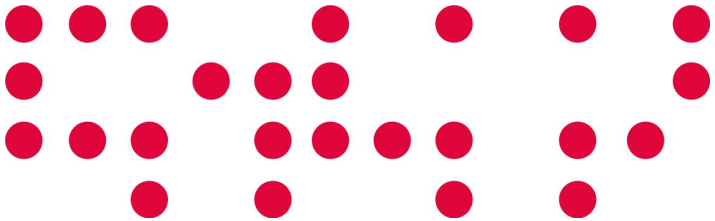
ASTIRIS-2B
Seguridad

Chelo Malagón
RedIRIS, IRIS-CERT

Córdoba, 15 de Noviembre de 2010

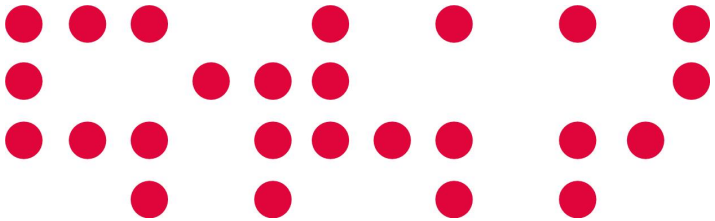
Índice



Informe IRIS-CERT

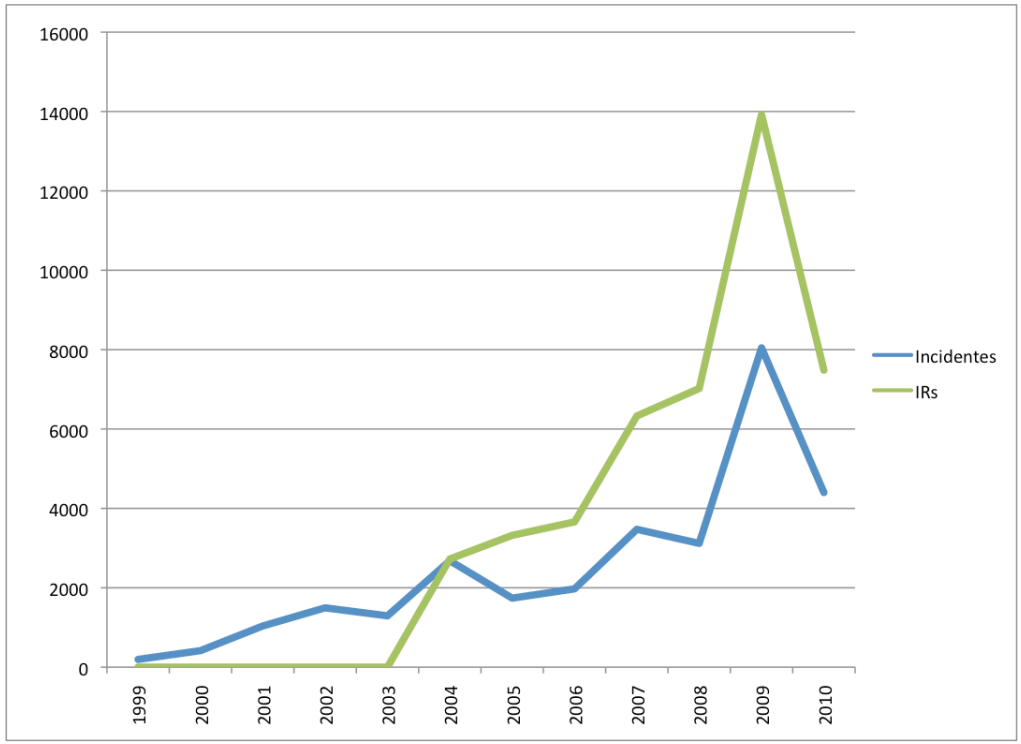
Índice

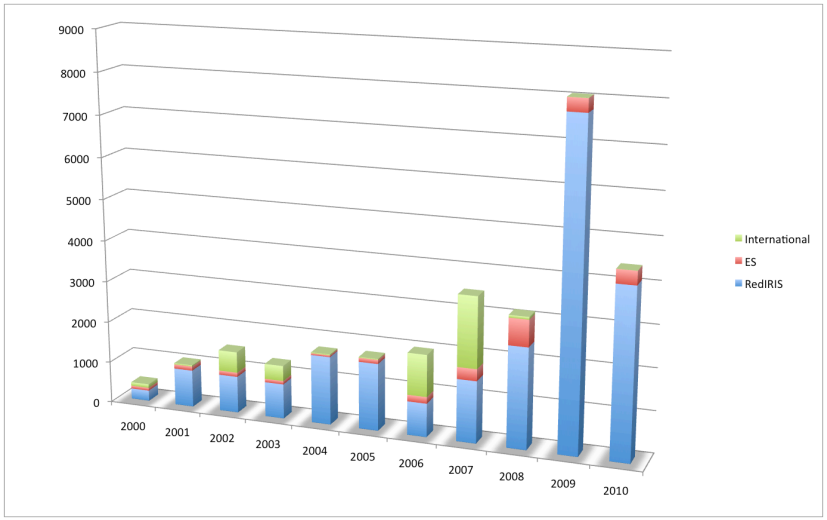
1. **Gestión de incidentes**
   - **Estadísticas**
   - **Procedimiento IH**
2. **Formación en seguridad 2011**
3. **Esquema Nacional de Seguridad**
   - **Estado del arte**
   - **Actuaciones**

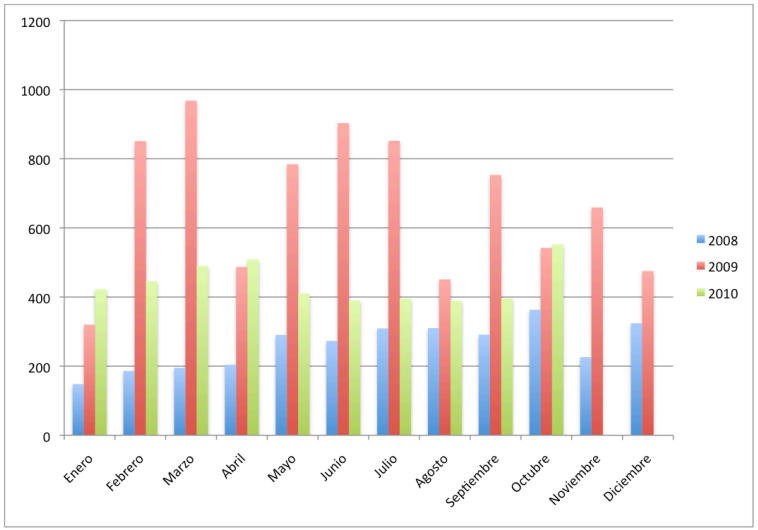


Gestión de incidentes
Estadísticas

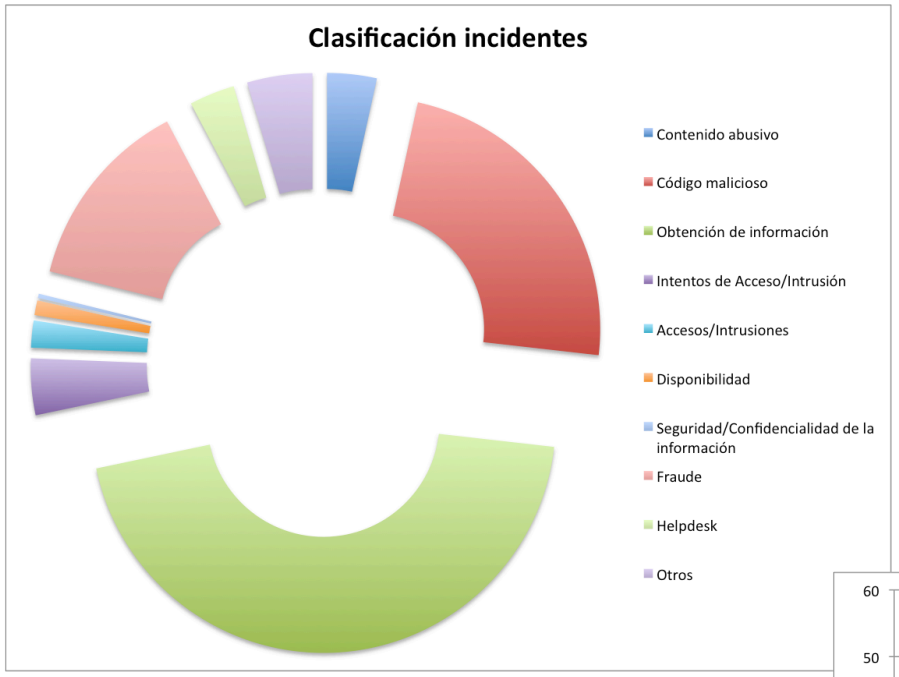
Incidentes 2010

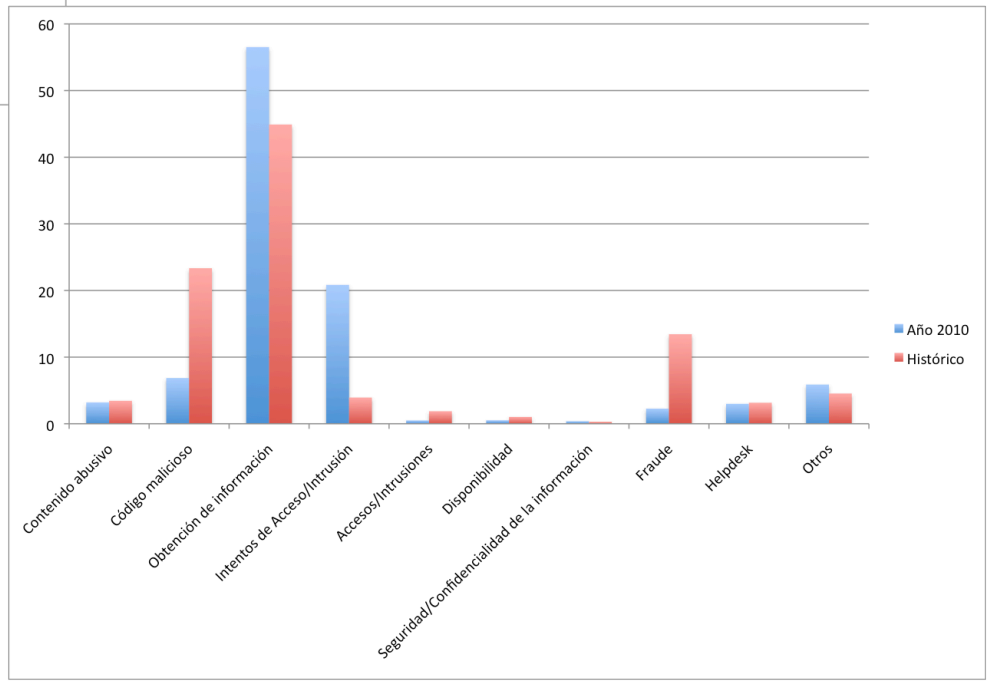




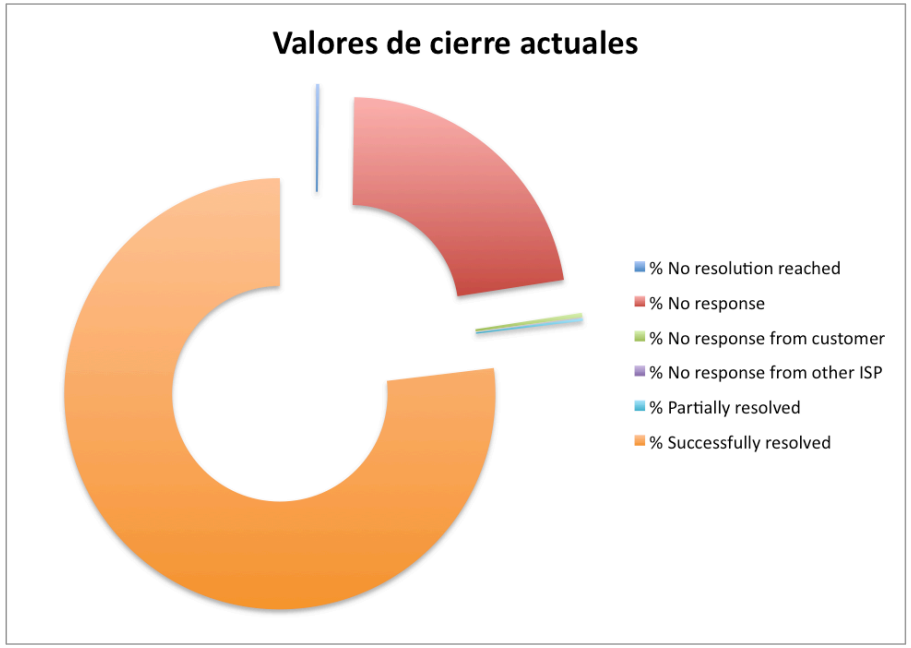


Incidentes 2010





Incidentes 2010



¡¡ Nuevos valores de cierre a partir de Enero de 2011 !!

Algunos incidentes

Troyanos Bancarios

- Acuerdo S21Sec (Sep 2010)
  - Credenciales de usuarios de dominios de las instituciones de RedIRIS infectados por troyanos
    - Subject: *[URGENTE] Datos capturados por troyano bancario*

id: 54595
bot_id: CEA935C463404EF_B4DF7611720BF6A2
botnet: -- default --
bot_version: 33556224
path_source: **http://campusvirtual.unauniversidad.es/path/index.php**
path_dest:
time_system: 1285765492
time_tick: 1308343
time_localbias: 3600
os_version: (language_id: 3082
process_name: C:\Archivos de programa\Mozilla Firefox\firefox.exe
process_user: CEA935C463404EF\Remi
type: 11
context: **http://campusvirtual.unauniversidad.es/path/index.php**
Referer: **http://campusvirtual.unauniversidad.es/path/**
User input: **El contenido de un mensaje con credenciales .... Eliminado ... cliu fwdku y fxsiut vdxk Dl hfdy eñoswxty dxeñojewxfíu ewfñoih xefñl xflih ivufec cfrigu cf**
Data:

username=**username**
password=**password**
ipv4: **IP_proveedor**
country: ES
rtime: 1285850807

Páginas Maliciosas - Google

- *"Google Safe Browsing Alerts for Network Administrators"*
  - http://googleonlinesecurity.blogspot.com/2010/09/safe-browsing-alerts-for-network.html
  - AS766
    - Subject: *Posible código malicioso en InstituciónX*

Reflexionando …

Protestas virtuales organizadas

Individuals appearing in public as Anonymous. (Scientology, Los Angeles, February 2008). The masks used in this demonstration are taken from the book and film V for Vendetta.

"Espero que el futuro de las protestas sea la ACCIÓN. No el andar en círculos con pancartas inútiles que todo el mundo ignora." (Anonymous)

SEGURIDAD | El Ministerio reconoció el ciberataque

Las páginas del Ministerio de Cultura y de la SGAE se 'caen' por un ciberataque

La SGAE, entre las páginas atacadas con éxito en la 'Operation Payback'.

CiberPaís | volver a tecnología

La 'Operación PayBack' tumba durante más de 68 horas tres webs españolas

El ataque de denegación de servicio también afecta a Promusicae, según Panda

TOMÀS DELCLÓS - Barcelona - 08/10/2010

CAMPAÑA EN INTERNET

Los correos de los diputados, saturados de mensajes contra la ley Sinde

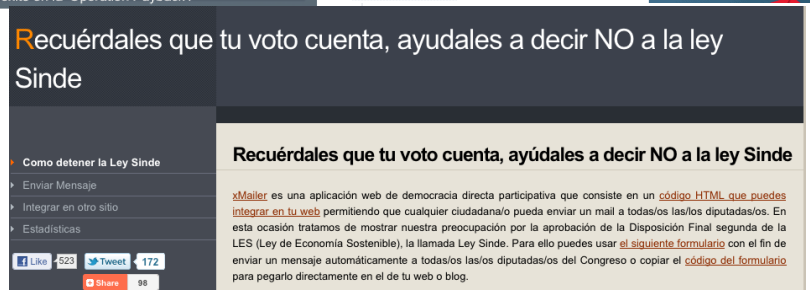
La ley que permitirá el cierre administrativo de las web de enlaces ha recibido contestación: más de 400.000 correos electrónicos enviados a los parlamentarios pidiendo que no se apruebe.

Televisores de plasma y LCD al mejor precio

2010-11-11 Imprimir Enviar Corregir Comentar

DANIEL RODRÍGUEZ HERRERA

Mediante **una herramienta** que permite enviar un mensaje a las cuentas de correo electrónico de todos los diputados –técnicamente equivalente a la de Hazte Oír para **enviar cartas al director**–, Hacktivistas.net ha logrado inundar de mensajes contra la Ley Sinde los correos de sus señorías. Desde que el lunes 8 de noviembre se pusiera en marcha los servidores del Congreso de los Diputados **han recibido más de 400.000 mensajes**.



((esRadio Emisión en D

INTERNET | En una lista publicada en 'The Pirate Bay'

Los datos de miles de usuarios de banda ancha en Reino Unido, 'colgados' en Internet

ELMUNDO.es | Madrid

Actualizado lunes 27/09/2010 **22:06 horas**

Los datos personales de cientos de usuarios de la compañía de banda ancha británica Sky han sido 'colgados' en Internet en **una lista en la que se incluye también una lista de las películas pornográficas que han compartido 'online'**.

Reforma del código penal (23 Diciembre 2010). Ley Orgánica 5/2010, de 22 Junio. Artículo 264

Pena de de 1 a 3 años – y multa- para los daños informáticos

(destrucción, alteración, inutilización o daño de datos, programas o documentos)

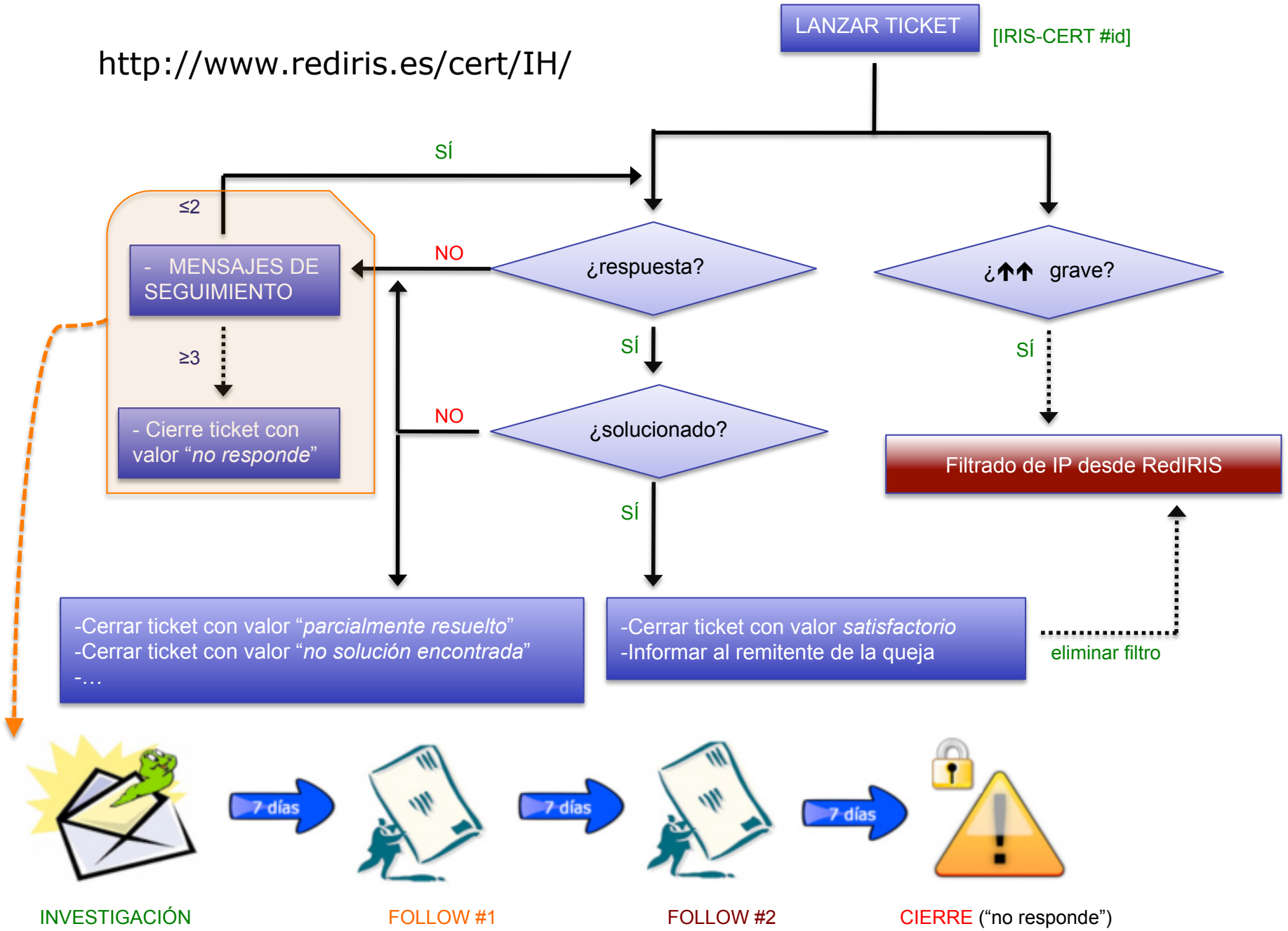
Vuestros usuarios pueden estar involucrados….

¿Tenemos que estar preparados?, ¿De que manera podemos dar respuesta?, ….

Gestión de incidentes
Política

Política de Atención de Incidentes

http://www.rediris.es/cert/IH/



Valores de cierre

IRIS-CERT encuentra la necesidad de distinguir el valor de cierre dependiendo de la resolución aportada por el origen del ataque.

Nuevos valores de cierre (operativos a partir de Enero 2011)

- Solucionado satisfactoriamente (aporta solución)
- Solucionado satisfactoriamente (no se aporta solución)
- Parcialmente resuelto
- Cierre ordenado por el cliente
- Falso positivo
- Problema no resuelto (se obtiene respuesta)
- Problema no resuelto (no se obtiene respuesta)

En el proceso de cierre del INCIDENTE se avisará a los destinatarios de la INVESTIGACIÓN con el valor de su resolución.

Los valores de cierre se utilizan para extraer indicadores institucionales (KPIs) → Panel de PERs.

http://www.rediris.es/cert/IH/

Formación en seguridad

Formación en seguridad 2011

Formación presencial en seguridad para el personal técnico de las instituciones de RedIRIS

- Impartido por personal de IRIS-CERT
- Dirigido al personal técnico de las instituciones de RedIRIS
- Instalaciones Red.es, GT, JJTT, instalaciones de centros y universidades voluntarias, …
- *Hands-on*
    - Aforo reducido
- Calendario anual orientativo publicado en la Web
- Certificados de asistencia
- Catálogo de cursos
    - RTIR
    - Análisis de flujos con nfsen/nfdump
    - Análisis de Malware
    - TRANSITS-I

Esquema Nacional de Seguridad

Esquema Nacional de Seguridad

Ley 11/2007, art 42: Esquema Nacional de Seguridad

- Establecer **Políticas de Seguridad** en la utilización de medios electrónicos
- Constituido por **principios básicos** y **requisitos mínimos** que permitan una protección adecuada de la información

Regulado en el **Real Decreto 3/2010**, de **8 de Enero 2010**

Ámbito de aplicación: Ley 11/2007, art 2

- Administración pública, ciudadanos en su relación con la administración pública y a las relaciones de las administraciones públicas entre sí
- ¿Es de aplicación en las Universidades Públicas?
  - **¡¡¡¡¡SI!!!!**
    - Administración Pública vinculada, que no dependiente, de las administraciones de las Comunidades Autónomas.

Adecuación de sistemas al ENS

- Los sistemas de las administraciones deberán estar adecuados al Esquema en el plazo de **doce meses**, aunque si hubiese circunstancias que impidan la plena aplicación, se dispondrá de un **plan de adecuación** que marque los plazos de ejecución (en ningún caso superiores a **48 meses** desde la entrada en vigor)

¿En que fase estáis? ¿estáis en alguna fase?

¿Que pensáis hacer? ¿pensáis hacer algo? ¿tenéis presupuesto? ¿solos o con ayuda?

¿Qué podemos hacer desde RedIRIS para ayudaros?

https://www.ccn-cert.cni.es/index.php?option=com_content&view=article&id=2420&Itemid=211&lang=es

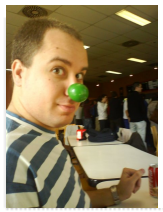
El superGRUPO

Diego R. Lopez
Coordinador
+34 95 505 66 23
diego.lopez@rediris.es

Carlos Fuentes Bermejo
CERT
+34 91 212 76 20
carlos.fuentes@rediris.es

Chelo Malagon Poyato
CERT
+34 91 212 76 20
chelo.malagon@rediris.es

Francisco Jesus Monserrat Coll
CERT
+34 91 212 76 20
francisco.monserrat@rediris.es



David Rodriguez Galiano
CERT
+34 91 212 76 20
david.rodriguez@soporte.rediris.es

MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

red.es

Edificio Bronce
Plaza Manuel Gómez Moreno s/n
28020 Madrid. España

Tel.: 91 212 76 20 / 25
Fax: 91 212 76
www.red.es