTs gubernamentales

- **Reunión mundial de grupos de seguridad nacionales**

Tras la conferencia FIRST en Baltimore el CERT/CC de la Universidad Carnelie-Mellon y el grupo de seguridad del gobierno estadounidense, US-CERT, organizaron una reunión con grupos de seguridad nacionales.

A esta reunión acudieron grupos de seguridad de todo el mundo, (Holanda, Suecia, Alemania, Japón, Korea, Australia, Katar, Brasil, Estados Unidos, etc.) y se trataron sobre todo los diversos proyectos que en cada país se están realizando a la hora de coordinar a nivel nacional la gestión de incidentes y los distintos proyectos de monitorizacion y alerta temprana que se están realizando.

Por parte de España acudieron el grupo de seguridad de RedIRIS, IRIS-CERT, y un

La conferencia anual sobre seguridad por excelencia se celebrará en 2007 en España

Reunión mundial de grupos de seguridad nacionales en Baltimore con asistencia española

representante de INTECO (Instituto Nacional para las Tecnologías de la Comunicación), organismo de reciente creación que va a albergar el centro nacional de respuesta a incidencias de seguridad en Internet.

Desde su creación en el año 1995 y sobre todo tras convertirse en miembro de FIRST en 1997, IRIS-CERT ha sido el punto de contacto para incidencias de seguridad cuando, desde fuera de España se necesitaba contactar con los responsables de algún equipo bajo el dominio ".es".

Desde los comienzos hasta el año 2000, RedIRIS albergó el registro de nombres de Internet en España, NIC.es, y por lo tanto desde el exterior era el punto de contacto más fiable a la hora de buscar a los responsables de un equipo que estuviera en un dominio ".es".

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

Desde su creación y sobre todo tras convertirse en miembro de FIRST, IRIS-CERT ha sido el punto de contacto para incidencias de seguridad bajo el dominio ".es"

Servicio SCS

- **Servicio de Certificados de Servidor (SCS)**

El uso de canales cifrados (https, correo seguro, etc.) para la comunicación entre usuario y aplicaciones es cada día mayor en las redes académicas y de investigación. Este uso requiere de la existencia de unas Autoridades de Certificación (CA) que afirmen, mediante los correspondientes certificados de servidor, que estos son quienes dicen ser antes del establecimiento de ese canal seguro.

El uso de canales cifrados es cada día mayor en las redes académicas y de investigación

Aunque la mayoría de las NRENs, centros afiliados y otras instituciones disponen de su propia CA, no son, en su mayoría, reconocidas, por defecto, por los principales clientes utilizados por los usuarios. Por ello, cuando se establece la comunicación con un servidor que tiene un certificado emitido por alguna de estas CA, no reconocidas, el usuario recibe una ventana emergente con un aviso de desconfianza en el servidor al que está intentando conectarse.

Ante tal situación el usuario se encuentra pues con tres problemas:

- Molestia

  El usuario recibe una ventana emergente, no solicitada, con un mensaje que le desconcierta, en la mayoría de los casos, y le hace perder la atención en lo que quería hacer.

- Desconfianza

  Se muestra un mensaje de desconfianza. El ordenador indica que se está accediendo a un servidor cuya identidad no está asegurada. Tampoco la identidad de quien firma su certificado de servidor. El usuario percibe que puede que no sea el servidor al que deseaba acceder.

- Riesgo en la seguridad de la transacción

  El usuario está tan acostumbrado a recibir ventanas emergentes que, habitualmente, suele no leer el texto mostrado en dicha ventana. Simplemente sabe que si da al botón de aceptar las cosas funcionan.

  Ello conlleva a que, ante un intento de suplantación de servidor, el usuario usualmente acepte la conexión y ponga en peligro la seguridad de la transacción e incluso de su equipo.

El servicio SCS *(www.rediris.es/pki/scs/)* intenta solventar el problema de las ventanas emergentes que plantean, al usuario, una desconfianza en los certificados que no tienen CA incorporadas directamente en el navegador.

Para ello TERENA ha contratado a un proveedor comercial la firma de los certificados de servidor para las ocho NRENs involucradas en el proyecto y sus instituciones afiliadas y desde el día 1 de junio el servicio está disponible en nuestra comunidad.

El procedimiento de solicitud es muy simple, el responsable técnico del servicio rellena un documento de condiciones de uso donde especifica los nombres FQDN que van a aparecer en el certificado. Este documento es firmado por él y por el PER de la organización y enviado a RedIRIS. Posteriormente, vía web, solicita el certificado y recibe un e-mail con información que debe enviar a RedIRIS. Una vez enviados todos los documentos, debidamente firmados, por él y por el PER el certificado es emitido.

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

Esquema SCHAC

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

El 14 de mayo fué aprobada formalmente la primera versión de la especificación SCHAC durante la reunión del TF-EMC2 en Catania.

La especificación SCHAC-IAD-rel1 *(SCHAC Individual Attribute Data, Release 1)* incorpora un conjunto de 19 atributos clasificados en siete categorías genéricas de acuerdo con la clasificación establecida en un proyecto con Internet2 *(www.terena.nl/activities/tf-emc2/schac.html)*.

Principalmente es un esquema orientado a facilitar el intercambio de datos entre instituciones académicas en proyectos como ECTS (Bolonia) y en esquemas de federación (eduroam, PAPI, eduGAIN). Se ha creado armonizando los esquemas empleados en diferentes países y aunque no está orientado a LDAP está fuertemente influenciado por él.

La mayor parte de los atributos contienen valores de vocabularios normalizados como códigos ISO, lenguajes en formato RFC3066, tiempos en formato RFC3399 y URLs. También se usan URNs para facilitar el uso armonizado de identificadores idiosincráticos propios de una comunidad determinada.

TERENA ha creado una página web para el registro de URNs bajo el espacio de nombres urn:mace:terena.org:schac dedicado a mantener la información de los cinco atributos que actualmente tienen formato URN *(www.terena.nl/registry/terena.org/schac/)*. Se han definido algunos valores comunes a todos los países y se han delegado usando TLDs los espacios de nombre a todos los países para que puedan incorporar sus valores particulares.

Desde su aprobación varias organizaciones, a nivel internacional, lo han adoptado y han añadido sus atributos a sus esquemas. RedIRIS también va a incorporar algunos de los atributos de SCHAC a sus esquemas y recomendará su uso a todas las instituciones afiliadas.

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

Monitorización de flujos

- **Nuevo sistema en producción de recolección y análisis de flujos en la red troncal de RedIRIS**

Desde mediados de junio está en producción el nuevo sistema de recolección y análisis de flujos en la red troncal de RedIRIS utilizando para ello el nfdump y NfSen desarrollados por SWITCH (red académica suiza), cuyo desarrollo cuenta con el beneplácito del JRA2 (Security) de GÉANT2 *(www.rediris.es/cert/doc/reuniones/ cord/gt2006/nfsen_iris-cert.pdf)*. El nfdump es el colector y procesador de datos netflow en línea de comandos utilizado (http://sourceforge.net/projects/nfdump/), mientras que el NfSen nos proporciona un front-end web muy útil para el nfdump haciendo muy intuitiva y sencilla la interacción con la información netflow almacenada (http://sourceforge.net/projects/nfsen/).

En la actualidad todos los routers del backbone exportan datos netflow a nuestro servidor central, encargado de almacenar y procesar dicha información, que es utilizada en tiempo real para la detección de anomalías y posibles ataques mediante la ejecución de plugins, recolección de estadísticas y seguimiento de actividades de Ips y puertos involucradas en incidentes o actividad maliciosa, y análisis de incidentes perpretados en nuestra red sobre datos históricos (se dispone de información completa sobre tráfico del último mes).

El NfSen soporta netflow v5, 7 y 9 y es compatible con IPv6, utiliza una sintaxis de filtrado basada en pcap, y permite por una parte la agregación de flujos y definir diversas vistas sobre los datos almacenados, lo que unido al análisis de actividad en ventanas de tiempo específicas dotan al sistema de una gran versatilidad.

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

Listas blancas de correo electrónico

- **Las listas blancas: un mecanismo para optimizar los sistemas anti-spam**

Desde hace tiempo está muy extendido el uso de listas negras (blacklisting - DNSbl) como mecanismo de bloqueo en tiempo real de las

SCHAC es un esquema orientado a facilitar el intercambio de datos entre instituciones académicas

El uso de listas negras ha crecido mucho como consecuencia de que la mayor parte del spam procede de equipos personales infectados

transacciones SMTP en los servidores de correo, este sistema incluso está siendo incorporado en muchos productos comerciales antispam. Las listas negras son muy útiles para frenar el spam en los servidores pero al mismo tiempo ocasionan ciertos problemas a las instituciones, como por ejemplo los falsos positivos. Una forma de reducir estos problemas, manteniendo las listas negras, es el uso de listas blancas o listas de exclusión (whitelisting - DNSwl) que permiten aceptar el tráfico de determinadas instituciones independientemente de que estén incluidas en las listas negras.

El uso de listas negras ha crecido exponencialmente como consecuencia de que la mayor parte del spam procede de equipos personales infectados con virus, troyanos o gusanos (*zombies*) y es más económico bloquear las transacciones SMTP de *zombies* que analizar los contenidos. No obstante ocasionalmente puede ocurrir que, por descuido de algún usuario, un dominio bien gestionado sea incluido automáticamente en alguna DNSbl que estemos utilizando, provocando que *correo bueno* no llegue a sus destinatarios y las políticas de permanencia en las listas negras en algunos casos puede ser un proceso complejo.

Una lista blanca se compone de tres partes:

- Una base de datos de servidores (IP) cuyo tráfico de correo será siempre aceptado
- Una política de altas/bajas
- Los filtros en los servidores para chequear esta base de datos al aceptar el tráfico entrante.

Los objetivos de crear una lista blanca a nivel español (WLES) es evitar el bloqueo de transacciones SMTP de servidores de proveedores españoles. Esta iniciativa queda encajada tanto en el Grupo IRIS-MAIL como en el Foro ABUSES del que hemos hablado con anterioridad además de haber sido propuesto en el grupo de Trabajo HERMES de RedClara sobre seguridad en el correo electrónico.

Hay operadores de correo que son gestionados correctamente y su inclusión automática en una lista negra es una medida que ocasiona problemas al intercambio habitual de tráfico entre instituciones, universidades y proveedores; es aquí donde entrarían los beneficios de las listas blancas. Una lista blanca con dominios bien supervisados permitirá reducir muchos problemas y mejorar la calidad del tráfico SMTP.

El mecanismo más sencillo para acceder a la base de datos es vía DNS, cualquier servidor de correo podrá consultar vía DNS la base de datos de la WLES para chequear si la IP está incluida o no y recibir la respuesta adecuada. La mayor parte de los paquetes de los servidores (postfix, sendmail, qmail, exim, etc.) o módulos intermedios (spamassassin, amavis, mailscanner, etc.) permiten hacer chequeos DNS de listas blancas, aunque es un tema que habrá que especificar con más detalle para ayudar a los servidores que deseen implementarlo.

Es importante tener en cuenta que la política del servidor SMTP entrante es quien decidirá qué acciones tomar con los resultados obtenidos al chequear la whitelisting, esto no es responsabilidad de la Whitelisting WLES. El acceso a la zona WLES será pública y cualquier relay que confíe en su política podrá utilizarla.

Para la construcción de la base de datos será necesario disponer de infraestructura y *software* DNS y se creará una zona "wles.rediris.es" para almacenar la base datos.

El formato de estos registros deberá ser homogéneo al que se plantee en otros foros internacionales principalmente europeos. Para definir una entrada en la WLES serán necesarios dos registros:

- Uno de tipo Address RR A 127.0.0.2
- Y otro de tipo texto informativo incluyendo el ASN y/o nombre del ISP al que pertenecen.

Sirvan como ejemplos los siguientes:

- 138.100.4.8 responsable del correo @upm.es. La entrada en la WLES sería:

  8.4.100.138 A 127.0.0.2
  8.4.100.138 TXT "ASN 766. RedIRIS. Universidad Politécnica de Madrid"

- 213.4.149.64 responsable del correo @telefonica.net. La entrada en la WLES sería:

  64.149.4.213 IN A 127.0.0.2
  64.149.4.213 TXT "AS6813. Telefonica Data Espana"

Sería necesario definir una política de altas y bajas y un canal de difusión de altas adecuado. De forma consensuada podrán proponerse IPs de los servidores de correo de operadores de interés general (gmail, terra, telefonica.net, etc); una primera aproximación de los criterios de los relays que se incluyan en esta Whitelisting (WLES) serían:

Los objetivos de crear una lista blanca a nivel español es evitar el bloqueo de transacciones SMTP de servidores de proveedores españoles

Una lista blanca se compone de tres partes: una base de datos de servidores, una política de altas y bajas y los filtros en los servidores

- Tener una política activa para prevenir y evitar la difusión de virus, spam, etc.
- Disponer de un servicio de gestión de abuse (abuse@) que tenga potestad para detener la difusión de spam o virus de sus clientes.
- Que las cabeceras "Received:" de sus servidores sean de confianza.
- Que pertenezcan a un ISP incluido en el Foro ABUSES *(www.rediris.es/abuses)* al que pertenece RedIRIS.

Las incorporaciones serán recogidas en un formulario web para ser a continuación evaluadas por un comité y anunciadas por correo en los foros adecuados.

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

OSIRIS

- **Proyecto europeo para la integración de servicios en tiempo real**

El proyecto OSIRIS *(Open Source Infrastructure for Run-time Integration of Services)* sigue su curso. La última reunión del proyecto, mantenida en Lillehammer (Noruega) a principios de junio, se centró en los siguientes aspectos:

- Mostrar los avances realizados en cada uno de los paquetes de trabajo
- Definir las distintas unidades de la infraestructura (servicios, componentes, conectores)
- Buscar sinergias entre los demostradores del proyecto y las tecnologías disponibles en el consorcio
- Preparar la revisión del proyecto por parte de ITEA *(Information Technology for European Advancement)*
- Sentar las bases para la definición de la arquitectura del sistema

Fruto de la participación de RedIRIS en este proyecto son la integración de PAPI con el framework de autenticación y autorización JAAS *(Java Authentication and Authorization Service)* y con Shibboleth, que formarán parte del núcleo de seguridad de OSIRIS.

Se puede encontrar más información en la página del proyecto: *www.itea-osiris.org* y también en la página de ITEA *(www.itea-office.org)*.

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

Cruzando el Atlántico con la nueva Internet

- **Con motivo del Día Mundial de la Sociedad de la Información se realizó una videoconferencia con múltiples instituciones involucradas a través de las redes académicas nacionales**

El día 17 de mayo se realizó un encuentro virtual a través de las redes académicas entre instituciones americanas y europeas para tratar de debatir y promover el uso de Internet y las Tecnologías de la Información y la Comunicación en la cooperación a ambos lados del Atlántico.

El encuentro se hizo coincidir con el Día Mundial de la Sociedad de la Información y participaron sedes de instituciones y redes tan distantes como:

- Universidad Politécnica de Madrid, España: ETSI Telecomunicación
- Red CUDI, Méjico
- Red REUNA, Chile
- Red RNP, Brasil
- Red CEDIA, UTPL, Ecuador
- Red REACCIUM, Venezuela
- Red RAU, Uruguay
- Red CR2NET, Costa Rica
- RedIRIS, Madrid, España
- CRC, Ottawa, Canadá
- ULB, Brussels, Bélgica
- CRIBABB CONICET, Argentina
- Universidad Carlos III de Madrid, España
- INICTEL, Lima, Perú
- UNI, Lima, Peru
- PUCP, Lima, Perú
- UALM, Perú
- IPEN, Perú
- CIP, Perú

Asimismo se realizó una conexión con la Conferencia anual de TERENA que se estaba celebrando en Catania (Italia) y desde allí intervinieron Mario Campolargo, Gestor Jefe de Investigación de la Dirección General de la

RedIRIS participa en OSIRIS: proyecto europeo para la integración de servicios en tiempo real

Video-conferencia múltiple con motivo del Día Mundial de la Sociedad de la Información

Sociedad de la Información de la Comisión Europea; Florencio Utreras, Director Ejecutivo de REUNA (Red Universitaria Nacional) y Tomás de Miguel, Director de RedIRIS.

El evento tuvo una duración de unas cuatro horas y la herramienta de colaboración usada fue ISABEL con unos resultados muy positivos ya que no hubo incidencias remarcables.

ISABEL es una herramienta de colaboración en grupo multipunto que posee varias formas de funcionamiento: telemeeting, teleconference y teleclass. En este caso se utilizó el modo teleconference que permite entre otras cosas una moderación bastante avanzada de la sesión.

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