ASTIRIS-3B
CERT

Chelo Malagón y Francisco Monserrat

RedIRIS, IRIS-CERT

Valladolid, 29 de Noviembre de 2011

Índice

1. **Informe IRIS-CERT**

   Chelo Malagón (RedIRIS)
2. **Ejemplo de incidentes en las instituciones**
3. **Analizando algunos incidentes**
   1. **DNS recursivos**
   2. **Código malicioso en páginas Web**

   Francisco Monserrat (RedIRIS)
4. **Implantación del Esquema Nacional de Seguridad en la Administración. Caso práctico del Ministerio de Industria, Turismo y Comercio**

   Daniel Castillo Gusi (MITYC)

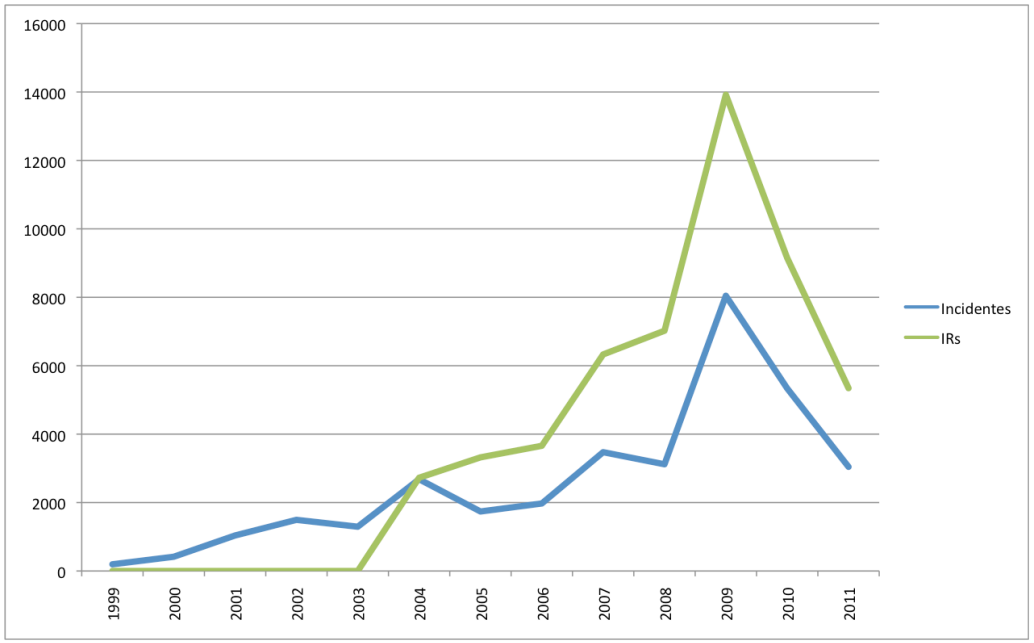
INFORME IRIS-CERT

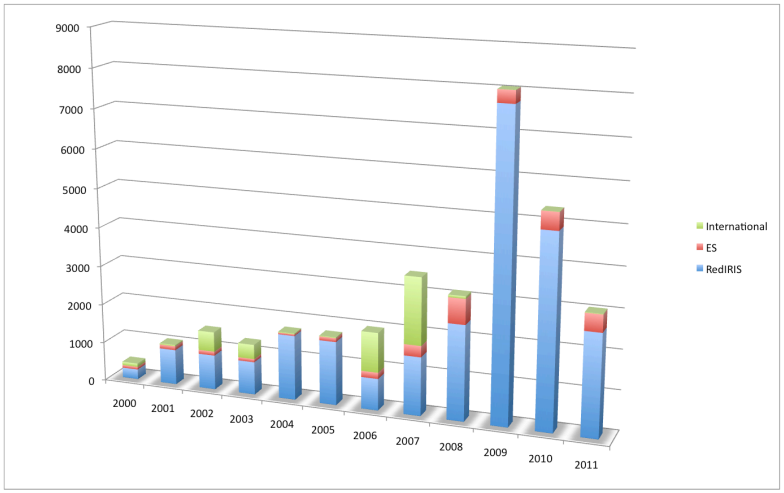
Índice

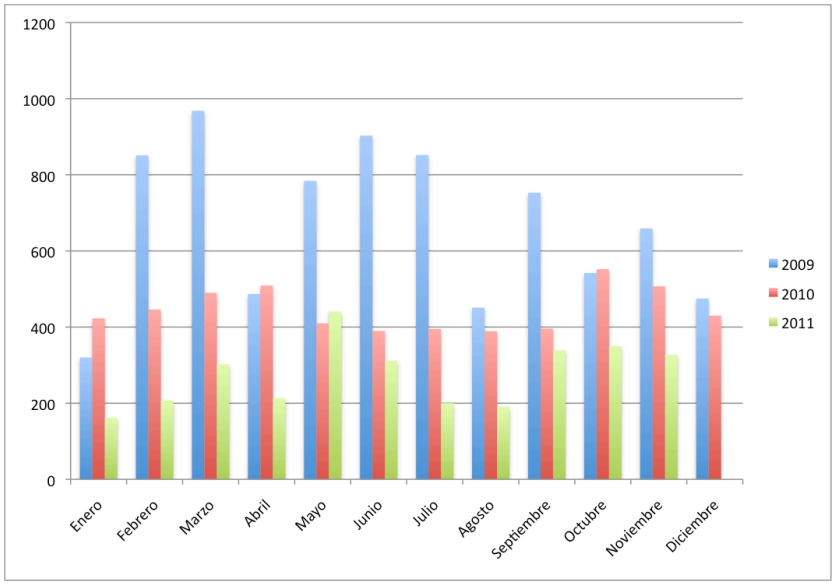
GESTIÓN DE INCIDENTES

ESTADÍSTICAS

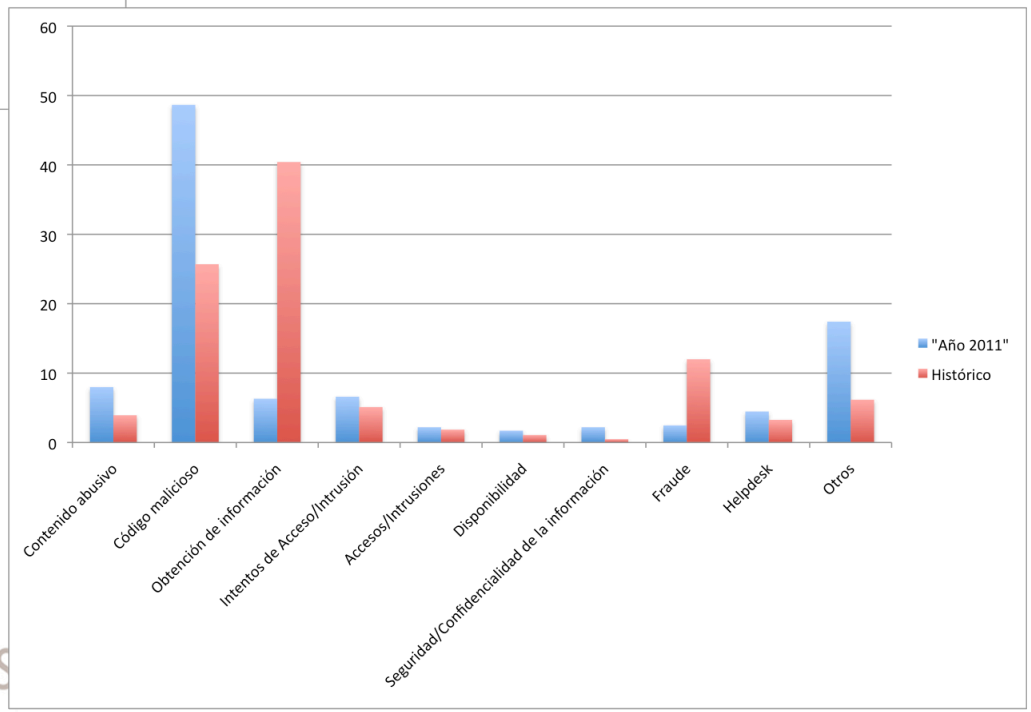
Incidentes 2011



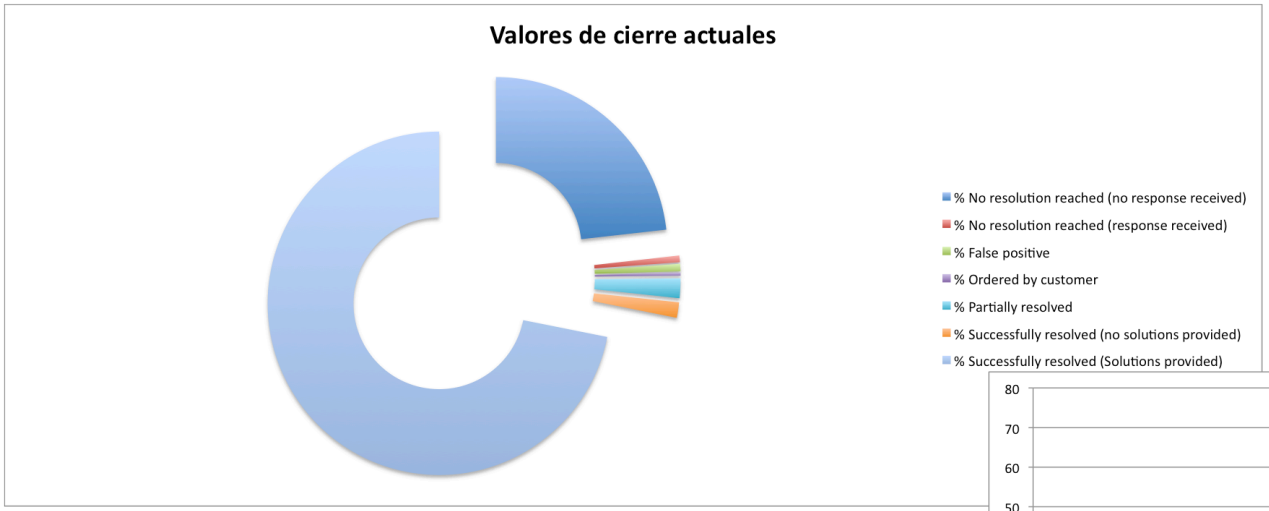




Incidentes 2011

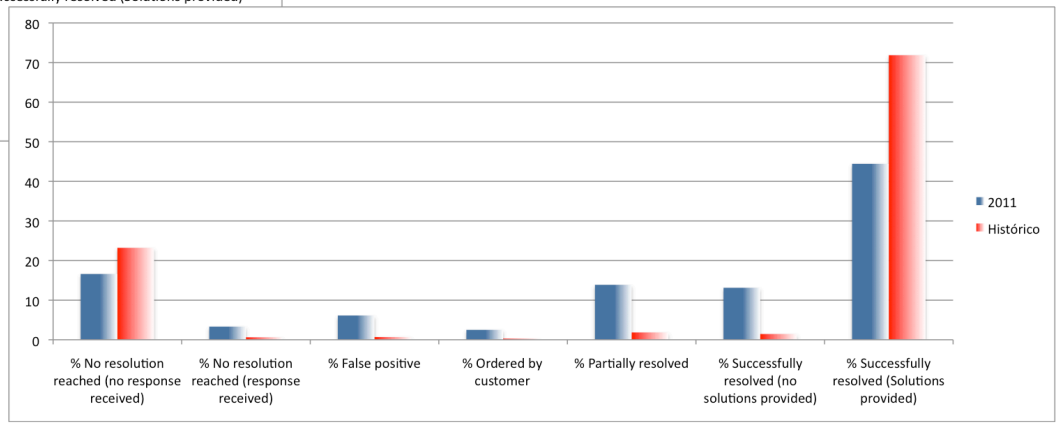


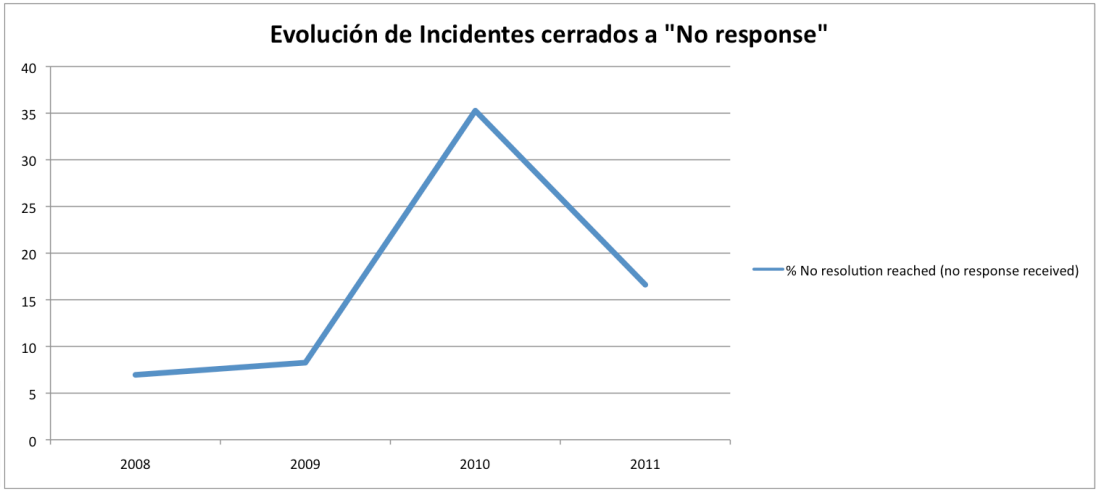
Incidentes 2011



Valor de cierre < año 2011	Valor de cierre > año 2011
Successfully resolved	Successfully resolved (solutions provided)
No resolution reached	No resolution reached (response received)
Partially resolved	Partially resolved
No response	No resolution reached (no response received)
No response from customer	
No response from other ISP	
---	Successfully resolved (no solutions provided)
---	Ordered by customer
---	False positive

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



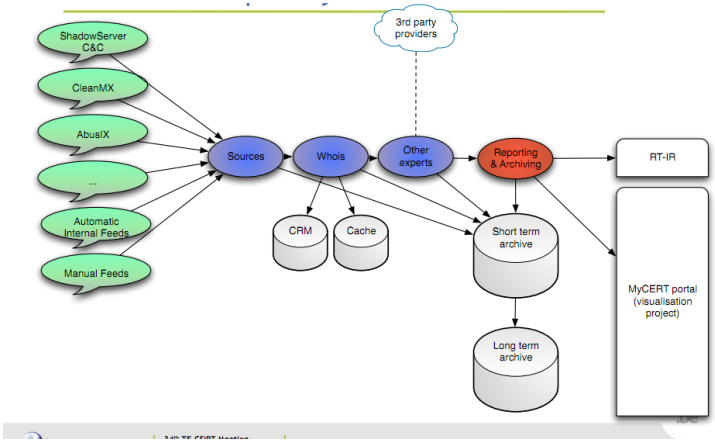


GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO
MINISTERIO DE CIENCIA E INNOVACIÓN
RedIRIS

Sistemas automáticos: Plugin Botnets

- Envío de alertas ante conexiones a servidores de C&C conocidos
  - http://sourceforge.net/apps/trac/nfsen-plugins/
- Fuentes públicas
  - Emergencythreads (ShadowServer)
    - http://rules.emergingthreats.net/blockrules/emerging-botcc.rules
  - aMaDa (abuse.ch)
    - http://amada.abuse.ch/blocklist.php
  - ZeusTracker (abuse.ch)
    - https://zeustracker.abuse.ch/
  - SpyEyeTracker (abuse.ch)
    - https://spyeyetracker.abuse.ch/
  - Fuentes propias

- **Problemas**
  - Gran cantidad de falsos positivos (11.78% del total)
    - Información incompleta (sólo IP)
    - **Solución** -> **Piloto de pruebas**
      - Al menos 2 instituciones voluntarias x 2 meses
      - A comenzar a principios de Febrero 2012
  - Gran cantidad de alertas (≈ 150xdía)
    - RedIRIS-Nova+Nuevas Fuentes
    - **Solución** -> Automatización
      - Inclusión del **AbuseHelper** en el workflow del RTIR (RTIRBot)
        - http://www.abusehelper.be/

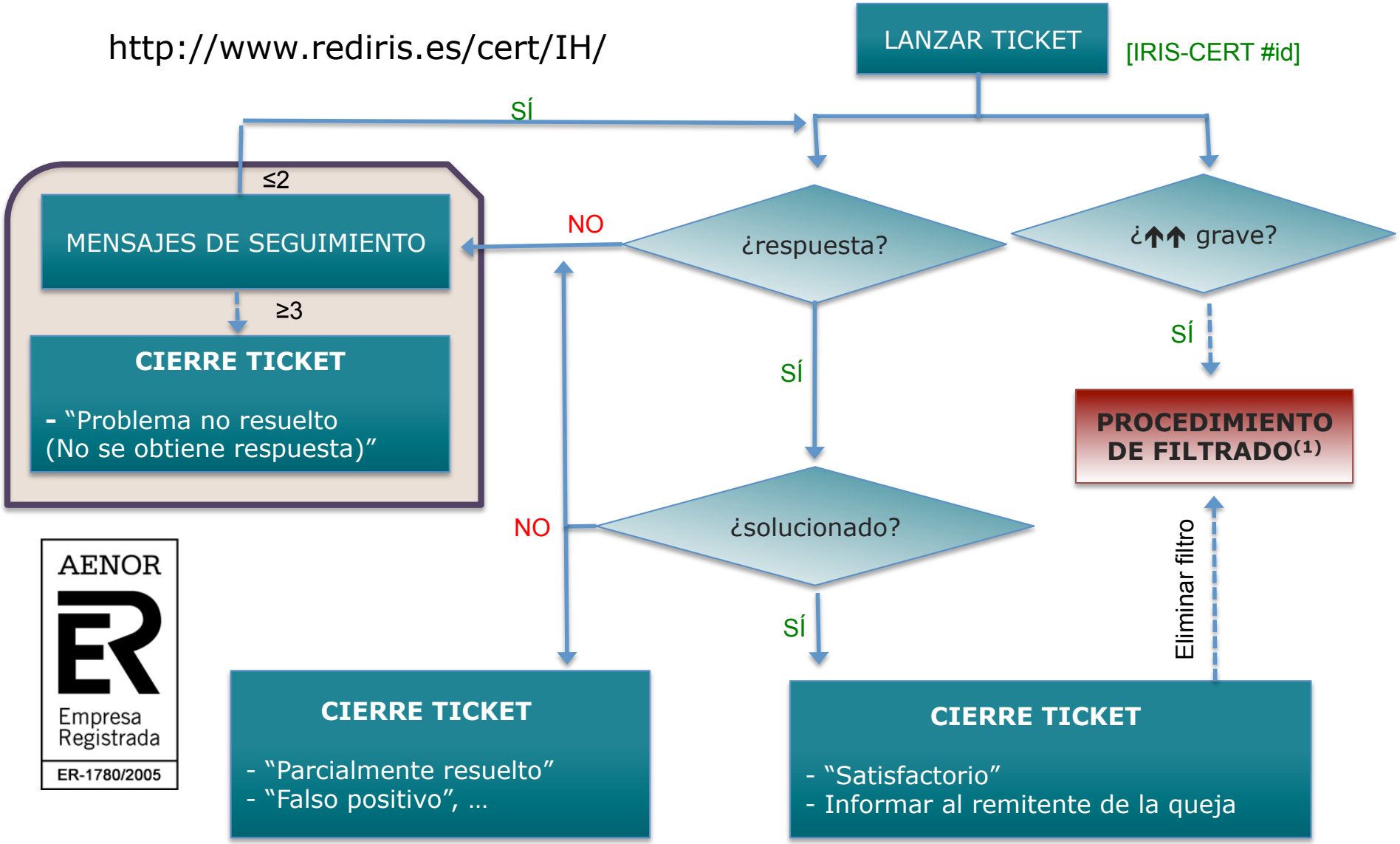


GESTIÓN DE INCIDENTES

CONSIDERACIONES

Procedimiento de Gestión de Incidentes

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



AENOR
ER
Empresa Registrada
ER-1780/2005

Protocolo de filtrado

Protocolo ordinario para la gestión incidentes en el CERT de RedIRIS (IRIS-CERT)

Procedimiento de aviso y actuación en incidentes de seguridad con necesidad de filtrado

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

¿Por qué responder a incidentes?

- Razones éticas
  - Evitar perjuicio a otros usuarios/redes
- Cuestión de imagen
  - A nivel de Red Académica y/o Red Regional
    - Somos una red concienciada
  - A nivel de institución
    - Panel de PERs
      - Los valores de cierre se utilizan para extraer indicadores institucionales (KPIs)
- Reaccionar de forma efectiva ante incidentes graves
  - Aplicar medidas de contención
- Obligaciones normativas
  - Código Penal
    - Ley Orgánica 5/2010, de 22 Junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de Noviembre. Artículo 264.
  - ENS
    - Capítulo III. Requisitos mínimos de Seguridad: Gestión de incidentes de seguridad
  - Reglamento para la protección de Infraestructuras Críticas
    - PSO (Plan de Seguridad Operativo) y PPE (Plan de Protección Específico)
  - Estrategia Española de Seguridad: Una responsabilidad de todos

Algunas consideraciones más

Direcciones de reporte

- Información de contacto individual + lista de fan-out
  - Evitar que pasen por los sistemas anti-malware de las instituciones
  - Mantener los datos de contacto actualizados en todo momento

Redes regionales

- Se contactará directamente con la institución, siempre con copia a la red regional

Ordenes judiciales

- Petición de información sobre datos de más de un año de antigüedad

Protocolo TPL para intercambio de información

- Determina la sensibilidad y ámbito de distribución de la información compartida por IRIS-CERT -> Marcas TPL (**RED**, **AMBER**, **GREEN**, **WHITE**)
  - http://www.rediris.es/cert/protocolo_tpl.html

PROYECTOS, ACTIVIDADES Y FOROS

Formación en seguridad 2012

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

- Impartido por personal de IRIS-CERT
  - Opcionalmente externo
- Dirigido al personal técnico de las instituciones afiliadas a RedIRIS
- Instalaciones Red.es, GT, JJTT, instalaciones de centros y universidades voluntarias, …
- Formato *Hands-on*
  - Aforo reducido (≈ 15-20 personas)
- Calendario anual orientativo a publicar en la Web
- Certificados de asistencia oficiales de TERENA
  - TRANSITS-I
  - TRANSITS-II
    - Pendiente ver condiciones y disponibilidad por parte de TERENA

- TRANSITS-I (Oporto) 29-30 Marzo
  - http://www.terena.org/activities/csirt-training/transits-i/porto/
- TRANSITS-II (Praga) 2-4 Abril
  - http://www.terena.org/activities/csirt-training/transits-ii/prague/

Grupo de Trabajo SIRA

Grupo de Trabajo de Seguridad Informática en la Red Académica

- Formalmente finalizado en Noviembre 2011
- Resultados del proyecto
  - Herramienta para la evaluación de la Gestión de la Seguridad de la Información (**FORMSIRA**)
    - https://formsira.rediris.es/
      - Soporte: sira-support@rediris.es
  - Encuesta sobre el estado de implantación del ENS (Abril 2011)
  - Presentaciones de diferentes herramientas de ayuda a la implantación ENS
  - Recuperación de espíritu de colaboración de RedIRIS

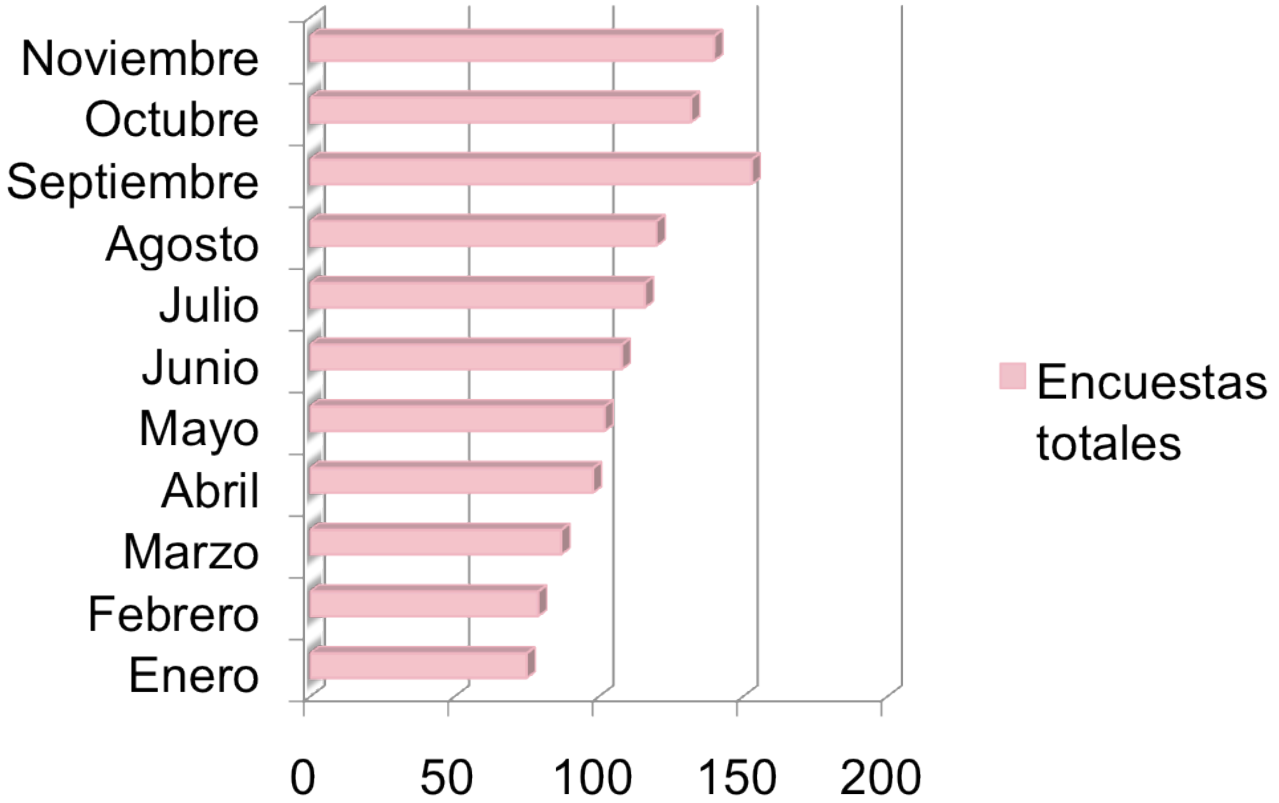
    http://www.rediris.es/cert/historico/sira/

¡¡Tenemos un sucesor!! - > **Grupo de Trabajo IRIS-ENS**

- Apoyo en la aplicación del ENS en las instituciones afiliadas
  - Lista + Wiki (autenticación SIR)
- Objetivos a corto plazo
  - Dinamización del Grupo y dotación de contenidos útiles en el Wiki
  - Posibilidad de lanzamiento de actividades específicas tipo FORMSIRA

    http://www.rediris.es/cert/tareas/actividades/ens/

Uso FORMSIRA



Esquema Nacional de Seguridad (ENS)

TRANSPARENCIA PRESENTADA EN LAS JJTT 2010 (CÓRDOBA)

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!!!!**
    - Pública vinculada, que no dependiente, de las
      de las Comunidades Autónomas.

Adecuación

Enero 2011

Enero 2014

- Los sistemas de las administracione uados al Esquema en el plazo de **doce meses**, aunque si hubies que impidan la plena aplicación, se dispondrá de un **plan de ade ación** que marque los plazos de ejecución (en ningún caso superiores a **48 mese**s 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

Esquema Nacional de Seguridad (ENS)

Novedades (I)

- Publicación de nuevas guías (borradores)
  - CCN-STIC 810: Creación de un CERT; CCN-STIC 811: Interconexión en el ENS; CCN-STIC 812: Seguridad en Entornos y Aplicaciones Web; CCN-STIC 814: Seguridad en el correo electrónico
- MPT y CCN
  - Nuevas guías:
    - Métricas e indicadores
    - Herramientas
    - Productos certificados
    - Redes Inalámbricas
    - Gestión de Incidentes (CCN-STIC 817) + Mejora guía CCN-STIC 403 (Gestión de incidentes)
      - Categorización de incidentes
      - Criterio común para establecer la criticidad de incidentes
      - Principios básicos sobre cuando informar al CCN-CERT
      - Métricas sobre gestión de incidentes

      ⟹ Nuestro objetivo: Reconocimiento formal de IRIS-CERT como interlocutor y canalizador único para incidentes de sistemas bajo el ENS para RedIRIS
  - Mejora borradores + PILAR + MAGERIT
  - Reglamento de evaluación del estado de seguridad de la Administración

Esquema Nacional de Seguridad (ENS)

Novedades (II)

- Nuevo curso CCN
  - VII Curso de Gestión STIC - Implantación del ENS (on-line+presencial)
    - https://www.ccn-cert.cni.es/
- CRUE
  - Estudio UNIVERSITIC 2011
    - Incluye 35 aspectos específicos sobre estado de implantación del ENS en SUE
      - http://www.crue.org/export/sites/Crue/Publicaciones/Documentos/Universitic/universitic2011web.pdf
    - Datos a 31/12/2010
      - *"El ENS no ha calado en las instituciones se refleja en que solo el 9% dicen aplicarlo, aunque en el 38% de ellas está en desarrollo su adopción"*
      - *"Las universidades que ya han adoptado el ens declaran haber aplicado 13,63 acciones de media sobre un total de 35 acciones aconsejables, lo que indica que el 39% de las medidas recogidas en el ens están en funcionamiento"*
  - Áreas de actividad prioritarias para la CRUE
    - Formación y concienciación
    - Racionalización de recursos

  ⇒ En evaluación: Propuesta de servicios de CRUE-TIC

IRIS-CERT en …

… Foros

- Los de siempre: Foro Abuses, CSIRT.ES, TF-CSIRT, FIRST, APWG, EGI, …
- Foro de Seguridad 2012
    - TEMÁTICA + SEDE

… nuevos Grupos

- Futuro miembro del Grupo de Trabajo GPIC (Grupo Informal de Protección de Infraestructuras Críticas)
    - Organismos públicos y privados + CERTs
    - Desarrollar un marco de referencia común sobre IC
    - Desarrollo de planes
    - Foro de encuentro y debate
    - ….

…. la Estrategia Española de Seguridad

http://www.lamoncloa.gob.es/NR/rdonlyres/9BD221CA-A32A-4773-ACB7-ECD3FC6C9B9E/0/ESTRATEGIAESPANOLADESEGURIDAD.pdf

¡Muchas gracias!

Más de 20 años al servicio de la investigación