XVII Grupo de Coordinación

IRIS- CERT

Informe de Operación

Logroño, 24 de Octubre, 2005

Agenda

Informe de operación IRIS-CERT

Nuevas iniciativas

- **EnREDA** (Entorno de Recogida de Evidencias Digitales y Análisis)
- **ANAMARIS** (ANálisis de Actividad MAliciosa y Respuesta a IncidenteS)
- **ACRI** (Almacén Colaborativo de Reglas de Intrusión)

La Política de Seguridad de Red de la Universidad de Castilla-La Mancha. Evangelino Valverde Álvarez (UCLM)

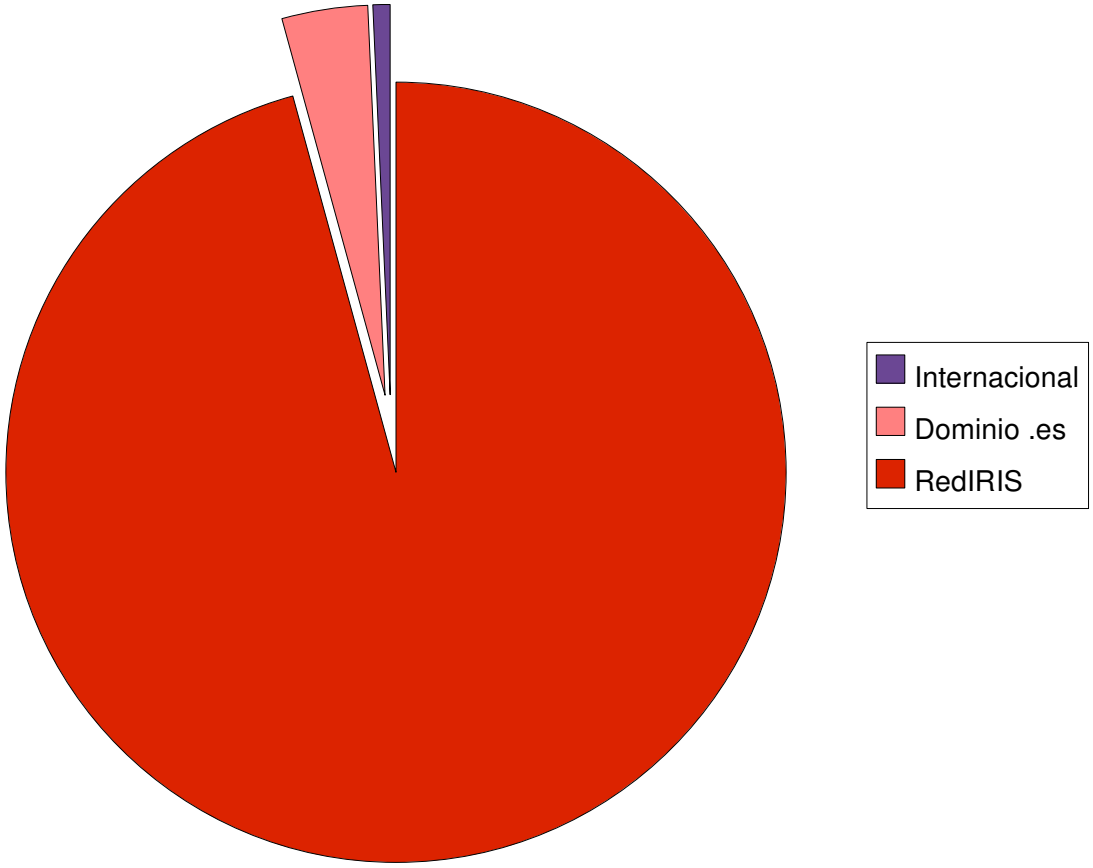
Los CERTS académicos y su aportación a la sociedad. Juan Carlos Guel López (CUDI - Universidad de Méjico)

Incidentes totales: 1013 (30%↓)

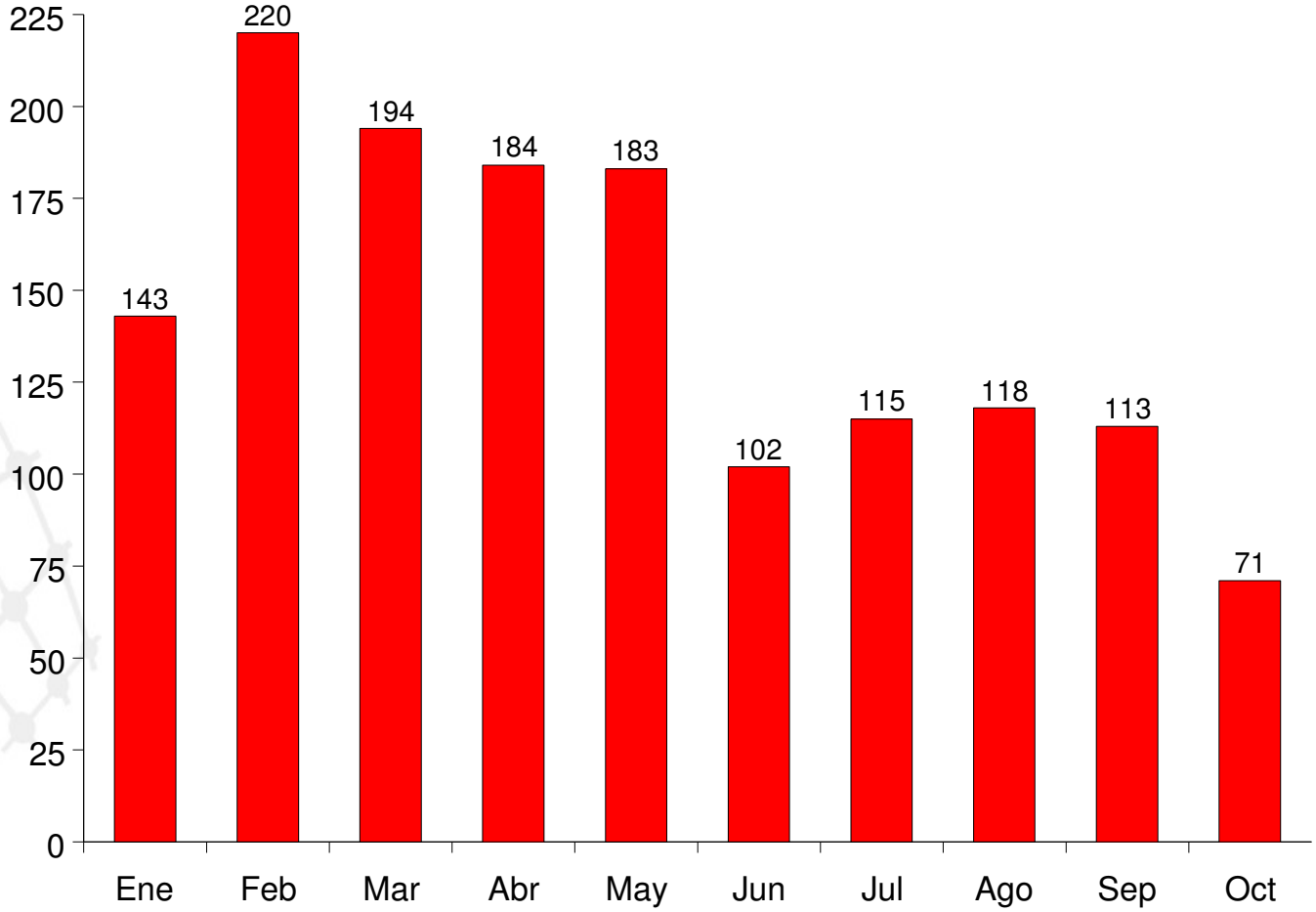
- Infracción de copyright: 346
- Correos como Cc: 17
- *Helpdesk*: 41
- Informativos:26

Total: 1443 (36%↓)

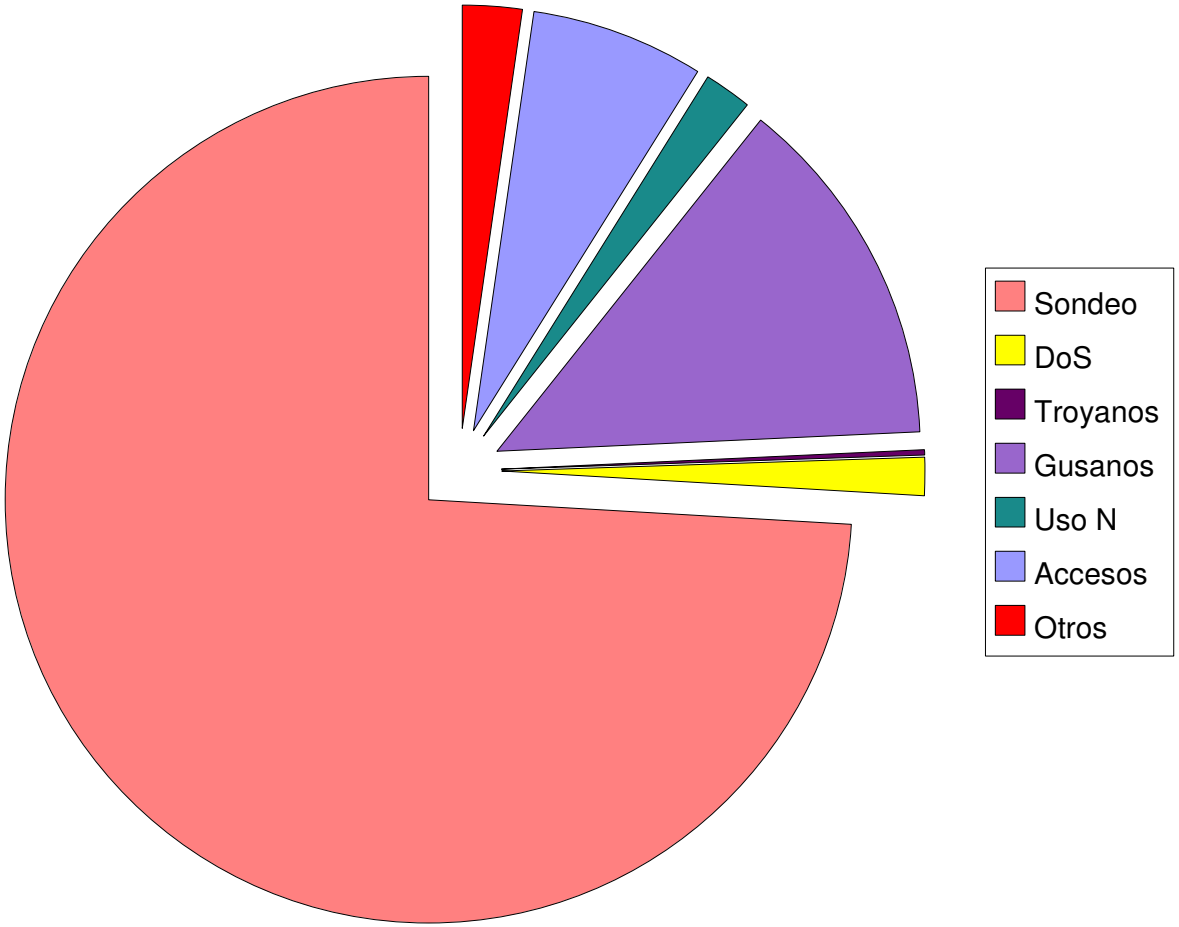
Informe de Incidentes
Enero-Octubre 2005



Informe de Incidentes
Enero-Octubre 2005



Informe de Incidentes
Enero-Octubre 2005



Otras cosas

GN2-JRA2 (Security)

- Pruebas distintas herramientas de análisis de flujos (NERD, NFSEN, ...)

Proyecto RTIR

- Firmado contrato BestPractical ampliación de funcionalidades RTIR

Repositorio Políticas de Seguridad

- http://www.rediris.es/cert/links/politicas.es.html

IV Foro de Seguridad, 30-31 Marzo 2006 (San Sebastián) - EHU

- Seguridad en Wireless

Cursos SANS

- Descuentos comunidad académica

Y más cosas

Nuevos recursos sobre cómo formar un CERT

- http://www.rediris.es/cert/links/csirt.es.html
- CSIRT Starter Kit

  http://www.terena.nl/tech/task-forces/tf-csirt/starter-kit.htm
- CSIRT mentoring

  http://www.terena.nl/tech/task-forces/tf-csirt/mentoring.htm
- TRANSITS (Training of Network Security Incident Teams Staff)

  http://www.ist-transits.org/

Informe anual de 2005 disponible Enero 2006

- http://www.rediris.es/cert/doc/informes/

EnREDA (Entorno de Recogida de Evidencias Digitales y Análisis)

Disponer de un entorno para la realización de análisis forense en sistemas vivos y muertos

Coordinación

- Rafael Calzada (UC3M) + IRIS-CERT

Estado

- En desarrollo

Foro técnico especializado con el objetivo de fomentar el análisis de actividad maliciosa y dar respuesta a incidentes de forma coordinada en la comunidad

Objetivos

- Mejorar la detección temprana de actividad maliciosa
- Analizar nuevas amenazas y estudiar sus contra- medidas
- Respuesta coordinada de incidentes
- Correlación de actividad maliciosa
- Intercambio de técnicas, herramientas y scripts
- Transferencia de conocimiento al resto de la comunidad

Coordinación

- Carles Fragoso (CESCA) + IRIS- CERT

Miembros

- Administradores habituales de seguridad perimetral (IDS/ ADS externo, cortafuegos, enrutadores de borde, etc..)

Recursos

- Lista de distribución
- Repositorio/ BBDD de conocimiento (Wiki)

Estado

- Completada fase de constitucón de miembros
- Debate para la definición de objetivos y líneas de actuación
- Primeros contenidos en ANAMARIS- Wiki

Proyectos

- Sondas de monitorización de espacio IP oscuro (darknet)
- Listas negras IP/ DNS para la contención de máquinas infectadas
- Recogida automática de código malicioso (mwcollect)
- Heramientas de colaboración (IM, ToIP...)

http://www.rediris.es/cert/proyectos/anamaris.es.html