CÓMO CREAR UN CSIRT PASO A PASO

Producto WP2006/5.1(CERT-D1/D2)

Índice

1 Resumen de gestión

El presente documento describe el proceso de creación de un equipo de respuesta a incidentes de seguridad informática (CSIRT) desde todas las perspectivas pertinentes, como la gestión empresarial, la gestión de procesos y el punto de vista técnico. Este documento recoge dos de los productos descritos en el apartado 5.1 del Programa de trabajo de la ENISA para 2006:

- El presente documento: *«Informe escrito sobre cómo crear un CERT o una instalación similar paso a paso, con ejemplos»* (**CERT-D1**).
- El capítulo 12 y ficheros exteriores: «*Extracto del plan de trabajo detallado que permite aplicarlo fácilmente en la práctica»* (**CERT-D2**).

2 Aviso jurídico

3 Agradecimientos

La ENISA desea dar las gracias a todas las instituciones y personas que han contribuido a la realización de este documento, y en especial a:

- Henk Bronk, consultor que produjo de la primera versión del documento.
- CERT/CC, y sobre todo al equipo de desarrollo de CSIRT, que aportó material de gran utilidad, así como las muestras de material del anexo.
- GovCERT.NL, que facilitó *CERT-in-a-box.*

- El equipo de TRANSITS, que aportó la muestra de material del anexo.
- Los compañeros de la sección de Políticas de seguridad del Departamento técnico, autores del apartado 6.6.
- Las incontables personas que revisaron el documento.

4 Introducción

Las redes de comunicación y los sistemas de información constituyen ya un factor esencial del desarrollo económico y social. La informática y las redes se han convertido en servicios públicos ubicuos, del mismo modo que la electricidad y el agua corriente.

Por ello, la seguridad de las redes de comunicación y los sistemas de información, y en particular su disponibilidad, son una cuestión que afecta cada vez más a la sociedad, pues los sistemas de información más importantes pueden enfrentarse a problemas debido a la complejidad de los sistemas, a accidentes, a errores y a ataques a las infraestructuras físicas que prestan servicios vitales para el bienestar de los ciudadanos de la UE.

El 10 de marzo de 2004 se creó una Agencia Europea de Seguridad de las Redes y de la Información (ENISA)[1]. Su objetivo era garantizar un nivel elevado y efectivo de seguridad de las redes y de la información en la Comunidad Europea y desarrollar una cultura de la seguridad de las redes y la información en beneficio de los ciudadanos, los consumidores, las empresas y las organizaciones del sector público de la Unión Europea, contribuyendo así al funcionamiento armonioso del mercado interior.

Desde hace varios años, diferentes grupos europeos dedicados a la seguridad, como los CERT/CSIRT, los equipos de detección y respuesta a abusos y los WARP, colaboran para que Internet sea más seguro. La ENISA desea apoyar el esfuerzo realizado por estos grupos aportando información acerca de las medidas que garantizan un nivel adecuado de calidad de los servicios. Además, la Agencia desea potenciar su capacidad de asesorar a los Estados miembros de la UE y los órganos comunitarios en cuestiones relacionadas con la cobertura de grupos específicos de usuarios de las TI con servicios de seguridad adecuados. Por lo tanto, basándose en los resultados del Grupo de trabajo ad-hoc de cooperación y apoyo a los CERT, creado en 2005, este nuevo Grupo de trabajo se encargará de asuntos relativos a la prestación de servicios de seguridad adecuados («servicios de los CERT») a (categorías o grupos de) usuarios específicos.

La ENISA apoya la creación de nuevos CSIRT con la publicación del presente informe, «*Cómo crear un CSIRT paso a paso con una lista de comprobación complementaria»,* que ayudará al lector a crear su propio CSIRT.

[1] Reglamento (CE) nº 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información. Una «agencia europea» es un órgano creado por la UE para realizar una tarea técnica, científica o de gestión muy concreta perteneciente al «ámbito comunitario» («primer pilar») de la UE.

Público destinatario

Los principales grupos destinatarios de este informe son las instituciones, públicas o no, que decidan crear un CSIRT para proteger su propia infraestructura de TI o la de sus grupos de interés.

Cómo utilizar este documento

Este documento explica qué es un CSIRT, qué servicios puede prestar y qué pasos hay que dar para ponerlo en marcha. De este modo se pretende presentar al lector una visión general adecuada y práctica del enfoque, la estructura y el contenido de la creación de un CSIRT.

El capítulo 4, *«Introducción»,* es una introducción al presente informe.

El capítulo 5, *«Estrategia general de planificación y creación de un CSIRT»,* define en su primer apartado qué es un CSIRT. También da información sobre los diferentes entornos en que puede funcionar un CSIRT y los servicios que puede prestar.

En el capítulo 6, *«Desarrollar un plan comercial»,* se describe el enfoque de la gestión comercial del proceso de creación.

El capítulo 7, *«Promover el plan comercial»,* se ocupa del modelo de negocio y las cuestiones relacionadas con la financiación.

El capítulo 8, *«Ejemplos de procedimientos operativos y técnicos»,* describe el procedimiento de adquisición de la información y su inclusión en un boletín de seguridad. También describe un proceso de tratamiento de incidentes.

El capítulo 9, *«Formación del personal del CSIRT»,* ofrece un resumen de la formación que puede ofrecer un CSIRT. A título de ejemplo, en el anexo se presenta una muestra de material didáctico.

El capítulo 10, *«Ejercicio: producción de un aviso»,* contiene un ejercicio sobre la realización de uno de los servicios básicos (o centrales) del CSIRT: la producción de un boletín de seguridad (o aviso).

El capítulo 12, *«Descripción del plan de proyecto»,* se centra en el plan de proyecto complementario (lista de comprobación) que se incluye en esta guía. Dicho plan tiene como objetivo ser una herramienta fácil de usar para la aplicación de esta guía.

Convenciones usadas en este documento

Para orientar al lector, cada capítulo empieza con un resumen de los pasos dados hasta el momento en el proceso de creación de un CSIRT. Dichos resúmenes se presentan en recuadros como el siguiente:

Hemos dado el primer paso.

Cada capítulo concluye con un ejemplo práctico de los pasos tratados. En este documento, el «CSIRT ficticio» será un pequeño CSIRT independiente de una institución o empresa mediana. En el apéndice se incluye un resumen.

CSIRT ficticio

5 Estrategia general de planificación y creación de un CSIRT

Para que el proceso de creación de un CSIRT empiece con buen pie, es importante tener una idea clara de los servicios que el equipo puede prestar a sus clientes, a los que en el «mundo de los CSIRT» se suele llamar «grupo atendido» o «grupo de clientes atendido». Por lo tanto, es necesario conocer las necesidades de los clientes atendidos, para prestarles servicios adecuados en el momento preciso y con la calidad necesaria.

¿Qué es un CSIRT?

CSIRT significa *Computer Security Incident Response Team* (equipo de respuesta a incidentes de seguridad informática). El término CSIRT es el que se suele usar en Europa en lugar del término protegido CERT, registrado en EE.UU. por el *CERT Coordination Center* (CERT/CC).
Se usan diferentes abreviaturas para el mismo tipo de equipos:

- CERT o CERT/CC *(Computer Emergency Response Team / Coordination Center,* equipo de respuesta a emergencias informáticas / Centro de coordinación)
- CSIRT *(Computer Security Incident Response Team,* equipo de respuesta a incidentes de seguridad informática)
- IRT *(Incident Response Team,* equipo de respuesta a incidentes)
- CIRT *(Computer Incident Response Team,* equipo de respuesta a incidentes informáticos)
- SERT *(Security Emergency Response Team,* equipo de respuesta a emergencias de seguridad)

La primera vez que apareció un gusano importante en la infraestructura global de TI fue a finales de los años ochenta. El gusano, llamado Morris[2], se propagó rápidamente y logró infectar numerosos sistemas de TI de todo el mundo.

Este incidente actuó como una alarma: de repente todo el mundo se dio cuenta de que existía una gran necesidad de cooperación y coordinación entre administradores de sistemas y gestores de TI para enfrentarse a este tipo de casos. Por ser el tiempo un factor decisivo, se tenía que establecer un enfoque más organizado y estructural de la gestión de los incidentes relacionados con la seguridad de las TI. Así, unos días después del «incidente Morris», la DARPA *(Defence Advanced Research Projects Agency,* Agencia de Investigación de Proyectos Avanzados de Defensa) creó el primer CSIRT: el *CERT Coordination Center* (CERT/CC[3]), ubicado en la Universidad Carnegie Mellon, en Pittsburgh (Pensilvania).

Poco después el modelo se adoptó en Europa, y en 1992 el proveedor académico holandés SURFnet puso en marcha el primer CSIRT de Europa, llamado SURFnet-CERT[4]. Siguieron otros muchos equipos, y en la actualidad el «*Inventario de actividades*

[2] Más información acerca del gusano Morris en http://en.wikipedia.org/wiki/Morris_worm.

[3] CERT-CC, http://www.cert.org.

[4] SURFnet-CERT: http://cert.surfnet.nl/.

de CERT en Europa» de la ENISA[5] incluye más de 100 equipos bien conocidos localizados en Europa.

Con el tiempo, los CERT ampliaron sus capacidades y pasaron de ser una mera fuerza de reacción a prestadores de servicios de seguridad completos que incluyen servicios preventivos como alertas, avisos de seguridad, formación y servicios de gestión de la seguridad. Pronto el término «CERT» se consideró insuficiente, y a finales de los años noventa se acuñó el término «CSIRT». En la actualidad, ambos términos (CERT y CSIRT) se usan como sinónimos, si bien CSIRT es el más preciso de los dos.

5..1 La expresión *«clientes atendidos »*

A partir de ahora (en las colectivos CSIRT), utilizaremos el término «grupo atendido» o «grupo de clientes atendido» para referirnos a la base de clientes de un CSIRT.

5..2 Definición de CSIRT

Un CSIRT es un equipo de expertos en seguridad de las TI cuya principal tarea es responder a los incidentes de seguridad informática. El CSIRT presta los servicios necesarios para ocuparse de estos incidentes y ayuda a los clientes del grupo al que atienden a recuperarse después de sufrir uno de ellos.

Para mitigar los riesgos y minimizar el número de respuestas necesarias, la mayor parte de los CSIRT ofrecen también a sus clientes servicios preventivos y educativos. Publican avisos sobre las vulnerabilidades del software y el hardware en uso e informan a los usuarios sobre los programas maliciosos y virus que se aprovechan de estas deficiencias. De este modo, los clientes atendidos pueden corregir y actualizar rápidamente sus sistemas. Véase en el apartado 5.2, *«Servicios posibles de un CSIRT»,* una lista completa de los servicios posibles.

5..3 Ventajas de tener un CSIRT

Disponer de un equipo dedicado a la seguridad de las TI ayuda a las organizaciones a mitigar y evitar los incidentes graves y a proteger su patrimonio.

Otras posibles ventajas son:

- Disponer de una coordinación centralizada para las cuestiones relacionadas con la seguridad de las TI dentro de la organización (punto de contacto).
- Reaccionar a los incidentes relacionados con las TI y tratarlos de un modo centralizado y especializado.
- Tener al alcance de la mano los conocimientos técnicos necesarios para apoyar y asistir a los usuarios que necesitan recuperarse rápidamente de algún incidente de seguridad.
- Tratar las cuestiones jurídicas y proteger las pruebas en caso de pleito.
- Realizar un seguimiento de los progresos conseguidos en el ámbito de la seguridad.
- Fomentar la cooperación en la seguridad de las TI entre los clientes del grupo atendido (sensibilización).

[5] Inventario de ENISA: http://www.enisa.europa.eu/cert_inventory/

CSIRT ficticio (paso 0)

Entender qué es un CSIRT:

El CSIRT de muestra tendrá que servir a una organización mediana con una plantilla de 200 trabajadores. La organización tiene su propio departamento de TI y otras dos sucursales en el mismo país. Las TI desempeñan un papel muy importante en la empresa, pues se utilizan para la comunicación interna, en las redes de datos y en un servicio electrónico 24 horas al día, 7 días a la semana. La organización dispone de una red propia y de una conexión redundante a Internet por medio de dos proveedores de servicios de Internet diferentes.

5..4 Descripción de los diferentes tipos de CSIRT

Hemos dado el primer paso:

1. Entender qué es un CSIRT y qué puede aportar.

>> El próximo paso será responder a la pregunta siguiente: *«¿A qué sector prestará servicios el CSIRT?»*

Cuando se pone en marcha un CSIRT es muy importante, como con cualquier otro negocio, formarse una idea clara de quiénes forman su grupo de clientes y a qué tipo de entorno se enfocarán los servicios que se presten. Actualmente distinguimos los «sectores» siguientes:

- CSIRT del sector académico
- CSIRT comercial
- CSIRT del sector de la protección de la información vital y de la información y las infraestructuras vitales (CIP/CIIP)
- CSIRT del sector público
- CSIRT interno
- CSIRT del sector militar
- CSIRT nacional
- CSIRT del sector de la pequeña y mediana empresa (PYME)
- CSIRT de soporte

CSIRT del sector académico

Descripción

Los CSIRT del sector académico prestan servicios a centros académicos y educativos, como universidades o centros de investigación, y a sus campus virtuales.

Grupo de clientes atendido

El grupo típico de clientes atendido por estos CSIRT está formado por el personal y los estudiantes de las universidades.

CSIRT comercial

Descripción

Los CSIRT comerciales prestan servicios comerciales a sus clientes. En el caso de un proveedor de servicios de Internet, el CSIRT presta principalmente servicios relacionados con el abuso a los clientes finales (conexión por marcación telefónica, ADSL) y servicios de CSIRT a sus clientes profesionales.

Grupo de clientes atendido
Por lo general, los CSIRT comerciales prestan sus servicios a un grupo de clientes que paga por ello.

CSIRT del sector CIP/CIIP
Descripción
Los CSIRT de este sector se centran principalmente en la protección de la información vital (CIP) y de la información y las infraestructuras vitales (CIIP). Por lo general, estos CSIRT especializados colaboran estrechamente con un departamento público de protección de la información y las infraestructuras vitales. Estos CSIRT abarcan todos los sectores vitales de las TI del país y protegen a los ciudadanos.

Grupo de clientes atendido
Sector público; empresas de TI de importancia fundamental; ciudadanos.

CSIRT del sector público
Descripción
Los CSIRT del sector público prestan servicios a agencias públicas y, en algunos países, a los ciudadanos.

Grupo de clientes atendido
Las administraciones y sus agencias. En algunos países también prestan servicios de alerta a los ciudadanos (por ejemplo, en Bélgica, Hungría, los Países Bajos, el Reino Unido y Alemania).

CSIRT interno
Descripción
Los CSIRT internos únicamente prestan servicios a la organización a la que pertenecen, lo que describe más su funcionamiento que su pertenencia a un sector. Numerosas organizaciones de telecomunicaciones y bancos, por ejemplo, cuentan con sus propios CSIRT internos. Por regla general, estos CSIRT no mantienen sitios web públicos.

Grupo de clientes atendido
Personal y departamento de TI de la organización a la que pertenece el CSIRT.

CSIRT del sector militar
Descripción
Los CSIRT de este sector prestan servicios a organizaciones militares con responsabilidades en infraestructuras de TI necesarias con fines de defensa.

Grupo de clientes atendido
Personal de instituciones militares y de entidades estrechamente relacionadas con éstas, como por ejemplo del Ministerio de Defensa.

CSIRT nacional
Descripción
Un CSIRT nacional se considera un punto de contacto de seguridad del país. En algunos casos, el CSIRT del sector público también actúa como punto de contacto nacional (como sucede con UNIRAS en el Reino Unido).

Grupo de clientes atendido
Este tipo de CSIRT no suele tener un grupo de clientes directo, pues se limita a desempeñar un papel de intermediario para todo el país.

CSIRT del sector de la pequeña y mediana empresa (PYME)
Descripción
Se trata de un CSIRT organizado por sí mismo que presta servicios a las empresas del ramo o a un grupo de usuarios similar.

Grupo de clientes atendido
El grupo de clientes atendido por estos CSIRT pueden ser las PYME y su personal, o grupos de interés especial como la «Federación de municipios» de un país.

CSIRT de soporte
Descripción
Los CSIRT de soporte se centran en productos específicos. Suelen tener por objetivo desarrollar y facilitar soluciones para eliminar vulnerabilidades y mitigar posibles efectos negativos.

Grupo de clientes atendido
Propietarios de productos.

Tal como se describe a propósito de los CSIRT nacionales, a veces un mismo equipo sirve a diferentes sectores. Esto influye, por ejemplo, en el análisis de los clientes atendidos y sus necesidades.

CSIRT ficticio (paso 1)
Fase inicial En la fase inicial, el nuevo CSIRT se organiza como un CSIRT interno que presta servicios a la empresa a la que pertenece, el departamento de TI local y su personal. También apoya y coordina entre las diferentes sucursales el tratamiento de los incidentes relacionados con la seguridad de las TI.

Servicios posibles de un CSIRT

Hemos dado los dos primeros pasos:

1. Entender qué es un CSIRT y qué puede aportar.
2. Determinar a qué sector prestará servicios el nuevo CSIRT.

>> El próximo paso será responder a la pregunta siguiente: *«¿Qué servicios se prestarán a los clientes atendidos?»*

Son muchos los servicios que un CSIRT puede prestar, pero hasta ahora ningún CSIRT los presta todos. Así pues, la selección del conjunto adecuado de servicios constituye una decisión crucial. A continuación se presenta una breve visión general de todos los servicios conocidos de CSIRT, tal como se definen en el «Manual del CSIRT» publicado por el CERT/CC[6].

Servicios reactivos	**Servicios proactivos**	**Manejo de instancias**
• **Alertas y advertencias** • **Tratamiento de incidentes** • **Análisis de incidentes** • **Apoyo a la respuesta a incidentes** • **Coordinación de la respuesta a incidentes** • Respuesta a incidentes *in situ* • Tratamiento de la vulnerabilidad • Análisis de la vulnerabilidad • Respuesta a la vulnerabilidad • Coordinación de la respuesta a la vulnerabilidad	• **Comunicados** • Observatorio de tecnología • Evaluaciones o auditorías de la seguridad • Configuración y mantenimiento de la seguridad • Desarrollo de herramientas de seguridad • Servicios de detección de intrusos • Difusión de información relacionada con la seguridad	• *Análisis de instancias* • *Respuesta a las instancias* • *Coordinación de la respuesta a las instancias* ***Gestión de la calidad de la seguridad*** • *Análisis de riesgos* • *Continuidad del negocio y recuperación tras un desastre* • *Consultoría de seguridad* • *Sensibilización* • *Educación / Formación* • *Evaluación o certificación de productos*

Fig. 1 Lista de servicios de los CSIRT del CERT/CC[7].

En los **servicios básicos (en negrita)** se distingue entre servicios reactivos y servicios proactivos. Los proactivos están orientados a la prevención de incidentes mediante la sensibilización y la formación, mientras que los reactivos se centran en el tratamiento de los incidentes y la mitigación de los daños resultantes.

El **manejo de instancias** incluye el análisis de cualquier fichero u objeto encontrado en un sistema que pueda intervenir en acciones maliciosas, como restos de virus, gusanos, secuencias de comandos, troyanos, etc. También incluye el tratamiento y la difusión de la información resultante entre los proveedores y otros interesados, con el fin de evitar que el software malicioso se siga extendiendo y mitigar los riesgos.

Los **servicios de gestión de la seguridad y la calidad** tienen objetivos a más largo plazo e incluyen la consultoría y las medidas de tipo educativo.

Véase en el apéndice una explicación detallada de los servicios de los CSIRT.

[6] Manual del CSIRT publicado por el CERT/CC: http://www.cert.org/archive/pdf/csirt-handbook.pdf.

[7] Lista de los servicios de los CSIRT del CERT/CC: http://www.cert.org/csirts/services.html.

La elección de los servicios adecuados para los clientes es muy importante y se tratará con más detalle en el apartado 6.1*, «Definir el modelo financiero»*.

La mayor parte de los CSIRT empiezan con la distribución de «alertas y advertencias», emiten «comunicados» y ofrecen «tratamiento de incidentes» a los distintos clientes del grupo. Estos servicios básicos suelen resultar valiosos para los clientes atendidos y normalmente se consideran «valor añadido» real.

Empezar con un grupo de clientes «piloto» pequeño, prestarle servicios básicos durante un periodo de tiempo «piloto» y pedirle su opinión al respecto posteriormente es una buena práctica.

Los usuarios piloto interesados suelen facilitar comentarios constructivos y ayudar a desarrollar servicios a medida.

CSIRT ficticio (paso 2)

Elección de los servicios adecuados

En la fase inicial se dispone que el nuevo CSIRT se centrará principalmente en prestar algunos de los servicios básicos a los empleados.

Se resuelve que, tras una fase piloto, se puede tomar en consideración la ampliación de la cartera de servicios y se pueden añadir algunos «servicios de gestión de la seguridad». Esta decisión se basará en los comentarios del grupo piloto y se tomará en estrecha cooperación con el Departamento de garantía de la calidad.

Análisis del grupo de clientes atendido y declaración de servicios

Hemos dado los tres primeros pasos:

1. Entender qué es un CSIRT y qué puede aportar.
2. Determinar a qué sector prestará servicios el nuevo CSIRT.
3. Establecer qué tipos de servicios puede prestar un CSIRT a su grupo de clientes.

>> El próximo paso será responder a la pregunta siguiente: *«¿Qué tipo de enfoque conviene adoptar para poner en marcha el CSIRT?»*

El próximo paso será centrarse más en el grupo de clientes atendidos con el objetivo principal de elegir los canales de comunicación adecuados:

- Definir el enfoque de la comunicación con el grupo de clientes atendido;
- Definir los servicios;
- Preparar un plan de ejecución / proyecto realista;
- Definir los servicios del CSIRT;
- Definir la estructura organizativa;

- Definir la política de seguridad de la información;
- Contratar al personal adecuado;
- Utilizar la oficina del CSIRT;
- Buscar colaboraciones con otros CSIRT y posibles iniciativas nacionales.

Estos pasos se describirán con más detalle en los párrafos siguientes y se pueden aprovechar en el plan comercial y el plan del proyecto.

5..1 Enfoque de la comunicación con el grupo de clientes atendido

Como ya hemos dicho, es muy importante conocer las necesidades del grupo de clientes atendido, tener clara la propia estrategia de comunicación y determinar cuáles son los canales de comunicación más adecuados para transmitir información al grupo.

La teoría de la gestión puede enfocar de diferentes maneras el análisis de un grupo de destinatarios. En este documento describiremos dos de ellas: los análisis DOFA y PEST.

Análisis DOFA
Un análisis DOFA es una herramienta de planificación estratégica que se usa para evaluar las **d**ebilidades, **o**portunidades, **f**ortalezas y **a**menazas de un proyecto, una empresa o cualquier otra situación que exija tomar decisiones. La técnica se atribuye a Albert Humphrey, que en los años sesenta y setenta dirigió un proyecto de investigación en la Universidad de Stanford basado en datos de las empresas incluidas en la lista Fortune 500[8].

Fortalezas	**Debilidades**
Oportunidades	**Amenazas**

Fig. 2 Análisis DOFA.

[8] Análisis DOFA en Wikipedia: http://en.wikipedia.org/wiki/SWOT_analysis.

Análisis PEST

El análisis PEST es otra herramienta importante y muy utilizada para estudiar el grupo de clientes atendido con el objetivo de entender las circunstancias **p**olíticas, **e**conómicas, **s**ocioculturales y **t**ecnológicas del entorno en que trabaja un CSIRT. Este análisis ayudará a determinar si la planificación sigue siendo adecuada al entorno y probablemente a evitar acciones basadas en premisas erróneas.

Factores políticos • Asuntos ecológicos / medioambientales • Legislación actual en el mercado local • Legislación futura • Legislación europea e internacional • Procesos y órganos reguladores • Políticas públicas • Mandato y cambio del gobierno • Políticas comerciales • Financiación, subvenciones e iniciativas • Grupos de presión del mercado local • Grupos de presión internacionales	**Factores económicos** • Situación económica local • Tendencias de la economía local • Economía y tendencias en otros países • Fiscalidad general • Fiscalidad específica de los productos y servicios • Estacionalidad y asuntos climáticos • Ciclos de mercado y comerciales • Factores específicos de la industria • Rutas comerciales y tendencias de distribución • Motivadores de los clientes / usuarios • Tipos de interés y tasas de cambio
Factores sociales • Tendencias del estilo de vida • Cuestiones demográficas • Actitud y opinión del consumidor • Opinión de los medios de comunicación • Modificaciones de la ley que afectan a factores sociales • Imagen de la marca, la empresa y la tecnología • Patrones de compra del consumidor • Moda y modelos a seguir • Grandes acontecimientos e influencias • Acceso y tendencias de compra • Factores étnicos y religiosos • Publicidad y relaciones públicas	**Factores tecnológicos** • Desarrollo de tecnologías competidoras • Financiación de la investigación • Tecnologías asociadas / dependientes • Tecnología / soluciones sustitutas • Madurez de la tecnología • Madurez y capacidad de la fabricación • Información y comunicaciones • Mecanismos / tecnología de compra • Legislación sobre tecnología • Potencial de innovación • Acceso a la tecnología, licencias, patentes • Cuestiones relacionadas con la propiedad intelectual

Fig. 3 Patrón de análisis PEST.

En Wikipedia se puede consultar una descripción detallada del análisis PEST[9].

Ambas herramientas proporcionan una visión completa y estructurada de las necesidades del grupo atendido. Los resultados completarán la propuesta comercial y, por lo tanto, ayudarán a obtener financiación para crear el CSIRT.

Canales de comunicación

Un tema importante que cabe incluir en el análisis es el de los posibles métodos de comunicación y distribución de la información («cómo comunicarse con el grupo de clientes atendido»).

[9] Análisis PEST en Wikipedia: http://en.wikipedia.org/wiki/PEST_analysis.

Conviene plantearse la posibilidad de realizar periódicamente visitas personales a los distintos clientes del grupo atendido. Está demostrado que las reuniones cara a cara facilitan la cooperación. Si ambas partes desean colaborar, estas reuniones darán lugar a una relación más abierta.

Por lo general, los CSIRT utilizan diversos canales de comunicación. Los siguientes han demostrado su utilidad práctica, por lo que merece la pena tomarlos en consideración:

- Sitio web público;
- Zona reservada a los miembros en el sitio web;
- Formularios web para comunicar incidentes;
- Listas de correo;
- Correo electrónico personalizado;
- Teléfono / fax;
- SMS;
- Las «anticuadas» cartas tradicionales, en soporte de papel;
- Informes mensuales o anuales.

Además de usar el correo electrónico, los formularios web, el teléfono o el fax para facilitar el tratamiento de los incidentes (recibir informes de incidentes del grupo de clientes atendido, coordinarse con otros equipos o realizar comentarios y prestar apoyo a la víctima), la mayoría de los CSIRT publican sus avisos de seguridad en un sitio web abierto al público y en listas de correo.

! Si es posible, la información se ha de difundir de un modo seguro. Por ejemplo, el correo electrónico puede llevar una firma digital con PGP y los datos delicados sobre incidentes siempre se deben enviar encriptados.

Para más información, véase el apartado 8.5, *«Herramientas disponibles para CSIRT»*, así como el apartado 2.3 de la *RFC2350*[10].

[10] http://www.ietf.org/rfc/rfc2350.txt.

CSIRT ficticio (paso 3a)

Análisis del grupo de clientes atendido y de los canales de comunicación adecuados

Una sesión de *brainstorming* con un grupo de directivos destacados y el grupo de clientes atendido generó datos suficientes para un análisis DOFA que permitió establecer la necesidad de servicios básicos:

- Alertas y advertencias
- Tratamiento de los incidentes (análisis, apoyo a las respuestas y coordinación de las respuestas)
- Comunicados

Se debe garantizar una difusión organizada de la información, de modo que alcance a tantos clientes del grupo atendido como sea posible. Por ello se ha resuelto que las alertas, las advertencias y los comunicados en forma de avisos de seguridad se den a conocer al público en un sitio web creado con tal fin y se comuniquen por correo electrónico. El CSIRT facilita correo electrónico, teléfono y fax para recibir los informes de incidencias. Para el próximo paso está previsto un formulario web unificado.

Véase en la página siguiente un ejemplo de análisis DOFA.

Fortalezas • La empresa tiene cierto conocimiento del tema. • Les gusta el plan y están dispuestos a colaborar. • Contamos con apoyo y fondos del Consejo de Administración.	**Debilidades** • La comunicación entre los diferentes departamentos y sucursales es escasa. • No hay coordinación con los incidentes de TI. • Fragmentación excesiva en «pequeños departamentos».
Oportunidades • Enorme flujo de información sobre la vulnerabilidad no estructurada. • Gran necesidad de coordinación. • Reducción de las pérdidas por incidentes. • Muchos cabos sueltos en cuestión de seguridad de las TI. • Educación del personal en seguridad de las TI.	**Amenazas** • Escasez de fondos. • Escasez de personal. • Grandes expectativas. • Cultura.

Fig. 4 Ejemplo de análisis DOFA.

5..2 Declaración de servicios

Tras analizar las necesidades y los deseos del grupo de clientes atendido en cuanto a los servicios del CSIRT, el paso siguiente debería ser redactar una declaración de servicios.

La declaración de servicios es una descripción de la función básica de la organización en la sociedad respecto a los productos y servicios que ofrece a sus clientes y permite comunicar con claridad la existencia y la función del nuevo CSIRT.

Se aconseja redactar una declaración de servicios compacta pero no demasiado densa, pues lo normal es que no cambie durante un par de años.

A continuación presentamos dos ejemplos de declaración de servicios de CSIRT en funcionamiento:

«<Nombre del CSIRT> ofrece información y asistencia a <sus clientes (definición del grupo de clientes atendido)> en la aplicación de medidas proactivas para reducir su

riesgo de incidentes de seguridad informática, así como para responder a tales incidentes cuando se produzcan.»

«Para ofrecer apoyo a <grupo atendido> en la prevención y la respuesta a incidentes de seguridad relacionados con las TI.»[11]

Es muy importante y necesario empezar con la declaración de servicios como primer paso. Consúltese en el apartado 2.1 de la *RFC2350*[12] una descripción más detallada de la información que debería publicar un CSIRT.

CSIRT ficticio (paso 3b)
La dirección del CSIRT ficticio ha preparado la siguiente declaración de servicios: *«El CSIRT ficticio ofrece información y asistencia al personal de la empresa a la que pertenece para reducir su riesgo de incidentes de seguridad informática, así como para responder a tales incidentes cuando se produzcan.»* De este modo, el CSIRT ficticio deja claro que es un CSIRT interno y que su cometido principal es ocuparse de las cuestiones relacionadas con la seguridad de las TI.

[11] Declaración de servicios de Govcert.nl: http://www.govcert.nl.

[12] http://www.ietf.org/rfc/rfc2350.txt.

6 Desarrollar un plan comercial

Hemos dado los pasos siguientes:

1. Entender qué es un CSIRT y qué puede aportar.
2. Determinar a qué sector prestará servicios el nuevo CSIRT.
3. Establecer qué tipos de servicios puede prestar un CSIRT a sus clientes.
4. Analizar el entorno y el grupo de clientes atendido.
5. Definir los servicios.

>> El próximo paso será definir el plan comercial.

El resultado del análisis da una buena idea de las necesidades y los puntos débiles (reconocidos) del grupo atendido, por lo que se tendrá en cuenta en el paso siguiente.

Definir el modelo financiero

Después del análisis se eligió un par de servicios básicos con los que empezar. El próximo paso será reflexionar sobre el modelo financiero: qué parámetros de la prestación de servicios son a la vez adecuados y asequibles.

En un mundo perfecto, la financiación se adaptaría a las necesidades del grupo de clientes atendido; en la realidad, la cartera de servicios que se pueden ofrecer se debe adaptar a un presupuesto dado. Por lo tanto, es más real empezar por planificar las cuestiones monetarias.

6..1 Modelo de costes

Los dos factores que más influyen en los costes son la determinación de las horas de servicio y el número (y la especialidad) de los trabajadores que se van a emplear. ¿Es necesario responder a los incidentes y prestar apoyo técnico 24 horas al día y 7 días a la semana, o basta con que se presten dichos servicios en horas de oficina?

Dependiendo de la disponibilidad deseada y del equipamiento de la oficina (por ejemplo, ¿es posible trabajar desde casa?) convendrá trabajar de guardia o con un horario programado.

Una posibilidad es prestar servicios proactivos y reactivos en horas de oficina. Fuera de este horario, habrá un trabajador de guardia que únicamente prestará determinados servicios, por ejemplo, sólo en caso de grandes desastres e incidentes.

Otra opción sería establecer cooperaciones internacionales con otros CSIRT. Ya hay ejemplos de colaboraciones que funcionan «siguiendo el sol». Por ejemplo, la cooperación entre equipos europeos y americanos ha sido provechosa y ha supuesto una buena manera de acceder a otras capacidades. El CSIRT de Sun Microsystems, por ejemplo, que cuenta con numerosas oficinas en diferentes zonas horarias de todo el

mundo (y todas ellas pertenecen al mismo CSIRT) ofrece servicios 24 horas al día y 7 días a la semana, mediante cambios de turno constantes entre equipos de todo el globo. De este modo se limitan los costes, pues los equipos trabajan siempre en horario normal de oficina y prestan servicios a la parte del mundo donde es de noche.

Es una buena práctica analizar de un modo detallado con el grupo de clientes atendido la necesidad de servicios 24 horas al día, 7 días a la semana. No tiene mucho sentido enviar alertas y advertencias por la noche si el receptor no las va a leer hasta la mañana siguiente. La línea que separa «necesitar un servicio» de «querer un servicio» es muy sutil, pero es sobre todo el horario de trabajo el que marca una diferencia enorme en la cantidad de personal y en las instalaciones necesarias, por lo que repercute en el modelo de costes.

6..2 Modelo de ingresos

Una vez conocidos los costes hay que pensar en los posibles modelos de ingresos: cómo se pueden financiar los servicios previstos. A continuación se presentan varias posibilidades que cabe evaluar:

Uso de los recursos existentes
Siempre conviene evaluar los recursos de que disponen otras partes de la empresa. ¿Hay ya personal adecuado (por ejemplo, en el departamento de TI) con la experiencia y los conocimientos necesarios? Es probable que se pueda llegar a un acuerdo con la dirección para contar con ese personal en el CSIRT en la etapa inicial, o para poder contar con esos trabajadores en caso de necesidad.

Cuotas
Otra posibilidad es vender los servicios a los clientes por una cuota anual o trimestral. Los servicios adicionales, como el asesoramiento y las auditorías de seguridad, se podrían abonar aparte.

Más posibilidades: que los servicios a los constituyentes (internos) sean gratuitos, pero los que se presten a clientes externos sean de pago. Otra idea es publicar avisos y boletines informativos en el sitio web público y contar con una sección «sólo para los miembros» en la que se dé información especial, más detallada o a medida.

La práctica ha demostrado que los fondos conseguidos mediante la «suscripción por servicio» son limitados, especialmente en la fase inicial. Por ejemplo, el equipo tiene unos costes básicos fijos y el equipamiento se ha de pagar por adelantado. La financiación de estos costes con la venta de servicios del CSIRT es difícil y requiere un análisis financiero muy detallado para encontrar un «punto de equilibrio» en que los ingresos igualen a los gastos.

Subvenciones
Otra vía que merece la pena considerar es la de pedir una subvención al Estado o a un órgano público, pues en la actualidad son muchos los países que disponen de fondos para proyectos de seguridad de las TI. Un buen principio podría ser ponerse en contacto con el Ministerio del Interior.

Evidentemente, también se pueden combinar diferentes modelos de ingresos.

Definir la estructura organizativa

La estructura organizativa adecuada de un CSIRT depende enormemente de la estructura de la organización a la que pertenece y del grupo de clientes atendido, así como de la posibilidad de contratar expertos permanentemente o para cubrir necesidades puntuales.

Un CSIRT típico define las funciones siguientes en el equipo:

General
- Director general

Personal
- Director de la oficina
- Contable
- Asesor de comunicaciones
- Asesor jurídico

Equipo técnico operativo
- Jefe del equipo técnico
- Técnicos del CSIRT, encargados de la prestación de servicios
- Investigadores

Consultores externos
- Contratados cuando se necesitan

Resulta de gran ayuda contar con un abogado en el equipo, especialmente durante la etapa inicial del CSIRT. Los costes aumentarán, pero se ahorrará tiempo y se evitarán problemas legales.

Dependiendo de la variedad de conocimientos técnicos del grupo atendido, si la visibilidad del CSIRT es considerable también resulta muy útil contar con un experto en comunicaciones. Estos expertos pueden traducir las cuestiones técnicas difíciles en mensajes más comprensibles para el grupo de clientes atendido. El experto en comunicaciones también hará llegar a los expertos técnicos comentarios del grupo atendido, trabajando como «traductor» y «coordinador» entre ambos grupos.

A continuación presentamos algunos ejemplos de modelos organizativos en uso en CSIRT operativos:

6..1 El modelo de empresa independiente

Es un CSIRT extendido que actúa como una organización independiente, con sus propios directivos y empleados.

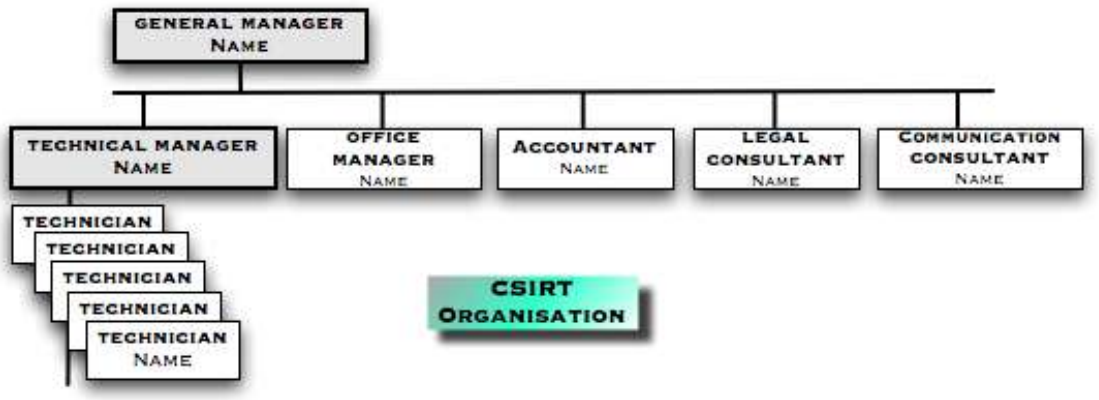


Fig. 5 Modelo de empresa independiente.

6..2 El modelo incrustado

Este modelo se puede usar si se va a crear un CSIRT dentro de una organización existente, usando un departamento de TI ya existente, por ejemplo. El CSIRT está dirigido por un jefe de equipo responsable de las actividades. El jefe de equipo reúne a los técnicos necesarios cuando resuelve incidentes o trabaja en actividades del CSIRT. Puede pedir asistencia especializada a la organización existente.

Este modelo también se puede adaptar a situaciones concretas que vayan surgiendo. En este caso, el equipo tiene asignado un número fijo de trabajadores a tiempo completo o equivalentes. Por ejemplo, el departamento de quejas de un proveedor de servicios de Internet es, sin duda, un empleo a tiempo completo para un trabajador a tiempo completo o equivalente o (en la mayoría de los casos) para más de uno.

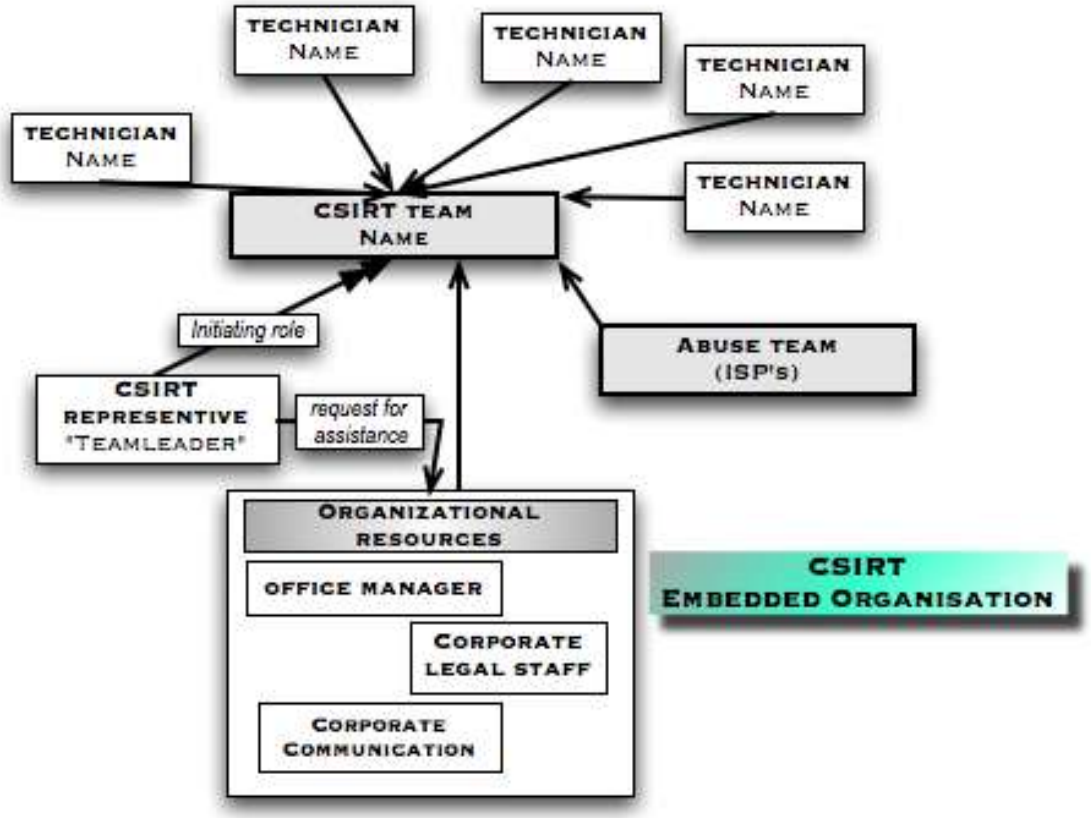


Fig. 6 Modelo organizativo incrustado.

6..3 El modelo universitario

Como su nombre indica, el modelo universitario es el que adoptan principalmente los CSIRT académicos y de investigación. La mayor parte de las organizaciones académicas y de investigación están formadas por diversas universidades y campus con diferentes ubicaciones, diseminados por una región o incluso por todo un país (como en el caso de las Redes nacionales de investigación). Por lo general estas organizaciones son independientes entre sí y poseen su propio CSIRT. Estos CSIRT se suelen organizar en torno a un CSIRT «madre» o CSIRT central que los coordina y es el único punto de contacto con el mundo exterior. Por lo general, el CSIRT central ofrece también servicios básicos, además de distribuir información sobre incidentes entre los CSIRT universitarios adecuados.

Algunos CSIRT intercambian sus servicios básicos con los otros CSIRT universitarios, con lo que los gastos generales del CSIRT central disminuyen.

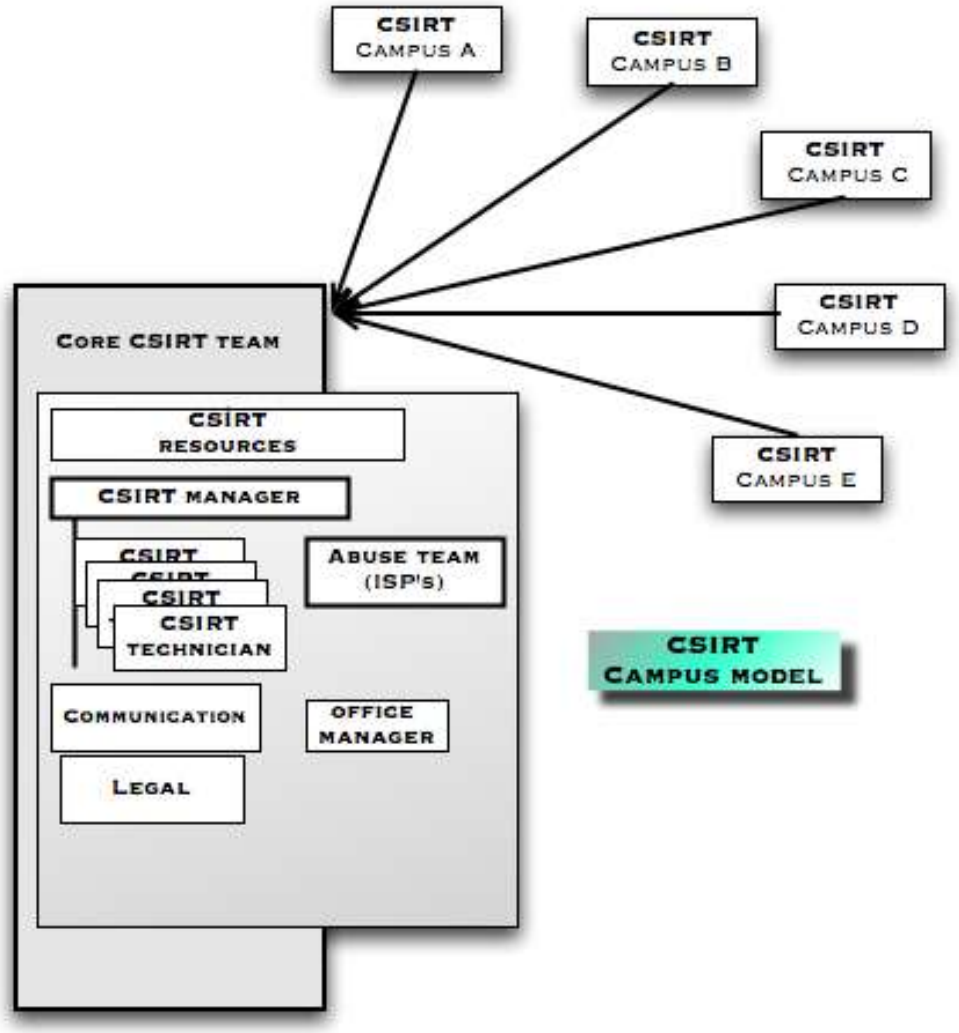


Fig. 7 Modelo universitario.

6..4 El modelo voluntario

Este modelo corresponde a un grupo de personas (especialistas) que se unen para asesorarse y apoyarse entre sí (y para asesorar y apoyar a otros) voluntariamente. Se trata de un colectivo que actúa de forma espontánea y depende enormemente de la motivación de los participantes.

Este modelo lo adopta, por ejemplo, el colectivo WARP[13].

Contratar al personal adecuado

Tras decidir qué servicios se prestarán y qué nivel de apoyo se dará y elegir el modelo organizativo, el próximo paso será encontrar el número adecuado de trabajadores cualificados.

Es casi imposible presentar cifras reales sobre el número de técnicos necesarios desde este punto de vista, pero los valores siguientes han demostrado ser una buena aproximación:

- Para prestar dos servicios básicos (distribución de boletines de seguridad y tratamiento de incidentes): un mínimo de **4** trabajadores a tiempo completo o equivalentes.

- Para un servicio completo en horario de oficina y servicios de mantenimiento: un mínimo de **entre 6 y 8** trabajadores a tiempo completo o equivalentes.

- Para un turno dotado de todo el personal necesario 24 horas al día, 7 días a la semana (2 turnos fuera del horario de oficina), el mínimo es de unos **12** trabajadores a tiempo completo o equivalentes.

Estas cifras también tienen en cuenta las bajas por enfermedad, las vacaciones, etc. Por otra parte, hay que consultar los convenios laborales locales. El trabajo fuera del horario de oficina puede suponer otros costes por pago de complementos.

A continuación se presenta una breve visión general de las principales competencias de los expertos técnicos de un CSIRT

Descripción general de los cometidos del personal técnico:

Capacidades personales

- Flexibilidad, creatividad y espíritu de equipo.
- Gran capacidad de análisis.
- Capacidad de tratar cuestiones técnicas de una manera sencilla.
- Confidencialidad y capacidad de trabajo sistemático.
- Buenas aptitudes organizativas.
- Resistencia al estrés.

[13] Iniciativa WARP: http://www.enisa.europa.eu/cert_inventory/pages/04_02_02.htm#12

- Gran capacidad para comunicarse y escribir.
- Mente abierta y ganas de aprender.

Competencias técnicas

- Amplio conocimiento de la tecnología y los protocolos de Internet.
- Conocimiento de los sistemas Linux y Unix (dependiendo del equipo del grupo de clientes atendido).
- Conocimiento de los sistemas Windows (dependiendo del equipo del grupo de clientes atendido).
- Conocimiento de los equipos de infraestructura de redes (enrutador, switches, DNS, proxy, correo, etc.).
- Conocimiento de las aplicaciones de Internet (SMTP, HTTP(s), FTP, telnet, SSH, etc.).
- Conocimiento de las amenazas a la seguridad (DDoS, phishing, defacing, sniffing, etc.).
- Conocimiento de la evaluación del riesgo y las implementaciones prácticas.

Otras características

- Disposición a trabajar 24 horas al día, 7 días a la semana o de guardia (según cuál sea el modelo de servicio).
- Distancia de viaje máxima (en caso de emergencia, disponibilidad en la oficina; tiempo de viaje máximo).
- Nivel educativo.
- Experiencia laboral en el ámbito de la seguridad de las TI.

CSIRT ficticio (paso 4)

Definición del plan comercial

Modelo financiero

La empresa tiene un negocio electrónico que funciona 24 horas al día, 7 días a la semana, y un departamento de TI que también funciona 24 horas al día, 7 días a la semana, por lo que se decide prestar un servicio completo en horario de oficina y uno de urgencias el resto del tiempo. Los servicios al grupo de clientes atendido serán gratuitos, pero durante la fase piloto y de evaluación se estudiará la posibilidad de prestar servicios a clientes externos.

Modelo de ingresos

Durante las fases inicial y piloto, la financiación del CSIRT correrá a cargo de la empresa a la que pertenece. Durante las fases piloto y de evaluación se discutirá una financiación adicional que incluirá la posibilidad de vender servicios a clientes externos.

Modelo organizativo

La organización a la que pertenece el CSIRT es una pequeña empresa, por lo que se elige el modelo incrustado.

En horario de oficina, tres trabajadores se encargarán de los servicios básicos (distribución de avisos de seguridad y tratamiento y coordinación de incidentes).

El departamento de TI de la empresa ya dispone de personal con capacidades adecuadas. Se llega a un acuerdo con dicho departamento para que el nuevo CSIRT pueda pedirle apoyo si lo necesita. También pueden recurrir a la segunda línea de técnicos de guardia.
Habrá un equipo central del CSIRT con cuatro miembros a tiempo completo y otros cinco miembros del CSIRT. Uno de ellos también estará disponible en turno rotativo.

Personal
El jefe del CSIRT tiene experiencia en seguridad y apoyo de primer y segundo nivel y ha trabajado en el ámbito de la gestión de crisis. Los otros tres miembros del equipo son especialistas en seguridad. Los miembros del equipo procedentes del departamento de TI que intervienen a tiempo parcial son especialistas en su parte de la infraestructura de la empresa.

Uso y equipamiento de la oficina

El equipamiento y el uso del espacio de la oficina y la seguridad física son temas muy amplios, por lo que no podemos describirlos aquí de forma exhaustiva. Este capítulo trata estas cuestiones brevemente.

Se puede encontrar más información sobre seguridad física en:
http://en.wikipedia.org/wiki/Physical_security
http://www.sans.org/reading_room/whitepapers/physcial/
http://www.infosyssec.net/infosyssec/physfac1.htm

«Preparar el edificio»
Dado que los CSIRT suelen manejar información muy delicada, es una buena práctica dejar que el equipo asuma el control de la seguridad física de la oficina, siempre y cuando las instalaciones, la infraestructura y la política de seguridad de la información de la organización lo permitan.

Los gobiernos, por ejemplo, trabajan con sistemas de clasificación y son muy estrictos en el manejo de información confidencial. Conviene preguntar a la empresa o institución por las normas y políticas locales.

Por lo general, los CSIRT nuevos dependen de la cooperación de la organización a la que pertenecen para enterarse de las normas y políticas locales y otras cuestiones jurídicas.

En este documento no se pretende realizar una descripción exhaustiva del equipo y las medidas de seguridad necesarios. Sin embargo, a continuación se incluye una breve lista de las instalaciones básicas del CSIRT:

Normas generales relativas al edificio
- Utilice controles de acceso.
- Restrinja el acceso a la oficina del CSIRT, como mínimo, al personal del CSIRT.
- Controle las oficinas y las entradas con cámaras.
- Archive la información confidencial bajo llave o en una caja fuerte.
- Use sistemas de TI seguros.

Normas generales relativas al equipamiento de TI
- Use equipos a los que el personal sea capaz de prestar apoyo.
- Proteja todos los sistemas.
- Corrija y actualice todos los sistemas antes de conectarlos a Internet.
- Use software de seguridad (cortafuegos, antivirus múltiples, programas antiespías, etc.).

Mantenimiento de los canales de comunicación
- Sitio web público.
- Zona de acceso restringido a los miembros en el sitio web.
- Formularios web para comunicar incidentes.
- Correo electrónico (que soporte PGP / GPG / S/MIME).
- Software de lista de correo.
- Disponga de un número de teléfono reservado al grupo de clientes atendido:
    - Teléfono,
    - Fax,
    - SMS.

Sistema(s) de localización de registros
- Base de datos de contacto con información sobre los miembros del equipo, otros equipos, etc.
- Herramientas CRM.
- Sistema de resguardos de tratamiento de incidentes.

Uso del «estilo corporativo» desde el principio para
- Diseño del correo electrónico estándar y boletín de aviso estándar.
- Cartas «anticuadas» en soporte de papel.
- Informes mensuales o anuales.
- Formulario de información de incidentes.

Otras cuestiones
- Cuente con comunicación fuera de banda en previsión de posibles ataques.
- Prevea redundancia en la conectividad a Internet.

Para más información acerca de las herramientas específicas de un CSIRT, véase el apartado 8.5, *«Herramientas disponibles para CSIRT».*

Desarrollar una política de seguridad de la información

Determinados tipos de CSIRT siguen una política de seguridad de la información personalizada que, además de describir el estado ideal de los procesos y procedimientos operativos y administrativos, ha de tener en cuenta la legislación y las normas, especialmente las relativas a la fiabilidad del CSIRT. Por lo general, el CSIRT está sujeto a las leyes y los reglamentos nacionales, que a menudo se aplican en el marco de la legislación europea (normalmente, directivas) y otros acuerdos internacionales. Las normas no siempre son directamente vinculantes: a veces pueden ser preceptivas o estar recomendadas por las leyes y los reglamentos.

A continuación se incluye una breve lista de leyes y políticas:

Nacionales
- Diferentes leyes sobre la tecnología de la información, la telecomunicación, los medios de comunicación;
- Leyes sobre protección de datos y privacidad;
- Leyes y reglamentos sobre retención de datos;
- Legislación sobre finanzas, contabilidad y gestión corporativa;
- Códigos de conducta sobre gobernanza corporativa y de las TI.

Europeas
- Directiva sobre firmas electrónicas (1993/93/CE);
- Directivas sobre protección de datos (1995/46/CE) y sobre privacidad en las comunicaciones electrónicas (2002/58/CE);
- Directivas sobre las redes y los servicios de comunicación electrónica (2002/19/CE – 2002/22/CE);
- Directivas sobre derecho de sociedades (por ejemplo, Octava Directiva en materia de derecho de sociedades).

Internacionales
- Acuerdo de Basilea II (especialmente en lo referente a la gestión de riesgos operativos);
- Convenio del Consejo de Europa sobre la delincuencia cibernética;
- Convenio del Consejo de Europa para la protección de los derechos humanos (artículo 8, sobre privacidad);
- Normas internacionales de contabilidad (preceptivas en cierta medida para los controles de las TI).

Normas
- Norma británica BS 7799 (seguridad de la información);
- Normas internacionales ISO2700x (sistemas de gestión de la seguridad de la información);
- IT-Grundschutzbuch alemana, EBIOS francesa y otras variaciones nacionales.

Para averiguar si su CSIRT está respetando la legislación nacional e internacional, consulte a su asesor legal.

Las preguntas más básicas a las que ha de responder con sus políticas de tratamiento de la información son:

- ¿Cómo se «clasifica» la información?
- ¿Cómo se maneja la información, especialmente en lo que se refiere a exclusividad?
- ¿Qué consideraciones se adoptan a la hora de revelar información, y en particular cuando se transmite a otros equipos o sitios información relacionada con incidentes?
- ¿Se han de tomar en consideración cuestiones legales relativas al manejo de información?
- ¿Cuenta con una política sobre el uso de criptografía para proteger la exclusividad y la integridad de los archivos y / o la comunicación de datos, y en particular el correo electrónico?
- ¿Incluye dicha política posibles condiciones límite legales tales como la custodia de claves por terceros o la exigibilidad de la desencriptación en caso de pleito?

CSIRT ficticio (paso 5)

Equipamiento y ubicación de la oficina

Dado que la seguridad física de la empresa a la que pertenece ya es eficaz, el nuevo CSIRT está bien cubierto en este aspecto. Se prepara una «sala de guerra» desde donde se coordinará la acción en caso de emergencia. Se adquiere una caja fuerte para el material de encriptación y los documentos delicados. Se instala una línea telefónica aparte que incluye una centralita para contactar con la línea directa en horario de oficina, y con el móvil «de guardia» fuera del horario de oficina, ambos con el mismo número.

También se puede usar el equipamiento existente y el sitio web corporativo para publicar información relacionada con el CSIRT. Se instala y se mantiene una lista de correo en la que hay una parte de la comunicación a la que sólo pueden acceder los miembros del equipo y otros equipos. Todos los detalles de contacto de los miembros del personal se guardan en una base de datos, y una copia impresa de éstos se deposita en la caja fuerte.

Reglamentación

Al tratarse de un CSIRT incrustado en una empresa que cuenta con políticas de seguridad de la información, las políticas correspondientes del CSIRT se han establecido con ayuda del asesor jurídico de la empresa.

Búsqueda de colaboración con otros CSIRT y posible participación en iniciativas nacionales

Ya hemos hecho referencia un par de veces a que existen otras iniciativas de CSIRT y a que es muy necesario que los CSIRT colaboren entre sí. Es una buena práctica ponerse en contacto con otros CSIRT lo antes posible para establecer la relación necesaria con los colectivos CSIRT. Por lo general, los CSIRT en funcionamiento se muestran muy dispuestos a ayudar a los nuevos equipos a establecerse.

El «*Inventario de actividades del CERT en Europa*» de la ENISA[14] es un buen punto de partida para buscar otros CSIRT establecidos en el país, así como actividades nacionales de colaboración entre CSIRT.

Si desea que le ayuden a buscar una fuente adecuada de información sobre los CSIRT, póngase en contacto con los expertos en CSIRT de la ENISA:

CERT-Relations@enisa.europa.eu

A continuación se presenta un resumen de las actividades de los colectivos CSIRT. En el «*Inventario*» encontrará una descripción más completa e información más detallada.

Iniciativa de los CSIRT europeos

Grupo de trabajo CSIRT[15]

El Grupo de trabajo CSIRT promueve la colaboración entre los equipos de respuesta a incidentes de seguridad informática (CSIRT) europeos. Los principales objetivos de este grupo de trabajo son ofrecer un foro de intercambio de experiencias y conocimientos, crear servicios piloto para los colectivos CSIRT europeos y ayudar a la creación de nuevos CSIRT.

Las metas más destacadas del grupo de trabajo son:

- Ofrecer un foro de intercambio de experiencias y conocimientos;
- Crear servicios piloto para los grupos CSIRT europeos;
- Fomentar unas normas y procedimientos comunes para responder a los incidentes de seguridad;
- Ayudar a la creación de nuevos CSIRT y a la formación del personal de los CSIRT;
- Las actividades del Grupo de trabajo CSIRT se centran en Europa y sus países vecinos, de conformidad con el mandato aprobado por el Comité técnico de TERENA el 15 de septiembre de 2004.

Iniciativa del CSIRT global

FIRST[16]

FIRST es la organización de CSIRT más importante y es líder mundial reconocido en la respuesta a incidentes. Los equipos de respuesta a incidentes que pertenecen a FIRST pueden dar a los incidentes de seguridad una respuesta más eficaz, tanto reactiva como proactiva.

FIRST reúne a diferentes equipos de respuesta a incidentes de seguridad informática de organizaciones públicas, comerciales y educativas. FIRST intenta fomentar la cooperación y la coordinación en la prevención de incidentes, estimular una reacción rápida a los incidentes y promover la puesta en común de información entre sus miembros y todo el colectivo.

[14] Inventario de ENISA: http://www.enisa.europa.eu/cert_inventory

[15] Grupo de trabajo CSIRT: http://www.enisa.europa.eu/cert_inventory/pages/04_01_02.htm#06

[16] FIRST: http://www.enisa.europa.eu/cert_inventory/pages/05_02.htm

Aparte de ser una red de confianza en el colectivo global de respuesta a incidentes, FIRST presta servicios de valor añadido.

CSIRT ficticio (paso 6)
Buscar cooperación Gracias al Inventario de la ENISA, se encontraron rápidamente algunos CSIRT del mismo país, con los que se establecieron contactos. Se concertó una visita sobre el terreno entre uno de ellos y el jefe del equipo, recientemente contratado, que obtuvo información sobre las actividades de los CSIRT nacionales y asistió a una reunión con ellos. La reunión resultó muy útil para recoger ejemplos de métodos de trabajo y conseguir el apoyo de un par de equipos.

7 Promover el plan comercial

Hasta ahora hemos dado los pasos siguientes:

1. Entender qué es un CSIRT y qué puede aportar.
2. Determinar a qué sector prestará servicios el nuevo CSIRT.
3. Establecer qué tipos de servicios puede prestar un CSIRT a sus clientes.
4. Analizar el entorno y los clientes atendidos.
5. Definir los servicios.
6. Desarrollar el plan comercial.
    a. Definir el modelo financiero.
    b. Definir la estructura organizativa.
    c. Empezar a contratar personal.
    d. Utilizar la oficina y equiparla.
    e. Desarrollar una política de seguridad de la información.
    f. Buscar socios de cooperación.

>> El próximo paso será incluir todo lo anterior en un plan de proyecto y poner manos a la obra.

Una buena manera de empezar a definir un proyecto es proponer un modelo de negocio que sirva de base para el plan del proyecto y se pueda usar para solicitar apoyo a la gestión y conseguir presupuesto u otros recursos.

Tener siempre informada a la dirección ha demostrado ser útil para mantener elevada la sensibilización respecto a los problemas de seguridad de las TI y, de este modo, contar con un apoyo continuo para el propio CSIRT.

La puesta en marcha de un modelo de negocio empieza con el análisis de los problemas y las oportunidades siguiendo un modelo de análisis de los descritos en el apartado 5.3, *«Análisis del grupo de clientes atendido y declaración de servicios»*, y el establecimiento de un contacto estrecho con el grupo potencial.

Como ya hemos explicado, al poner en marcha un CSIRT hay que pensar en muchas cosas. Lo mejor es ajustar el material mencionado a las necesidades del CSIRT, conforme van surgiendo.

Cuando se informa a la dirección es una buena práctica actualizar el modelo todo lo posible, recurriendo a artículos recientes de la prensa o a Internet, y explicar por qué el servicio del CSIRT y la coordinación interna de los incidentes resultan cruciales para proteger el patrimonio de la empresa. También hay que dejar claro que para estabilizar un negocio es indispensable un apoyo continuo en cuestiones de seguridad de las TI, especialmente en las empresas o instituciones que dependen de ellas.

(Hay una frase de Bruce Schneier que resulta muy adecuada aquí: *«La seguridad no es un producto, sino un proceso*[17]*»)*

El gráfico siguiente, facilitado por el CERT/CC, es una herramienta muy conocida que ilustra los problemas de seguridad:

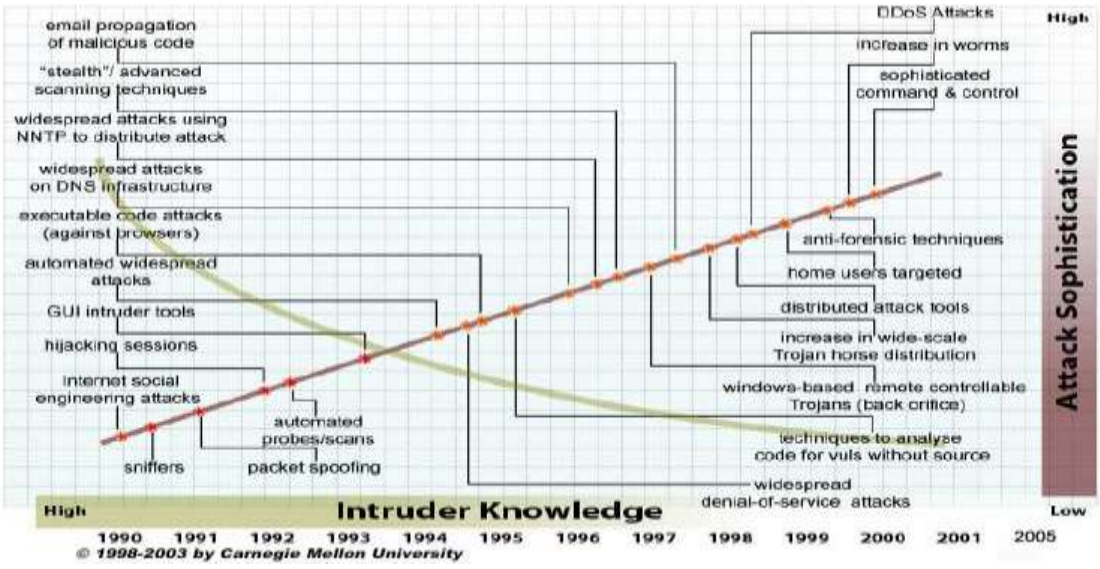


Fig. 8 Conocimiento de los intrusos y perfeccionamiento del ataque (fuente: CERT-CC[18]*).*

El gráfico muestra las tendencias en seguridad de las TI, y en especial la disminución de las capacidades necesarias para realizar ataques cada vez más sofisticados.

Otro aspecto que merece la pena mencionar es el de la reducción continua del tiempo que transcurre entre la disponibilidad de actualizaciones de software para vulnerabilidades y el inicio de los ataques:

Corrección -> Ataque		**Tasa de propagación**	
Nimda:	11 meses	Code red:	Días
Slammer:	6 meses	Nimda:	Horas
Nachi:	5 meses	Slammer:	Minutos
Blaster:	3 semanas		
Witty:	1 día (!)		

La recopilación de los datos de los incidentes, las mejoras potenciales y las lecciones aprendidas contribuyen también a una buena presentación.

[17] Bruce Schneier: http://www.schneier.com/.

[18] http://www.cert.org/archive/pdf/info-sec-ip.pdf.

Descripción de planes de negocios y activadores a los que responde la dirección

Una presentación a la dirección que sólo incluya la promoción del CSIRT no constituye un modelo de negocio, pero, en la mayor parte de los casos, si se realiza de un modo adecuado conseguirá que la dirección apoye al CSIRT. Por otra parte, el modelo de negocio no se debería considerar simplemente una cuestión de gestión, sino que también se habría de utilizar en la comunicación con el equipo y el grupo de clientes atendido. El término «modelo de negocio» puede sonar muy comercial y alejado de la práctica diaria del CSIRT, pero ayuda a orientar y dirigir la creación de un CSIRT.

Las respuestas a las preguntas que siguen se podrían usar para diseñar un buen modelo de negocio (los ejemplos dados son hipotéticos y sólo se usan a título ilustrativo. Las respuestas «reales» dependen en gran medida de las circunstancias «reales»).

- ¿En qué consiste el problema?
- ¿Qué objetivos le gustaría alcanzar en relación con el grupo de clientes atendido?
- ¿Qué pasará si no se hace nada?
- ¿Qué pasará si se actúa?
- ¿Cuánto costará?
- ¿Qué se conseguirá?
- ¿Qué calendario se seguirá?

¿En qué consiste el problema?
Por lo general, la idea de crear un CSIRT surge cuando la seguridad de las TI ha pasado a ser una parte esencial de la actividad principal de una empresa o institución o cuando los incidentes relacionados con la seguridad de las TI se convierten en un riesgo para el negocio, por lo que las operaciones de mitigación del riesgo pasan a ser habituales.

La mayor parte de las empresas e instituciones cuentan con un departamento de apoyo que funciona de forma regular, o bien con un servicio de asistencia técnica, pero los incidentes de seguridad no se suelen tratar adecuadamente ni de un modo tan estructurado como se debería. A menudo, el ámbito de trabajo donde se ha producido el incidente de seguridad precisa unas capacidades y una atención especiales. Además, un enfoque más estructurado beneficiará a la empresa y reducirá los riesgos que corre y los daños que pueda sufrir.

En la mayoría de los casos el problema consiste en una falta de coordinación y en no aplicar al tratamiento de los incidentes los conocimientos existentes, que podrían impedir que en el futuro surgieran otros incidentes y evitar posibles pérdidas financieras y daños a la reputación de la institución.

¿Qué objetivos le gustaría alcanzar en relación con el grupo de clientes atendido?
Como ya se ha explicado, el CSIRT atenderá a un grupo y le ayudará a resolver problemas e incidentes de seguridad de las TI. Otros objetivos serían elevar el nivel de

conocimientos sobre la seguridad de las TI e implantar la cultura de sensibilización acerca de la seguridad.

Tal cultura intenta que se adopten desde el principio medidas proactivas y preventivas, con lo que se reducen los costes de funcionamiento.

En muchos casos, al implantar esta cultura de cooperación y asistencia a una empresa o institución se puede fomentar la eficacia en general.

¿Qué pasará si no se hace nada?
Un manejo desestructurado de la seguridad de las TI puede provocar daños mayores, además de afectar a la reputación de la institución. También puede haber pérdidas financieras y consecuencias legales.

¿Qué pasará si se actúa?
Aumentará la concienciación acerca de la posibilidad de que aparezcan problemas de seguridad, lo cual ayudará a resolverlos con mayor eficacia y a evitar futuras pérdidas.

¿Cuánto costará?
Dependiendo del modelo organizativo, costará los salarios de los miembros del equipo y la organización, el equipamiento, las herramientas y las licencias del software.

¿Qué se conseguirá?
Dependiendo del negocio y de las pérdidas sufridas en el pasado, los procedimientos y las prácticas de seguridad ganarán transparencia, con lo que se protegerá un patrimonio empresarial esencial.

¿Qué calendario se seguirá?
Véase en el capítulo 12*, «Descripción del plan del proyecto»,* la descripción de un ejemplo de plan de proyecto.

Ejemplos de modelos de negocio existentes y enfoques
A continuación presentamos varios ejemplos de modelos de negocio que merece la pena estudiar en el caso de un CSIRT:

- http://www.cert.org/csirts/AFI_case-study.html
  Creación del CSIRT de una institución financiera: estudio de un caso

  La finalidad de este documento es poner en común las lecciones aprendidas por una institución financiera (llamada AFI en el documento) a medida que desarrollan y aplican un plan para abordar cuestiones relacionadas con la seguridad y un equipo de respuesta a incidentes de seguridad informática (CSIRT).

- http://www.terena.nl/activities/tf-csirt/meeting9/jaroszewski-assistance-csirt.pdf
  Resumen del modelo de negocio de CERT POLSKA (diapositivas en formato PDF).

- http://www.auscert.org.au/render.html?it=2252
  En los años noventa, crear un equipo de respuesta a incidentes podía ser una tarea desalentadora. Muchos de los que intervenían en la creación no tenían experiencia en ese tipo de tareas. El documento examina el papel que puede desempeñar un equipo de respuesta a incidentes en el grupo y las cuestiones que convendría abordar durante su creación y una vez haya empezado a funcionar. Podría ser de ayuda para equipos en funcionamiento de respuesta a incidentes, pues pone sobre el tapete cuestiones que no se han tratado previamente.

- http://www.sans.org/reading_room/whitepapers/casestudies/1628.php
  Estudio de un caso sobre seguridad de la información y protección de la empresa, por Roger Benton.

  Se trata de un estudio práctico de la migración, en una compañía de seguros, a un sistema de seguridad para toda la empresa. Constituye un intento de proporcionar una vía para crear un sistema de seguridad o migrar a él. Inicialmente, el único mecanismo para controlar el acceso a los datos corporativos era un sistema de seguridad en línea primitivo. Los riesgos eran graves, pues no había controles de integridad fuera del entorno en línea. Cualquiera que tuviese unas nociones básicas de programación podía añadir, cambiar y / o borrar datos de producción.

- http://www.esecurityplanet.com/trends/article.php/10751_688803
  Estrategia de seguridad electrónica de Marriott: colaboración empresa-TI

  La experiencia de seguridad electrónica de Chris Zoladz, de Marriott International, Inc.'s, no es un proyecto, sino un proceso. Éste es el mensaje que Zoladz hizo llegar en la reciente conferencia y exposición sobre seguridad electrónica celebrada en Boston, patrocinada por Intermedia Group. Como vicepresidente de protección de la información de Marriott, Zoladz informa a través del departamento jurídico, pese a no ser un abogado. Su función consiste en averiguar dónde se almacena la información empresarial más valiosa de Marriott y cómo entra y sale de la empresa. Marriott tiene definida una responsabilidad aparte en relación con la infraestructura técnica de apoyo a la seguridad, que corresponde al arquitecto de seguridad de las TI.

CSIRT ficticio (paso 7)

Promover el plan comercial

Se ha decidido recoger hechos y cifras de la historia de la empresa, lo que resultará muy útil para realizar un estudio estadístico de la situación de la seguridad de las TI. Esta recopilación debería seguir adelante una vez el CSIRT se haya establecido y esté en funcionamiento, para mantener las estadísticas actualizadas.

Se establecieron contactos y se mantuvieron entrevistas acerca de sus modelos de negocio con otros CSIRT nacionales que prestaron apoyo recopilando diapositivas con información acerca de los últimos desarrollos en incidentes de seguridad de las TI, así como de los costes de tales incidentes.

En este ejemplo de CSIRT ficticio no había una necesidad acuciante de convencer a la dirección de la importancia de las empresas de TI, por lo que no resultó difícil conseguir luz verde para ponerse manos a la obra. Se prepararon un modelo de negocio y un plan de proyecto que incluían una estimación de los costes de establecimiento y funcionamiento.

8 Ejemplos de procedimientos operativos y técnicos (métodos de trabajo)

Hasta ahora hemos dado los pasos siguientes:

1. Entender qué es un CSIRT y qué puede aportar.
2. Determinar a qué sector prestará servicios el nuevo CSIRT.
3. Establecer qué tipos de servicios puede prestar un CSIRT a su grupo de clientes.
4. Analizar el entorno y el grupo de clientes atendido.
5. Definir los servicios.
6. Desarrollar el plan comercial.
   a. Definir el modelo financiero.
   b. Definir la estructura organizativa.
   c. Empezar a contratar personal.
   d. Utilizar la oficina y equiparla.
   e. Desarrollar una política de seguridad de la información.
   f. Buscar socios con los que cooperar.
7. Promover el plan comercial.
   a. Conseguir que se apruebe el modelo de negocio.
   b. Encajarlo todo en un plan de proyecto.

>> El próximo paso será poner el CSIRT en funcionamiento.

Tras definir convenientemente los métodos de trabajo establecidos, mejoraremos la calidad y el tiempo necesario por incidente o caso de vulnerabilidad.

Tal como se describe en los recuadros de los ejemplos, el CSIRT ficticio ofrecerá los servicios fundamentales de un CSIRT básico:

- Alertas y advertencias;
- Tratamiento de los incidentes;
- Comunicados.

Este capítulo presenta ejemplos de métodos de trabajo que describen los servicios básicos de un CSIRT y da cuenta de la recopilación de información procedente de diferentes fuentes, la comprobación de su pertinencia y su autenticidad y su devolución al grupo de clientes atendido. Por último, incluye ejemplos de los procedimientos más básicos y de herramientas específicas de los CSIRT.

Evaluación de la base de instalación del grupo de clientes atendido

El primer paso es ponerse al corriente de los sistemas de TI que tiene instalados el grupo atendido. De este modo, el CSIRT podrá evaluar la pertinencia de la información que llegue y filtrarla antes de volverla a distribuir, de modo que el grupo no se vea abrumado con información que le resulte de escasa utilidad.

Es una buena práctica empezar de un modo sencillo, por ejemplo usando una hoja de Excel como ésta:

Categoría	Aplicación	Software	Versión	SO	Versión del SO	Grupo atendido
Ordenador personal	Oficina	Excel	x-x-x	Microsoft	XP-prof	A
Ordenador personal	Navegador	Internet Explorer	x-x-	Microsoft	XP-prof	A
Red	Enrutador	CISCO	x-x-x	CISCO	x-x-x-	B
Servidor	Servidor	Linux	x-x-x	L-distro	x-x-x	B
Servicios	Servidor web	Apache		Unix	x-x-x	B

Con la función filtro, en Excel es muy fácil seleccionar el software adecuado y ver qué clientes del grupo atendido usan cada tipo de software.

Generación de alertas, advertencias y comunicados

La generación de alertas, advertencias y comunicados sigue siempre el mismo esquema:

- Recopilación de información;
- Evaluación de la información sobre la pertinencia y la fuente;
- Evaluación del riesgo basada en la información recopilada;
- Distribución de la información.

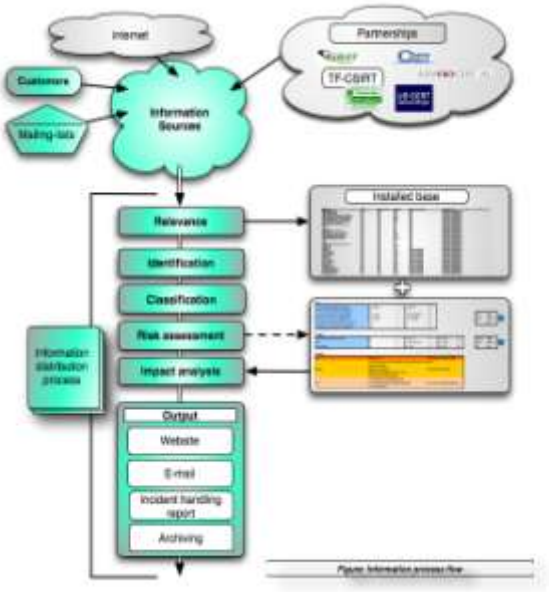


Fig. 9 : Esquema del proceso de información.

En los párrafos siguientes se describe con más detalle este esquema.

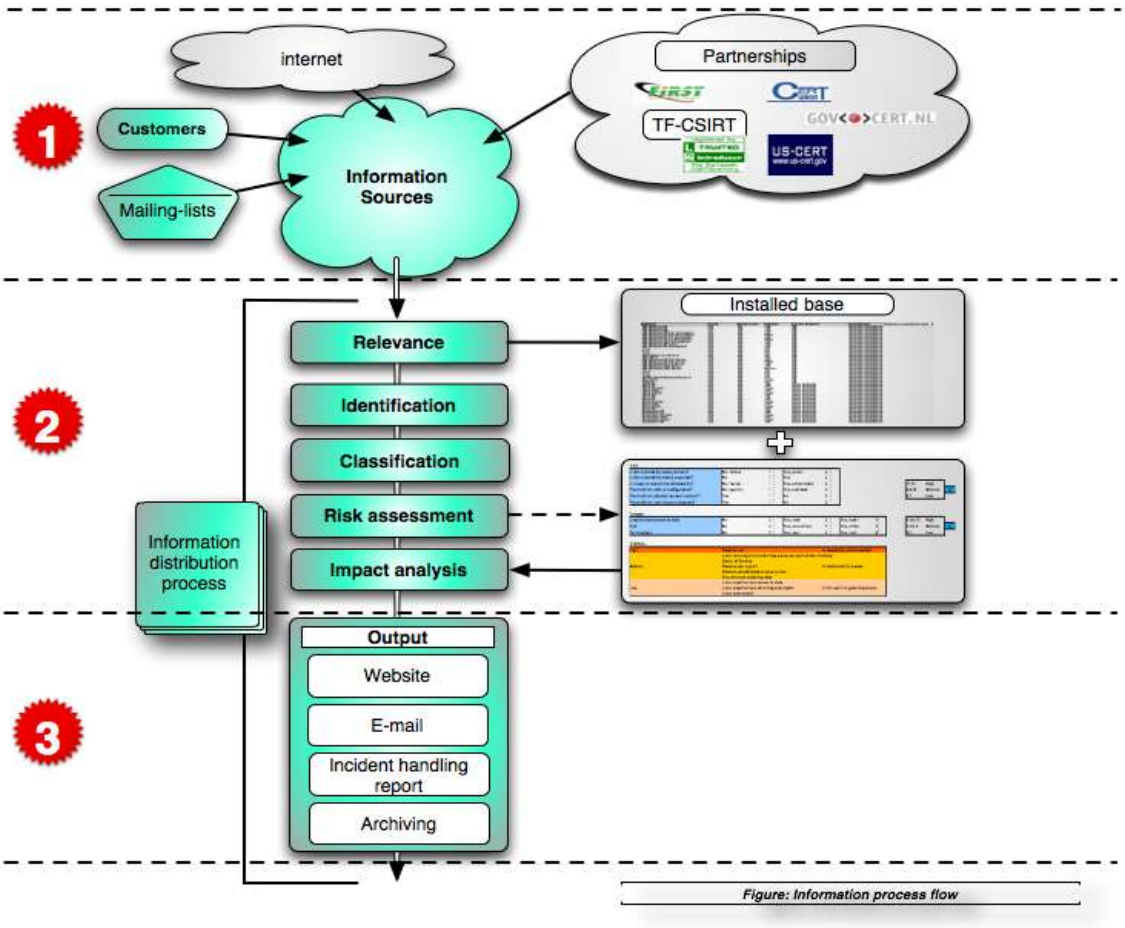


Figure: Information process flow

1 Paso 1: Recopilación de información sobre la vulnerabilidad

Por lo general hay dos tipos importantes de fuentes de información que aportan información a los servicios:

- Información sobre la vulnerabilidad de los sistemas de TI (propios);
- Informes sobre incidentes.

Dependiendo del tipo de empresa y de la infraestructura de sus TI, existen numerosas fuentes públicas y cerradas de información sobre vulnerabilidad:

- Listas de correo públicas y cerradas;
- Información sobre vulnerabilidad facilitada por los proveedores de los productos;
- Sitios web;
- Información publicada en Internet (Google, etc.);
- Socios públicos y privados que proporcionan información sobre vulnerabilidad (FIRST, TF-CSIRT, CERT-CC, US-CERT…).

Toda esta información aumenta el nivel de conocimiento sobre las vulnerabilidades específicas de los sistemas de TI.

Como ya hemos comentado, en Internet hay muchas fuentes de información sobre seguridad de buena calidad y fácil acceso. El Grupo de trabajo ad-hoc de la ENISA «servicios de los CERT» de 2006 está preparando una lista más completa que debería estar terminada para finales de 2006[19].

Paso 2: Evaluación de la información y valoración del riesgo

Con este paso se realizará un análisis del impacto de la vulnerabilidad específica de la infraestructura de TI del grupo de clientes atendido.

Identificación
La fuente de la información entrante sobre vulnerabilidad siempre ha de ser identificada, y antes de transmitir la información al grupo atendido se ha de determinar si la fuente es de confianza. En caso contrario, se podrían generar alertas innecesarias que provocarían molestias gratuitas en los procesos empresariales y al final perjudicarían a la reputación de los CSIRT.

[19] Grupo de trabajo ad-hoc «servicios de los CERT»:
http://www.enisa.europa.eu/pages/ENISA_Working_group_CERT_SERVICES.htm.

El procedimiento siguiente muestra un ejemplo de identificación de la autenticidad de un mensaje:

Procedimiento de identificación de la autenticidad de un mensaje y su fuente

Lista de comprobación general

1. ¿La fuente es conocida y está registrada como tal?
2. ¿La información llega por un canal regular?
3. ¿El mensaje contiene información «extraña« que «parece» errónea?
4. Si intuitivamente una información parece dudosa, antes de actuar hay que volver a verificarla.

Correo electrónico - Fuentes

1. ¿La dirección de la fuente es conocida por la organización y figura en la lista de fuentes?
2. ¿Es correcta la firma PGP?
3. Si surgen dudas con un mensaje, compruebe la cabecera completa.
4. Si surgen dudas, use «nslookup» o «dig» para comprobar el dominio del remitente[20].

WWW - Fuentes

1. Cuando conecte con un sitio web protegido, compruebe los certificados del navegador (https ://).
2. Compruebe el contenido y la validez (técnica) de la fuente.
3. Si duda, no entre en los vínculos ni descargue software.
4. Si duda, haga un «lookup» y un «dig» en el dominio, así como un «traceroute».

Teléfono

1. Escuche el nombre atentamente.
2. ¿Reconoce la voz?
3. Si tiene dudas, pida un número de teléfono y llame usted al autor de la llamada.

Fig. 10 Ejemplo de procedimiento de identificación de la información.

Pertinencia

La anterior visión general del hardware y el software instalado se puede usar para filtrar la información entrante sobre vulnerabilidad relativa a la pertinencia, a fin de encontrar una respuesta a dos preguntas: «¿Utiliza este software el grupo atendido?» y «¿Es esta información pertinente para dicho grupo?»

Clasificación

Una parte de la información recibida se puede clasificar o marcar como restringida (por ejemplo, los informes sobre incidentes que lleguen de otros equipos). Al manejar la información siempre se han de tener en cuenta las indicaciones del remitente y la propia política de seguridad de la información. Una buena norma básica es *«no distribuir*

[20] Herramientas para comprobar identidades de la CHIHT:
http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

información si no está claro qué se supone que es; en caso de duda, pedir permiso al remitente para hacerlo».

Evaluación del riesgo y análisis de las consecuencias
Existen diversos métodos para determinar el riesgo y las consecuencias de una (posible) vulnerabilidad.

El riesgo se define como la oportunidad potencial de que se pueda aprovechar una vulnerabilidad. Algunos de los factores más importantes que cabe tener en cuenta son:

- ¿Es bien conocida la vulnerabilidad?
- ¿Está muy extendida?
- ¿Es fácil de explotar?
- ¿Se trata de una vulnerabilidad que se puede explotar de forma remota?

Todas estas preguntas ayudan a formarse una idea adecuada de la gravedad de la vulnerabilidad.
Para calcular el riesgo se puede recurrir a una fórmula muy sencilla:

Impacto = riesgo X daños potenciales

Los daños potenciales pueden ser:

- Acceso no autorizado a los datos;
- Denegación de servicio (DOS);
- Obtención o ampliación de permisos.

(Para clasificaciones más elaboradas, véase el final de este capítulo).

Tras contestar a estas preguntas se puede añadir una clasificación global al aviso, informando de riesgos y daños potenciales. Se suelen usar términos simples como BAJO, MEDIO y ALTO.

Otros sistemas de evaluación del riesgo más completos son:

El sistema de clasificación de GOVCERT.NL[21]

El CSIRT del gobierno holandés, GOVCERT.NL, utiliza una matriz de evaluación del riesgo creada en la fase inicial de Govcert.nl que sigue actualizando de acuerdo con las últimas tendencias.

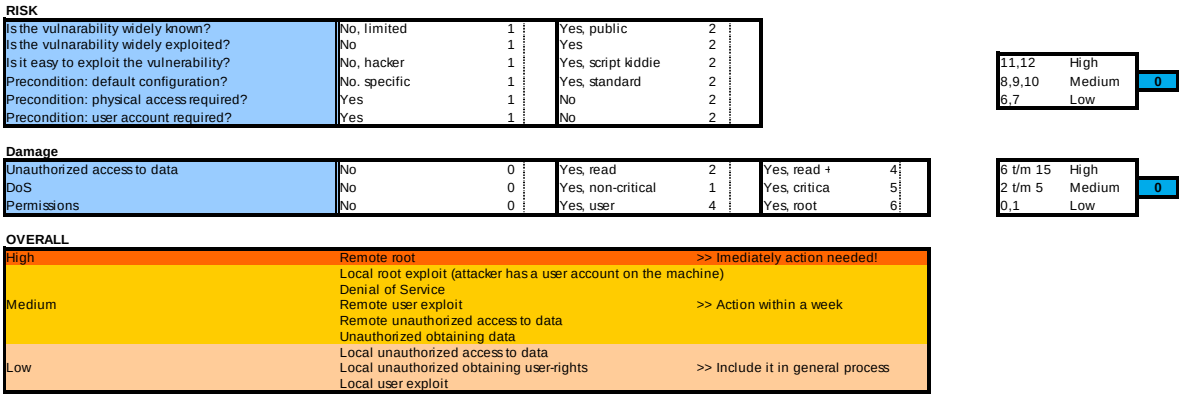


Fig. 11 El sistema de clasificación de GOVCERT.NL.

Descripción del formato común de aviso del EISPP[22]

El Programa Europeo para la Promoción de la Seguridad de la Información (EISPP, *European Information Security Promotion Programme)* es un proyecto financiado por la Comunidad Europea formando parte del V Programa Marco. El proyecto EISPP intenta desarrollar un marco europeo que, además de servir para compartir conocimientos sobre seguridad, defina el contenido y los modos de hacer llegar a las PYME la información sobre seguridad. Si las PYME europeas cuentan con los servicios de seguridad de las TI necesarios, su confianza crecerá y se animarán a usar el comercio electrónico, lo que les brindará mayores y mejores oportunidades de nuevos negocios. El proyecto EISPP es pionero en la idea de la Comisión Europea de formar una red europea de conocimientos técnicos en la Unión Europea.

Formato alemán de aviso (DAF, *Deutsches Advisory Format)*[23]

DAF es una iniciativa del CERT-Verbund alemán y un componente básico de una infraestructura de generación e intercambio de avisos de seguridad por diferentes equipos. DAF se ha creado a la medida de las necesidades de los CERT alemanes. El estándar lo han desarrollado y lo mantienen CERT-Bund, DFN-CERT, PRESECURE y Siemens-CERT.

[21] Matriz de vulnerabilidad: http://www.govcert.nl/download.html?f=33

[22] EISSP: http://www.enisa.europa.eu/cert_inventory/pages/04_03.htm#03

[23] DAF: http://www.enisa.europa.eu/cert_inventory/pages/04_03.htm#02

Paso 3: Distribución de la información

Cada CSIRT puede elegir entre diferentes métodos de distribución, según las preferencias del grupo de clientes atendido y su propia estrategia de comunicación:

- Sitio web;
- Correo electrónico;
- Informes;
- Archivo e investigación.

Los avisos de seguridad distribuidos por un CSIRT deberían seguir siempre la misma estructura, para mejorar la legibilidad y permitir que el lector encuentre rápidamente la información pertinente.

Un aviso debe contener, como mínimo, la información siguiente:

Título del aviso ……
Número de referencia …… **Sistemas afectados** **-** …… **-** …… **SO relacionado y versión** …… **Riesgo** (Alto-Medio-Bajo) …… **Consecuencias / daños potenciales** (Altos-Medios-Bajos) …… **ID externos:** (ID de las CVE y los boletines de vulnerabilidad) ……
Descripción general de la vulnerabilidad …… **Consecuencias** …… **Solución** …… **Descripción (detalles)** …… **Apéndice** ……

Fig. 12 Ejemplo de proyecto de aviso.

Véase en el capítulo 10*, «Ejercicio»,* un ejemplo completo de aviso de seguridad.

Tratamiento de los incidentes

Como mencionamos en la introducción de este capítulo, durante el tratamiento de los incidentes el tratamiento de la información es muy similar al que se lleva a cabo durante la compilación de alertas, advertencias y comunicados. Sin embargo, la parte de la recopilación de información suele ser diferente, pues normalmente los datos relacionados con incidentes se recogen ya sea con la recepción de informes de incidentes enviados por el grupo de clientes atendido o por otros equipos, ya con la recepción de los comentarios de las partes interesadas durante el tratamiento de un incidente. Por lo general, la información circula (encriptada) por correo electrónico; a veces se hace necesario usar el teléfono o el fax.

Cuando se recibe información por teléfono, es una buena práctica anotar todos y cada uno de los detalles enseguida, bien con una herramienta de tratamiento / informe de accidentes, bien tomando notas de la conversación. Inmediatamente, antes de que la llamada termine, se debe generar un número de incidente (si no se ha asignado ya uno) y comunicárselo al informador por teléfono (o en un resumen enviado por correo electrónico a continuación). Este número servirá de referencia en posteriores comunicaciones.

El resto de este capítulo describe el proceso básico de tratamiento de incidentes. En el documento del CERT/CC «*Defining Incident Management processes for CSIRTs*» (Definición de procesos de gestión de incidentes para CSIRT)[24] se puede consultar un análisis muy minucioso del proceso completo de gestión de incidentes y todos los esquemas y subesquemas correspondientes.

[24] Definición de procesos de gestión de incidentes: http://www.cert.org/archive/pdf/04tr015.pdf.

Básicamente, el tratamiento de incidentes sigue este esquema:

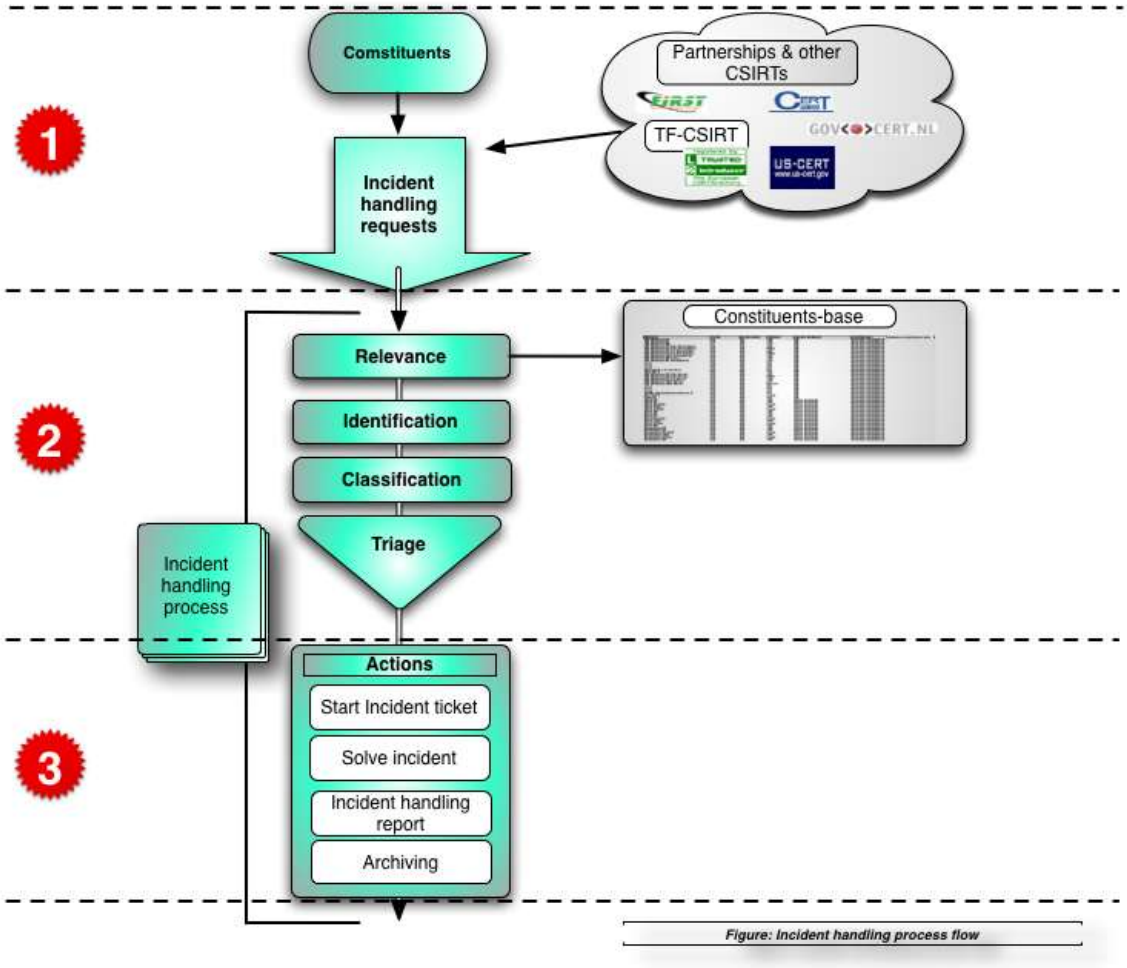


Fig. 13 Esquema del tratamiento de incidentes.

Paso 1: Recepción de los informes de incidentes

Como ya hemos comentado, los comunicados de incidentes llegan al CSIRT por diferentes canales, sobre todo por correo electrónico, pero también por teléfono o fax.

Conviene insistir en que es una buena práctica anotar todos los detalles con un formato fijo mientras se recibe el comunicado de incidente, para asegurarse de que no se olvida ningún dato importante. A continuación presentamos un ejemplo de formulario:

FORMULARIO DE COMUNICACIÓN DE INCIDENTE

Sírvase rellenar este formulario y enviarlo por fax o correo electrónico a: ……..
Las líneas marcadas con un asterisco (*) son de respuesta obligatoria.

Nombre y organización
1. Nombre*:
2. Nombre de la organización*:
3. Sector:
4. País*:
5. Ciudad:
6. Dirección de correo electrónico*:
7. Número de teléfono*:
8. Otros:

Ordenador(es) afectado(s)
9. Número de ordenadores:
10. Nombre del ordenador e IP*:
11. Función del ordenador*:
12. Zona horaria:
13. Hardware:
14. Sistema operativo:
15. Software afectado:
16. Ficheros afectados:
17. Seguridad:
18. Nombre del ordenador e IP:
19. Protocolo/puerto:

Incidente
20. Número de referencia:
21. Tipo de incidente:
22. Inicio del incidente:
23. El incidente aún no se ha resuelto: Sí NO
24. Hora y método de descubrimiento:
25. Vulnerabilidades conocidas:
26. Ficheros sospechosos:
27. Medidas:
28. Descripción detallada*:

Fig. 14 Contenido de un comunicado de incidente.

Paso 2: Evaluación del incidente

En esta fase se comprueban la autenticidad y la pertinencia del incidente comunicado y éste se clasifica.

Identificación

Para evitar acciones innecesarias conviene comprobar que el creador del aviso sea fidedigno y si pertenece al grupo de clientes atendido o al de algún CSIRT asociado. Se aplicarán normas similares a las descritas en el apartado 8.2, *«Generación de alertas, advertencias y comunicados»*.

Pertinencia

En este paso se comprueba si la petición de tratamiento de incidente procede del grupo de clientes atendido por el CSIRT, o si el incidente comunicado afecta a sistemas de TI del grupo atendido. Si no es así, el comunicado se suele enviar al CSIRT pertinente[25].

Clasificación

Con este paso se prepara el *triage* clasificando el incidente según su gravedad. No corresponde a este documento dar detalles sobre la clasificación de incidentes. Una buena forma de empezar es utilizar el sistema de clasificación de casos del CSIRT (ejemplo para CSIRT empresarial):

Incident Categories

All incidents managed by the CSIRT should be classified into one of the categories listed in the table below.

Incident Category	Sensitivity*	Description
Denial of service	S3	• DOS or DDOS attack.
Forensics	S1	• Any forensic work to be done by CSIRT.
Compromised Information	S1	• Attempted or successful destruction, corruption, or disclosure of sensitive corporate information or Intellectual Property.
Compromised Asset	S1, S2	• Compromised host (root account, Trojan, rootkit), network device, application, user account. This includes malware-infected hosts where an attacker is actively controlling the host.
Unlawful activity	S1	• Theft / Fraud / Human Safety / Child Porn. Computer-related incidents of a criminal nature, likely involving law enforcement, Global Investigations, or Loss Prevention.
Internal Hacking	S1, S2, S3	• Reconnaissance or Suspicious activity originating from inside the Company corporate network, excluding malware.
External Hacking	S1, S2, S3	• Reconnaissance or Suspicious Activity originating from outside the Company corporate network (partner network, Internet), excluding malware.
Malware	S3	• A virus or worm typically affecting multiple corporate devices. This does not include compromised hosts that are being actively controlled by an attacker via a backdoor or Trojan. (See Compromised Asset)
Email	S3	• Spoofed email, SPAM, and other email security-related events.
Consulting	S1, S2, S3	• Security consulting unrelated to any confirmed incident.
Policy Violations	S1, S2, S3	• Sharing offensive material, sharing/possession of copyright material. • Deliberate violation of Infosec policy. • Inappropriate use of corporate asset such as computer, network, or application. • Unauthorized escalation of privileges or deliberate attempt to subvert access controls.
* - Sensitivity will vary depending on circumstances. Guidelines are provided.		

Fig. 15 Sistema de clasificación de un incidente (fuente: FIRST)[26].

[25] Herramientas de comprobación de identidades de la CHIHT:
http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

Triage

El *triage* es un sistema que utiliza el personal sanitario o de urgencias para racionar recursos médicos limitados cuando el número de personas que precisan asistencia supera los recursos disponibles, con el fin de tratar al mayor número de pacientes posible[27].

El CERT/CC facilita la siguiente descripción:

El triage *es un elemento esencial de la capacidad de gestionar incidentes, especialmente en un CSIRT establecido. El* triage *resulta decisivo para entender lo que se está comunicando en toda la organización. Es el vehículo por el que toda la información llega a un único punto de contacto, lo que permite adoptar una visión empresarial de la actividad y correlacionar de un modo exhaustivo todos los datos comunicados. El* triage *permite realizar una evaluación inicial de un informe entrante y lo registra a la espera de que se le dé curso. También constituye un punto de partida para empezar a trabajar con la documentación y con la entrada de datos de un informe o una petición, si no se ha hecho ya en el proceso de detección.*

La función de triage *facilita una instantánea de la situación de toda la actividad comunicada (informes abiertos y cerrados, acciones pendientes, número de informes de cada tipo recibidos). Este proceso puede ayudar a identificar problemas de seguridad potenciales y a establecer prioridades de trabajo. La información recogida durante el* triage *también se puede usar para determinar pautas de vulnerabilidad e incidentes y generar estadísticas para los ejecutivos de alto nivel[28].*

Sólo se deben encargar del *triage* los miembros del equipo con más experiencia, pues el proceso requiere un conocimiento profundo de las repercusiones potenciales de los incidentes en cada parte del grupo atendido, así como la capacidad de decidir qué miembro del equipo debe encargarse del incidente.

[26] Clasificación de casos del CSIRT: http://www.first.org/resources/guides/csirt_case_classification.html.

[27] *Triage* en Wikipedia: http://en.wikipedia.org/wiki/Triage.

[28] Definición de los procesos de gestión de incidentes: http://www.cert.org/archive/pdf/04tr015.pdf.

Paso 3: Acciones

Por lo general, los incidentes sometidos a *triage* se incluyen en la cola de peticiones de una herramienta de tratamiento de incidentes cuyos usuarios dan los pasos siguientes.

Resguardo de incidente
El número del resguardo de incidente ya se debería haber generado en un paso previo (por ejemplo, cuando se comunicó el incidente por teléfono). Si no es así, el primer paso será crearlo, para utilizarlo en las comunicaciones posteriores sobre el incidente.

Ciclo de vida del incidente
Al tratar un accidente no se sigue una línea de pasos que al final llevan a una solución, sino un círculo de pasos que se aplican repetidamente hasta que el incidente se resuelve por fin y todas las partes implicadas disponen de toda la información necesaria. Este círculo, que se conoce como «ciclo de vida del incidente», contiene los procesos siguientes:

Análisis:	Se analizan todos los detalles del incidente comunicado.
Información de contacto:	Se ha de obtener información de contacto para poder comunicar los datos sobre el incidente a todas las partes implicadas, como otros CSIRT, las víctimas y probablemente los propietarios de los sistemas que podrían haber sido utilizados para realizar un ataque.
Asistencia técnica:	Se ayuda a las víctimas a recuperarse rápidamente de los resultados del incidente y se recoge más información sobre el ataque.
Coordinación:	Se informa a otras partes implicadas, como los responsables del CSIRT del sistema de TI utilizado para un ataque u otras víctimas.

Esta estructura se llama «ciclo de vida» porque cada uno de los pasos lleva a otro, y el último conduce a un nuevo análisis, con lo que el ciclo vuelve a empezar. El proceso finaliza cuando todas las partes afectadas han recibido y comunicado toda la información necesaria.

Para una descripción más detallada del ciclo de vida de un incidente, consúltese el manual del CSIRT publicado por el CERT/CC[29].

Informe de tratamiento de incidente
Prepare informes que le ayudarán a responder a las preguntas de la dirección sobre los incidentes. También es una buena práctica escribir un documento (sólo de uso interno) sobre las «lecciones aprendidas», que servirá para que el personal evite errores en el tratamiento de futuros incidentes.

[29] Manual del CSIRT: http://www.cert.org/archive/pdf/csirt-handbook.pdf.

Archivo
Consulte las normas de archivo descritas en el apartado 6.5, *«Desarrollar una política de seguridad de la información»*.

En el apartado A.1 del anexo, *«Otras lecturas»,* se proponen guías completas sobre gestión de incidentes y sobre el ciclo de vida de éstos.

Ejemplo de plan de respuesta

La definición de los tiempos de respuesta se suele dejar de lado, pero debe formar parte de todo acuerdo de nivel de servicio bien construido entre el CSIRT y el grupo al que atiende. Es de suma importancia dar al grupo atendido información sobre los incidentes durante el tratamiento de éstos, tanto en su interés como por la reputación del equipo.
Los tiempos de respuesta se deben comunicar claramente al grupo atendido para evitar expectativas infundadas. El sencillo plan siguiente se puede usar como punto de partida para un acuerdo de nivel de servicio más detallado.

Aquí tenemos un ejemplo de plan práctico de respuesta desde el punto de vista de una petición de asistencia entrante:

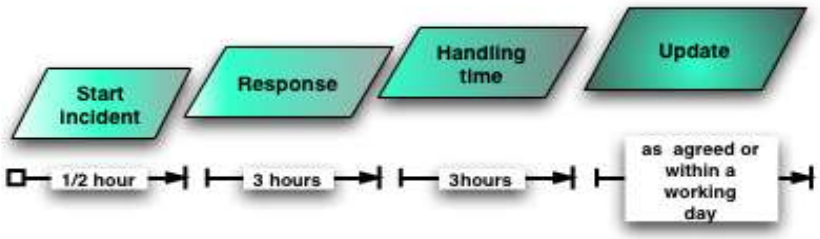


Fig. 16 Ejemplo de plan de respuesta.

También es una buena práctica informar al grupo de clientes atendido sobre sus propios tiempos de respuesta, especialmente cuando se contacta con el CSIRT por una emergencia. En la mayor parte de los casos es mejor ponerse en contacto con el CSIRT en una fase temprana, y es una buena práctica animar al grupo atendido a hacerlo en caso de duda.

Herramientas disponibles para CSIRT

Este apartado formula sugerencias sobre herramientas comunes que usan los CSIRT. Sólo presenta ejemplos; se pueden encontrar más consejos en la *Clearinghouse of Incident Handling Tools*[30] (CHIHT).

Software de encriptación de correos electrónicos y mensajes

- GNUPG http://www.gnupg.org/
  GnuPG es el software completo y de aplicación gratuita del proyecto GNU de la norma OpenPGP, definida en la *RFC2440*. GnuPG permite encriptar y firmar los datos y comunicaciones.

- PGP http://www.pgp.com/
  Variante comercial

Herramientas de tratamiento de incidentes

Administración de incidentes y seguimiento, rastreando acciones.

- RTIR http://www.bestpractical.com/rtir/
  RTIR es un sistema gratuito y de código fuente abierto para el tratamiento de incidentes. Su diseño responde a las necesidades de los CERT y otros equipos de respuesta a incidentes.

Herramientas de CRM

Si el grupo atendido es muy amplio y necesita localizar todos los detalles, una base de datos CRM le será útil. Existen diferentes variedades, de las que ofrecemos algunos ejemplos:

- SugarCRM http://www.sugarcrm.com/crm/

- Sugarforce (versión libre de código fuente abierto) http://www.sugarforge.org/

Verificación de la información

- Website watcher http://www.aignes.com/index.htm
  Este programa detecta actualizaciones y cambios en los sitios web.

- Watch that page http://www.watchthatpage.com/
  El servicio envía por correo electrónico información sobre cambios en páginas web (gratuito y comercial).

[30] CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

Búsqueda de información de contacto
Buscar el contacto más indicado para la comunicación de incidentes no es tarea sencilla. Se pueden usar, por ejemplo, las siguientes fuentes de información:

- RIPE[31]
- IRT-object[32]
- TI[33]

Además, la CHIHT ofrece listas de herramientas para buscar información de contacto[34].

CSIRT ficticio (paso 8)

Establecimiento de flujos de procesos y procedimientos educativos y técnicos
El CSIRT ficticio se dedica a la prestación de servicios de CSIRT básicos:

- Alertas y advertencias;
- Comunicados;
- Tratamiento de incidentes.

El equipo desarrolló las estadísticas actualizadas todos sus miembros pueden entender fácilmente. El CSIRT ficticio contrató también a un abogado experto en responsabilidades y política de seguridad de la información. El equipo adoptó herramientas útiles y encontró, en conversaciones con otros CSIRT, información útil sobre cuestiones operativas.

Se generó una plantilla fija para avisos de seguridad y comunicados de incidentes. El equipo usa RTIR para el tratamiento de incidentes.

[31] RIPE whois: http://www.ripe.net/whois.

[32] IRT-object en la base de datos de RIPE: http://www.enisa.europa.eu/cert_inventory/pages/04_02_01.htm#08

[33] Trusted Introducer: http://www.enisa.europa.eu/cert_inventory/pages/04_01_03.htm#07

[34] Herramientas de verificación de identidades de la CHIHT:
http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

9 Formación del personal del CSIRT

Hasta ahora hemos dado los pasos siguientes:

1. Entender qué es un CSIRT y qué puede aportar.
2. Determinar a qué sector prestará servicios el nuevo CSIRT.
3. Establecer qué tipos de servicios puede prestar un CSIRT a su grupo atendido.
4. Analizar el entorno y el grupo de clientes atendido.
5. Definir los servicios.
6. Desarrollar el plan comercial.
   a. Definir el modelo financiero.
   b. Definir la estructura organizativa.
   c. Empezar a contratar personal.
   d. Utilizar la oficina y equiparla.
   e. Desarrollar una política de seguridad de la información.
   f. Buscar socios con los que cooperar.
7. Promover el plan comercial.
   a. Conseguir que se apruebe el modelo de negocio.
   b. Encajarlo todo en un plan de proyecto.
8. Poner el CSIRT en funcionamiento.
   a. Crear métodos de trabajo.
   b. Aplicar las herramientas del CSIRT.

>> El próximo paso será formar al personal.

En este capítulo se tratan las dos fuentes principales de formación para los CSIRT: los cursos de TRANSITS y del CERT/CC.

TRANSITS

TRANSITS ha sido un proyecto europeo dirigido a fomentar la creación de equipos de respuesta a incidentes de seguridad informática (CSIRT) y mejorar los ya existentes abordando el problema de la carencia de personal cualificado. La tarea se ha acometido impartiendo al personal de los (nuevos) CSIRT cursos de formación especializada en cuestiones organizativas, operativas, técnicas, comerciales y jurídicas relacionadas con los servicios que prestan estos equipos.

En particular, TRANSITS

- Ha desarrollado, actualizado y revisado regularmente el material de los cursos modulares;
- Ha organizado talleres de formación en los que se facilitó el material necesario;
- Ha hecho posible la participación del personal de los (nuevos) CSIRT en estos talleres, y ha insistido especialmente en la participación de los países candidatos;
- Ha distribuido el material de los cursos y asumido la explotación de los resultados[35].

[35] TRANSITS: http://www.enisa.europa.eu/cert_inventory/pages/04_02_02.htm#11

La ENISA facilita y apoya los cursos de TRANSITS. Si desea información sobre los requisitos y los precios de la inscripción en estos cursos, póngase en contacto con los expertos en CSIRT de la ENISA:

CERT-Relations@enisa.europa.eu

Encontrará muestras de material de estos cursos en el anexo de este documento.

CERT/CC

La complejidad de las infraestructuras informáticas y de red y el reto de la administración dificultan la gestión adecuada de la seguridad de las redes. Los administradores de redes y de sistemas no cuentan con personal ni con prácticas de seguridad suficientes para defenderse de los ataques y minimizar los daños. Por ello, el número de incidentes de seguridad informática va en aumento.
Cuando se producen incidentes de seguridad informática, las organizaciones deben responder rápida y eficazmente. Cuanto más rápidamente reconoce una organización un incidente, lo analiza y responde a él, más fácil le resultará limitar los daños y recuperar los costes. Crear un equipo de respuesta a incidentes de seguridad informática (CSIRT) es una manera magnífica de contar con esa capacidad de respuesta rápida y ayudar a evitar incidentes futuros.

CERT-CC ofrece cursos para directivos y personal técnico en ámbitos como la creación y la gestión de equipos de respuesta a incidentes de seguridad informática (CSIRT), la respuesta a los incidentes de seguridad y el análisis de éstos y la mejora de la seguridad de las redes. Salvo si se indica lo contrario, los cursos se imparten en Pittsburgh, Pensilvania. Algunos miembros de nuestro personal imparten también cursos de seguridad en la Universidad Carnegie Mellon.

Cursos del CERT/CC[36] sobre CSIRT disponibles

Creación de un equipo de respuesta a incidentes de seguridad informática (CSIRT)
Gestión de un equipo de respuesta a incidentes de seguridad informática (CSIRT)
Fundamentos del tratamiento de incidentes
Tratamiento avanzado de incidentes para personal técnico

Encontrará muestras de material de estos cursos en el anexo de este documento.

CSIRT ficticio (paso 9)
Formar al personal El CSIRT ficticio decide enviar a todo su personal técnico a los siguientes cursos de TRANSITS que se organicen. El jefe del equipo asiste también al curso «*Gestión de un CSIRT*» del CERT/CC.

[36] Cursos del CERT/CC: http://www.sei.cmu.edu/products/courses.

10 Ejercicio: producción de un aviso

Hasta ahora hemos dado los pasos siguientes:

1. Entender qué es un CSIRT y qué puede aportar.
2. Determinar a qué sector prestará servicios el nuevo CSIRT.
3. Establecer qué tipos de servicios puede prestar un CSIRT a su grupo atendido.
4. Analizar el entorno y el grupo de clientes atendido.
5. Definir los servicios.
6. Desarrollar el plan comercial.
   a. Definir el modelo financiero.
   b. Definir la estructura organizativa.
   c. Empezar a contratar personal.
   d. Utilizar la oficina y equiparla.
   e. Desarrollar una política de seguridad de la información.
   f. Buscar socios con los que cooperar.
7. Promover el plan comercial.
   a. Conseguir que se apruebe el modelo de negocio.
   b. Encajarlo todo en un plan de proyecto.
8. Poner el CSIRT en funcionamiento.
   a. Crear métodos de trabajo.
   b. Aplicar las herramientas del CSIRT.
9. Formar al personal.

>> El próximo paso será practicar y prepararse para el trabajo real.

A título ilustrativo, este capítulo describe un ejemplo de práctica cotidiana de un CSIRT: la creación de un aviso de seguridad.

El desencadenante fue el siguiente aviso original de seguridad enviado por Microsoft:

Identificador del boletín	**Boletín de seguridad de Microsoft MS06-042**
Título del boletín	**Actualización acumulativa de seguridad para Internet Explorer (918899)**
Resumen	Esta actualización resuelve diversas vulnerabilidades de Internet Explorer que podrían permitir la ejecución remota de programas.
Clasificación de gravedad máxima	Vital
Consecuencias de la vulnerabilidad	Ejecución remota de programas
Software afectado	**Windows, Internet Explorer.** Para más información, véase el apartado Software afectado y sitios de descargas.

Este boletín aborda una vulnerabilidad detectada últimamente en Internet Explorer. El proveedor publica diferentes correcciones de este software para las distintas versiones de Microsoft Windows.

Tras recibir esta información de vulnerabilidad a través de una lista de correo, el CSIRT ficticio empieza a aplicar el esquema descrito en el apartado 8.2, *«Generación de alertas, advertencias y comunicados»*.

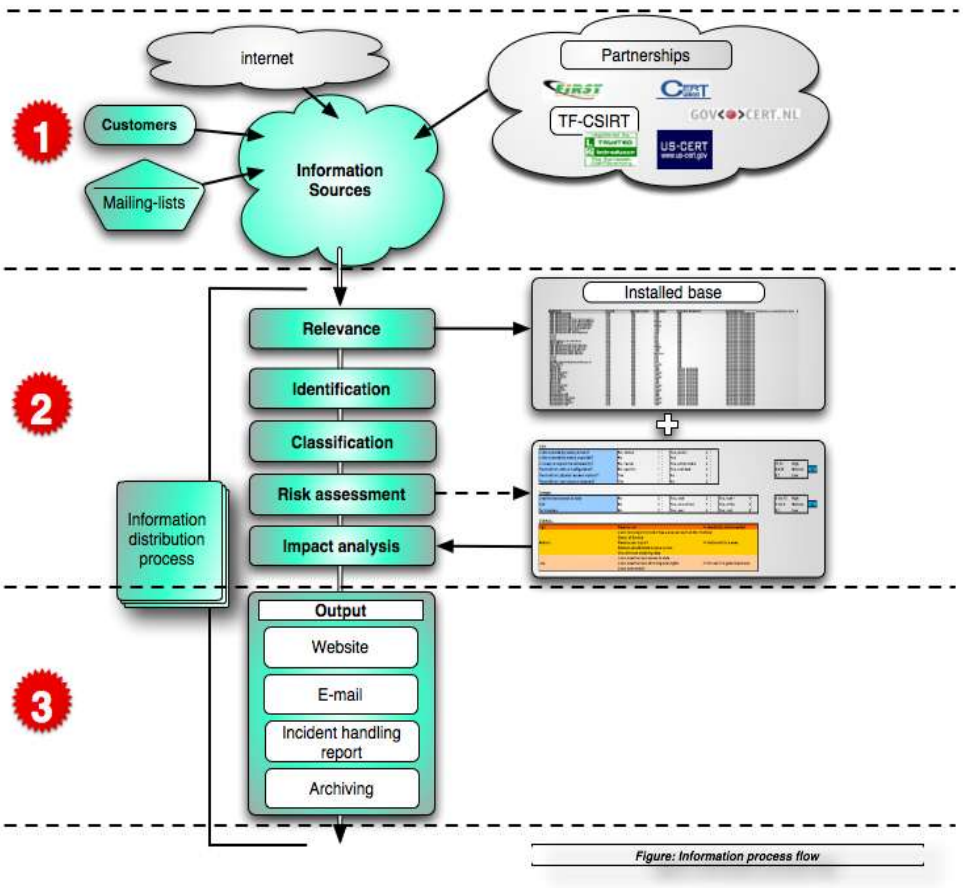


Figure: Information process flow

Paso 1: Recopilación de información sobre la vulnerabilidad

El primer paso es entrar en el sitio web del proveedor. Allí, el CSIRT ficticio verifica a autenticidad de la información y reúne más datos sobre la vulnerabilidad y sobre los sistemas de TI afectados.

Paso 2: Evaluación de la información y valoración del riesgo

Identificación
La información ya se ha verificado cotejando los datos recibidos por correo electrónico con el texto que aparece en el sitio web del proveedor.

Pertinencia
El CSIRT ficticio compara la lista de sistemas afectados que ha encontrado en el sitio web con la de los sistemas que usa el grupo atendido. Se da cuenta de que al menos uno de los clientes del grupo atendido usa Internet Explorer, por lo que la información sobre la vulnerabilidad es pertinente.

Categoría	Aplicación	Software	Versión	SO	Versión del SO	Grupo atendido
Ordenador personal	Navegador	Internet Explorer	x-x-	Microsoft	XP-prof	A

Clasificación
La información es pública, por lo que se puede utilizar y redistribuir.

Evaluación del riesgo y análisis de las consecuencias
Las respuestas a las preguntas siguientes muestran un riesgo y unas consecuencias de nivel *alto* (considerado *crítico* por Microsoft).

RIESGO

¿Es bien conocida la vulnerabilidad?	S
¿Está muy extendida?	S
¿Es fácil de explotar?	S
¿Se trata de una vulnerabilidad que se puede explotar de forma remota?	S

DAÑOS
Las consecuencias posibles son la accesibilidad remota y la ejecución remota de programas. Esta vulnerabilidad presenta numerosos problemas, lo que hace que el riesgo de daños sea *alto*.

Paso 3: Distribución

El CSIRT ficticio es un CSIRT interno. Sus canales de comunicación disponibles son el correo electrónico, el teléfono y un sitio web interno. El CSIRT produce este aviso, derivado de la plantilla del apartado 8.2, *«Generación de alertas, advertencias y comunicados»*.

Título del aviso
Vulnerabilidades múltiples detectadas en Internet Explorer

Referencia
082006-1

Sistemas afectados

- Todos los ordenadores que funcionan con Microsoft

SO relacionados y versión

- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 1 y Microsoft Windows XP Service Pack 2
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows Server 2003 y Microsoft Windows Server 2003 Service Pack 1
- Microsoft Windows Server 2003 for Itanium-based Systems y Microsoft Windows Server 2003 con SP1 for Itanium-based Systems
- Microsoft Windows Server 2003 x64 Edition

Riesgo (Alto-Medio-Bajo)
ALTO

Consecuencias/daños potenciales (Altos-Medios-Bajos)
ALTOS

ID externos: (ID de las CVE y los boletines de vulnerabilidad)
MS-06-42

Descripción de la vulnerabilidad
Microsoft ha encontrado varias vulnerabilidades críticas en Internet Explorer que pueden dar lugar a la ejecución remota de programas.

Consecuencias
Un atacante podría tomar el control total del sistema, instalar programas, añadir usuarios y ver, cambiar o borrar datos. Factor atenuante: todo eso sólo puede ocurrir si el usuario está conectado con derechos de administrador. Las consecuencias en los usuarios conectados con pocos derechos pueden ser menores.

Solución
Actualice inmediatamente Internet Explorer con una corrección.

Descripción (detalles)
Para más información, vea ms06-042.mspx.

Apéndice
Más información en ms06-042.mspx.

Esta información está lista para ser distribuida. Al tratarse de un boletín decisivo, se aconseja llamar además a los clientes del grupo atendido, si es posible.

CSIRT ficticio (paso 10)
Ejercicio Durante las primeras semanas de funcionamiento, el CSIRT ficticio usó como ejercicios varios casos falsos (obtenidos como ejemplos de otros CSIRT). Además emitió un par de avisos de seguridad basados en información real sobre vulnerabilidades distribuida por proveedores de hardware y software, después de adaptarla y ajustarla a las necesidades del grupo atendido.

11 Conclusión

Esta guía acaba aquí. El propósito del documento que está leyendo es dar una visión muy concisa de los diferentes procesos necesarios para crear un CSIRT. No pretende ser completo ni entrar en detalles. En el apartado A.1*, «Otras lecturas»,* del anexo encontrará bibliografía comentada sobre el tema que merece la pena leer.

Los siguientes pasos importantes del CSIRT ficticio serían:

- Recibir comentarios del grupo atendido para afinar los servicios prestados;
- Crear una rutina de trabajo diario;
- Practicar situaciones de emergencia;
- Permanecer en estrecho contacto con los diferentes colectivos CSIRT, para poder llegar a participar en su trabajo voluntario algún día.

12 Descripción del plan de proyecto

NOTA: El plan de proyecto es una primera estimación del tiempo necesario. Dependiendo de los recursos disponibles, la duración real del proyecto podría cambiar.

El plan de proyecto está disponible en diferentes formatos en CD y en el sitio web de la ENISA. Cubre completamente todos los procesos descritos en este documento.

El principal formato será Microsoft Project, para que se pueda usar directamente con esta herramienta de gestión de proyectos.

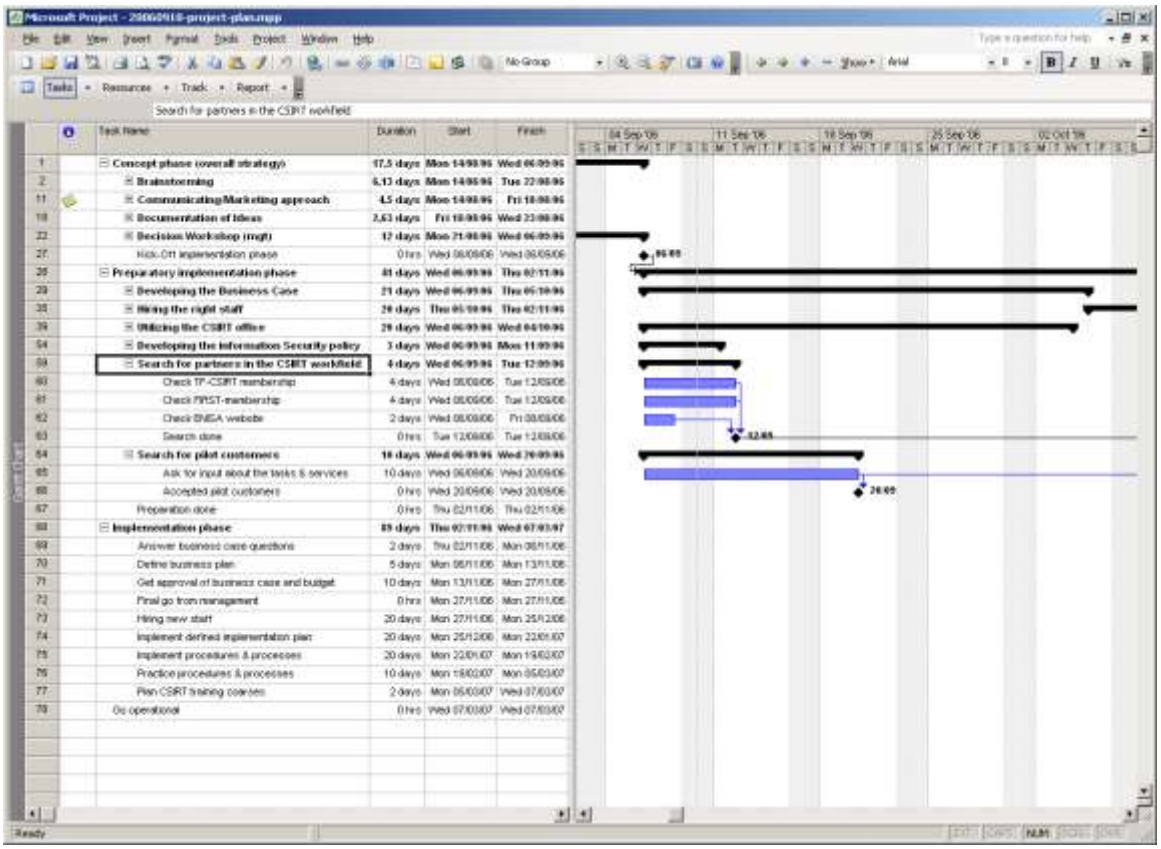


Fig. 17 Plan de proyecto.

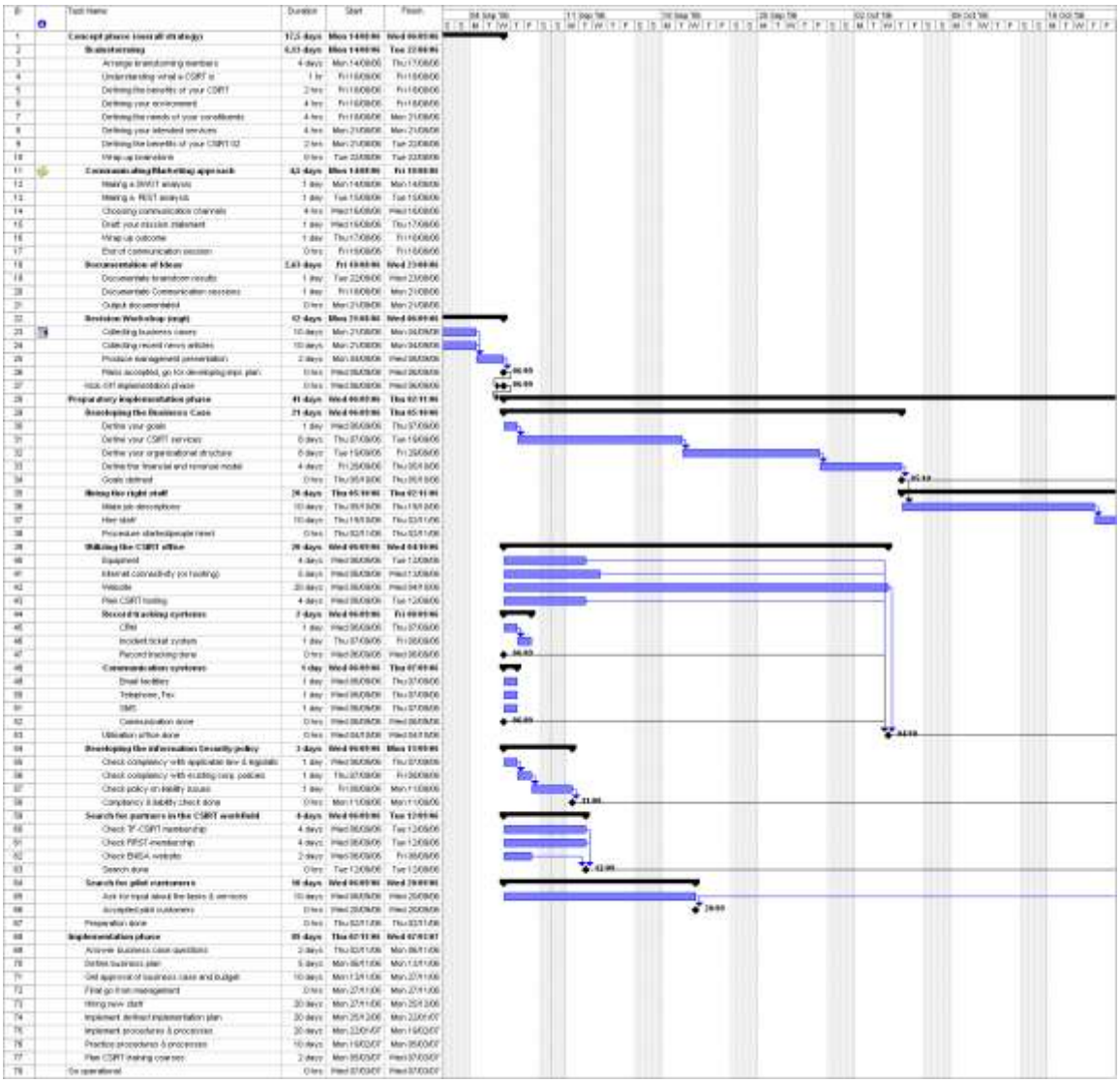


Fig. 18 El plan de proyecto con todas las tareas y una parte del diagrama de Gant.

El plan de proyecto está también disponible en formato CVS y XML. Otras utilizaciones se pueden solicitar a los expertos en CSIRT de la ENISA:

CERT-Relations@enisa.europa.eu

APÉNDICE

A.1 Otras lecturas

Manual del CSIRT (CERT/CC)
Libro de referencia muy completo donde se tratan todos los temas importantes para el funcionamiento de un CSIRT.
Fuente: http://www.cert.org/archive/pdf/csirt-handbook.pdf

Definición de procesos de gestión de incidentes para CSIRT: una obra en construcción
Análisis minucioso de la gestión de incidentes.
Fuente: http://www.cert.org/archive/pdf/04tr015.pdf

Situación actual de los equipos de respuesta a incidentes de seguridad informática (CSIRT)
Análisis completo del panorama mundial de CSIRT. Incluye historia, estadísticas y muchas cosas más.
Fuente: http://www.cert.org/archive/pdf/03tr001.pdf

CERT-in-a-box
Descripción completa de todo lo aprendido con la creación de GOVCERT.NL y *De Waarschuwingsdienst*, el servicio nacional holandés de alerta.
Fuente: http://www.govcert.nl/render.html?it=69

RFC 2350: Expectativas en el ámbito de la respuesta a incidentes de seguridad informática
Fuente: http://www.ietf.org/rfc/rfc2350.txt

Guía de tratamiento de incidentes de seguridad informática del NIST[37]
Fuente: http://www.securityunit.com/publications/sp800-61.pdf

Inventario de actividades del CERT en Europa de la ENISA
Obra de referencia que presenta información sobre los CSIRT europeos y sus diferentes actividades.
Fuente: http://www.enisa.europa.eu/cert_inventory/

[37] NIST: *National Institute of Standards and Technologies* (Instituto nacional de normas y tecnologías).

A.2 Servicios de un CSIRT

Con nuestro agradecimiento a CERT/CC, que nos facilitó esta lista:

Servicios reactivos	***Servicios proactivos***	***Manejo de instancias***
• Alertas y advertencias • Tratamiento de incidentes • Análisis de incidentes • Respuesta a incidentes *in situ* • Apoyo a la respuesta a incidentes • Coordinación de la respuesta a incidentes • Tratamiento de la vulnerabilidad • Análisis de la vulnerabilidad • Respuesta a la vulnerabilidad • Coordinación de la respuesta a la vulnerabilidad	• Comunicados • Observatorio de tecnología • Evaluaciones o auditorías de la seguridad • Configuración y mantenimiento de la seguridad • Desarrollo de herramientas de seguridad • Servicios de detección de intrusos • Difusión de información relacionada con la seguridad	• Análisis de instancias • Respuesta a las instancias • Coordinación de la respuesta a las instancias ***Gestión de la calidad de la seguridad*** • Análisis de riesgos • Continuidad del negocio y recuperación tras un desastre • Consultoría de seguridad • Sensibilización • Educación / Formación • Evaluación o certificación de productos

Fig. 19 Lista de servicios de los CSIRT del CERT/CC.

Descripción de los servicios

Servicios reactivos

Los servicios reactivos están diseñados para responder a peticiones de asistencia, comunicaciones de incidentes del grupo atendido por el CSIRT y cualquier amenaza o ataque que surja contra sistemas de CSIRT. Algunos de estos servicios se pueden iniciar por notificaciones de terceras partes o visualizando controles, registros de sistemas de detección de intrusos y alertas.

Alertas y advertencias

Este servicio incluye la difusión de información que describa el ataque de un intruso, una vulnerabilidad de la seguridad, una alerta de intrusos, un virus informático o un hoax y recomiende alguna vía de acción a corto plazo para enfrentarse al problema resultante. La alerta, advertencia o aviso se envía como reacción al problema surgido, para notificar la actividad a los clientes del grupo atendido y orientarlos para que protejan sus sistemas o para que recuperen los sistemas que se puedan haber visto afectados. La información la puede crear el propio CSIRT o bien puede redistribuirla si la ha recibido de los proveedores, de otros CSIRT o expertos en seguridad o de otros miembros del grupo de clientes atendido.

Tratamiento de incidentes

El tratamiento de incidentes incluye la recepción, el *triage* y la respuesta a peticiones y comunicaciones, así como el análisis de incidentes y acontecimientos. Algunas de las actividades de respuesta pueden ser:

- Actuaciones para proteger sistemas y redes afectadas o amenazadas por la actividad de intrusos;
- Aportación de soluciones y estrategias de mitigación a partir de avisos o alertas;
- Búsqueda de actividad de intrusos en otras partes de la red;
- Filtrado del tráfico de la red;
- Reconstrucción de sistemas;
- Corrección o reparación de sistemas;
- Desarrollo de otras estrategias de respuesta o provisionales.

Dado que existen diferentes maneras de desarrollar las actividades de tratamiento de incidentes dependiendo de los distintos tipos de CSIRT, este servicio se puede detallar más basándose en el tipo de actividades realizadas y en el tipo de asistencia prestada:

Análisis de incidentes

Existen muchos niveles de análisis de incidentes y numerosos subservicios. Básicamente, el análisis de incidentes es un examen de toda la información disponible y de las pruebas o instancias relacionadas con un incidente o evento. La finalidad del análisis es averiguar el alcance del incidente y de los daños que ha causado, la naturaleza del incidente y las estrategias definitivas o provisionales de respuesta de que se dispone. El CSIRT puede usar los resultados del análisis de vulnerabilidad y instancias (descritas a continuación) para entender lo que ha sucedido en un sistema concreto y analizarlo de la forma más completa y actualizada posible. El CSIRT correlaciona la actividad entre incidentes para determinar interrelaciones, tendencias, modelos y firmas intrusas. Dos de los subservicios que se pueden prestar dentro del análisis de incidencias, dependiendo del servicio, los objetivos y los procesos del CSIRT, son:

Recopilación de pruebas forenses

Se trata de la recogida, la conservación, la documentación y el análisis de las pruebas procedentes de un sistema informático comprometido para determinar cambios en el sistema y ayudar a reconstruir los eventos que han desembocado en el compromiso. Esta recopilación de información y pruebas se debe hacer de forma que documente una cadena demostrable de custodia admisible en los tribunales en virtud del régimen probatorio. Las tareas de recopilación de pruebas forenses incluyen, entre otras cosas, la realización de una copia bit a bit del disco duro de los sistemas afectados; la búsqueda de cambios en el sistema, tales como nuevos programas, archivos, servicios y usuarios; el examen de los procesos en ejecución y los puertos abiertos, y la búsqueda de troyanos y juegos de herramientas. Los miembros del personal del CSIRT que desempeñen esta función también deberán estar preparados para declarar como testigos periciales en procedimientos judiciales.

Seguimiento o rastreo

Se trata de rastrear los orígenes de un intruso o identificar sistemas a los que éste haya tenido acceso. Esta actividad podría incluir el seguimiento o rastreo de cómo entró el intruso en los sistemas afectados y las redes relacionadas, qué sistemas utilizó para acceder, dónde se originó el ataque y qué otros sistemas y redes se utilizaron como parte del ataque. También podría incluir la identificación del intruso. Esta tarea puede ser independiente, pero normalmente se realiza en colaboración con el personal encargado de la aplicación de la ley, los proveedores de servicios de Internet u otras organizaciones interesadas.

Respuesta a incidentes *in situ*

El CSIRT presta asistencia directa, *in situ*, para ayudar a los clientes del grupo atendido a recuperarse de un incidente. El CSIRT no se limita a prestar apoyo telefónico o por correo electrónico, sino que también se encarga de analizar físicamente los sistemas afectados y de repararlos y recuperarlos (véase más adelante). Este servicio incluye todas las acciones locales necesarias cuando se sospecha un incidente o cuando éste se produce. Si el CSIRT no está ubicado en el lugar afectado, algunos miembros del equipo deberán viajar a él para dar respuesta. En otros casos puede haber un equipo local respondiendo al incidente como parte de su rutina de trabajo, en especial cuando el tratamiento de incidentes forma parte del funcionamiento normal de los administradores del sistema, de la red o de la seguridad *in situ* de un CSIRT establecido.

Apoyo a la respuesta a incidentes

El CSIRT ayuda y orienta a las víctimas del ataque a recuperarse de un incidente por teléfono, por correo electrónico, por fax o mediante documentación. Esto puede incluir la prestación de asistencia técnica en la interpretación de los datos recogidos, la entrega de información sobre contactos o la orientación en cuanto a estrategias de mitigación y recuperación; en cambio no incluye acciones directas e *in situ* de respuesta a incidentes tal como se describen más arriba, sino que el CSIRT proporciona orientación remota para que el personal *in situ* pueda realizar por sí mismo las tareas de recuperación.

Coordinación de la respuesta a incidentes

El CSIRT coordina las tareas de respuesta entre las partes implicadas en el incidente. Por lo general, éstas incluyen a la víctima del ataque, los sitios relacionados con el ataque y cualquier otro sitio que precise asistencia para analizar el ataque. También puede incluir a las partes que dan soporte en TI a la víctima, como los proveedores de servicios de Internet, a otros CSIRT y a los administradores del sistema y la red. Las tareas de coordinación pueden abarcar la recogida de información sobre contactos, la notificación a los sitios de su implicación potencial (como víctimas o como orígenes de un ataque), la recogida de datos estadísticos sobre el número de sitios implicados y tareas dirigidas a facilitar el intercambio y el análisis de la información. Como parte de las tareas de coordinación puede ser preciso informar a los departamentos jurídico, de recursos humanos y de relaciones públicas de una organización, así como colaborar con ellos. También puede ser necesaria la coordinación con los encargados de la aplicación de la ley. Este servicio no incluye una respuesta a los incidentes directa e *in situ*.

Tratamiento de la vulnerabilidad

El tratamiento de la vulnerabilidad incluye la recepción de información y comunicaciones sobre vulnerabilidades del hardware y del software; el análisis de la naturaleza, los mecanismos y los efectos de las vulnerabilidades, y el desarrollo de estrategias de respuesta para detectar las vulnerabilidades y repararlas. Dado que existen diferentes maneras de desarrollar las actividades de tratamiento de la vulnerabilidad dependiendo de los diferentes tipos de CSIRT, este servicio se puede detallar más basándose en el tipo de actividades realizadas y en el tipo de asistencia prestada:

Análisis de la vulnerabilidad

El CSIRT realiza análisis y exámenes técnicos de las vulnerabilidades del hardware o el software. Esto incluye la verificación de las sospechas de vulnerabilidad y el examen técnico de la vulnerabilidad del hardware o el software para averiguar dónde se encuentra y cómo se puede explotar. El análisis puede incluir la revisión del código fuente, el uso de un depurador para averiguar dónde se produce la vulnerabilidad, o la reproducción del problema en un sistema de prueba.

Respuesta a la vulnerabilidad

Consiste en establecer la respuesta adecuada para mitigar o reparar una vulnerabilidad, lo que puede incluir el desarrollo o la búsqueda de correcciones y soluciones provisionales, así como la notificación a terceros de la estrategia de mitigación, posiblemente creando y distribuyendo avisos o alertas. Este servicio puede incluir la aplicación de la respuesta instalando correcciones, o mediante soluciones provisionales.

Coordinación de la respuesta a la vulnerabilidad

El CSIRT notifica la vulnerabilidad a las diferentes partes de la empresa o del grupo de clientes atendido e informa de cómo repararla o mitigarla. El CSIRT comprueba que la estrategia de respuesta a la vulnerabilidad se haya aplicado con éxito. Este servicio puede incluir la comunicación con los proveedores, con otros CSIRT, con expertos técnicos, con los clientes del grupo atendido y con los individuos o grupos que fueron los primeros en detectar la vulnerabilidad y comunicarla. Las actividades consisten en facilitar el análisis de una vulnerabilidad o una comunicación de vulnerabilidad; coordinar los cronogramas de envío de los documentos, correcciones o soluciones provisionales correspondientes, y sintetizar los análisis técnicos realizados por las diferentes partes. El servicio puede incluir también el mantenimiento de un archivo o una base de conocimientos pública o privada de información sobre la vulnerabilidad, junto con las estrategias de respuesta correspondientes.

Manejo de instancias

Llamamos instancia a cualquier fichero u objeto encontrado en un sistema que pueda estar destinada a investigar o atacar sistemas y redes o que se esté usando para esquivar medidas de seguridad. Las instancias incluyen, entre otras cosas, los virus informáticos, los troyanos, los gusanos, las secuencias de comandos maliciosas y los juegos de herramientas.

El tratamiento de las instancias incluye la recepción de información y copias de las instancias usadas en los ataques de intrusos, el reconocimiento y otras actividades no autorizadas o perjudiciales. Una vez recibida, la instancia se analiza, lo que incluye un examen de su naturaleza, sus mecanismos, su versión y su uso, así como el desarrollo

(o la propuesta) de estrategias de respuesta para detectarlas, eliminarlas y defenderse de ellas. Dado que existen diferentes maneras de desarrollar las actividades de tratamiento de instancias dependiendo de los diferentes tipos de CSIRT, este servicio se puede detallar más basándose en el tipo de actividades realizadas y en el tipo de asistencia prestada:

Análisis de instancias

El CSIRT realiza un examen y un análisis técnicos de cualquier instancia detectada en un sistema. El análisis debe incluir la identificación del tipo de fichero y la estructura de la instancia, comparando una instancia nueva con otras anteriores o con otras versiones de la misma instancia, en busca de similitudes y diferencias, la aplicación de ingeniería inversa o el desensamblaje del código para determinar el propósito y la función de la instancia.

Respuesta a las instancias

Este servicio consiste en determinar cuáles son las acciones adecuadas para detectar y eliminar las instancias de un sistema, así como en prevenir que éstas se instalen. Ello puede implicar la creación de firmas que se puedan añadir a un software antivirus o sistemas de detección de intrusos.

Coordinación de la respuesta a las instancias

Este servicio consiste en poner en común y sintetizar con otros investigadores, CSIRT, proveedores y demás expertos en seguridad los resultados de los análisis y las estrategias de respuesta a una instancia. Las actividades incluyen la notificación y la síntesis del análisis técnico de diferentes fuentes. También pueden incluir el mantenimiento de un fichero público o de los clientes atendidos en el que figuren las instancias conocidas y sus consecuencias, así como las estrategias de respuesta correspondientes.

Servicios proactivos

Los servicios proactivos están diseñados para mejorar la infraestructura y los procesos de seguridad de los clientes atendidos antes de que se produzca o se detecte un incidente o evento cualquiera. Los principales objetivos son evitar los incidentes y reducir su impacto y su alcance en caso de que ocurran.

Comunicados

Incluyen, entre otras cosas, las alertas de intrusos, las advertencias de vulnerabilidad y los avisos sobre seguridad. Estos comunicados informan a los clientes atendidos de nuevos desarrollos con repercusiones a medio o largo plazo, tales como vulnerabilidades o herramientas de intrusión recientemente detectadas. Los comunicados permiten a los clientes proteger sus sistemas y redes de nuevos problemas antes de que éstos se planteen.

Observatorio de la tecnología

El CSIRT supervisa y observa los nuevos desarrollos técnicos, las actividades de los intrusos y las tendencias en identificación de futuras amenazas. Los temas analizados se pueden ampliar para incluir las disposiciones jurídicas y legislativas, las amenazas sociales o políticas y las nuevas tecnologías. Este servicio comprende la lectura de listas de correo de seguridad, sitios web de seguridad y noticias y artículos periodísticos de carácter científico, tecnológico, político y público para extraer información relacionada con la seguridad de los sistemas y las redes de los clientes. Esto puede incluir la comunicación con otras partes consideradas autoridades en estos ámbitos, con el fin de asegurarse de que se obtiene la información y la interpretación más precisas. El resultado de este servicio podría ser algún tipo de comunicado, unas directrices o unas recomendaciones centradas en las cuestiones de seguridad a medio o largo plazo.

Evaluaciones o auditorías de la seguridad

Este servicio consiste en el estudio y el análisis detallados de la infraestructura de seguridad de una organización, basados en los requisitos establecidos por ésta o por otras normas industriales aplicables. También puede incluir un estudio de las prácticas de seguridad de la organización. Entre los numerosos tipos de auditorías y evaluaciones que existen cabe destacar:

Revisión de las infraestructuras

Revisión manual de las configuraciones del hardware y el software, los enrutadores, los cortafuegos, los servidores y demás dispositivos informáticos, para asegurarse de que se adaptan a las políticas de seguridad de mejores prácticas y las configuraciones estándar de la organización o de la industria.

Revisión de las mejores prácticas

Entrevistas con los empleados y los administradores del sistema y de la red para determinar si sus prácticas de seguridad se adaptan a la política de seguridad definida por la organización o a otras normas industriales establecidas.

Escaneo

Uso de detectores de vulnerabilidades o de virus para averiguar qué sistemas y redes son vulnerables.

Pruebas de penetración

Comprobación de la seguridad de un sitio atacando deliberadamente sus sistemas y redes.

Para realizar estas auditorías o evaluaciones se ha de contar con la autorización de la dirección, pues las políticas de algunas empresas prohíben este tipo de enfoques. Este servicio puede incluir el desarrollo de un conjunto de prácticas comunes que se someten a las pruebas o evaluaciones, además del desarrollo de un conjunto de capacidades o unos requisitos de certificación del personal que efectúa las pruebas, evaluaciones, auditorías o análisis. También podría subcontratarse a un tercero o a un proveedor de servicios de gestión de la seguridad con los conocimientos técnicos adecuados en la realización de auditorías y evaluaciones.

Configuración y mantenimiento de herramientas, aplicaciones, infraestructuras y servicios de seguridad

Este servicio identifica o da orientación adecuada para configurar y mantener de un modo seguro las herramientas, las aplicaciones y la infraestructura informática general que usan los clientes atendidos por el CSIRT y el propio CSIRT. Además de orientar, el CSIRT puede actualizar la configuración y realizar el mantenimiento de las herramientas y servicios de seguridad, como los sistemas de detección de intrusos, el escaneo de la red o el control de los sistemas, filtros, envoltorios, cortafuegos, redes privadas virtuales (VPN) y mecanismos de autenticación. El CSIRT puede incluso prestar estos servicios formando parte de su función principal, y también puede configurar los servidores, los ordenadores personales y portátiles, los asistentes digitales personales (PDA) y otros dispositivos inalámbricos de acuerdo con las pautas de seguridad, así como encargarse de su mantenimiento. El servicio incluye la presentación a la dirección de cualquier cuestión o problema que surja con las configuraciones o con el uso de herramientas y aplicaciones que el CSIRT considere susceptible de dejar un sistema vulnerable a un ataque.

Desarrollo de herramientas de seguridad

Este servicio abarca el desarrollo de cualquier herramienta específica para un cliente que el grupo de clientes o el propio CSIRT necesiten o deseen. Esto puede incluir, por ejemplo, el desarrollo de actualizaciones correctivas de seguridad para el software a medida utilizado por el grupo de clientes o la distribución de software protegido que se pueda utilizar para reconstruir ordenadores comprometidos. También puede comprender el desarrollo de herramientas o secuencias de comandos que amplíen la funcionalidad de las herramientas de seguridad existentes, tales como un nuevo plug-in para una vulnerabilidad o escáner de red, secuencias de comandos que faciliten el uso de la tecnología de encriptación o mecanismos de distribución automática de actualizaciones correctivas.

Servicios de detección de intrusos

Los CSIRT que prestan este servicio revisan los registros de sistemas de detección de intrusos existentes, analizan e inician una respuesta para cualquier evento que supere un umbral definido o envían alertas de conformidad con un acuerdo de nivel de servicios definido o una estrategia de alcance. La detección de intrusos y el análisis de los registros de seguridad asociados puede ser una tarea desalentadora, y no sólo en lo que se refiere a determinar en qué lugar del entorno situar los sensores, sino también en lo relativo a la recopilación y el posterior análisis de las grandes cantidades de datos capturados. En muchos casos se necesitan herramientas o conocimientos especializados para sintetizar e interpretar la información y poder identificar alarmas, ataques o eventos de red falsos y aplicar estrategias adecuadas para eliminarlos y minimizarlos. Algunas organizaciones optan por subcontratar esta actividad a terceros con más experiencia en estos servicios, como proveedores de servicios de gestión de la seguridad.

Difusión de información relacionada con la seguridad

Este servicio proporciona al grupo de clientes una colección completa y de búsqueda fácil de información útil para mejorar la seguridad. Dicha información puede incluir:

- Directrices de comunicación e información de contacto del CSIRT,
- Ficheros de alertas, advertencias y otros comunicados,
- Documentación acerca de las mejores prácticas actuales,
- Asesoramiento general sobre seguridad informática,
- Políticas, procedimientos y listas de comprobación,
- Desarrollo de actualizaciones correctivas y difusión de información,
- Enlaces con proveedores,
- Estadísticas y tendencias actuales de la comunicación de incidentes,
- Otras informaciones que puedan mejorar las prácticas generales de seguridad.

Esta información la puede desarrollar y publicar el CSIRT u otra parte de la organización (TI, recursos humanos o relaciones con los medios) y puede incluir informaciones procedentes de fuentes externas tales como otros CSIRT, proveedores, y expertos en seguridad.

Servicios de gestión de la calidad de la seguridad

Los servicios de esta categoría no son exclusivos del tratamiento de incidentes ni de los CSIRT. Son servicios establecidos y muy conocidos, diseñados para mejorar la seguridad general de una organización. Merced a la experiencia adquirida con la prestación de los servicios reactivos y proactivos descritos más arriba, un CSIRT puede aportar a esos servicios de gestión de la calidad perspectivas únicas de las que en caso contrario no dispondrían. Estos servicios están diseñados para tener en cuenta los comentarios recibidos y las lecciones aprendidas basándose en los conocimientos adquiridos al responder a incidentes, vulnerabilidades y ataques. Al incorporar estas experiencias a los servicios tradicionales establecidos (descritos más adelante) como parte de un proceso de gestión de la calidad de la seguridad, pueden mejorar los esfuerzos de seguridad a largo plazo de una organización. Según cuáles sean sus responsabilidades y sus estructuras organizativas, un CSIRT puede prestar estos servicios o participar en ellos como parte de las tareas de un equipo mayor.
Las descripciones siguientes explican cómo puede el CSIRT aprovechar en sus conocimientos técnicos cada uno de estos servicios de gestión de la calidad de la seguridad.

Análisis de riesgos

Los CSIRT pueden añadir valor a las evaluaciones y los análisis de riesgos. De este modo, la capacidad de la organización de evaluar amenazas reales, realizar evaluaciones cualitativas y cuantitativas realistas de los riesgos de los activos de información y evaluar las estrategias de protección y respuesta puede mejorar. Los CSIRT que prestan este servicio podrían desarrollar o ayudar a desarrollar actividades de análisis de riesgo de la seguridad de la información de los nuevos sistemas y procesos empresariales o evaluar las amenazas y los ataques contra los activos y sistemas del grupo de clientes atendido.

Planificación de la continuidad de los negocios y la recuperación tras un desastre

Tanto los incidentes que han ocurrido como las previsiones en este ámbito y las tendencias en seguridad hacen pensar que cada vez serán más los incidentes con potencial de provocar una degradación grave de las operaciones comerciales. Por lo tanto, en las tareas de planificación se deberían tener en cuenta la experiencia y las recomendaciones del CSIRT a la hora de determinar cómo conviene responder a tales incidentes si se quiere garantizar la continuidad de las operaciones comerciales. Los CSIRT que brindan este servicio participan en la planificación de la continuidad del negocio y la recuperación tras un desastre en los eventos relacionados con los ataques y las amenazas a la seguridad informática.

Consultaría sobre seguridad

Los CSIRT pueden asesorar y orientar sobre las mejores prácticas de seguridad aplicables en las operaciones comerciales del grupo de clientes atendido. Un CSIRT que preste este servicio interviene en la preparación de recomendaciones o la identificación de los requisitos de compra, instalación o protección de los nuevos sistemas, dispositivos de red, aplicaciones de software o procesos comerciales de toda la empresa. Este servicio incluye orientación y asistencia en el desarrollo de las políticas de seguridad de la organización o de los clientes atendidos. También puede incluir la declaración testimonial o el asesoramiento a órganos legislativos u otras entidades públicas.

Sensibilización

Los CSIRT pueden estar preparados para saber cuándo necesitan los clientes más información y orientación para cumplir mejor las prácticas de seguridad aceptadas y las políticas de seguridad de la organización. La mayor sensibilización general sobre seguridad entre los clientes no sólo mejora su grado de entendimiento de las cuestiones relacionadas con la seguridad, sino que además les ayuda a conseguir que su labor cotidiana resulte más segura. De este modo se puede reducir el número de ataques con éxito y aumentar la probabilidad de que los distintos clientes del grupo atendido detecten y comuniquen ataques, con lo que los tiempos de recuperación disminuirán y las pérdidas desaparecerán o se minimizarán.
Los CSIRT que prestan este servicio buscan oportunidades de aumentar la sensibilización en cuanto a seguridad publicando artículos y desarrollando pósteres, boletines, sitios web u otros recursos informativos que explican las mejores prácticas en seguridad y aconsejan sobre las precauciones que conviene tomar. Las actividades pueden incluir también la organización de reuniones y seminarios para mantener al día a los clientes en cuanto a los procedimientos de seguridad en uso y las amenazas potenciales a los sistemas de la organización.

Educación / Formación

Este servicio incluye proporcionar a los clientes información sobre cuestiones relacionadas con la seguridad informática, por medio de seminarios, talleres, cursos y tutoriales. Los temas tratados pueden incluir orientaciones para la comunicación de incidentes, métodos de respuesta adecuados, herramientas de respuesta a incidentes, métodos de prevención de incidentes y otras informaciones necesarias para proteger de incidentes de seguridad informática, detectarlos, comunicarlos y responder a ellos.

Evaluación o certificación de productos

En el marco de este servicio, el CSIRT puede realizar evaluaciones de herramientas, aplicaciones y otros servicios destinados a garantizar la seguridad de los productos y el cumplimiento de las prácticas en materia de seguridad del CSIRT o la organización. Las herramientas y aplicaciones examinadas pueden ser de código fuente abierto o productos comerciales. Este servicio se puede prestar en forma de evaluación o a través de un programa de certificación, dependiendo de las normas que apliquen la organización o el CSIRT.

A.3 Ejemplos

CSIRT ficticio

Paso 0 - Entender qué es un CSIRT:

El CSIRT de muestra tendrá que servir a una institución mediana con un personal de 200 trabajadores. La institución tiene su propio departamento de TI y otras dos sucursales en el mismo país. Las TI desempeñan un papel muy importante en la empresa, pues se utilizan para la comunicación interna, en las redes de datos y en una empresa electrónica las 24 horas del día, los 7 días de la semana. La institución dispone de una red propia y de una conexión redundante a Internet por medio de dos proveedores de servicios de Internet diferentes.

- -

Paso 1: Fase inicial

En la fase inicial, el nuevo CSIRT se organiza como un CSIRT interno que presta servicios a la empresa a la que pertenece, el departamento de TI local y su personal. También apoya y coordina entre las diferentes sucursales el tratamiento de los incidentes relacionados con la seguridad de las TI.

- -

Paso 2: Elección de los servicios adecuados

En la fase inicial se dispone que el nuevo CSIRT se centrará principalmente en prestar algunos de los servicios básicos a los empleados.

Se resuelve que, tras una fase piloto, se puede tomar en consideración la ampliación de la cartera de servicios y se pueden añadir algunos «servicios de gestión de la seguridad». Esta decisión se basará en los comentarios del grupo piloto de clientes y se tomará en estrecha cooperación con el Departamento de garantía de la calidad.

- -

Paso 3: Análisis de los clientes atendidos y de los canales de comunicación adecuados

Una sesión de *brainstorming* un grupo de directivos destacados y el grupo de clientes atendido generó datos suficientes para un análisis DOFA que permitió establecer la necesidad de servicios básicos:

- Alertas y advertencias
- Tratamiento de los incidentes (análisis, apoyo a las respuestas y coordinación de las respuestas)
- Comunicados

Se debe garantizar una difusión organizada de la información, de modo que alcance a tantos clientes del grupo atendido como sea posible. Por ello se ha resuelto que las alertas, las advertencias y los comunicados en forma de avisos de seguridad se publiquen en un sitio web dedicado y se comuniquen en una lista de correo. El CSIRT facilita correo electrónico, teléfono y fax para recibir los informes de incidencias. Para el próximo paso está previsto un formulario web unificado.

- -

Paso 4: Declaración de servicios

La dirección del CSIRT ficticio ha preparado la siguiente declaración de servicios:
«El CSIRT ficticio ofrece información y asistencia al personal de la empresa a la que pertenece para reducir su riesgo de incidentes de seguridad informática, así como para responder a tales incidentes cuando se produzcan.»

De este modo, el CSIRT ficticio deja claro que es un CSIRT interno y que su cometido principal es ocuparse de las cuestiones relacionadas con la seguridad de las TI.

- -

Paso 5: Definición del plan comercial

Modelo financiero
La empresa tiene un negocio electrónico que funciona 24 horas al día, 7 días a la semana, y un departamento de TI que también funciona 24 horas al día, 7 días a la semana, por lo que se decide prestar un servicio completo en horario de oficina y uno de urgencias el resto del tiempo. Los servicios al grupo atendido serán gratuitos, pero durante la fase piloto y de evaluación se estudiará la posibilidad de prestar servicios a clientes externos.

Modelo de ingresos
Durante las fases inicial y piloto, la financiación del CSIRT correrá a cargo de la empresa a la que pertenece. Durante las fases piloto y de evaluación se discutirá una financiación adicional que incluirá la posibilidad de vender servicios a clientes externos.

Modelo organizativo
T La organización a la que pertenece el CSIRT es una pequeña empresa, por lo que se elige el modelo incrustado.
En horario de oficina, tres trabajadores se encargarán de los servicios básicos (distribución de avisos de seguridad y tratamiento y coordinación de incidentes).

El departamento de TI de la empresa ya dispone de personal con capacidades adecuadas. Se llega a un acuerdo con dicho departamento para que el nuevo CSIRT pueda pedirle apoyo si lo necesita. También pueden recurrir a la segunda línea de técnicos de guardia.
Habrá un equipo central del CSIRT con cuatro miembros a tiempo completo y otros cinco miembros del CSIRT. Uno de ellos también estará disponible en turno rotativo.

Personal
El jefe del CSIRT tiene experiencia en seguridad y apoyo de primer y segundo nivel y ha trabajado en el ámbito de la gestión de crisis. Los otros tres miembros del equipo son especialistas en seguridad. Los miembros del equipo procedentes del departamento de TI que intervienen a tiempo parcial son especialistas en su parte de la infraestructura de la empresa.

- -

Paso 5 Uso de la oficina y política de seguridad de la información

Equipamiento y ubicación de la oficina
Dado que la seguridad física de la empresa a la que pertenece ya es eficaz, el nuevo CSIRT está bien cubierto en este aspecto. Se prepara una «sala de guerra» desde donde se coordinará la acción en caso de emergencia. Se adquiere una caja fuerte para el material de encriptación y los documentos delicados. Se instala una línea telefónica aparte que incluye una centralita para contactar con la línea directa en horario de oficina, y con el móvil «de guardia» fuera del horario de oficina, ambos con el mismo número.

También se puede usar el equipamiento existente y el sitio web corporativo para publicar información relacionada con el CSIRT. Se instala y se mantiene una lista de correo en la que hay una parte de la comunicación a la que sólo pueden acceder los miembros del equipo y otros equipos. Todos los detalles de contacto de los miembros del personal se guardan en una base de datos, y una copia impresa de éstos se deposita en la caja fuerte.

Reglamentación
Al tratarse de un CSIRT incrustado en una empresa que cuenta con políticas de seguridad de la información, las políticas correspondientes del CSIRT se han establecido con ayuda del asesor jurídico de la empresa.
- -
Paso 7 Buscar cooperación

Gracias al Inventario de la ENISA, se encontraron rápidamente algunos CSIRT del mismo país, con los que se establecieron contactos. Se concertó una visita sobre el terreno entre uno de ellos y el jefe del equipo, recientemente contratado, que obtuvo información sobre las actividades de los CSIRT nacionales y asistió a una reunión con ellos.
La reunión resultó muy útil para recoger ejemplos de métodos de trabajo y conseguir el apoyo de un par de equipos.
- -
Paso 8 Promover el plan comercial

Se ha decidido recoger hechos y cifras de la historia de la empresa, lo que resultará muy útil para realizar un estudio estadístico de la situación de la seguridad de las TI. Esta recopilación debería seguir adelante una vez el CSIRT se haya establecido y esté en funcionamiento, para mantener las estadísticas actualizadas.

Se establecieron contactos y se mantuvieron entrevistas acerca de sus modelos de negocio con otros CSIRT nacionales que prestaron apoyo recopilando diapositivas con información acerca de los últimos desarrollos en incidentes de seguridad de las TI, así como de los costes de tales incidentes.

En este ejemplo de CSIRT ficticio no había una necesidad acuciante de convencer a la dirección de la importancia de las empresas de TI, por lo que no resultó difícil conseguir luz verde para ponerse manos a la obra. Se prepararon un modelo de negocio y un plan de proyecto que incluían una estimación de los costes de establecimiento y funcionamiento.

- -

Paso 9 Establecimiento de flujos de procesos y procedimientos educativos y técnicos

El CSIRT ficticio se dedica a la prestación de servicios de CSIRT básicos:

- Alertas y advertencia;
- Comunicados;
- Tratamiento de incidentes.

El equipo desarrolló procedimientos que funcionan bien y que todos sus miembros pueden entender fácilmente. El CSIRT ficticio contrató también a un abogado experto en responsabilidades y política de seguridad de la información. El equipo adoptó herramientas útiles y encontró, en conversaciones con otros CSIRT, información útil sobre cuestiones operativas.

Se generó una plantilla fija para avisos de seguridad y comunicados de incidentes. El equipo usa RTIR para el tratamiento de incidentes.

- -

Paso 10 Formar al personal

El CSIRT ficticio decide enviar a todo su personal técnico a los siguientes cursos de TRANSITS que se organicen. El jefe del equipo asiste también al curso «*Gestión de un CSIRT*» del CERT/CC.

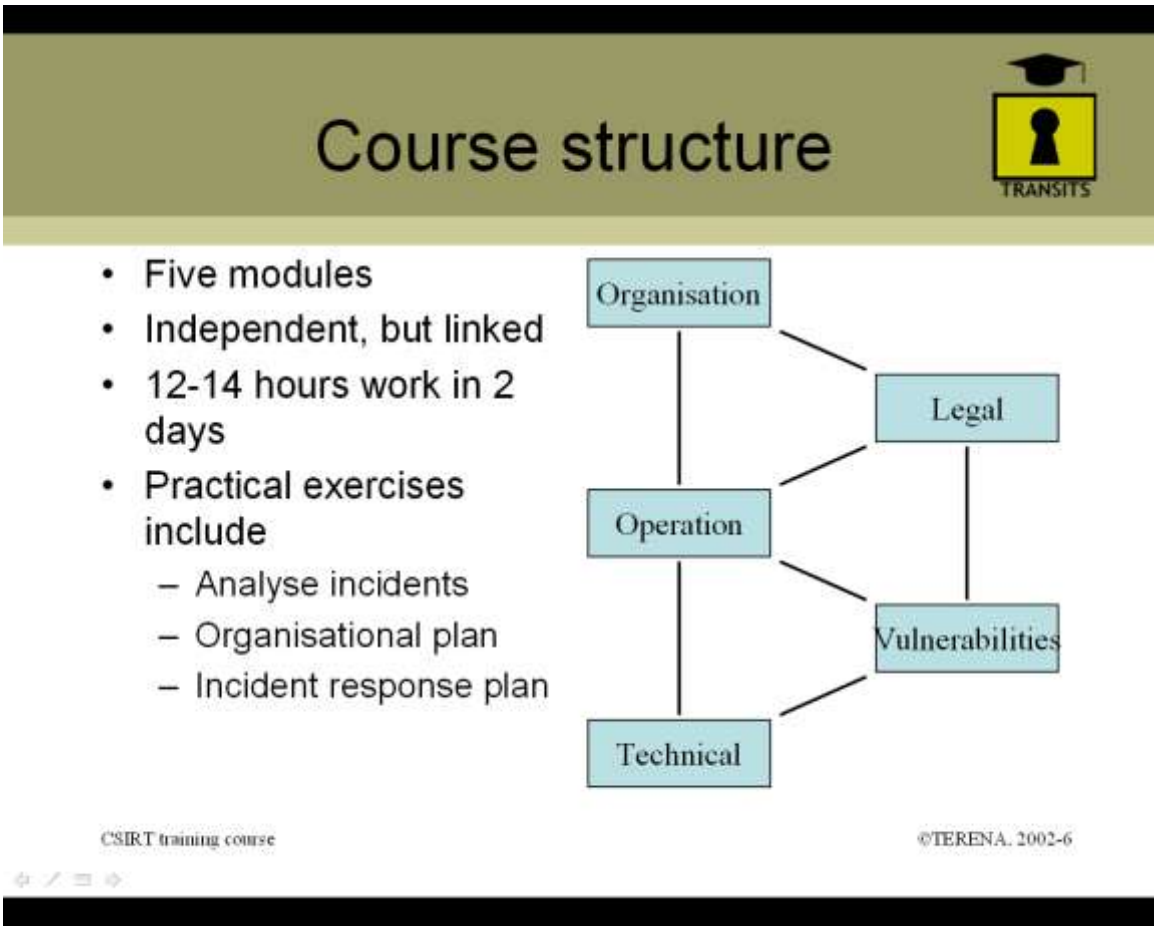
- -

Paso 11: Ejercicio

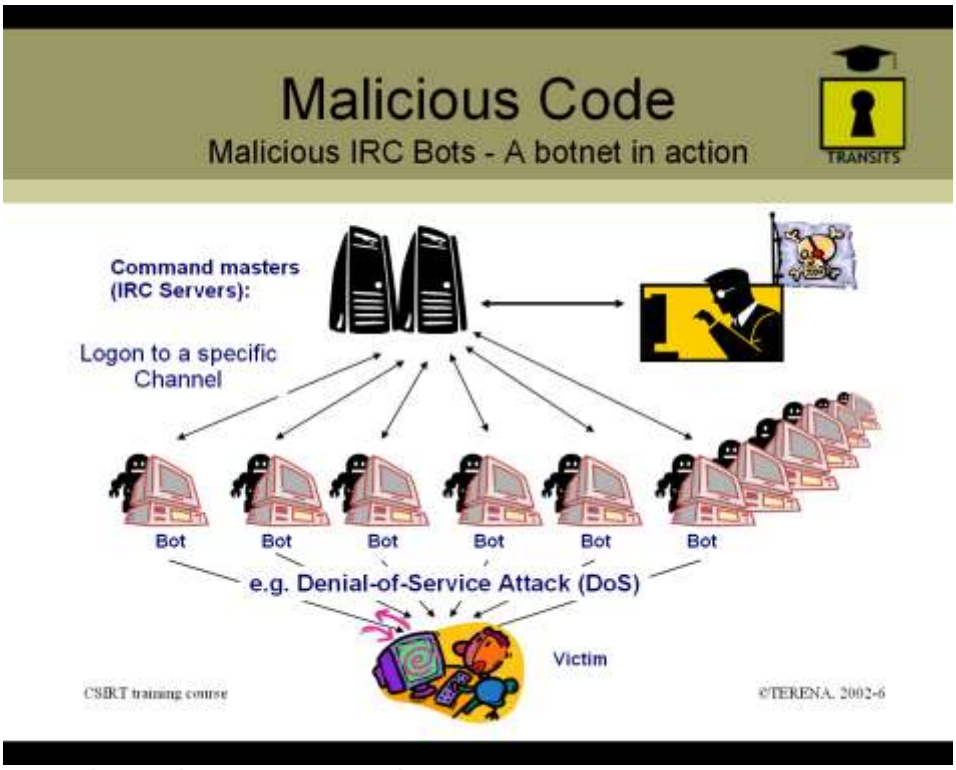
Durante las primeras semanas de funcionamiento, el CSIRT ficticio usó como ejercicios varios casos falsos (obtenidos como ejemplos de otros CSIRT). Además emitió un par de avisos de seguridad basados en información real sobre vulnerabilidades distribuida por proveedores de hardware y software, después de adaptarla y ajustarla a las necesidades del grupo de clientes atendido.

Muestras de material de los cursos sobre CSIRT

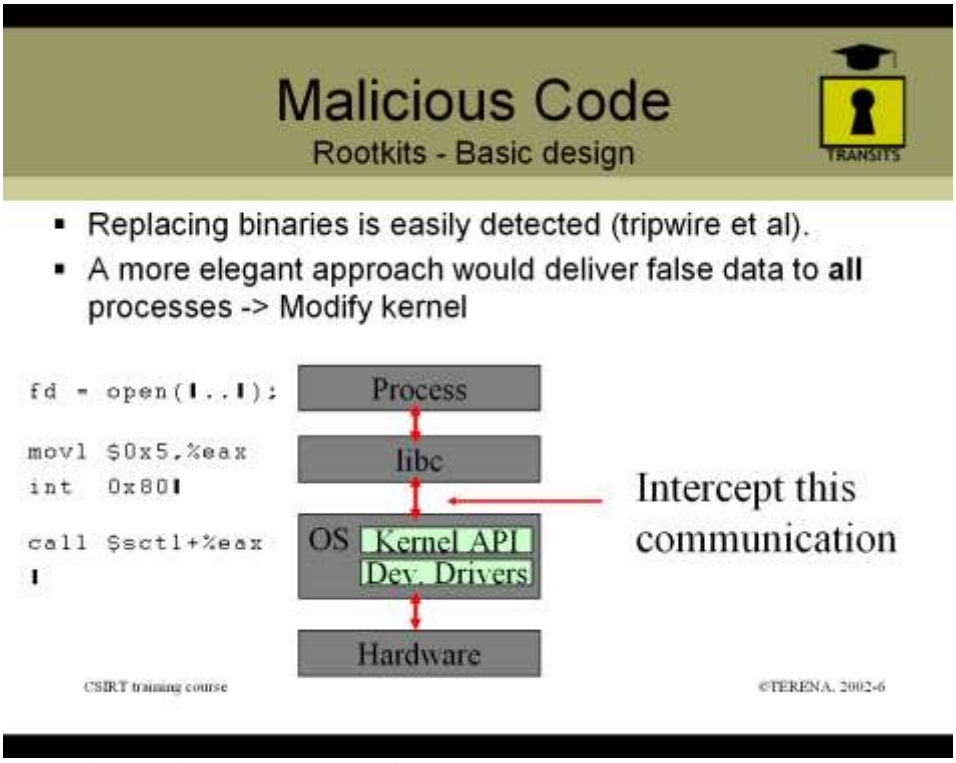
TRANSITS (con la autorización de Terena, http://www.terena.nl)



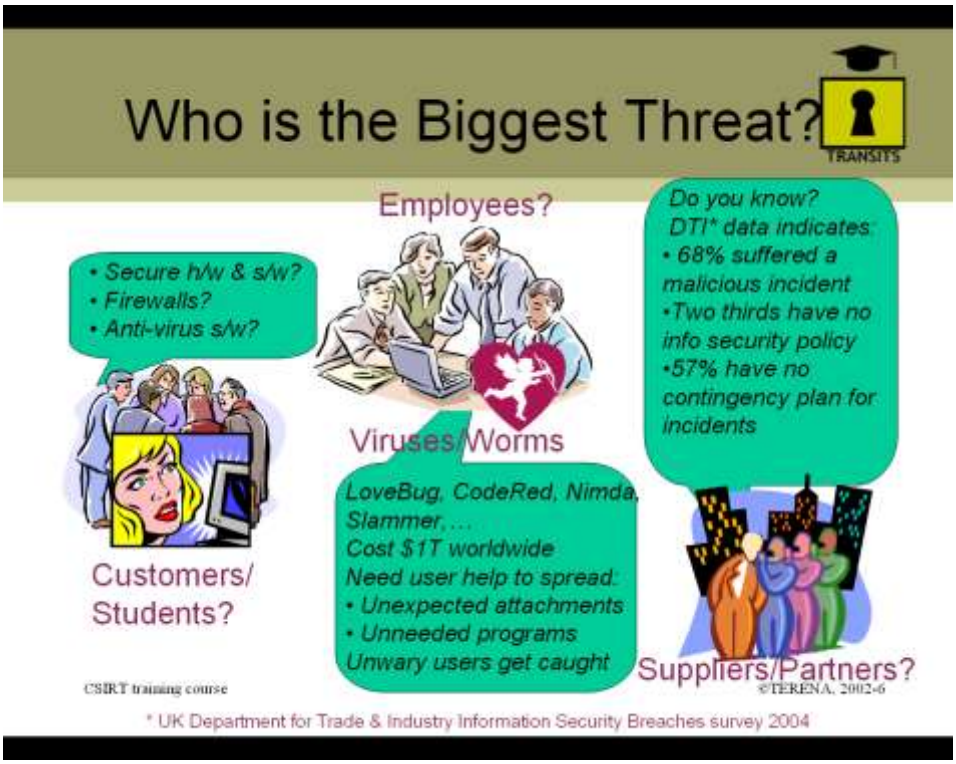
Visión general: Estructura del curso.



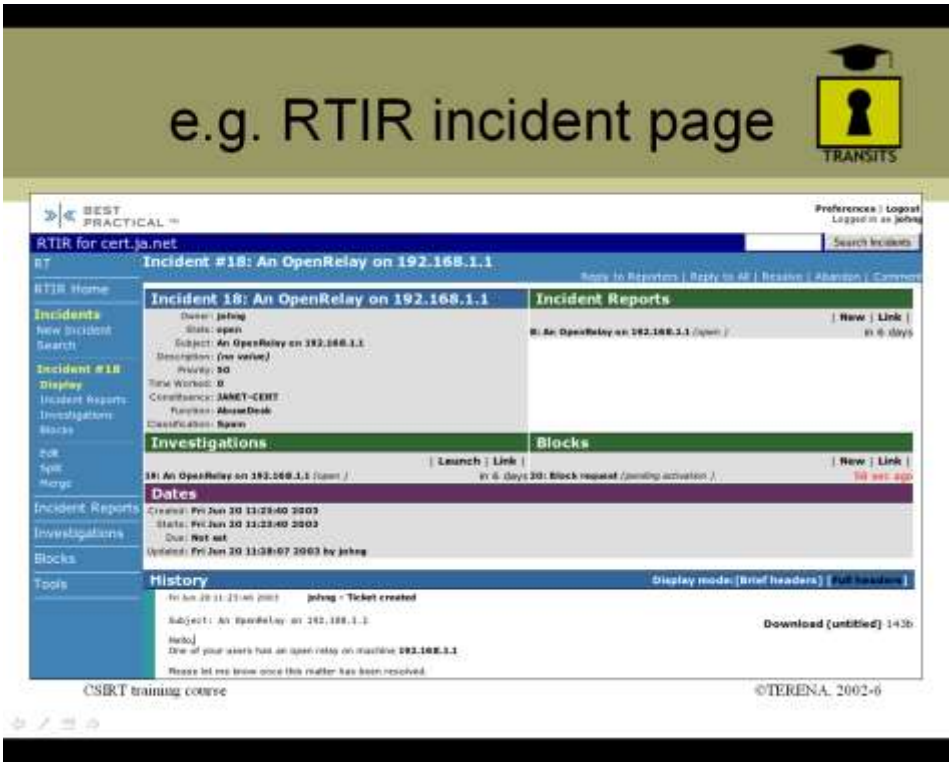
Del *Módulo técnico*: Descripción de una botnet.



Del *Módulo técnico*: Diseño básico de un rootkit.



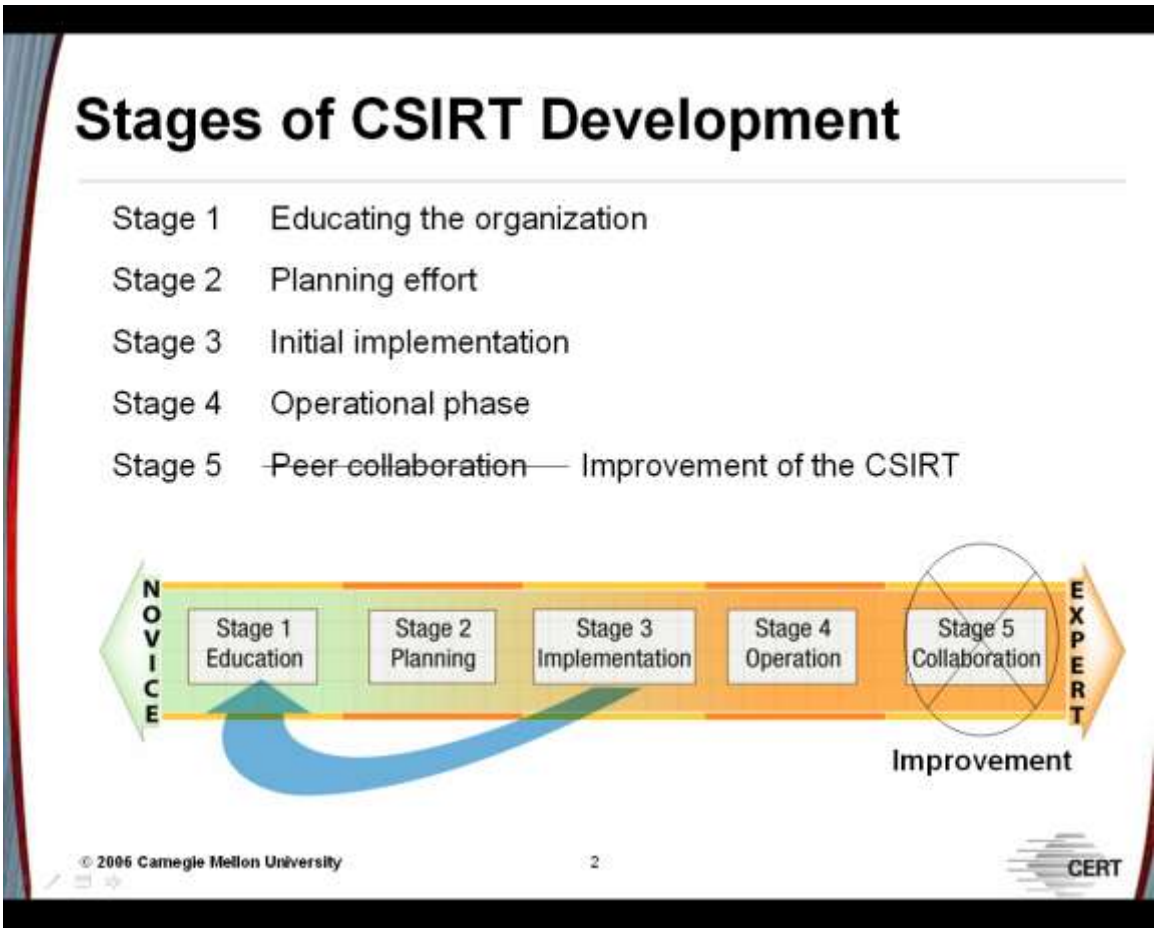
Del *Módulo sobre organización*: Interna o externa: ¿dónde reside la mayor amenaza?



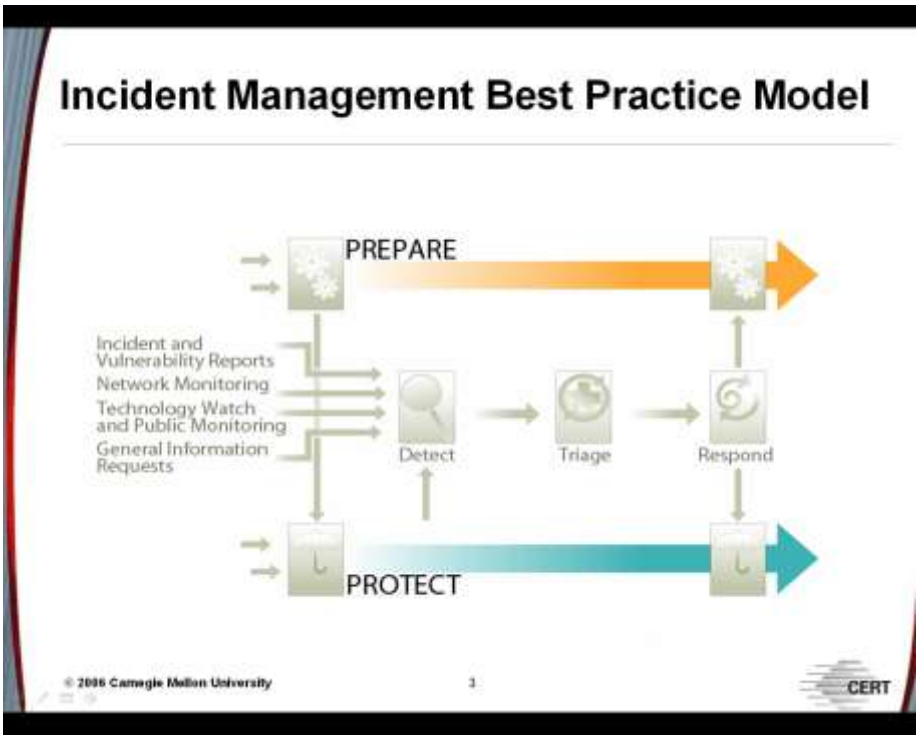
Del *Rastreo operativo*: Rastreador de peticiones de respuestas a incidentes *(Request Tracker for Incident Response*, RTIR).

«Setting up of CSIRTs» **(Creación de CSIRT) (con la amable autorización de CERT/CC, http://www.cert.org)**

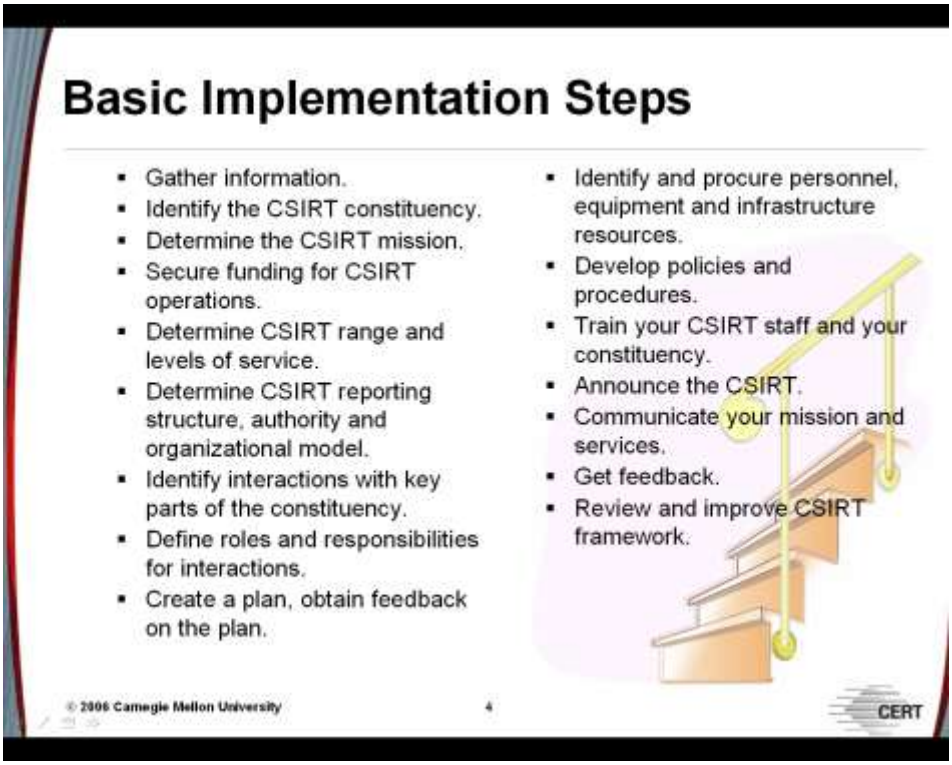
La ENISA agradece al Equipo de desarrollo de CSIRT del Programa CERT que le haya permitido usar el contenido de sus cursos de formación.



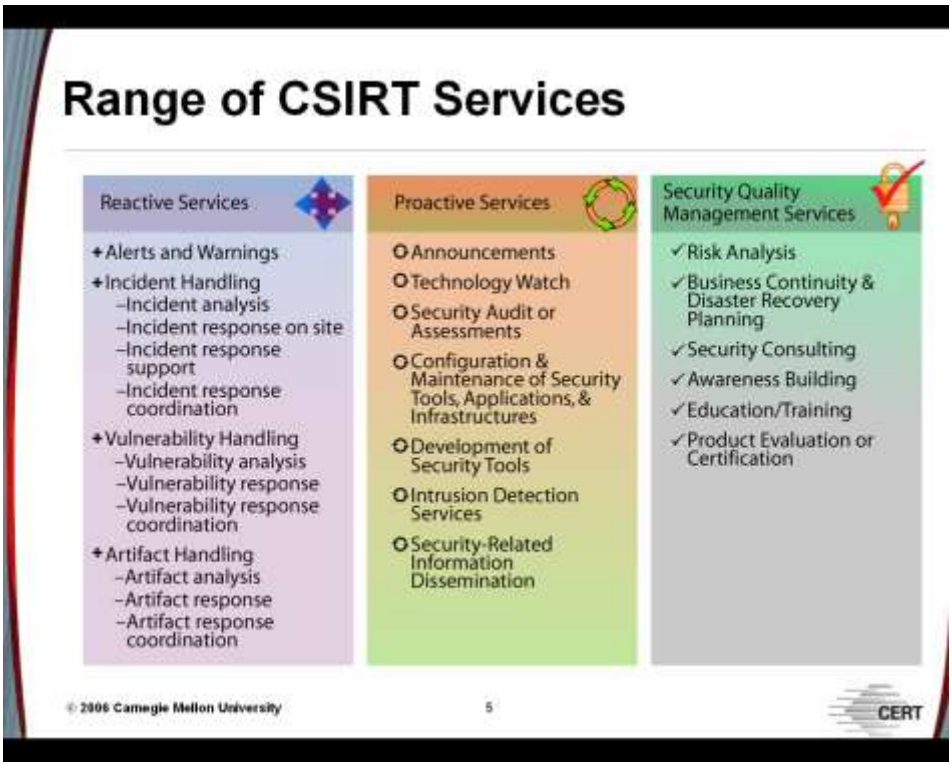
Del *Curso de formación del CERT/CC:* Etapas del desarrollo de un CSIRT.



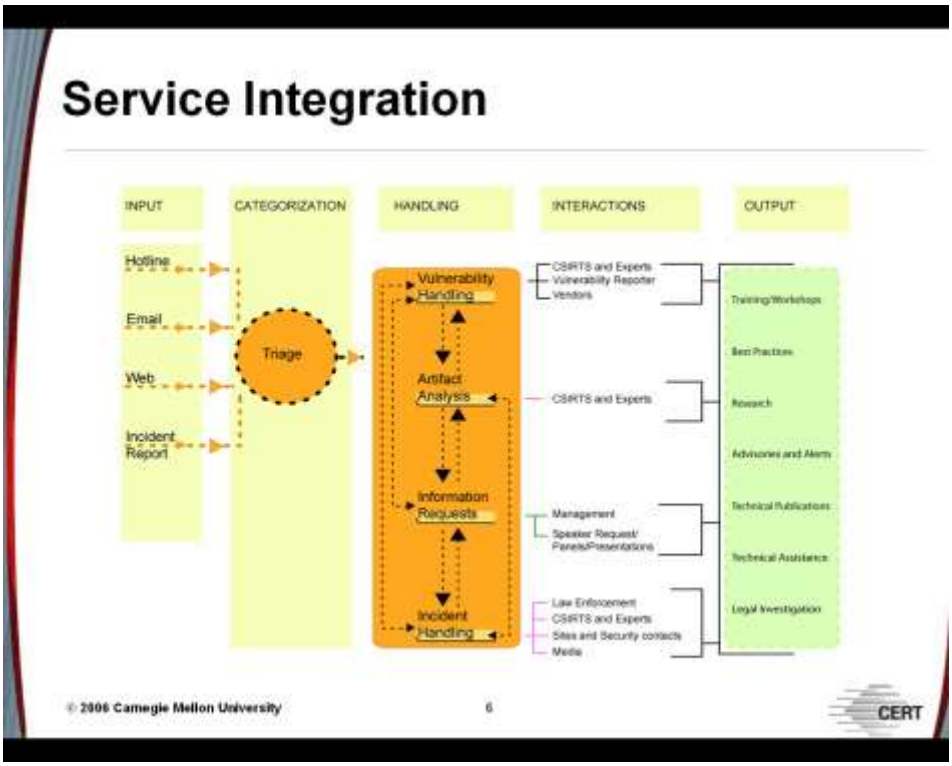
Del *Curso de formación del CERT/CC:* Mejores prácticas en la gestión de incidentes.



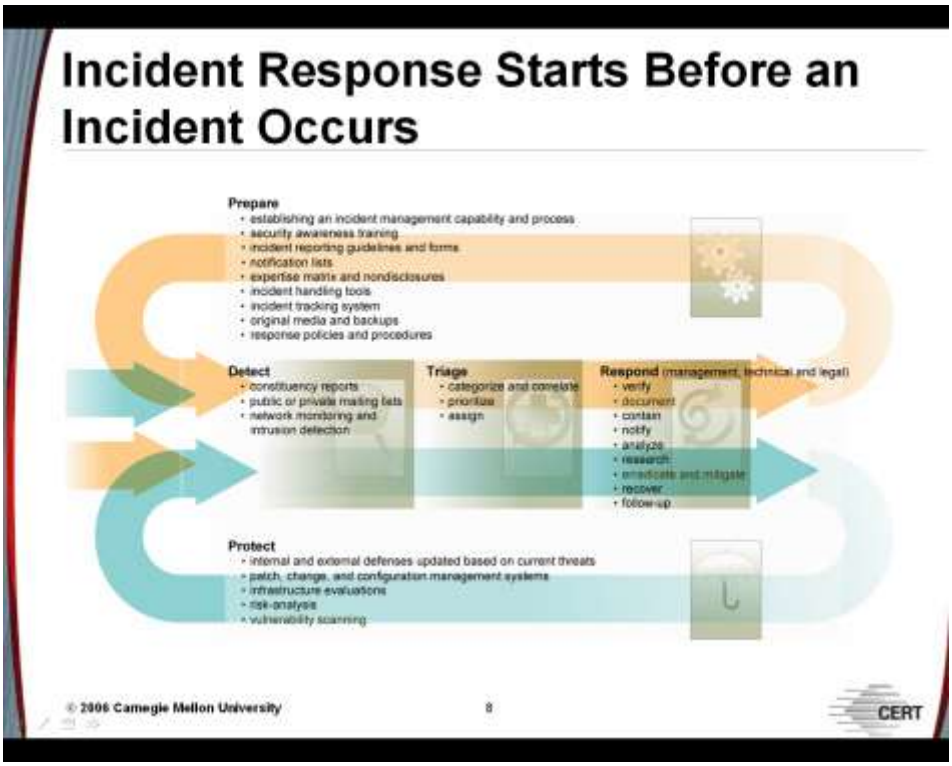
Del *Curso de formación del CERT/CC:* Pasos que se han de dar para crear un CSIRT.



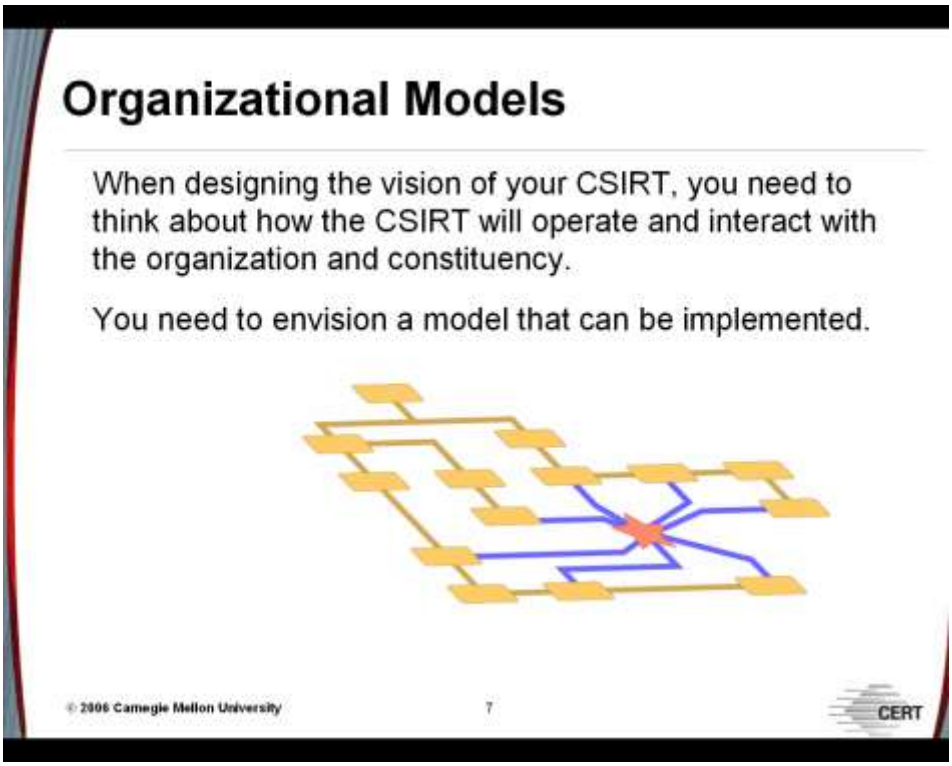
Del *Curso de formación del CERT/CC:* Servicios que puede prestar un CSIRT.



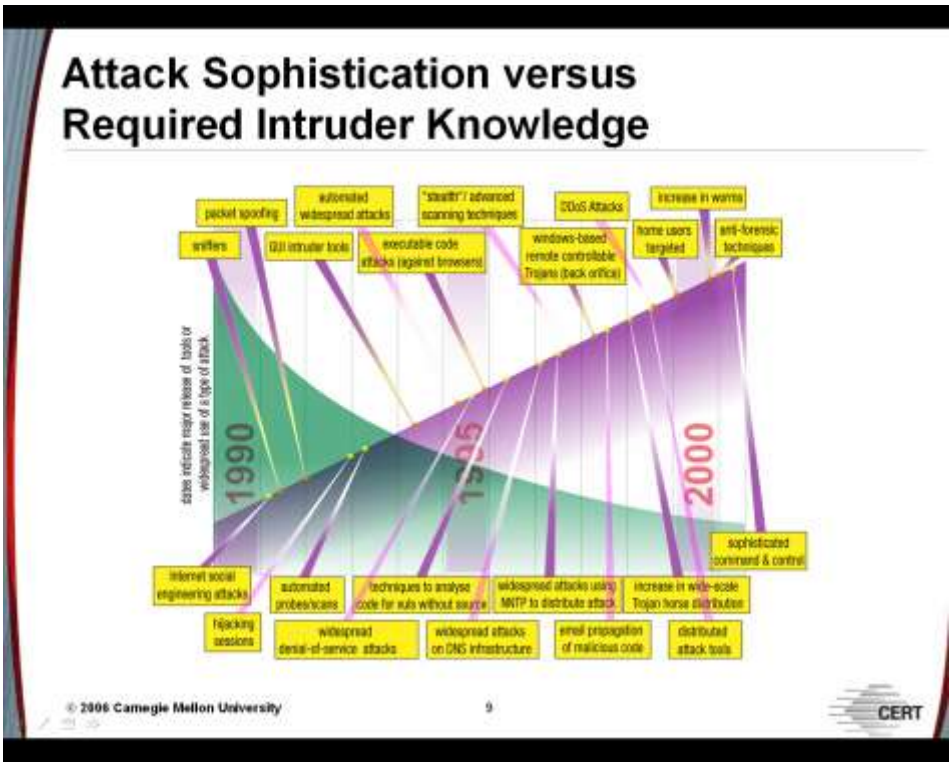
Del *Curso de formación del CERT/CC:* Esquema de la gestión de un incidente.



Del *Curso de formación del CERT/CC:* Respuesta a un incidente.



Del *Curso de formación del CERT/CC:* ¿Cómo se organizará el CSIRT?



Del *Curso de formación del CERT/CC:* A menos conocimientos, más daños.