Contents

1 Introducción

El presente documento constituye el informe de incidentes de seguridad que afectan a la Red Académica y de Investigación Española, RedIRIS, para el año 2012.

El siguiente documento comprende tanto el análisis de las estadísticas sobre los incidentes atendidos por el Equipo de Seguridad de RedIRIS IRIS-CERT durante el año 2012, como la correspondiente comparativa con años anteriores. Ésto nos permite seguir la evolución de lo acontecido a lo largo de los años.

Este informe incluye también una descripción genérica de los problemas que creemos han sido más significativos durante ese año.

Este documento se publica en la Web de IRIS-CERT bajo el apartado Informes anuales y junto a los informes publicados desde el año 2002. Además, su disponibilidad se anuncia en la lista de coordinación de seguridad de RedIRIS, IRIS-CERT.

Estamos abiertos a cualquier sugerencia que nos permita mejorar la calidad del presente informe. Para ello, puedes contactar con nosotros en la dirección cert @ rediris . es, y enviarnos tus sugerencias.

2 Estadísticas

Esta sección recoge aquellos problemas de seguridad de los que hemos tenido noticia directa en el CERT de RedIRIS, bien por notificaciones externas e

internas desde la comunidad, o por los sistemas de detección automática implantados.

La clasificación de los incidentes dentro de la taxonomía de alto nivel que tenemos definida, se realiza a partir de la información que nos hacen llegar los contactos técnicos de seguridad operativos en las instituciones afiliadas, por lo que su exactitud depende absolutamente de cuán exactos sean éstos a la hora de describir el problema sufrido y las medidas adoptadas para su resolución. Por lo tanto, para que este informe sea lo más veraz posible necesitamos la colaboración de los mismos.

IRIS-CERT tiene publicado en su web los posibles valores de cierre con los que operamos en función a la respuesta recibida por parte de las instituciones afiliadas.

Para finalizar en aquí existe una exhaustiva descripción de todo el procedimiento de gestión de Incientes, que ha obtenido la certificación de sistemas de calidad ISO 9001.

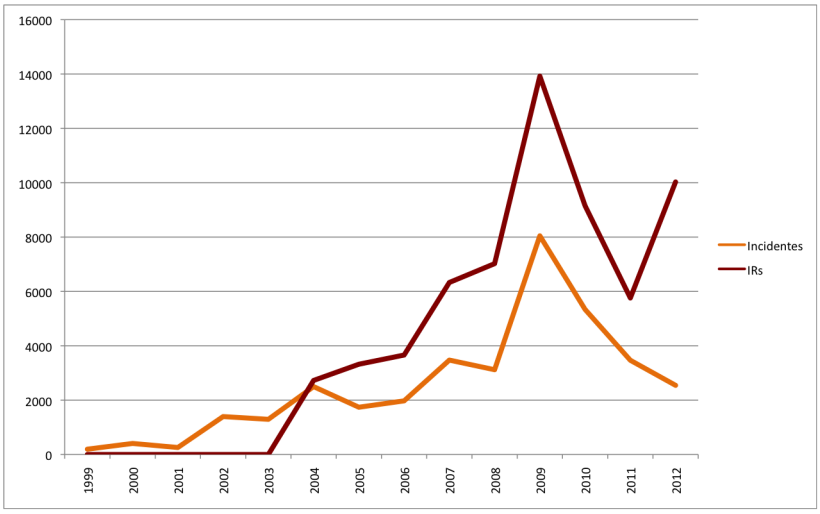
2.1 Cifras para el año 2012

Durante el 2012 se han recibido un total de **10028** *Incidents Reports*[1], lo que supone un **74.15 % más de quejas recibidas que el año pasado**.

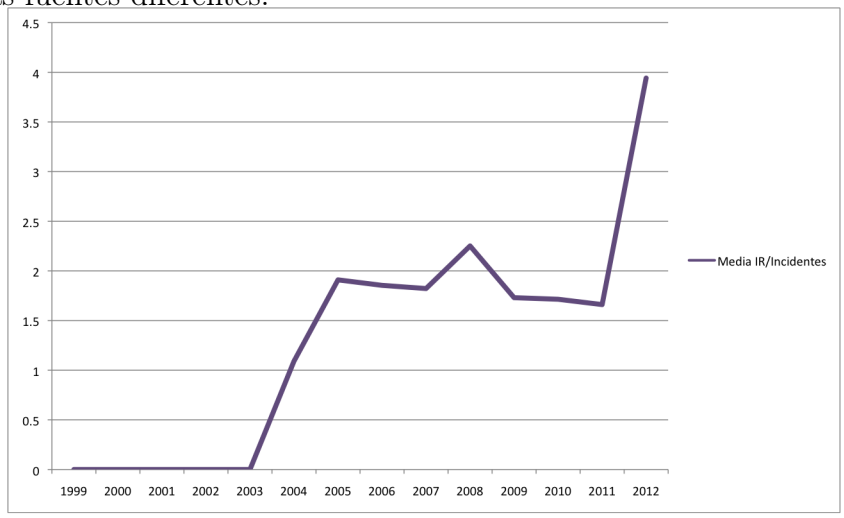
Esos 10028 *Incidents Reports* han generado un total de **2544** Incidentes[2] en nuestro sistema, lo que supone un **26.6% menos que en el 201**1, en el que se atendieron un total de 3469 Incidentes.

[1]Cualquier información que se recibe en los buzones del CERT (una vez eliminado el SPAM).

[2]Entidad superior que agrupa a todos los *Incidents Reports* e *Investigations* relativas a un mismo problema (normalmente a una misma IP).



El número medio de quejas por incidente ha sido de 3.94. Es decir, de media se han recibido casi cuatro quejas por cada incidente abierto con las instituciones. Si comparamos con el año 2011, se ha duplicado de media el número de denuncias por incidente, recibiéndose pues más información desde mas fuentes diferentes.



Como se puede deducir con los datos anteriores, este año se han recibido más denuncias, se ha duplicado el número medio de quejas por incidente, y se confirma una ligera disminución en el número de incidentes totales atendidos durante el 2012.[3]

[3]**NOTA aclaratoria**: El pico de IRs e Incidents registrados en el 2009 se debe fundamentalmente a la repercusión en nuetra red del Conficker y a la puesta en marcha de

De esos 2544 incidentes, **130** han tenido como destino el buzón de consultas o ***HelpDesk* de IRIS-CERT**.

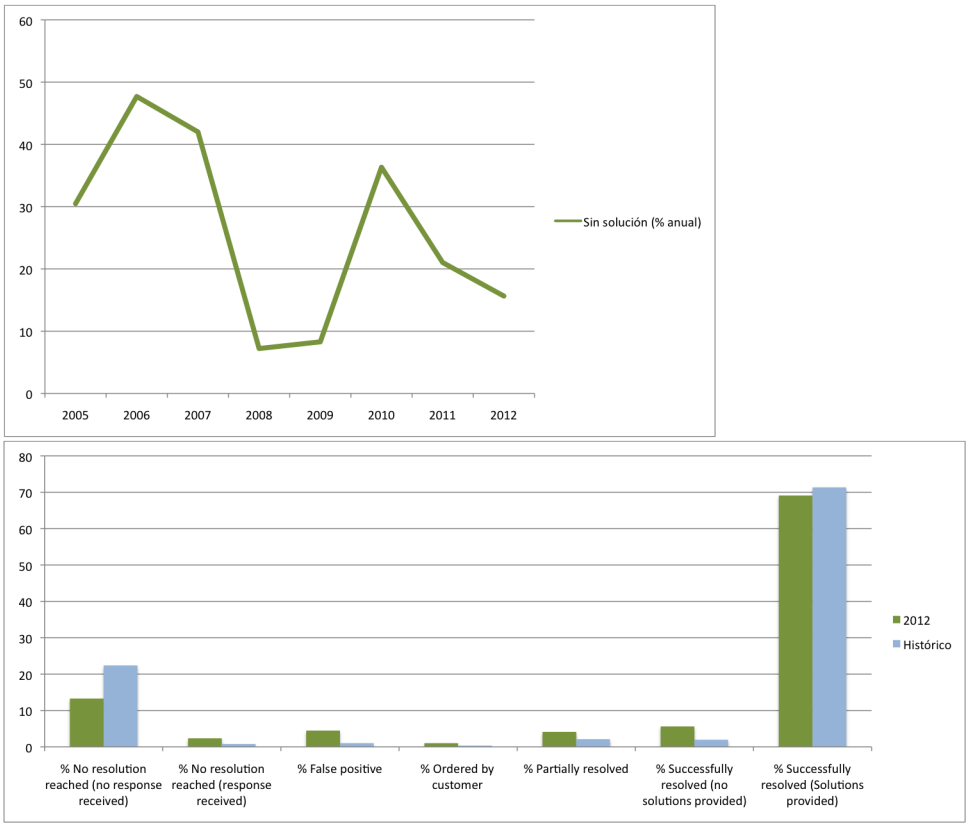
La distribución por valores de cierre sobre el total de Incidentes atendidos durante el 2012 es la siguiente:

- 338 a *"Problema no resuelto (No se obtiene respuesta)"*.
- 60 a *"Problema no resuelto (Se obtiene respuesta)"*.
- 114 a *"Falso positivo"*.
- 26 a *"Cierre ordenado por el cliente"*.
- 105 a *"Parcialmente resuelto"*.
- 143 a *"Solucionado satisfactoriamente (No se aportan soluciones)"*.
- 1758 a *"Solucionado satisfactoriamente (Se aportan soluciones)"*.

Si tenemos en cuenta que "Problema no resuelto" es la suma de los incidentes cuyo valor de cierre es *"Problema no resuelto (No se obtiene respuesta)*" y "*Problema no resuelto (Se obtiene respuesta)*", el número total de incidentes no resueltos durante el año 2012 ha sido 398, lo que supone un importante decremento con respecto al año 2011, donde tuvimos un total de 739 incidentes no resueltos. Esto significa que vamos por buen camino, aunque todavía un **15.6% de los incicentes totales que reportamos a nuestras instituciones no son solventados**[4]. Os damos las gracias por vuestra colaboración a este respecto, y os animamos a seguir trabajando en esta línea y que nos sigáis remitiendo, en la medida de vuestras posibilidades, toda la información que se desprenda de vuestras investigaciones internas.

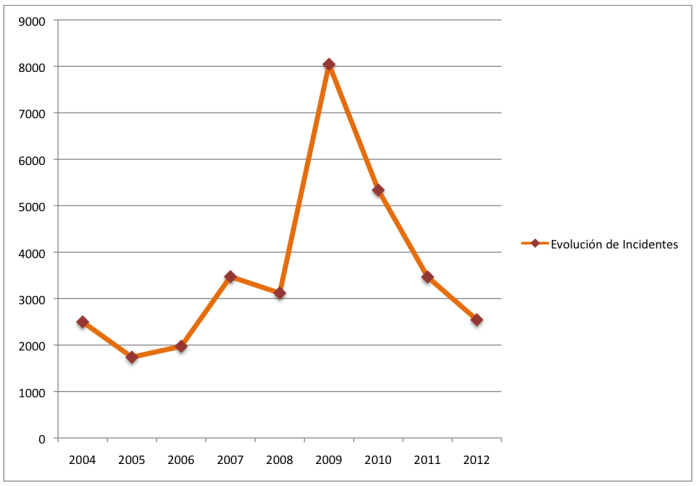
nuevos plugins de detección por parte de IRIS-CERT.

[4]El año 2011 no se solventaron un 21.30% del total de incidentes reportados.



2.2 Evolución histórica de los incidentes

En el siguiente gráfico se muestra la evolución de los incidentes de seguridad a lo largo de los años desde el año 1999.



Las cifras detalladas son las siguientes: [5]

Año	Incidentes Totales	Incremento
1999	195	-
2000	416	113.333%
2001	1038	149.51%
2002	1495	44.02%
2003	1294	-13.44%
2004	2682	107.26%
2005	1739	-35.16%
2006	1973	13.45%
2007	3473	76%
2008	3119	-10.19%
2009	8045	157.93%
2010	5337	-33.66%
2011	3469	-35.00%
2012	2544	-26.66%

Existen varias razones para explicar el descenso de incidentes atendidos durante 2012. Por una parte, se han recibido más quejas desde el exterior pero relativas a un mismo problema. Muchos reportes recibidos correspondían al Grumbot y no han podido ser atendidos debido al elevado número que han llegado a nuestros buzones y a que la información contenida en los informes era incompleta y no permitía a las instituciones detectar la máquina com-

[5] Estas cifras corresponden a los incidentes totales, sin realizar ninguna eliminación por tipo de incidente tratado.

prometida cuando la máquina infectada estaba detrás de una red NAT.

Además, se han dejado de atender algunas quejas procedentes de sistemas automáticos externos que requieren mucha dedicación de recursos, puesto que desde Agosto de 2012 el CERT no dispone del recurso que proporcionaba el primer nivel de atención de incidentes.

Otra razón que explica este descenso es que, como ya ocurrió el año pasado, debido a la migración a RedIRIS-NOVA nuestra principal fuente de detección de ataques interna (los flujos de red) no ha operado al 100% de sus posiblidades, teniendo un importante impacto en el número de IRs reportados de forma automática a nuestro sistema de gestión. Además, aunque a principios de año se puso en marcha un piloto en el que participaron varias instituciones afiliadas para disminuir el número de falsos positivos en uno de nuestros plugins de detección (concretamente el plugin de detección de conexiones a C&C de botnets conocidas), tras analizar los resultados del piloto se decidió no poner en producción este plugin de nuevo ya que con las fuentes públicas disponibles no era posible minimizar este número de falsos positivos.

Durante el 2012 los incidentes que, por su envergadura, son dignos de reseña son:

- **Contenido abusivo.** Fundamentalmente SPAM, y debido principalmente al robo de credenciales de usuarios de nuestras instituciones. También se ha hecho uso generalizado de los webmails de nuestras instituciones para el envío de SPAM.

- **Contenido malicioso**. Se han procesado muchos incidentes sobre páginas Webs de nuestra comunidad que se utilizan para distribuir malware o que contienen código malicioso. La tecnología Java sigue siendo una de las principales vías de infección de los sistemas. Las vulnerabilidades descubiertas en varios sistema de gestión de contenidos (CMS), concretamente en Joomla! a finales de año, también han sido las causantes de muchos de los problemas de compromisos de páginas Web reportados. Por otro lado, también han sido frecuente la participación de máquinas de nuestra comunidad en botnets conocida. Por ejemplo, la Botnet Grumbot que tuvo mucho impacto en nuestra comunidad provocando un verdadero aluvión de quejas. Dentro de esta categoría de "Contenido Malicioso" también se incluyen las máquinas comprometidas, sobre todo a principios de año, por el DNSChanger.

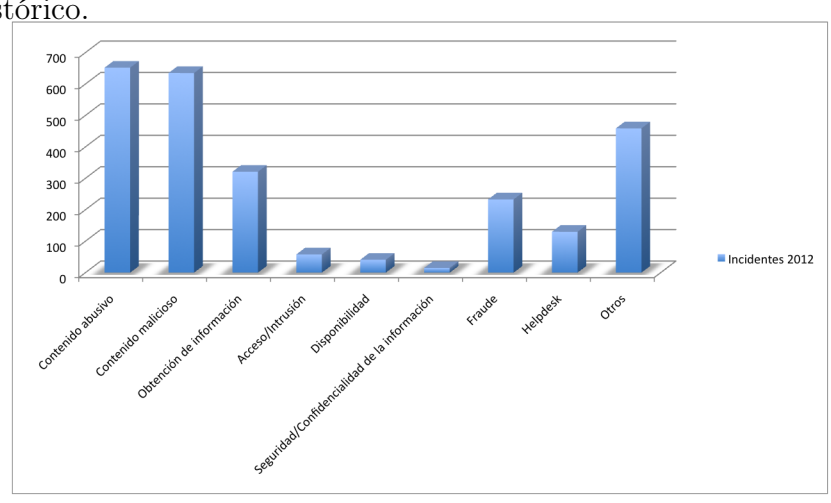
El DNSChanger es un malware que se encargaba de redirigir a las víctimas a páginas maliciosas controladas por un atacante sin conocimiento ni consentimiento del usuario. Aunque causó un gran revuelo en los medios de comunicación, cabe decir que tras el ánalisis que se realizó de este malware en nuestra red, realmente, no se detectó una infección masiva de equipos de nuestro sistema autónomo.

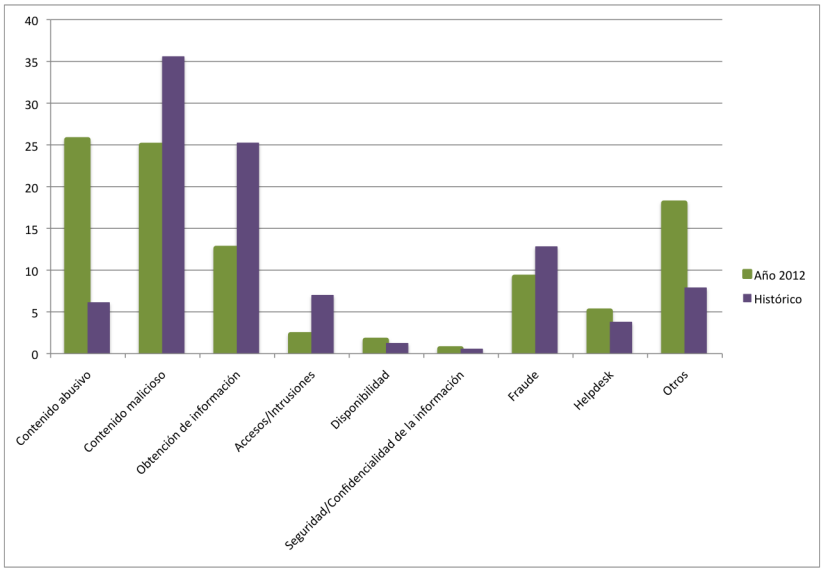
- **Fraude**. Sobre todo phishing, utilizando tanto el correo como la Web para su difusión.

- Hemos recibido también muchos incidentes en los que aparecemos como Copia y que pertenecen a máquinas fuera de nuestro ámbito de actuación, fundamentalmente relativos a casos de fraude en dominios .es (phishing y troyanos bancarios). Estos incidentes se nos reportan a modo informativo y explican, como se ve más abajo en la gráfica, el aumento de los incidentes que catalogamos como "**Otros**".

- **Obtención de información**. Como viene siendo habitual en los últimos años, recibimos muchos informes sobre escaneos de redes y puertos (muchos de ellos al puerto 22/tcp, ssh).

A continuación, mostramos una gráfica con la distribución de incidentes según la taxonomía de alto nivel que utilizamos y su comparativa con el histórico.

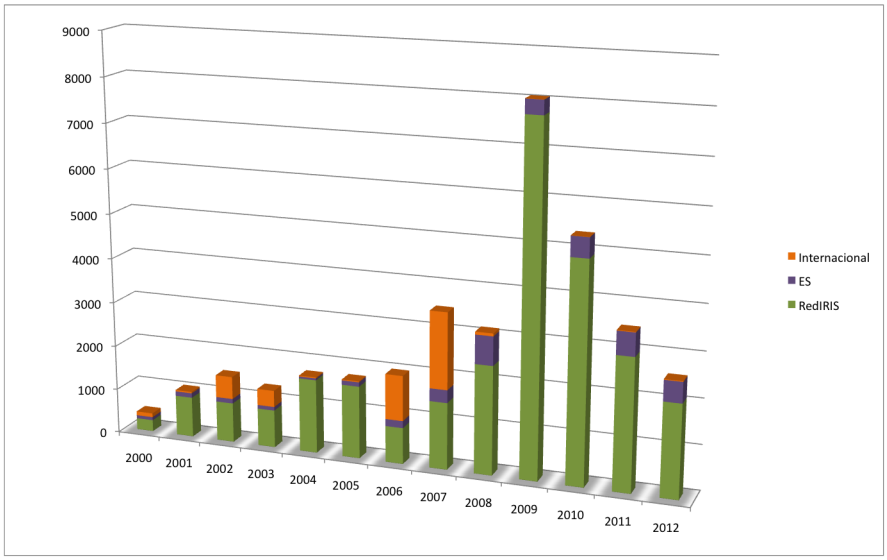




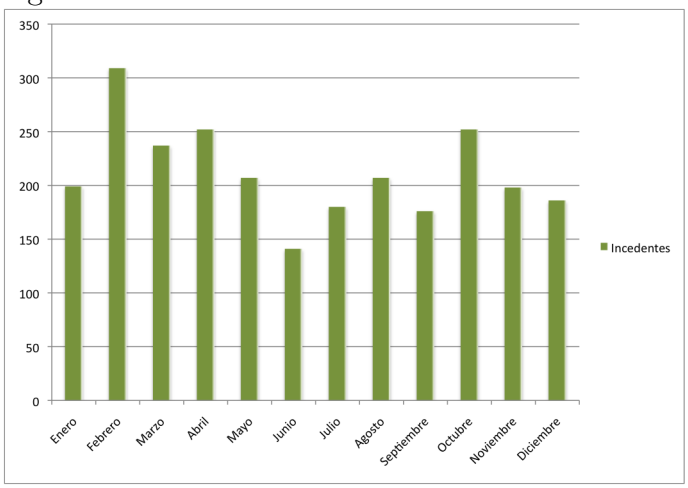
Se dispone de más información sobre la taxonomía que manejamos en la página web destinada a tal fin: http://www.rediris.es/cert/IH/taxonomia.html.

2.3 Otra información de interés

La siguiente gráfica muestra la distribución de los Incidentes atendidos durante el 2012 en función al ámbito de actuación (*constituency*). Como "RedIRIS" se clasifican todos aquellos incidentes que involucran, como origen o/y destino, a instituciones afiliadas y que constituyen el núcleo más importante de nuestro trabajo diario. Como "ES" se clasifican todos aquellos que afecten a máquinas del dominio .es, que normalmente corresponden a incidentes en los que se nos pone en copia a modo de información. Para finalizar, dentro de*"Internacional"* estarían todos aquellos incidentes que no afectan ni a máquinas de nuestra comunidad, ni del dominio .es y que por la razón que sea llegan al buzón del CERT, normalmente tanmbién como "Cc".



La siguiente gráfica muestra la distribución de los incidentes por meses a lo largo del año 2012.



Los datos son los siguientes:

Fecha	Total
2012/01	199
2012/02	309
2012/03	237
2012/04	252
2012/05	207
2012/06	141
2012/07	180
2012/08	207
2012/09	176
2012/10	252
2012/11	198
2012/12	186

En la gráfica anterior se aprecia un pico en el mes de Febrero que corresponde al DNSChanger, que hemos comentado anteriormente. El pico de Octubre corresponde principalmente a denuncias relativas a Grumbot y a envío de SPAM por robo de credenciales.

A nivel global, y no sólo en la red académica, la tendencia durante el 2012 ha continuado la línea de lo que comentábamos para 2011 en lo que respecta al fraude en sus diversas modalidades. Así podemos mencionar el conocido Troyano de la Policía, que secuestraba los ordenadores víctimas, haciendose pasar por la Policía Española.

En cuanto a los ataques a Infraestructuras Críticas, entornos industriales y ciberespionaje, y siguiendo con la tendencia de malware dirigido como el Stuxnet y el Duqu, en el 2012 han llegado a los medios otros especímenes como el Flame mucho más sofisticado que sus predecesores, y cuyo código además estaba firmado por Microsoft, lo que garantizó durante mucho tiempo su éxito (estuvo más de 5 años activo). Además, a consecuencia de ésto Microsoft actualizó sus políticas de seguridad PKI.

3 Líneas futuras de trabajo

- Debido a que el envío de spam causado por el robo de credenciales es uno de los problemas que está en auge en nuestra comunidad, se requerirá un gran esfuerzo por parte de las instituciones para concienciar a los usuarios sobres buenas prácticas y recomendaciones para evitar que sean víctimas de correos fraudulentos o/y phishing.

- La detección de máquinas con problemas de seguridad en sistemas NAT sigue siendo un problema importante en las instituciones afiliadas. Se insta desde RedIRIS a la instalación de proxies transparentes y a el registro de conexiones que permitan identificar las máquinas comprometidas y poner solución a los problemas reportados.

- IRIS-CERT seguirá trabajando durante el 2012 en el sistema de BlackHole BGP para el análisis de tráfico hacia IPs maliciosas y el reencaminamiento de tráfico y filtrado ante determinados ataques, especialmente para Denegaciones de Servicio que afecten a nuestras instituciones.

- IRIS-CERT quiere trabajar en la ampliación de los mecanismos reputación para su uso en filtrado de direcciones IPs en diversos entornos. Adermás, quiere comenzar a trabajar en el uso de RPZ (Response Policy Zones) para el bloqueo de dominios maliciosos utilizados por el malware activo en nuestra red.

- Mejora continua de los sistemas de detección proactiva desde RedIRIS, principalmente basados en flujos de red.

4 Autores

Equipo de Serguridad de RedIRIS
Servicio IRIS-CERT
cert@rediris.eshttp://www.rediris.es/cert
Claves PGP: http://www.rediris.es/servicios/keyserver/
Dpt. RedIRIS. - Entidad Pública empresarial Red.es
Plaza M. Gómez Moreno s/n. Edificio Bronce, 2ª planta. 28020 Madrid.
Tel:+34 91 212 76 25 Fax:+34 91 212 76 35