El papel de un IRT dentro de la Organización

Francisco Jesús Monserrat Coll

IRIS-CERT. RedIRIS. Red.es

25 de Noviembre de 2005

¿Qué vamos a tratar ?

Algunas preguntas ,

- ¿Para qué sirve un IRT dentro de mi organización ?
  - ¿Cuáles son sus funciones ?
  - ¿Qué problemas tiene que tratar ?
- ¿Donde se sitúa el IRT en mi Organización ?
- ¿Es el IRT un “ente” separado o forma parte de un departamento más genéricos.

No hay una única solución , veremos distintos enfoques

Plantear el IRT

Dependiendo de cada organización

- Identificar Aciertos y riesgos
- Entendiendo IRT Casos de estudio.
- Pensando acerca de la constitución y servicio de su IRT.
- Pensando acerca de dónde IRT se ubicará en la organización

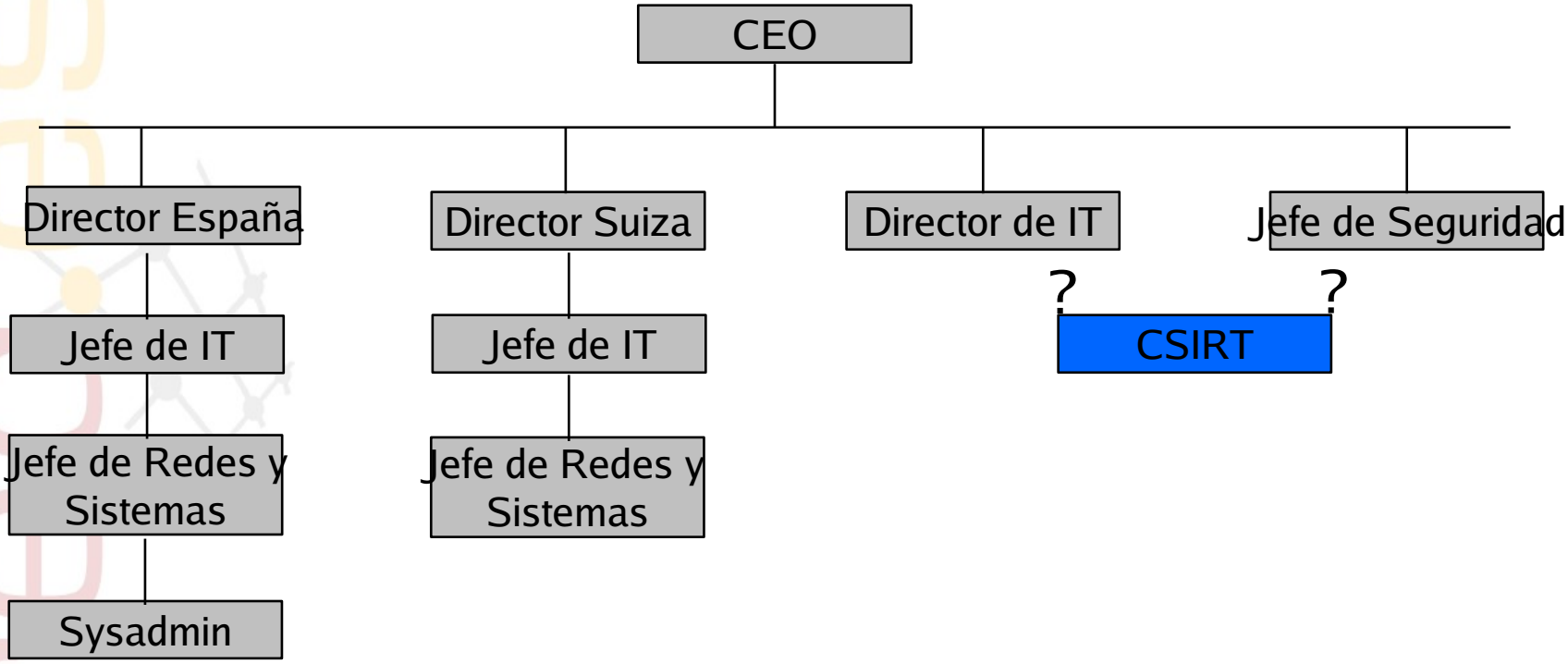
Vender su idea a otros.

- Necesidad de administración.
- Necesidad de fondos permanentes y financiación.
- Escriba la propuesta

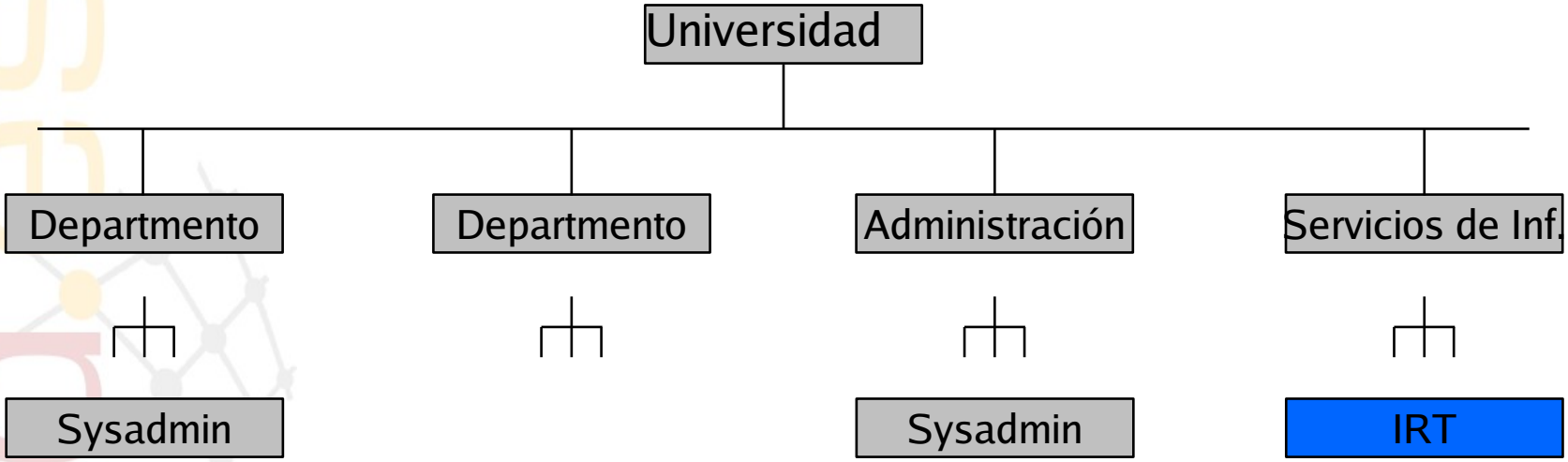
Algunos ejemplos de IRT

Ejemplo 1. Gran corporación

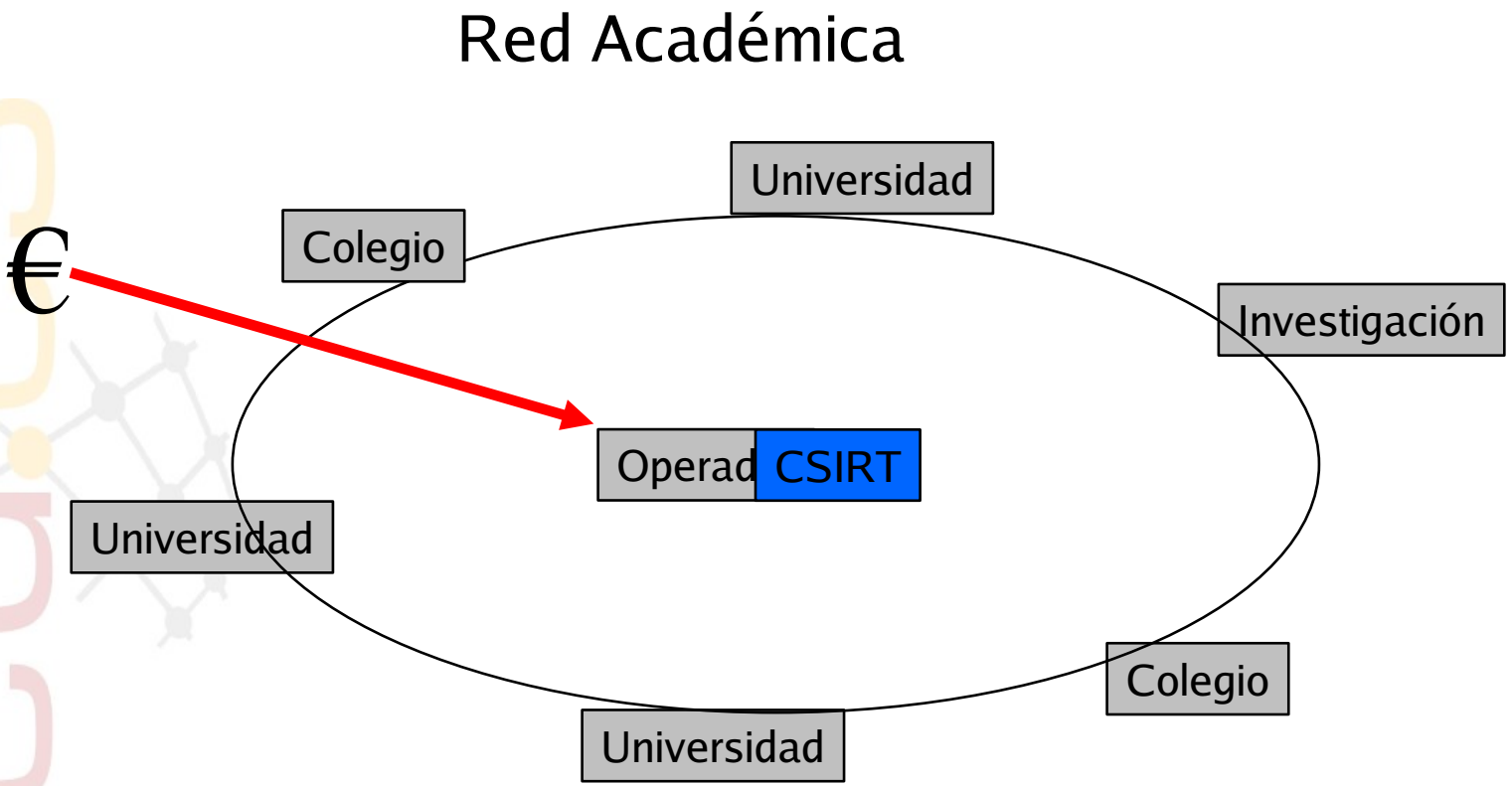
Gran Corporación



Ejemplo 2. Universidad



Ejemplo 3: Red Académica



Ejemplo 4. Otros IRT

IRT de ámbito nacional.

- Soporte a los habitantes de un país.
- Alertas a nivel global sobre peligros graves
- Coordinación con otros IRT

Proveedores de Internet e información.

Dos tendencias.

- Soporte a la infraestructura del servicio
- Soporte al usuario final.

IRIS-CERT, El grupo de seguridad de RedIRIS

- Proporciona infraestructura de red y servicios complementarios a la comunidad académica y de investigación española
- Establecida en 1991
- Financiada por el Plan Nacional de I+D+I
- Integrada como un departamento con autonomía e identidad propia en el seno de la Entidad Pública Empresarial Red.es
- En la actualidad conecta a 233 centros (Universidades, centros públicos de investigación, etc.)

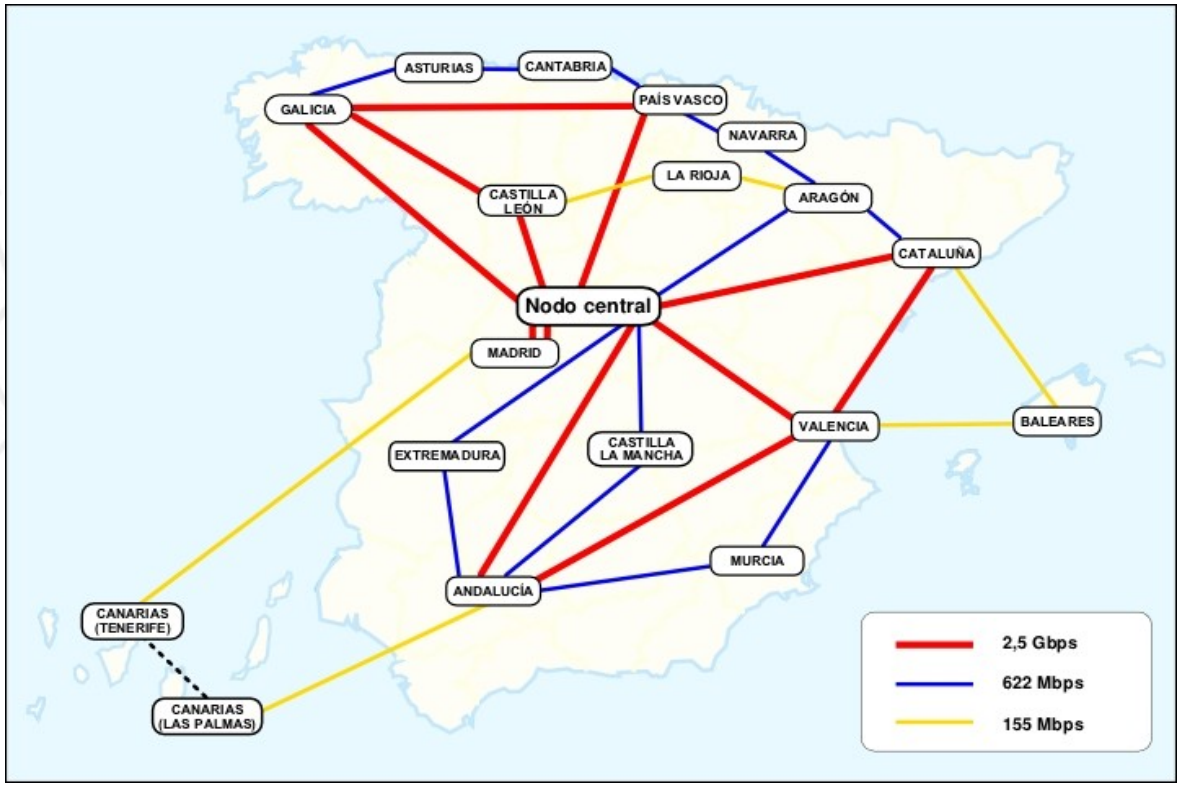
http://www.red.es

Organismo público español encargado del fomento de la sociedad de la información.

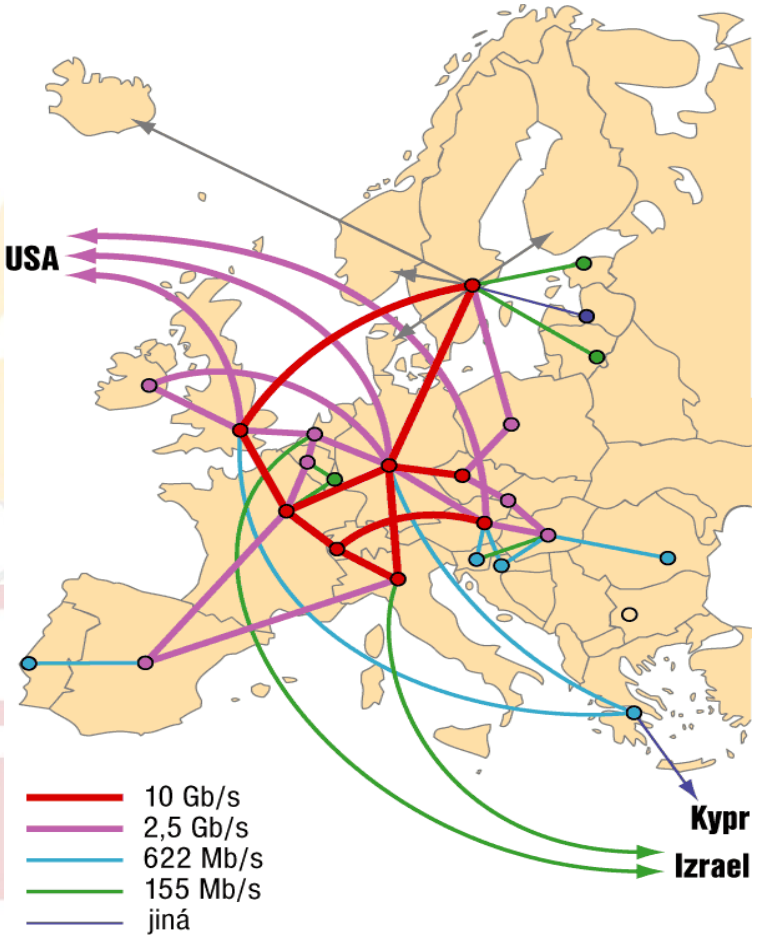
- **Reciente creación**
- **Agrupa a diversos servicios públicos relacionados con Internet**
  - Registro NIC para España.
  - Administración Electrónica
  - Alertas de seguridad http://www.alertaantivirus.es
  - Fomento de Internet (todos.es, Internet Rural, ...
  - RedIRIS

RedIRIS - Red Troncal -

- Un punto de presencia en cada Comunidad autónomona.
- La gestión a partir de este punto corresponde a cada una de las instituciones



Redes Académicas en Europa



Organización similar en otros países europeos:

- Una red nacional de I+D
- Interconexión de las distintas redes regionales entre si. (Geant)
- Conexión de esta red paneuropea a Internet2 y otras redes de investigación.
- Acuerdos adicionales de conexión de cada red con Carrier y proveedores nacionales.

RedIRIS – Servicios

Además de la interconexión y acceso a Internet RedIRIS proporciona diversos servicios a la comunidad científica:

- Coordinación de servicios de Internet
- Celebración de reuniones técnicas con los responsables de las Universidades y Organismos conectados
- Presencia en proyectos Internacionales
- Soporte a grupos de Investigación: listas de correo electrónico, espacio WWW, etc.
- Coordinación de incidentes de seguridad

http://www.rediris.es/cert

Equipo de atención de incidentes de seguridad de la Red Académica y de Investigación Española (CERT/CSIRT/IRT)

- Creado en 1995
- 4 personas dependiendo de un coordinador técnico

Ámbito de actuación (constituency)

- Servicio completo Instituciones conectadas a RedIRIS (AS766)
- Servicio limitado . dominio .es
  - gestión de incidentes y coordinación con otros equipos de seguridad

¿Por que se creo IRIS-CERT ?

Necesidad de coordinación de incidentes (1995)

- ¿Cómo se puede contactar desde el exterior para notificar problemas de seguridad en equipos de España ?
- ¿Cómo pueden los administradores de las Universidades contactar con otros IRT cuando tengan un problema de seguridad.
- ¿Cómo difundir a estos administradores información de seguridad ?

El grupo de seguridad aparece como una consecuencia de estas necesidades:

- Coordinado con las Universidades
- Separado de la operación de la red.

Servicios proporcionados

Servicios Reactivos

- Soporte en la Respuesta de Incidentes
- Coordinación con otros equipos de seguridad dominio .es
- Análisis
  - De equipos (Forense)
  - De binarios y de intrusiones

Servicios Proactivos

- Observación de tendencias
- Mantenimiento de herramientas y documentación (WWW/FTP)
- Avisos de seguridad a las instituciones afiliadas

IRIS-CERT Actividades

- Detección temprana de ataques:
  - Sistemas Trampa para detectar nuevos patrones de ataques
  - Monitorización de tráfico
- Coordinación de seguridad
  - Con las instituciones conectadas a RedIRIS
  - Con los ISP Españoles
  - Grupos de Seguridad internacionales

Otros servicios y Grupos de Trabajo

Soporte a ac

Gestión y mantenimiento de un Servidor de Claves Públicas PGP ➪ servicio público

- http://www.rediris.es/keyserver/

- Infraestructura de Clave Pública para la Comunidad RedIRIS (RedIRIS-PKI) ➪ servicio restringido a la comunidad RedIRIS
  - http://www.rediris.es/pki/

- IRIS-CERT puede actuar como punto de contacto entre las instituciones afiliadas y las Fuerzas de Seguridad del Estado
  - Sólo asesoramiento técnico

Relación con la comunidad

Autoridad compartida

Es obligatorio disponer de al menos un punto de contacto de seguridad por cada institución afiliada a RedIRIS (servicio completo)

- Dado por el PER (Punto de Enlace con RedIRIS)
- Se suscriben a la lista de coordinación de seguridad (IRIS-CERT)
- Mantenimiento de información de contacto en BBDD interna

No es obligatorio este punto de contacto para las instituciones con servicio limitado

Conclusiones

Conclusiones

No hay una solución única sobre como incorporar un IRT dentro de una organización.

- Las experiencias de otros IRT son muy valiosos
- El apoyo de la organización es fundamental.
  - Medios, personal, etc.
  - Definición exacta de las funciones y ámbito de actuación del IRT

El IRT evoluciona con el tiempo

- No se puede abarcar todo desde el principio
- Empezar con los servicios necesarios e ir creciendo en función de la organización.

Más información

- TRANSIT, **http://www.ist-transits.org/** iniciativa de TERENA para la formación de miembros de equipos de respuesta . Algunas partes de esta presentación están inspiradas en el material del curso.

- TF-CSIRT , **http://www.terena.nl/tech/task-forces/tf-csirt/** , reuniones de coordinación de grupos de seguridad Europeos, participación abierta .

- Trusted Introducer, **http://ti.terena.nl** , directorio de grupos de seguridad europeos.

- FIRST, **http://www.first.org** , agrupa a los grupos de seguridad a nivel mundial.

E-COAT, **http://www.e-coat.org** , iniciativa de coordinación de grupos de abuse Europeos