Informe de incidentes de seguridad año 2002

cert@rediris.es

13 de enero de 2003

Índice

1. Introducción

Este informe de incidentes de seguridad pretende reflejar los aspectos más relevantes detectados en la gestión de incidentes de seguridad gestionados por el grupo de seguridad de RedIRIS, IRIS-CERT, durante el año 2002.

Es nuestra intención que este informe actualizado sea presentado al menos una vez al año en la lista de coordinación de seguridad de RedIRIS, de forma que se pueda informar detalladamente de los problemas de seguridad a los responsables de las instituciones afiliadas y presentar una evolución continua de los incidentes de seguridad.

Además de las estadísticas, se presenta en este informe algunos enlaces de interés a los problemas más comunes,vulnerabilidades o gusanos detectados durante el año, de manera que los responsables de seguridad de las instituciones afiliadas puedan saber donde consultar para resolver los problemas.

Además, recomendamos echar un vistazo al informe correspondiente al periodo comprendido entre Octubre del año 2001 a Mayo del 2002 disponible aqui, donde además se hace un breve resumen de las posibles soluciones a los problemas de seguridad más frecuentas que se han producido y una descripción de los procedimientos y herramientas de ataque que con más frecuencia se han detectado a lo largo de este periodo.

Con toda seguridad este informe presenta bastantes lagunas que esperamos ir solucionando a lo largo del tiempo, hasta que refleje de una forma fiable los problemas de seguridad existentes.

2. Estadísticas

Todas estas cifras son orientativas puesto que los sistemas de gestión que actualmente utilizamos hace que no podamos presentar unas estadísticas completas, sino solamente unos esbozos de los principales problemas de seguridad que hemos detectado. Esperemos que esto cambie cuando implantemos el RT como herramienta de gestión de incidentes y realicemos paralelamente unas estadísticas más en consonancia con las necesidades reales de nuestra audiencia.

En estas estadísticas solamente aparecen aquellos problemas de seguridad de los que tenemos directamente noticia. En otras ocasiones y ante la infección de gusanos hemos conseguido poner logs en los routers para poder detectar máquinas infectadas e informar a los implicados lo antes posible para evitar males mayores.

Algunos de los datos más significativos son:

- El número de incidentes atendidos por IRIS-CERT durante el año 2002 ha sido de 1495, lo que implica un incremento del 44.02 % con respecto al año anterior (se atendieron unos 1038 incidentes). Nos ha sorprendido este incremento tan "bajo"si lo comparamos con los incrementos de los años anteriores (113.333 % en el 2000 con respecto al 1999, 149.51 % en el 2001 con respecto en el 2000), puesto que han sido muchos los problemas de seguridad, sobre todo a lo que a gusanos se refiere, que hemos detectado durante el presente año. Si tenemos en cuenta que en el informe de gestión de incidentes presentado en los GT de Madrid de Junio de 2002 estábamos hablando de 764, nos parece poco el haber atendido unos 731 entre Julio y Diciembre (más si pensamos que en

Julio el Code Red dio mucho trabajo y que en Septiembre el Slapper, el Opaserv y el Bugbear han tenido gran repercusión en la comunidad RedIRIS). La conclusión a que llegamos es que hemos atendido un promedio de 3 quejas por incidente y como contabilizamos los incidentes por IP el número que presentamos no refleja el gran trabajo que hemos dedicado a la atención de incidentes durante el año 2002.

- Durante el 2002, 1392 incidentes han involucrado a instituciones afiliadas, esto es, sólo 103 de los incidentes atendidos no tienen nada que ver con la red académica y de investigación española, afectando a máquinas del dominio .es del que de momento también somos responsables dando soporte de gestión de incidentes.

- Más de la mitad de los 1392 incidentes que han involucrado a instituciones afiliadas han sido denuncias (la mayoría de los casos desde fuera de España) de equipos atacantes o comprometidos dentro de nuestra comunidad (un total de 846, es decir, un 56 % de esos 1392).

- En cuanto a incidentes de ámbito internacional (en origen o destino) hemos atendido 1381 (un 92 %). Como hemos comentado anteriormente, sobre todo han sido situaciones en las que se ha recibido una denuncia desde el exterior relativa a un equipo de la red académica.

- También hemos recibido correos en los que aparecía la dirección de IRIS-CERT como Copia (Cc:), bien desde dentro de nuestra comunidad o desde grupos de seguridad internacionales. Nuestra política ante este tipo de incidentes, como comentamos en los últimos grupos en Madrid, es que no los atendemos directamente sino que anotamos el origen para fines estadísticos y no nos involucramos en su resolución a no ser que se nos lo pida expresamente.

- En el 2002 hemos atendido 20 incidentes de SPAM, lo que no quiere decir que no haya habido más. Lo que ocurre es que estos 20 incidentes corresponden a los meses de Enero a Junio puesto que como comentamos en los GT 2002 de Madrid, IRIS-CERT ya no se iba a ocupar de este tipo de incidentes, pasando su gestión al responsable de correo electrónico en la comunidad Jesús Sanz de las Heras.

- Hemos recibido, así mismo, unos 50 incidentes relacionados con problemas de Copyright. IRIS-CERT no ha abierto incidente relacionado con

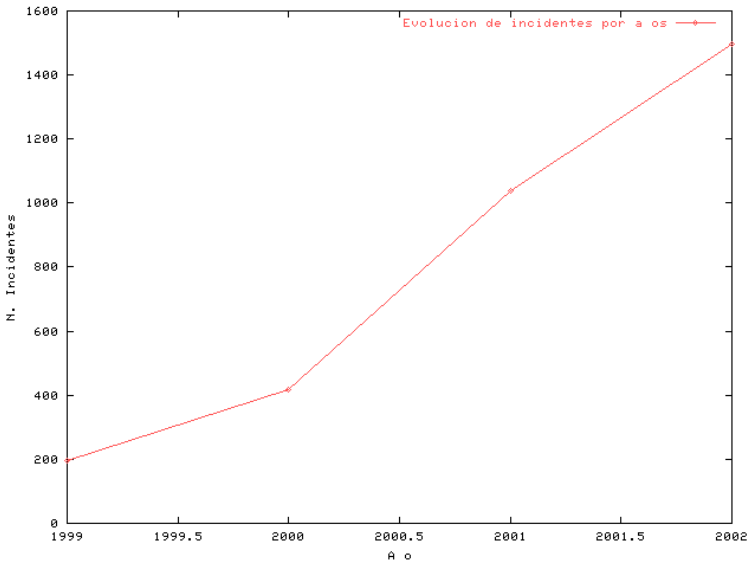

Figura 1: Evolución de incidentes por años

este tema, pero si que ha redirigido este tipo de mensajes a su punto de contacto en la Universidad o centro afiliado para que sean ellos los encargados de gestionarlos según sus políticas internas.

2.1. Evolución de los incidentes

En la figura anterior, se observa la evolución de los incidentes de seguridad desde el año 1999. En 1999 se atendieron 195 incidentes, en el 2000 416 (un 113.333 % más que en el año anterior), en el 2001 1038 (un 149.51 % más que el 2000). En el 2002, como se os ha comentado anteriormente, se han atendido 1495.

Observamos un incremento significativo de incidentes a partir del año 2001. Este incremento se corresponde fundamentalmente con la aparición, en verano de ese año, de problemas de seguridad asociados con servidores Internet Information Server de Microsoft y con la aparición de los gusanos Code Red y Nimda.

Hay que indicar además que gran la mayoría de los incidentes de seguridad se producen tras la recepción de un correo o queja de denuncia desde el exterior de las instituciones de RedIRIS, sobre todo debidas a escaneos de

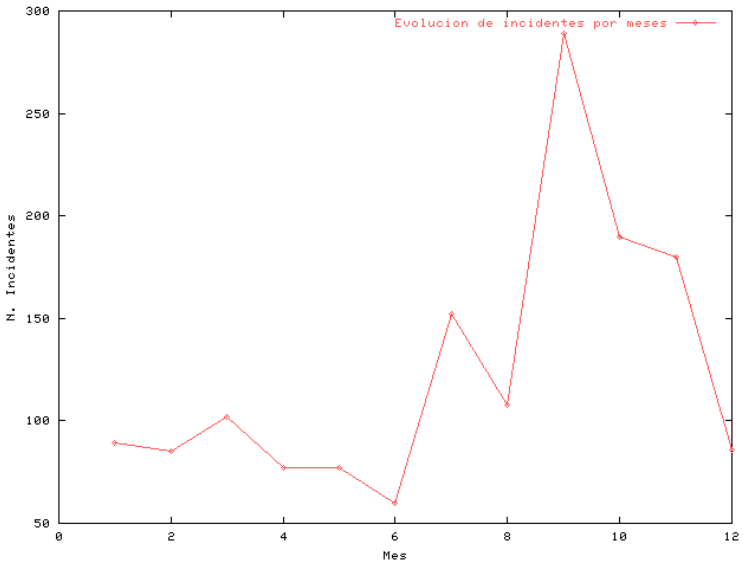

Figura 2: Evolución de incidentes por meses

puertos o pruebas , por lo que los escaneos, sobre todo los provocados por este tipo de gusanos son los informes más numerosos.

Como ha pasado hasta ahora es de esperar que la tendencia a lo largo de los años sucesivos, sea de incremento cada vez mayor de incidentes.

En la anterior gráfica podemos ver la proporción de incidentes atendidos por IRIS-CERT durante este año y distribuida por meses.

Los datos detallados son los siguientes:

Fecha	**Total**	**%**	**P. Baja**	**P. Normal**	**P. Alta**	**P. Emergencia**
2002/01	89	5 %	19	12	5	0
2002/02	85	5 %	26	11	48	0
2002/03	102	6 %	34	28	40	0
2002/04	77	5 %	31	13	33	0
2002/05	77	5 %	8	30	39	0
2002/06	60	4 %	25	9	26	0
2002/07	152	10 %	65	27	60	0
2002/08	08	7 %	81	6	21	0
2002/09	289	19 %	72	21	196	0
2002/10	190	12 %	27	37	126	0
2002/11	180	12 %	88	27	65	0
2002/12	86	5 %	39	25	22	0

El mayor incremento de incidentes lo detectamos en Septiembre con un total de 289 incidentes atendidos en este mes. Es en este mes cuando empiezan a aparecer por una parte el Slapper (Apache/mod_ssl Worm), que comenzó a propagarse por Internet sobre el 13 de Septiembre y que afecta a máquinas Linux que corren el Apache con el OpenSSL activo. Otro gusano que empieza a propagarse a finales de este mes de Septiembre (sobre el 29 o 30 de dicho mes) es el Bugbear, alias Tanatos. En este caso, el gusano se propaga a través de mail y de recursos compartidos de redes locales. Además tiene capacidad de desactivar software de seguridad y antivirus en las máquinas que infecta, así como la instalación de un backdoor que escucha en el puerto 36794/tcp. En Octubre la mayoría de informes que recibimos sobre escaneos al puerto 137/tcp, no se debían a Bugbear como al principio pensábamos, sino a un nuevo gusano llamado Opaserv que también se replica a través de recursos compartidos.

El impacto de estos gusanos (fundamentalmente del Bugbear) en la comunidad RedIRIS ha sido muy grande. El gusano Bugbear ha sido responsable de distintos problemas de DoS (Denegación de Servicio) en los routers troncales de la red académica y cortes en algunos de los centros afiliados.

En Mayo también apareció un gusano que esta vez afectaba a servidores SQL de Microsoft con la cuenta de usuario "sa"sin password. La repercusión de este gusano no ha sido tan evidente como la de los anteriores en nues-

tra comunidad, pero aun a finales de año se siguen recibiendo denuncias relacionas con infecciones de este gusano en la comunidad RedIRIS, caracterizadas por escaneos generalizados al puerto 1433/tcp. El objetivo de este gusano es obtener una relación de los usuarios del sistema y sus contraseñas, así como datos sobre la red y la configuración de las BDs instaladas en la máquina infectada.

Si observamos el pico que muestra la figura en el mes de Julio, se debe al que podíamos denominar el gusano del verano 2002. Este gusano afecta a servidores NT y Windows 2000 con el servidor Index Server, instalado por defecto con el Internet Information Server (también instalado este último en muchas ocasiones por defecto). Este gusano del verano 2002 no era otro que el conocido el Code Red que ya apareció el año pasado.

Aún a finales de año se sigue detectando actividad de los gusanosi mencionados en esta sección (Slapper, Bugbear, Code Red, SQLsnake e incluso Nimda que, como el Code Red, empezó a propagarse en el año 2001).

En figura 3 se muestra la distribución de los incidentes atendidos por IRIS-CERT durante el año 2002 clasificados según la prioridad asignada (se puede consultar el criterio de prioridad que sigue el equipo aquí).

Esta gráfica no es realmente significativa puesto que la mayoría de los incidentes de seguridad se producen tras la recepción de un correo de queja o denuncia que en la mayoría de los casos se refiere a escaneos de puertos o pruebas. Estos escaneos, en los últimos tiempos, en muchos casos estaban relacionados con máquinas comprometidas por algún gusano de los comentados anteriormente (por el tipo de puerto indicado en la denuncia). En definitiva, muchos de los incidentes que se catalogan como escaneos (prioridad de baja a normal) al final son gusanos (prioridad alta) y algunos de los incidentes que se catalogan como gusanos al final se deben a escaneos simples. En los últimos tiempos hemos intentado catalogar de primeras como gusanos aquellos que mostraban escaneos a puertos relacionados con puertos de propagación de los gusanos activos en ese momento.

También tenemos que decir que la existencia de diversos mecanismos de denuncia automáticos, como http://www.dshield.org, o http://aris.securityfocus.com, hacen que se reciban cada vez más incidentes relacionados con escaneos de puertos y por tanto se incremente el porcentaje de incidentes de prioridad baja y normal.

La distribución de los incidentes atendidos por IRIS-CERT durante el

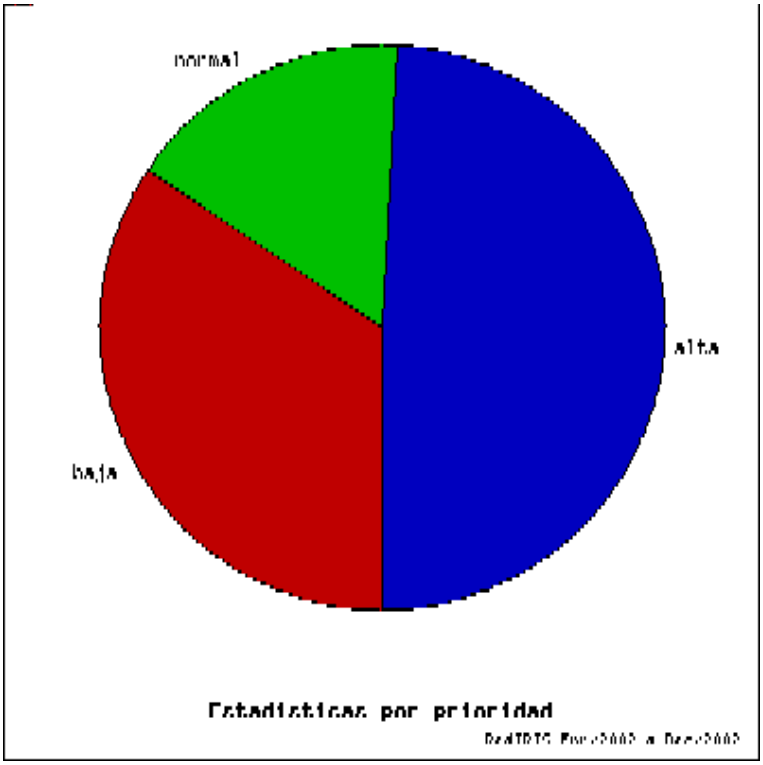

Figura 3: Porcentaje de incidentes por prioridad alcanzada

2002 en función a la prioridad alcanzada es la siguiente:

Prioridad	**Cantidad**	%
Baja	515	34 %
Normal	246	17 %
Alta	734	49 %
Emergencia	0	0 %

En la siguiente tabla aparecen reflejada el porcentaje de cada uno de los incidentes clasificados a partir del primer mensaje que se recibe. Es decir, si inicialmente se recibe un mensaje indicando un escaneo de puertos, el incidente se clasifica como un escaneo, aunque posteriormente al investigar se observe que se trata de un acceso a un equipo y se proceda a investigar el incidente[1].

Tipo de Incidente	**Cantidad**	%
Denegación de Servicio	23	2 %
Portscan	706	47 %
Acceso a cuentas privilegiadas	96	6 %
Troyanos	3	0 %
Gusano	619	41 %
Uso no autorizado	22	2 %
Otros	26	2 %

Las denuncias de uso no autorizado se han debido fundamentalmente a equipos Proxies mal configurados que permiten conexiones a equipos externos a la organización.

En cuanto a los incidentes catalogados como Otros, se han debido fun-

[1] Ya hemos comentado anteriormente que en los últimos tiempos hemos intentado catalogar de primeras como gusanos aquellos que mostraban escaneos a puertos relacionados con puertos de propagación de los gusanos activos en ese momento

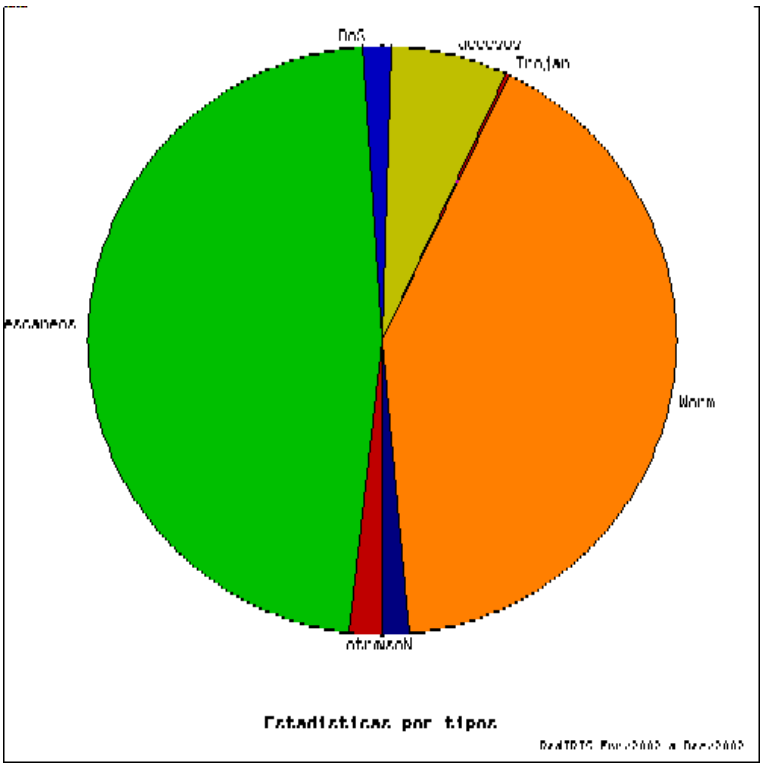

Figura 4: Porcentajes de incidentes

damentalmente a insultos o amenazas utilizando medios telemáticos, aunque en este caso nosotros lo que recomendamos es que los afectados se pongan en contacto directamente con la Policía y Guardia Civil. También se han catalogado dentro de este grupo incidentes referentes a Warez.

En cuanto a los referente a Troyanos sobre todo se han atendido incidentes relacionados con el BackOrifice.

Como se aprecia en la tabla, las denuncias por gusanos han sido muy frecuentes (un total de 619) debido a la proliferación durante este año de una variada gama de ellos (Slapper, Bugbear, Opaserv, SQLsnake,..), y a que continúan activos gusanos ya aparecidos en años anteriores (Code Red o Nimda).

En la figura 4, aparecen de una forma más clara los siete tipos más importantes de incidentes gestionados. Se observa de una forma más clara como los incidentes debidos a escaneos y a gusanos han supuesto un 88 % de los

incidentes gestionados.

En cuanto a los servicios más escaneados durante este año 2002, en máquinas Linux hemos detectado sobre todo escaneos a los puertos asociados a los servicios SSH y FTP y en menor medida al servicios RPC.

En cuanto a máquinas Solaris y debido a las vulnerabilidades descubiertas en diversos servicios RPC, los puertos más escaneados has sido los asociados con este tipo de servicio, sobre todo servicios auxiliares de los procesos de entorno gráfico y servidor de impresión.

A principios de Octubre apareció un programa que implementaba un ataque contra diversas implementaciones de SSH y que afectaba a diversos fabricantes y a la versión 1 del protocolo. En Junio de este año, se hicieron públicas diversas vulnerabilidades en el OpenSSH

Los servidores FTP, sobre todo los basados en la distribución de la Universidad de Washington (wu-ftpd) han tenido diversas vulnerabilidades en los últimos tiempos y siendo el ftp el blanco perfecto para los atacantes. Estas vulnerabilidades afectan a versiones del FTP sobre e distintas plataformas.

Los advisories donde se describen con detalle las vulnerabilidades asociadas con los servicios blanco de los atacantes durante el año, se detallan a continuación[2]:

- SSH (22/tcp)
  - http://www.cert.org/incident_notes/IN-2001-12.html
  - http://www.cert.org/advisories/CA-2002-18.html
- FTP (21/tcp)
  - http://www.cert.org/advisories/CA-2001-33.html
  - http://www.cert.org/advisories/CA-2001-07.html
- RPC (dtspcd, cmsd, tddserver)
  - http://www.cert.org/advisories/CA-2002-26.html
  - http://www.cert.org/advisories/CA-2002-20.html
- LPR (515/tcp)
  - ttp://www.cert.org/advisories/CA-2001-30.html

[2]Algunos advisories de los detallados a continuación corresponden a vulnerabilidades aparecidas ya en el año 2001

3. Links de interés

A continuación podéis encontrar algunos enlaces a documentos donde se describen algunos de los gusanos que han estado activos durante el año 2002:

1. Code Red
   - http://www.cert.org/advisories/CA-2001-19.html
   - http://www.cert.org/advisories/CA-2001-23.html
2. Code Red II
   - http://www.cert.org/incident_notes/IN-2001-09.html
3. Nimda
   - http://www.cert.org/advisories/CA-2001-26.html
4. Slapper
   - http://www.cert.org/advisories/CA-2002-27.html
5. Bugbear
   - http://www.f-secure.com/bugbear/
6. Opaserv
   - http://www.f-secure.com/opaserv/
7. SQLsnake
   - http://www.cert.org/incident_notes/IN-2002-04.html

4. Información adicional

4.1. Envío de información a IRIS-CERT

Muchas veces la notificación que se envía relativa a un escaneo de puertos o ataque sin importancia se convierte en realidad en un incidente más serio en el cual un atacante exterior ha conseguido acceder a una cuenta privilegiada del sistema (tradicionalmente lo que se conoce como un “root compromise”,

en Unix) y posteriormente se instalan determinadas herramientas por el atacante para ocultar su acceso y atacar a otros equipos.

Desde IRIS-CERT creemos conveniente realizar un estudio detallado de este tipo de incidentes, para intentar averiguar en la medida de lo posible las acciones realizadas por los atacantes, herramientas empleadas, y así poder aconsejar a los responsables de la institución las medidas a emplear.

Así, si en el estudio se detecta la presencia de un programa captura de tráfico (sniffer), es aconsejable alertar a los usuarios de la organización en general y a aquellos usuarios que aparecen en el fichero resultados del sniffer en particular que deben cambiar sus claves de acceso, para evitar que el atacante emplee estas claves con posterioridad para otros accesos.

Además el estudio de las herramientas usadas por los atacantes nos permite aconsejar en otras situaciones similares a otros responsables sobre los pasos a seguir para detectar un ataque.

Por ultimo muchas veces los programas utilizados para atacar a otros sitios mantienen un registro de los ficheros que se han atacado con éxito, pudiendo de esta forma avisar a los administradores de estos equipos del ataque, evitando así la propagación del ataque.

En los correos que se envían relativos a equipos posiblemente atacados se suele indicar una reseña a la Guia de recuperación de incidentes donde se indican los pasos a seguir.

Básicamente se le solicita a los administradores de los equipos que envíen:

1. Salida de la ejecución de comandos del sistema ("ps -aex","netstat -a",etc).

2. Ficheros de logs del equipo donde aparezcan los binarios instalados en el equipo.

3. Ficheros binarios (rootkit), instalados por el atacante para disimular el ataque.

4. Ficheros (logs, programas,código fuente, etc), instalados en directorios ocultos por los atacantes para atacar a otros equipos.

Esta información debe ser enviada al grupo de seguridad de RedIRIS, vía correo-e, cuando se trata de poca información o empleando uno de los siguientes medios:

- Por FTP, depositando el fichero en el directorio incoming del servidor FTP de RedIRIS
- vía HTTP, Utilizando Nuestra zona en el BSCW

En RedIRIS procederemos a analizar los ficheros que se nos envíen y enviar a los administradores la información que se pueda obtener de estos ficheros.

4.2. Recursos de coordinación de Seguridad

Como resumen, algunos enlaces que deben ser de sobre conocidos por todos aquellos que lean este documento, aunque no este de mas volver a citarlos:

- Página principal del CERT de RedIRIS
- Lista de coordinación de seguridad, IRIS-CERT, en esta lista deberían estar como mínimo una persona o responsable de cada una de las instituciones afiliadas, de forma que puedan recibir la información y alertas de seguridad que vayan surgiendo, antes de que se produzcan.

  En la actualidad muchas organizaciones afiliadas a RedIRIS no cuentan con una dirección de contacto de seguridad, lo que provoca que muchas veces se envíe directamente al PER de la organización los avisos de seguridad.
- Formulario de atención de incidentes, disponible en el servidor FTP de RedIRIS con indicación de la información a enviar ante un incidente de seguridad.
- Documentación de seguridad en el servidor de RedIRIS, http://www.rediris.es/cert/doc Recopilación de información de seguridad para diversos aspectos, instalación segura de equipos, análisis de ataques, etc.
- Listado de grupos de seguridad Europeos, http://ti.terena.nl/, para la búsqueda de grupos de seguridad en otros países.
- Lista pública de seguridad en castellano, CERT-ES@listserv.rediris.es, para consultas generales de seguridad.