fs2004
II Foro de Seguridad RedIRIS

Organización y Operación de un CSIRT

Chelo Malagón
RedIRIS, Red.es

USC UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

red.es

RedIRIS

Agenda (I)

- Introducción
  - Introduciendo el concepto
  - Razones para la existencia de un CSIRT
  - Barreras
- Organización de un CSIRT
  - Pasos para su creación
  - Diseño de la visión de un CSIRT
    - *CSIRT Framework*
    - Servicios
    - Modelo organizativo o estructura operativa
    - Financiación

Agenda (II)

- Operación de un CSIRT
  - Personal
  - Ubicación física
  - Comunicaciones
  - Sistemas
  - Procedimientos

Introducción

CSIRT (*Computer Security Incident Response Team*) (I)

- Punto central para analizar eventos, coordinar soluciones técnicas, asegurar que la información necesaria se transmite a aquellos que la necesitan, y adiestrar a otros equipos o individuos en la gestión de incidentes de seguridad

  SCHULTZ, 1989 Shultz, E. Eugene, The Computer Incident Advisory Capability (CIAC) Centre for Computer Security News, Vol 8, 1989

- Un CSIRT recibe, analiza y responde informes de incidentes recibidos desde los miembros de su comunidad (*constituency*), otros CSIRT, o terceras partes, coordinando la respuesta entre las partes implicadas

  CERT/CC: *Computer Security Incident Response Team FAQ*
  http://www.cert.org/csirts/csirt_faq.html

CSIRT (*Computer Security Incident Response Team*) (II)

- *Constituency*
  - Comunidad de la que el CSIRT es responsable y a la que ofrece sus servicios
- Incidente de Seguridad
  - Cualquier evento real o sospechoso relacionado con la seguridad de un sistema informático o red
  - El acto de violar una política de seguridad de forma implícita o explícita

Acrónimos

IRT (*Incident Response Team)*

IRC (*Incident Response Capability)*

IHT (*Incident Handling Team)*

IMT (*Incident Managing/Management Team)*

CSIRT (*Computer Security Incident Response Team)*

CIRT (*Computer Incident Response Team)*

CIRC (*Computer Incident Response Capability or Centre)*

SIRT (*Security Incident Response Team)*

SERT (*Security Emergency Response Team)*

CERT (*Computer Emergency Response Team)*

MSSP (*Managed Security Service Providers)*

MSP (*Managed Service Provider)*

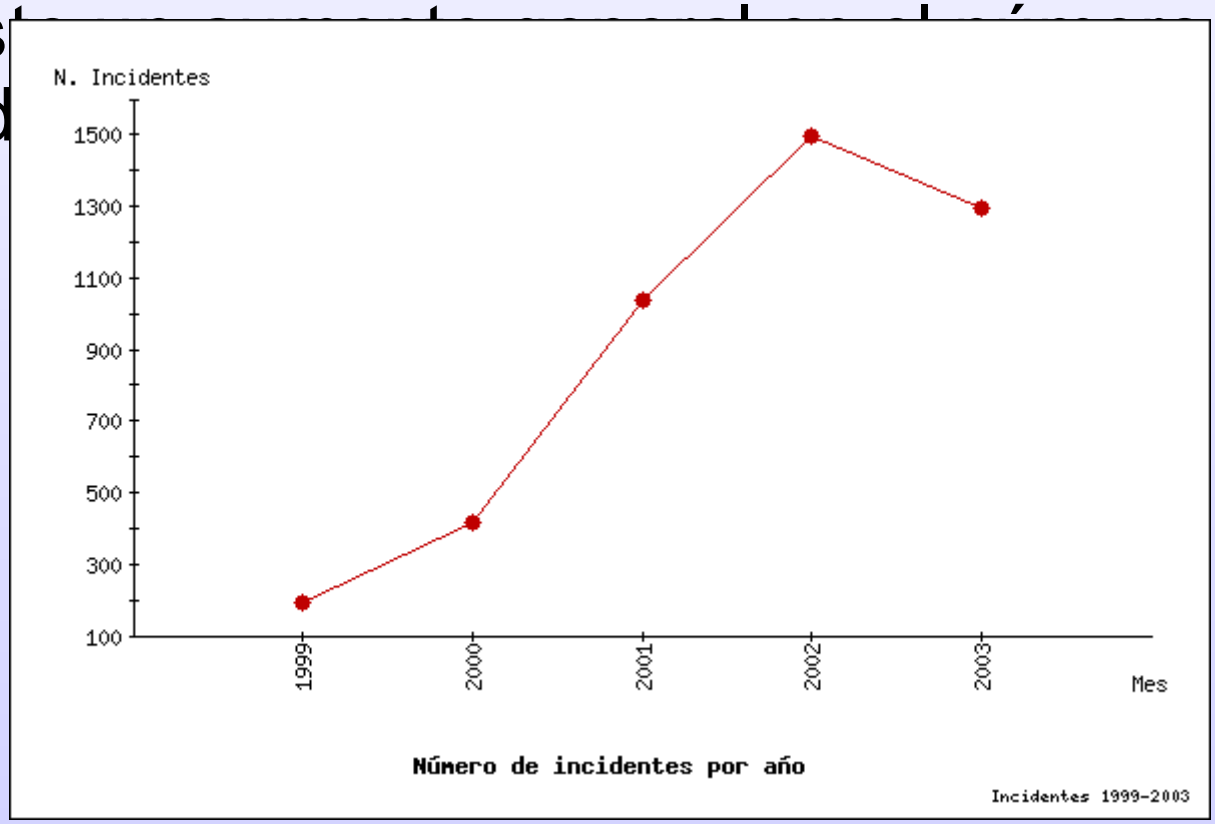
ERS (*Emergency Response Services)*

ISAC (*Information Sharing and Analysis Centres*)

- No existe ningún tipo de convención en cuanto al nombre a usar
- El nombre no dice nada de los servicios que presta el CSIRT
- Existen tantos tipos de CSIRT como culturas y tipos de comunidades

¿Por qué una organización necesita un CSIRT? (I)

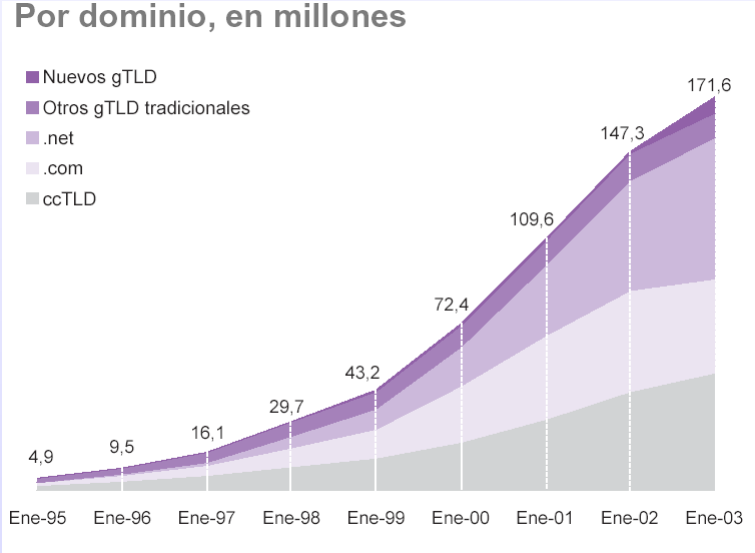
- Se está convirtiendo en una necesidad de negocio
  - Exis de incid

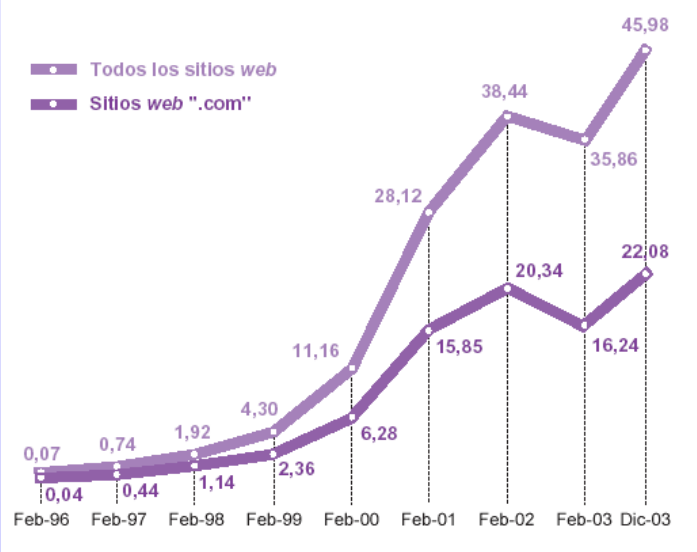


http://www.rediris.es/cert/doc/informes/2003/

¿Por qué una organización necesita un CSIRT? (II)

- Internet es una realidad





¿Por qué una organización necesita un CSIRT? (III)

- Es necesario que exista un equipo local que comprenda las necesidades y características locales, y opere en la misma zona horaria
- Reconocimiento internacional
  - 150 miembros del FIRST (*Forum of Incident Response and Security Teams)*

    http://www.first.org/team-info/
  - 97 CSIRTs conocidos en Europa

    http://www.ti.terena.nl/teams/level0.html
- Es crítico para una organización tener mecanismos para responder de forma rápida y eficiente ante una amenaza de seguridad
- Mejorar la seguridad en la comunidad en general (prevención)
  - Educar a los administradores de sistemas, publicar alertas, promover la implantación de políticas de seguridad,....

Barreras para el establecimiento de un CSIRT (I)

- Es difícil encontrar personal con experiencia y preparación previa → Falta de programas de formación específicos
  - *SANS GIAC Certified Incident Handler (GIAH)*

    http://www.giac.org/GCIH.php
  - *CERT®-Certified Computer Security Incident Handler*

    http://www.cert.org/certification/
  - *Certified Information Systems Security Professional (CISSP) and Systems Security Certified Practitioner (SSCP)*

    http://www.isc2.org/cgi/content.cgi?category=3
  - *TRANSITS (Training of Network Security Incident Teams Staff)*

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

Barreras para el establecimiento de un CSIRT (II)

- Escasez de información pública sobre Planes/Políticas de Respuesta de Incidentes (IRP), procedimientos de actuación, …
- Pocas herramientas que cubran sus necesidades (confidencialidad, integridad, *workflow* específico, almacenaje, …)
- Financiación
  - Presupuesto limitado en entornos académicos

¡¡¡Tomar CSIRT ya establecidos como

Organización de un CSIRT

Planificación del CSIRT

- ¿Cuál es la estructura organizativa y técnica de la organización?
- ¿A que comunidad se va a dar servicio? (*constituency*)
- ¿Cuáles son las metas y objetivos del CSIRT? (*mission statement*)
- ¿Qué servicios va a proporcionar?
- ¿Nivel de Autoridad?
- ¿Modelo organizativo o estructura operativa?
- ¿Papel y responsabilidades del personal que opera el CSIRT?
- ¿Qué equipamiento e infraestructura de red necesita para dar soporte a sus funciones diarias?
- ¿Cómo se va a financiar y sustentar?
- ¿Qué tipo de relaciones externas/internas se van a establecer y con quién?

Pasos para la creación de un CSIRT

- Obtener apoyo y participación de la dirección/organización para la planificación e implantación del CSIRT
- Determinar el plan estratégico para el desarrollo del CSIRT
- Obtener información relevante
- Diseñar la visión del CSIRT
- Notificar la visión del CSIRT y su plan operativo
- Comenzar con la puesta en marcha del CSIRT
- Divulgar el CSIRT
- Evaluar su efectividad

La paciencia es la clave

Participación y apoyo de la organización/dirección

- Tanto para la planificación como para la puesta en marcha del CSIRT
  - Provisión de recursos, financiación, tiempo, personas para la formación de un Grupo de Trabajo, …
  - Conocer la percepción y expectativas de la organización sobre las funciones y responsabilidades del futuro CSIRT
  - Obtener un compromiso para sustentar las operaciones y la autoridad del CSIRT a largo plazo

Plan estratégico

- Dar importancia a las personas y áreas claves que deberán apoyar el establecimiento del CSIRT → Grupo de Trabajo
  - Administradores de sistemas, responsable del departamento TI, responsables de redes y sistemas, representantes de recursos humanos, representantes del departamento legal, representantes de la comunidad …
  - Establecer plazos para la creación del CSIRT
    - Establecer un calendario de entrevistas
  - Definir como será el flujo de información entre el Grupo de Trabajo y la organización

Obtención de información relevante (I)

- Conocer y comprender la organización
  - Diseño de red (servicios básicos, riesgos, activos y puntos de control)
  - Jerarquía organizativa
  - Área de negocio

Documento

  - Diagrama esquemático de la organización (unidades, departamentos, …)
  - Interrelaciones
  - Misión de la organización
  - Donde está ubicada la sede/oficina central
  - Tamaño
  - Conexiones de red internas/externas

Obtención de información relevante (II)

- Conocer los riesgos a los que está expuesta la organización → estadísticas de incidentes
- Investigar qué tipo de capacidad/habilidad de respuesta está ya implementada en la organización
  - ¿Quién es el responsable último de la seguridad en la organización?
  - ¿Existe un CSIRT?
  - ¿Existen Políticas de Seguridad o AUP?
  - ¿Existen requerimientos administrativos?
- Listar las ventajas/desventajas de tener un CSIRT operacional

Diseño de la visión del CSIRT

- Identificar la comunidad a la que se va a dar servicio
- Definir la misión, objetivos y metas del CSIRT
- Servicios a proporcionar
- Modelo organizativo o estructura operacional
- Identificar los recursos necesarios (personal, equipamiento e infraestructura)
- Financiación del CSIRT

- **Notificación** de la visión del CSIRT y del plan operativo
  - Preparar un documento de propuesta de creación del CSIRT para la organización
    - Identificación de problemas organizativos o de proceso antes de la implementación
    - Una forma de publicitar al equipo y ganar apoyo

Puesta en marcha, divulgación y evaluación

- Comenzar con la puesta en marcha del CSIRT
  - Contratación del personal, equipamiento, desarrollo de políticas y procedimientos, definición de las especificaciones del sistema de gestión de incidencias, elección del sistema de gestión, desarrollo de guías, formularios y procedimientos para la notificación de incidentes, …
- Dar a conocer el CSIRT
  - Horario de operación, forma de contacto, guías y formularios, misión y servicios que proporciona, ….

Diseño de la visión de un CSIRT

CSIRT Framework

- *Mission Statement*
  - En qué se va basar tu trabajo
    - Listar que hará y no hará el equipo
- *Constituency*
  - A quién va a prestar sus servicios
  - Como se va a relacionar con esta comunidad
- Posicionamiento del equipo en la organización
- Relaciones con otros equipos

Mission Statement

- Proporciona una descripción clara del propósito y función del CSIRT
- Define las metas, objetivos y prioridades del equipo
- Como mucho 3 o 4 frases especificando la misión del CSIRT
  - Imprescindible para establecer la naturaleza, tipo y calidad de los servicios a proporcionar y definir sus políticas y procedimientos
  - Ayuda a las partes que interactuarán con el CSIRT a comprender su marco de trabajo
- Puede completar el "*mission statement*" de la organización padre
- En algunas ocasiones acompañado por una "declaración de propósitos" (*purpose statement*)
  - Explicación de las razones para la formación del

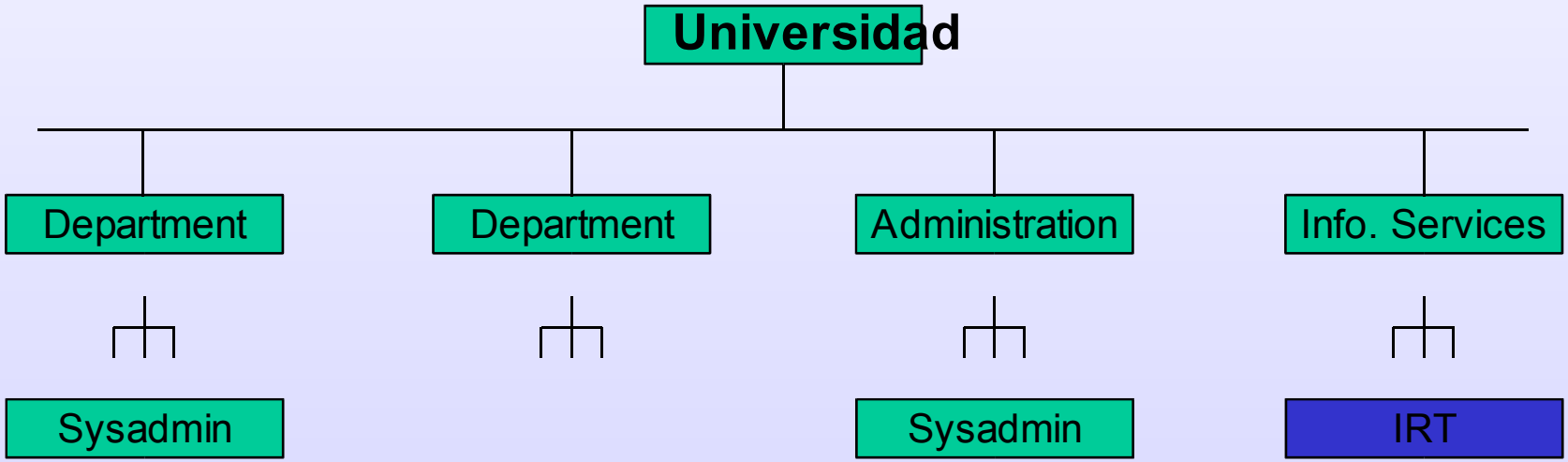
Constituency

- Definición de la comunidad a la que se va a prestar el servicio → **declaración formal** apoyada con una lista de nombres de dominio, AS, ..
  - Composición, localización física y geográfica, y sector
  - Factores organizativos:
    - Interno vs. Externo
    - Distribuido vs. Centralizado
- Forma de relacionarse con la comunidad
- Promoción del CSIRT dentro de la comunidad

CSIRT/Relación con la Comunidad

Niveles de Autoridad	Relación con la comunidad
Completa	Los miembros del CSIRT tienen la autoridad de llevar a cabo cualquier acción o decisión en nombre de su comunidad
Compartida	Los miembros del CSIRT tienen influencia en las decisiones de su comunidad, pero éstas siempre son compartidas
Sin autoridad	No tienen autoridad sobre su comunidad. Se limitan a aconsejar y diseminar información

Posicionamiento del CSIRT dentro de la organización



Relaciones con otros equipos

- **CSIRT no pueden ser islas →**
  - Objetivo primordial: interacción y coordinación entre equipos y fuerzas de seguridad del estado
  - CSIRT van a proporcionar un enlace tanto a grupos criminalísticos y legales, como a otros CSIRT
- Red de confianza
  - La confianza entre CSIRT se basa en un 90% en relaciones personales y sólo un 10% en la descripción formal de los servicios, declaraciones de calidad, visitas, etc..

Iniciativas

- Internacionales
  - *TERENA Trusted Introduced* (TI)

    http://www.ti.terena.nl/
  - FIRST (*Forum of Incident Response and Security Teams*)

    http://www.first.org/
  - TERENA TF-CSIRT *(Collaboration of Security Incident Response Teams)*

    http://www.terena.nl/tech/task-forces/tf-csirt/
    - CERT-TF (RARE) 1992-1994
    - SIRCE (Security Response Coordination for Europe) 1997-1999
    - CERT-COORD (TERENA) Sep 1999 – May 2000
- Nacionales
  - ESPX-CERT (Espanix)

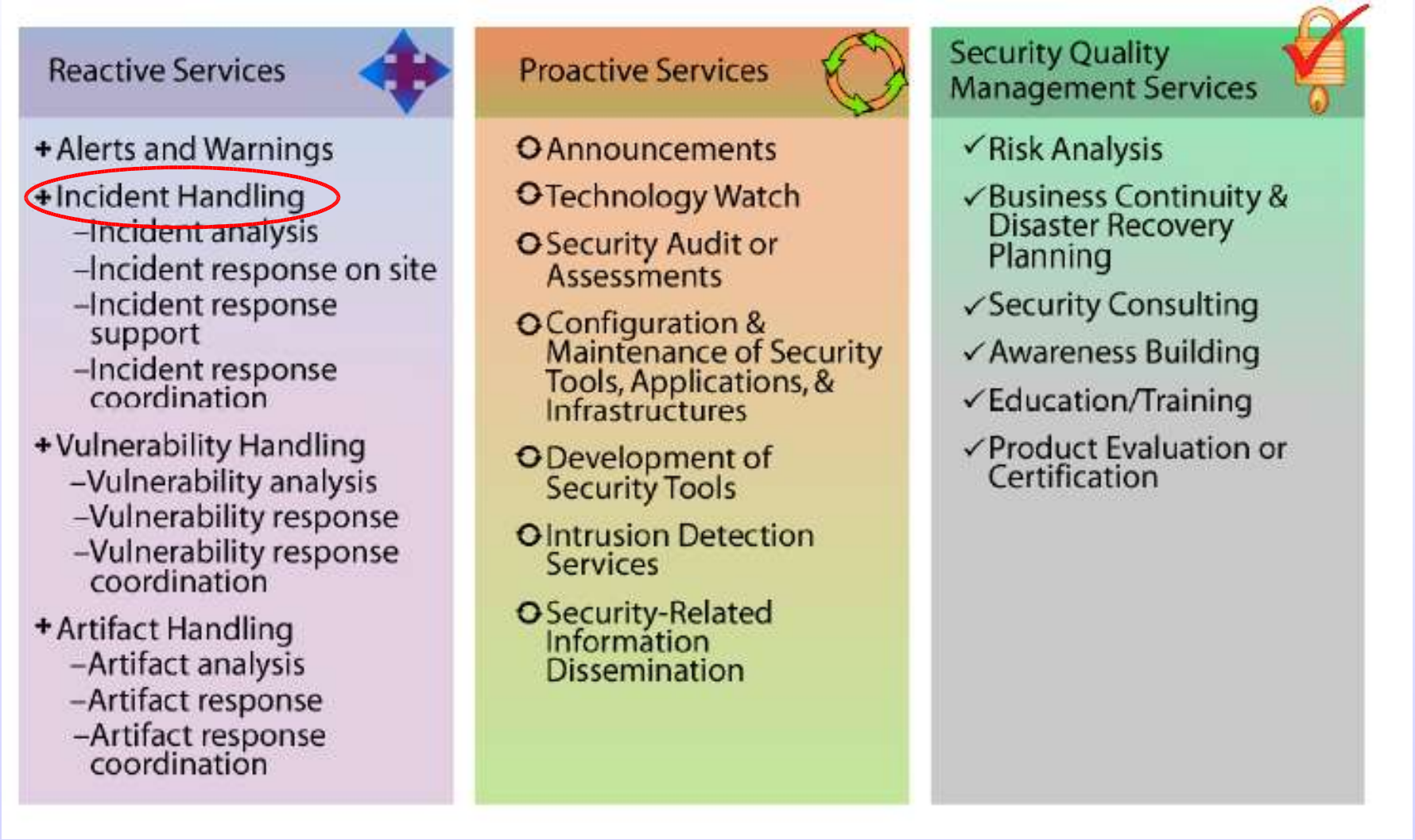
    http://www.rediris.es/list/info/espx-cert.es.html
  - GT Seguridad y Sociedad de la Información (Observatorio de las Comunicaciones y Sociedad de la Información, Red.es)

    http://www.observatorio.es/

Servicios – Categorías (I)

- Reactivos
  - Solicitados normalmente por la comunidad cuando se produce un incidente, una vulnerabilidad, código malicioso, etc..
  - Constituyen el núcleo del trabajo de un CSIRT
- Proactivos
  - Para evitar incidentes o minimizar su impacto
- De valor añadido
  - Para mejorar la seguridad en conjunto
  - Normalmente proporcionados por otras áreas de la organización
  - Son generalmente servicios proactivos pero sin impacto directo en la reducción del número de incidentes

Servicios – Categorías (II)



http://www.cert.org/csirts/services.html

Servicios

- Servicios obligatorios
  - Al menos uno relacionado con la **Atención de Incidentes**
    - *Incident Analysis, Incident Response on site, Incident Response Support o Incident Response Coordination*
- Servicios comunes (tanto proactivos, como reactivos, como de valor añadido)
  - Dependiendo de las necesidades de la comunidad
  - Algunos pueden ser proporcionados por otros departamentos en la organización o por grupos externos
  - Se debe ser realista
    - Mejor pocos pero de calidad → reputación
- Documentar los servicios que se van a prestar

Servicios básicos - Ejemplo

- Servicios reactivos
  - *alerts y warnings*
  - *incident handling*
    - *incident analysis*
    - al menos uno de los siguientes: *Incident Response on site, Incident Response Support o Incident Response Coordination*
  - *vulnerability handling*
    - *vulnerability response coordination*
- Servicios proactivos
  - *announcements*
- De valor añadido
  - *awareness building*
  - *security consulting* (especialmente, desarrollo de políticas de seguridad)

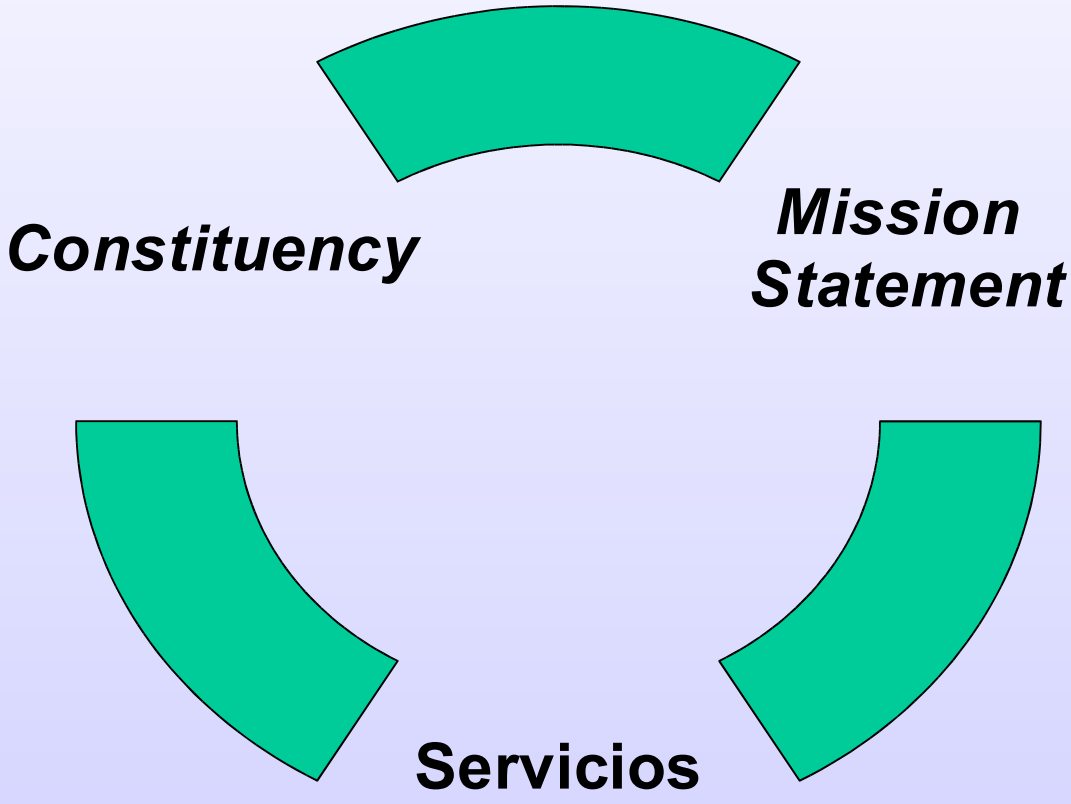
State of the Practice of CSIRT's report

(http://www.cert.org/archive/pdf/03tr001.pdf)

Como y cuando operará el equipo

- Forma de contacto
  - Teléfono: directo o a través de un *helpdesk*
  - Sólo correo electrónico
- Se va a proporcionar servicio…
  - Sólo en horas de oficina
  - Fuera de horas de oficina (sólo emergencias, …)
  - 7x24 (cualquier día, a cualquier hora)

Modelo Organizativo



Modelos Organizativos Básicos

- Equipo de Seguridad
  - No se establece un CSIRT formalmente
  - Se utiliza personal existente en la organización (TI)
  - Proporciona *Incident response on-site*
- CSIRT de Coordinación
  - Normalmente el CSIRT no pertenece a la misma organización que la comunidad a la que presta servicio
  - Centro de coordinación de incidentes e intercambio de información entre otros CSIRT, equipos de seguridad y/o organizaciones externas/internas
  - No se proporciona *Incident respond on-site*
- CSIRT Interno
  - El CSIRT pertenece a la misma organización que la comunidad a la que sirve
  - Su principal prioridad se centra en el manejo de incidentes
  - Se le ha otorgado autoridad y responsabilidad específica para la atención de incidentes

CSIRT Interno

- Distribuido
- Centralizado
- Distribuido/Centralizado

- Dependiendo de:
  - La distribución y tamaño de la comunidad
  - Los servicios que proporciona
  - Recursos y Financiación
  - Posición dentro de la organización

Servicios/Modelo Organizativo (I)

Service Category	Services		Security Team	Distributed	Centralized	Combined	Coordinating
Reactive	Alerts and Warnings		Additional	Core	Core	Core	Core
	Incident Handling	Incident Analysis	Core	Core	Core	Core	Core
		Incident Response On Site	Core	Additional	Additional	Additional	Unusual
		Incident Response Support	Unusual	Core	Core	Core	Core
		Incident Response Coordination	Core	Core	Core	Core	Core
	Vulnerability Handling	Vulnerability Analysis	Additional	Additional	Additional	Additional	Additional
		Vulnerability Response	Core	Additional	Unusual	Additional	Additional
		Vulnerability Response Coordination	Additional	Core	Core	Core	Core
	Artifact Handling	Artifact Analysis	Additional	Additional	Additional	Additional	Additional
		Artifact Response	Core	Additional	Unusual	Additional	Additional
		Artifact Response Coordination	Additional	Additional	Core	Core	Core

Servicios/Modelo Organizativo (II)

Service Category	Services	Security Team	Distributed	Centralized	Combined	Coordinating
Proactive	Announcements	Unusual	Core	Core	Core	Core
	Technology Watch	Unusual	Additional	Core	Core	Core
	Security Audits and Assessments	Unusual	Additional	Additional	Additional	Unusual
	Configuration and Maintenance of Security Tools, Applications, and Infrastructures	Core	Additional	Additional	Additional	Unusual
	Development of Security Tools	Additional	Additional	Additional	Additional	Additional
	Intrusion Detection Services	Core	Additional	Additional	Additional	Unusual
	Security-Related Information Dissemination	Unusual	Additional	Core	Core	Core
Security Quality Management	Risk Analysis	Unusual	Additional	Additional	Additional	Additional
	Business Continuity and Disaster Recovery Planning	Unusual	Additional	Additional	Additional	Additional
	Security Consulting	Unusual	Additional	Additional	Additional	Additional
	Awareness Building	Unusual	Additional	Additional	Additional	Core
	Education/Training	Unusual	Additional	Additional	Additional	Core
	Product Evaluation or Certification	Unusual	Additional	Additional	Additional	Additional

Financiación

- En entornos académicos financiación puede ser un problema
- El CSIRT debe ser una actividad solidamente presupuestada
  - No un proyecto anual que pueda terminarse en cualquier momento
- Es necesario justificar la financiación → informes y estadísticas
  - Decidir a quién se va informar y cuando
  - ¿Cuál será el proceso para informar a la comunidad?
- Se tiende a contratar servicios de seguridad a empresas externas
  - Los CSIRT deben competir con proveedores externos → se debe entender las características del mercado,

¿Cuánto cuesta crear un CSIRT?

- Depende de los recursos, servicios, estructura del CSIRT, entorno, circunstancias particulares, etc.
  - Costes de creación y operación (equipamiento y personal)
- Estrategias de financiación:
  - Normalmente financiados por una organización padre (universidad, entidad gubernamental, ..)
  - Otros mecanismos → subscripción, patrocinio gubernamental, académico, consorcio, cargo a proyecto, etc

Developing an Effective Incident Handling Cost Analysis Mechanism, by David A. Dittrich; SecurityFocus, June 12, 2002

http://online.securityfocus.com/infocus/1592

Incident Cost and Analysis Model Project

http://www.cic.uiuc.edu/groups/ITSecurityWorkingGroup/ICAMP.shtml

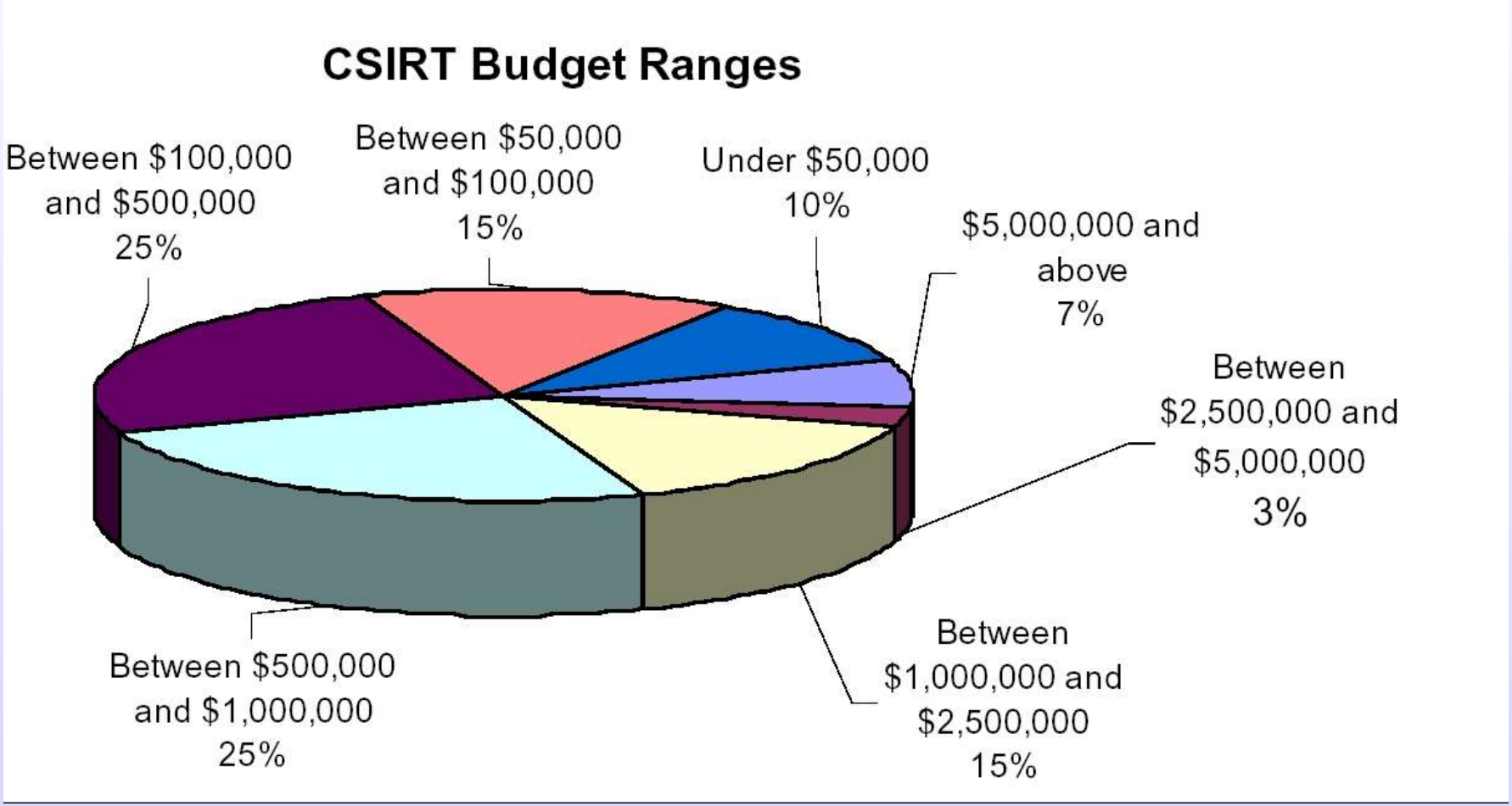
Computer Crime and Security Survey from Computer Security Institute (CSI) in partnership with the FBI

http://www.gocsi.com/press/20020407.html

2001 Information Security Industry Survey

http://www.infosecuritymag.com/articles/october01/images/survey.pdf

Presupuesto



State of the Practice of CSIRT's report

(http://www.cert.org/archive/pdf/03tr001.pdf)

Operación de un CSIRT

¿Qué es un CSIRT?

- Un Servicio
  - Bien definido y documentado
- Equipo de personas y su ubicación física
- Comunicaciones
  - Teléfono, e-mail, (fax, móvil, busca,….)
- Sistemas (software y hardware)
- Procedimientos
  - Todo el mundo sabe qué hacer
  - Preincidente, Respuesta de Incidente, Postincidente

Contratación del personal (I)

- Una vez que se define el servicio a proporcionar, se puede estimar:
  - Número de personas
    - 7x24: entre 4 y 6 personas
    - *on-call service*: al menos 3
  - Habilidades/Experiencia
- El personal debe ser de confianza
  - Proceso continuo
- Se puede utilizar personal ya existente en la organización
  - A tiempo parcial o completo
  - P.ej.: departamento legal, relaciones institucionales, *helpdesk*, expertos técnicos, etc..

Contratación del personal (II)

- Habilidades necesarias:
  - **Interpersonales**: sentido común, capacidad de comunicación oral y escrita, diplomacia, habilidad para seguir políticas y procedimientos, ganas de aprender, capacidad para trabajar bajo presión, capacidad para trabajar en equipo, integridad y responsabilidad, capacidad de resolución de problemas, buen manejo del tiempo y reconocimiento de errores
  - Técnicas: según los servicios que proporcione el CSIRT

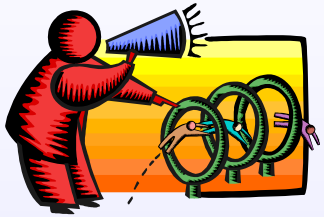
[*Handbook for CSIRTs*]

- Establecimiento de planes de formación

Entorno dinámico

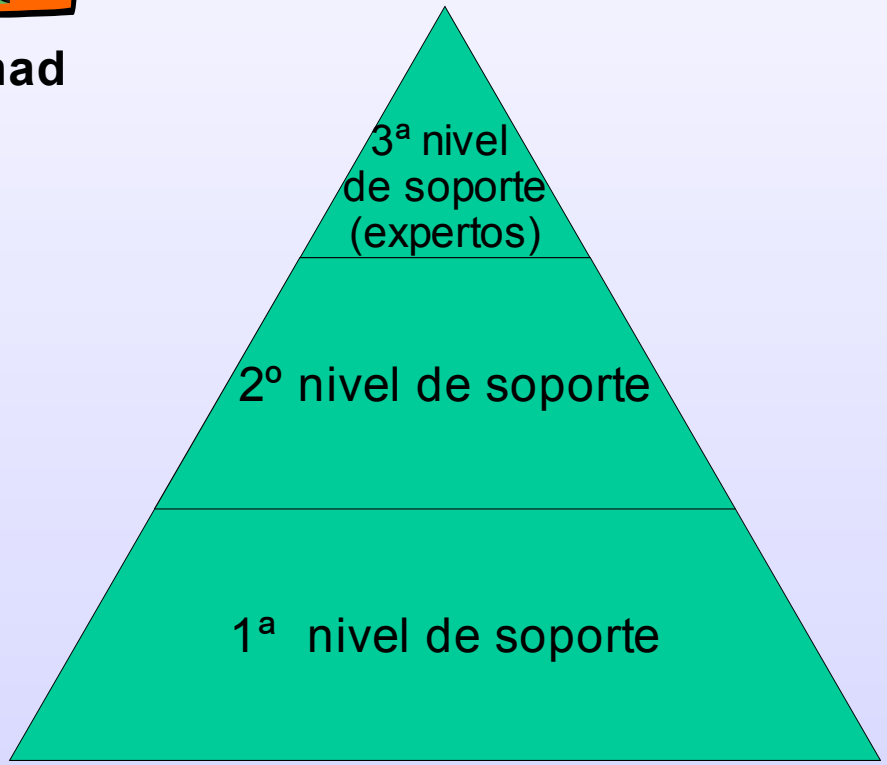
- Causas
  - Desgaste
  - Bajos salarios
- A tener en cuenta
  - Hacer que el trabajo sea variado e interesante
    - Rotación de turnos (atención de incidentes/trabajo rutinario)
    - No más del 80% esfuerzo/persona dedicado a atención de incidentes
  - Desarrollo profesional
    - Planes de formación
    - Asistencia a reuniones/conferencias/workshops
    - Participación en grupos de trabajo técnicos
    - Desarrollo de cursos
- Procedimientos formales ante la llegada/marcha del personal

Estructura del equipo



Coordinador

Mayor experiencia/habilidades



Menor experiencia/habilidades

Personal de soporte
(secretarias, RRHH, legal, administrativo, criminalístico, …)

Ubicación física

- El personal de un CSIRT maneja información sensible
  - Espacio separado, físicamente seguro
  - Habitaciones, cajones, archivadores con cerrojos
  - Backups, redes y ordenadores seguros
- Si se trabaja fuera de horario de oficina
  - Control de acceso físico
  - Espacio habitable (calefacción, comida, bebida, etc.)

Comunicaciones - Email

- La forma de contacto más común y eficiente
  - Acceso multiusuario a un único buzón
  - Una persona se puede encargar de recibir/catalogar/asignar; el resto a la gestión de incidentes
  - No consume tanto tiempo y recursos como el teléfono
- Comunicaciones seguras
  - Esencial **firma/**cifrado
  - Soporte PGP/GnuPG (estándares de facto)
    - Poco a poco X.509

Comunicaciones - Teléfono

- Más rápido, pero más intrusivo y costoso
- Un único número o un pool de extensiones
- ¿Qué clase de número?
  - Público, interno, tarifa especial, gratuito, tarifa unificada, ..
- Infraestructura de backup (ante fallos del PBX)
  - Móvil, VoIP, línea directa, ...
- ¿Qué ocurre cuando no estás en tu puesto?
- Uso de teléfonos/fax seguros

Búsqueda de contactos

- Intercambio de información y conocimiento
  - TF-CSIRT
  - FIRST
- Por incidente
  - ARIN, RIPE, APNIC, LACNIC
  - DNS
  - TF-CSIRT, FIRST
  - Abuse.net
- Objeto IRT en RIPE

  http://www.dfn-cert.de/team/matho/irt-object/

  http://www.cert.pl/cgi-bin/ipdig.pl
- EXP-CERT (Espanix)
  - ISPs locales
- GT y JJTT de RedIRIS
  - Responsables de seguridad
- *Trusted Introducer* (Europa)
  - Equipos Conocidos
  - Equipos Acreditados
    - Comprobaciones iniciales y periódicas
- FIRST (Internacional)
  - Miembros
    - Sólo comprobaciones iniciales

Comunicaciones - Acceso remoto

- ¿Se necesita acceso desde fuera de la oficina para …
  - acceder al correo o a la herramienta de gestión de incidentes?
  - acceder a los sistemas de archivos?
  - recibir/realizar llamadas telefónicas?
  - recibir alertas de emergencia (busca o SMS)?
- Túneles cifrados
  - SSL, SSH, VPN o servicio de acceso remoto
  - Sistemas de autenticación de dos partes P.ej. Token+PIN (SecurID)

Comunicaciones - Servidor WWW

- A incluir:
  - Ámbito de actuación y servicios ofrecidos
  - *Mission Statement*
  - Información de contacto
    - formularios de informe de incidente
      - http://www.sans.org/incidentforms/
  - Información y recomendaciones de seguridad
  - Procedimientos y políticas
  - FAQ, horario de operación, …
- Mantener la información actualizada
- Acceso seguro
- Versión en otros idiomas (inglés/idioma local)
- Servidor FTP anónimo

Comunicaciones - Publicidad

- Los CSIRT necesitan ser conocidos
  - En su comunidad
    - Páginas Web, listas de correo, reuniones, boletines de prensa,..
  - Fuera de su comunidad
    - Página Web, directorios, objeto IRT de RIPE, conferencias, …

Herramienta de gestión de incidentes - Requerimientos

- Debe almacenar el historial asociado a cada incidente
  - Todas las comunicaciones realizadas, acciones llevadas a cabo, ficheros de logs/evidencias (quizá cifrado)
  - Permitir a más de una persona trabajar sobre el mismo incidente si es necesario
- Es útil almacenar información adicional
  - Código de incidente, estado, prioridad, contactos, fecha, estado, …
  - Tipo de sistema atacado, tipo de incidente, causa, número de horas trabajadas, ….
- Servidor accesible de una forma segura

Razones para almacenar la información relativa a incidentes

- Mantener un archivo con el tipo de incidentes atendidos por el CSIRT a lo largo del año
- Identificación de tendencias y recopilación de estadísticas
- Mantener información detallada que pudiera ser admisible en un tribunal (si se demanda una investigación criminal)
- Administrar la carga de trabajo entre los miembros del equipo
- Proporcionar informes sobre el estado de un incidente
- Identificar tareas que se deben llevar a cabo para un incidente
- Ceder incidentes a otros miembros del equipo
- Identificar incidentes a gran escala

Características deseables

Habilidad para:	Soporte para:	Campos a almacenar:
• modificar categorización inicial • acceso y lectura a todos mensajes relacionados • acceso historial • responder a peticiones vía mail • asignar acciones y redistribuir incidentes a otros miembros del equipo • referencias cruzadas (correlación) • incident threading • clasificación • búsquedas • generar informes o estadísticas • cerrar/abrir/reabrir incidentes • uso de plantillas • activar recordatorios de incidentes que necesitan ser atendidos	• representación estandarizada de datos sobre incidentes (p.ej. IODEF) • módulo criptográfico • documentación de la cadena de custodia como parte de investigaciones • base de conocimiento • ejecución de comandos externos (consulta whois, traceroute, herramientas de análisis de logs, etc)	• información de contacto • zona horaria • información del sistema • estrategias de mitigación/resolución • acciones tomadas/recomendadas • acciones de seguimiento • coste del incidente • horas de trabajo • tiempo dedicado a su resolución • IP, descripción del problema, tipo de incidente, … • comunidad origen/destino

Herramienta de gestión de incidentes - Implementación

- Compromiso entre el sistema y los recursos humanos
  - En función a la carga de incidentes
  - Desde utilizar carpetas por incidente hasta herramientas más complejas
  - Uso de BB.DD. para realizar análisis de tendencias e informes/estadísticas
  - Automatización de tareas para maximizar la eficiencia
    - Búsqueda de contactos
    - Avisos cuando se requiere una acción sobre un incidente
    - Generación de mensajes estándar

Herramienta de gestión de incidentes - Soluciones

- No existe una solución perfecta
- Diversas soluciones disponibles
  - BB.DD. personalizadas, *helpdesk*, herramienta de seguimiento de incidencias, …
  - Libre distribución/comerciales
  - La mayoría necesitan algún tipo de personalización

CHIHT - *Clearinghouse of Incident Handling Tools*

http://chiht.dfn-cert.de/

MS Access, PostgreSQL, PHP, Oracle, MS SQL, RT/RTIR, Jitterbug, Clarify, Remedy, Magic Desk, …

Sistemas de monitorización

- Servicio de alerta temprana
  - Monitorización de logs - syslog, firewall, router (automático)
  - IDS/NIDS – cuidado con los falsos positivos
  - Chequeos de integridad - tripwire
  - Monitorización de configuraciones - routers y firewalls
  - Escaneo de puertos - routers, hosts, firewall
- Automatización
- Cooperación con la comunidad y propietarios de sistemas

Máquinas/Servidores

- Máquinas/portátiles de uso exclusivo para el personal
- Servidores e impresoras seguros e independientes
  - correo, gestión de incidentes, WWW
  - Backups independientes o cifrados
- Laboratorio de pruebas
- Si se realiza análisis forense es necesario disponer de un espacio de trabajo seguro

Procedimientos

- Preincidente
  - Reducción de riesgos
  - Preparar tanto al CSIRT como a usuarios
- Respuesta de Incidentes
- Postincidente
  - Analizar que es lo que ha ocurrido
  - Aprender la lección de otros CSIRTs y de la comunidad
- Monitorización/Informes

- Como mínimo, seguir "*CSIRT Best Practice*"
  - RFC 2350 (*Expectations for Computer Security Incident Response*)
  - RFC 2196 (*Site Security Handook*)

Procedimientos Preincidente

- Elaboración de políticas y planes
- Trabajo proactivo
  - Puede no ser función del CSIRT (pero alguien lo tiene que hacer)
- Información y herramientas
  - Lista de contactos internos y externos (creación y mantenimiento)
  - Lista de direcciones IP internas y externas (creación y mantenimiento)
  - *Response Toolkits* (creación y mantenimiento)
- Publicidad
  - Para resolver los incidentes tendrás que comunicarte con diversas personas
  - Asegúrate que te conocen y confían en ti de

Políticas y Planes (I)

- Código de conducta (organización)
  - Conjunto de reglas generales que rigen el comportamiento de los individuos de acuerdo al propósito, función y carácter de la organización
  - No más de una página
- Política de categorización de la información (CSIRT)
  - Para evitar inconsistencias y un servicio inapropiado
  - P.ej. información sensible/otro tipo, interna/externa/pública
- Política de divulgación/diseminación de información (CSIRT)
  - Guía sobre qué se puede decir, a quién y cuando

Políticas y Planes (II)

- Política con los medios de comunicación (organización)
  - Establecer reglas de comportamiento con los medios de comunicación
    - ¿Quien hará de interface con los medios?
- Política antes posibles errores humanos (organización)
  - Declaración de las posibilidades de los empleados ante errores o malos resultados; posibles consecuencias y acciones de la dirección

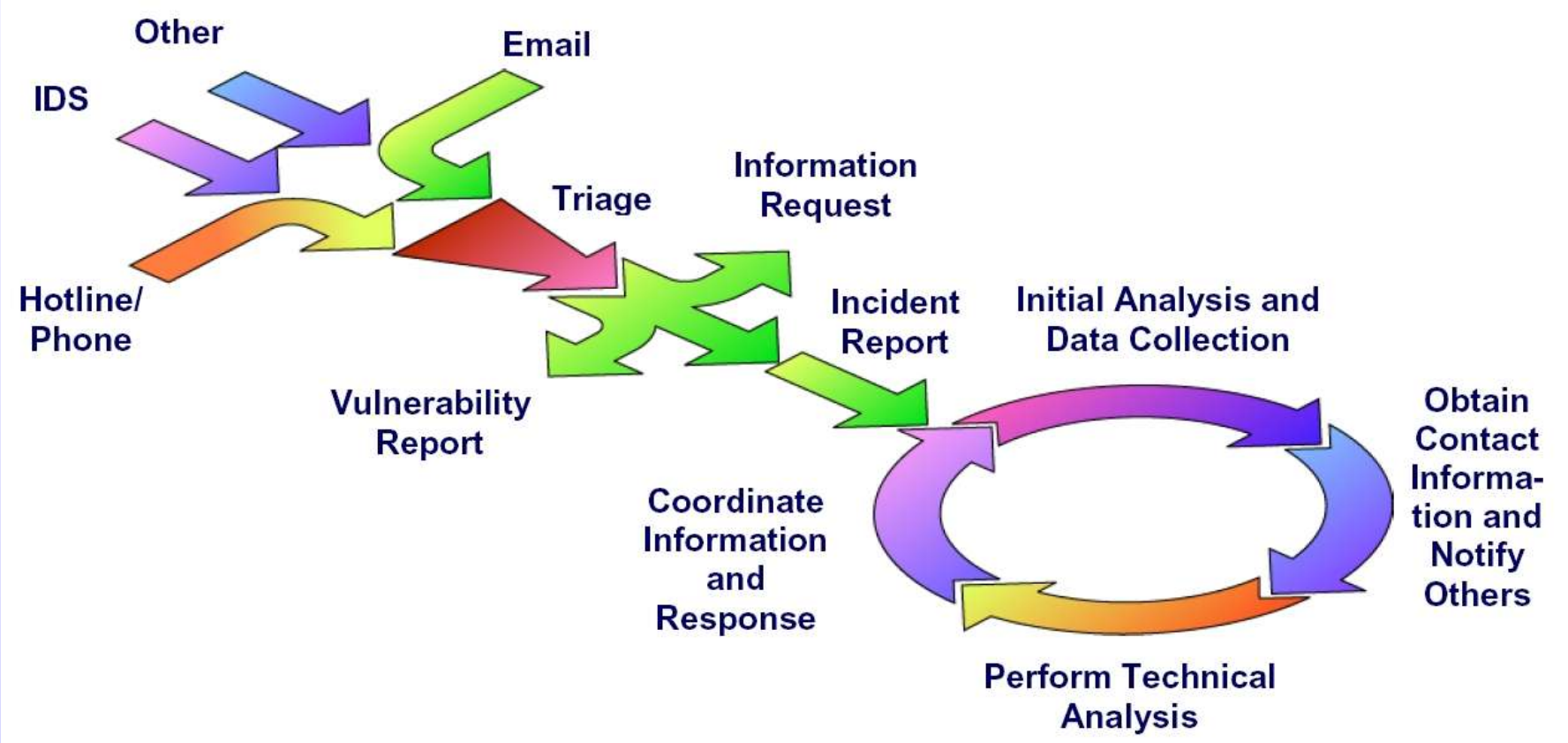
Políticas y Planes (III)

- Política de seguridad (organización)
  - Declaración formal de reglas que deben aceptar y cumplir todas aquellas personas que tienen acceso a la tecnología y bienes de una organización
  - Define qué se requiere, qué está permitido, y qué es aceptable
  - Define la autoridad y las responsabilidades
- Plan de seguridad (organización)
  - Qué se proporciona, quien lo recibe y quién lo proporciona
- Plan/Política de Respuesta de Incidentes (CSIRT)
  - Como y cuando será la respuesta y en qué consistirá
    - Política → http://www.securityfocus.com/infocus/1467
    - Plan → RFC 2350

Políticas y Planes (IV)

- Todos estos documentos deben estar relacionados entre sí
- No es necesario que sean extensos
  - Simples y claros
  - No abusar de lenguaje legal
    - Deseable revisión por el departamento legal
  - Deben reflejar la realidad

Ciclo de vida de un incidente



Procedimientos de Respuesta de Incidente

Documenta, o al menos piensa, qué hacer en cada paso:

1. Recepción y evaluación
2. Registro
3. Identificación y Análisis
4. Notificación (inicial y cuando haya más información disponible)
5. Escalado (por tipo de incidente o nivel de servicio)
6. Contención
7. Recopilación de evidencias
8. Recuperación

1. Recepción y Evaluación

¿Se trata de un incidente real?
¿Cómo de urgente es su resolución?

- Proceso de ordenación, categorización y priorización de los informes entrantes
  - Usar criterios previamente acordados (p.ej. ¿como de crítica es la máquina?)
    - Definir unos niveles de prioridad (baja, normal, alta, emergencia)
    - Definir una Taxonomía de alto nivel
      - INCH WG – IETF
        - http://www.ietf.org/html.charters/inch-charter.html
    - Puede depender del origen de la denuncia
  - De acuerdo con la Política de Seguridad y de Respuesta de Incidentes
- La prioridad/categoría puede cambiar con el

1. Registro

Registro de lo que tenemos, y de todo lo que vaya sucediendo y se vaya descubriendo

- Automatizar todo lo que sea posible
  - Al menos almacenar código de referencia/persona/fecha/hora en la que se realiza cada acción
  - Útil almacenar costes generados
- Esencial para:
  - aprender de la experiencia
  - generar de estadísticas, informes, e identificar tendencias
  - transferir/compartir el trabajo sobre incidentes
  - procesos judiciales
  - identificar tareas pendientes sobre incidentes
  - controlar la carga de trabajo del personal
  - correlacionar incidentes e identificar incidentes a gran escala

1. Identificación y Análisis

Recopilar y analizar todas las evidencias necesarias

- Para tener una idea clara del problema y su alcance
- Útil disponer de guías sobre recopilación de evidencias

- RFC 3227 (*Guidelines for Evidence Collection and Archiving*)
  - Los distintos sistemas legales tienen distintas reglas
- RFC 2196 (*Site Security Handook*). Capítulo 5.3.3 (Evaluación de daños)

1. Notificación

Notificación rápida y consistente a la/s persona/s adecuadas

- Parte del IRP
  - Proceso bien definido incluyendo el uso de plantillas
  - Contactar con todas las partes identificadas como esenciales para la resolución del incidente
  - Depende del SLA
- Notificaciones origen de denuncia
  - En muchas ocasiones para pedir información adicional (uso de formularios para evitar este problema)
  - Progresos realizados y resolución del problema
- Notificaciones destino de la denuncia
  - De acuerdo con la Política de divulgación/diseminación de información
  - Evitar el pánico
    - Mantener la calma, ser objetivo y profesional

Escalado y Contención

1. Escalado

   Modificar prioridad/categoría en función a la nueva información disponible

   - Para atender los incidentes por orden de preferencia real
   - Maximizar los recursos
   - Depende del SLA

4. Contención

   Como evitar daños mayores

   - Acordar acciones de antemano para ciertos tipos de incidentes
     - La rapidez es la clave
     - Sobre todo en horarios fuera de oficina
   - Conocer los puntos de control clave

Recopilación de evidencias y Recuperación

1. **Recopilación de Evidencias**

¿Se necesitan recopilar evidencias para procesos judiciales o sanciones disciplinarias?

- Herramientas e implicaciones legales conocidas de antemano
- Útil proporcionar guías
- Anotar todo lo que ocurra (notas firmadas y fechadas)
  - Uso de criptografía
  - Asesoramiento legal para determinar la forma de almacenar la información
- RFC 3227 (*Guidelines for Evidence Collection and Archiving*)
- RFC 2196 (*Site Security Handbook*) . Capítulo 5.4.2

5. **Recuperación**

Devolver el sistema y los datos a un estado seguro y no vulnerable

- Útil proporcionar guías

Plan de Respuesta de Incidentes (IRP)

- Aproximación *botton-up* (existe experiencia previa)
  - Poner en práctica lo que sabes acerca de atención de incidentes
    - Pensar en un incidente
      1. Anotar todos los pasos realizados desde su recepción hasta su resolución
- Aproximación *top-down* (no existe experiencia previa)
  - En función a lo que la organización requiere/espera del CSIRT
    - Pensar en lo que la organización necesita y porqué ha decido establecer un CSIRT
      1. Comprender las prioridades de la organización, que espera ganar y los beneficios que va a aportar el CSIRT

4. Anotar los recursos/autoridad que se necesita para desempeñar las tareas anteriores

Procedimientos Postincidente

- Castigo/Sanción
  - Identificar al atacante
  - Sancionar, procesar o demandar por los daños causados (si es necesario)
  - En muchos casos el CSIRT no podrá emprender acciones legales en nombre de terceros
- Monitorización extra de los sistemas recuperados
- Repasar notas y registro del incidente
  - Aprender de los errores
- Determinar el impacto del incidente

Objetivo: Reducir la probabilidad de que el incidente ocurra otra vez

Aprender de la experiencia

- Regularmente, y después de un incidente
  - Comprobar que la política todavía se ajusta a las necesidades
  - Asegurar que los procedimientos todavía funcionan y son aplicables
- Mantener/Mejorar
  - Auditar una selección de sistemas
  - Poner en marcha sesiones de formación y sistemas de alerta para los usuarios
  - Evitar auditorias propias si es posible

Monitorización/Informes

- Buena práctica para el desarrollo de los servicios
  - Informes y estadísticas
  - Monitorización para identificar cuellos de botella y nuevos requerimientos
  - Debe ser parte de un Sistema de Calidad
- Algunas veces se requiere desde la organización/comunidad

Muchas Gracias

chelo.malagon@rediris.es

;-)