Modelo de Coordinación y Atención de Emergencias en el ámbito de la Sociedad de la Información

Presentado en el marco del Premio de la Academia Canaria de Seguridad para trabajos de estudio e investigación en seguridad y emergencias

Febrero 2007

Tabla de Contenido

I. Resumen Ejecutivo 7

1. Resumen Ejecutivo. 8

II. Introducción 11

2. Introducción 12

Ejemplo de ataques a red informática bancaria 15

Ejemplo en planta generadora de electricidad 17

Ejemplo en ámbito asistencial y sanitario 18

III. Antecedentes 20

3. Antecedentes 21

3.1 Estándares de confidencialidad y seguridad de los datos 21

Ley Orgánica de Protección de Datos (LOPD) 24

Reglamento de Medidas de Seguridad (RMS) 25

3.2 Organismos e Iniciativas para la atención de incidencias en seguridad de la información 28

3.2.1 Iniciativa CSIRT Europea (TERENA TF-CSIRT)[1] 29

3.3 Iniciativa CSIRT Global (FIRST)[6] 31

3.4 IRIS-CERT[7] 32

3.5 Brigada de Investigación Tecnológica (BIT) – Policía Nacional[8] 34

3.6 Agencia Española de Protección de Datos[9] 36

3.7 Centro Criptológico Nacional[10] 37

IV. Marco Teórico 40

4. Marco Teórico 41

4.1 Centros de Atención de Emergencias Cibernéticas (CSIRT) 41

4.2 Ámbitos de los CSIRT 41

4.2.1 CSIRT Académico 42

4.2.2 CSIRT Comercial 42

4.2.3 CSIRT CIP/CIIP 42

4.2.4 CSIRT Gubernamental 43

4.2.5 CSIRT Interno 43

4.2.6 CSIRT Sector Militar 43

4.2.7 CSIRT Nacional 44

4.2.8 CSIRT de las Pequeñas y Medianas Empresas (PyMEs) 44

4.2.9 CSIRT para mayoristas de productos informáticos 44

4.2.10 CSIRT en Sanidad 45

4.3 Servicios ofrecidos por un CSIRT 45

4.4 Servicios Reactivos 49

4.5 Alertas y Advertencias 49

4.5.1 Gestión de Incidencias 50

4.5.2 Análisis de Incidencia 51

Recogida de evidencias forenses 52

Seguimiento de ruta (Tracking/Tracing) 54

4.5.3 Apoyo a Respuesta a Incidencias 54

4.5.4 Coordinación de Respuesta a Incidencias 54

4.5.5 Respuesta a Incidencias *in situ* 55

4.5.6 Gestión de Vulnerabilidades 56

4.5.7 Análisis de Vulnerabilidad 56

4.5.8 Respuesta a Vulnerabilidades 57

4.5.9 Coordinación de la respuesta a vulnerabilidades 57

4.6 Servicios Proactivos 58

4.6.1 Anuncios 58

4.6.2 Vigilancia de la tecnología (*Technology Watch*) 58

4.6.3 Auditorías o Evaluaciones de la Seguridad 59

Repaso de la Infraestructura 59

Repaso de Prácticas Recomendadas 60

Detección de Vulnerabilidades 60

Prueba de Penetración 60

4.6.4 Configuración y Mantenimiento de la Seguridad 61

4.6.5 Desarrollo de herramientas para la Seguridad 61

4.6.6 Servicios de Detección de Intrusos 62

4.6.7 Distribución de Información relacionada con la Seguridad 63

4.7 Gestión de Artefactos 64

4.7.1 Análisis del artefacto 64

4.7.2 Respuesta al artefacto. 65

4.7.3 Coordinación de la respuesta a artefactos 65

4.7.4 Servicios de la Calidad de la Seguridad 65

4.7.5 Análisis de Riesgos 66

4.7.6 Planificación de la Recuperación post-desastre y Continuidad de Negocio 67

4.7.7 Asesoramiento sobre la Seguridad 67

4.7.8 Desarrollo de la Conciencia (sensibilización). 68

4.7.9 Educación/Formación 69

4.7.10 Evaluación o Certificación de Productos 69
4.8 Relaciones con otros centros de atención de emergencias 69
4.9 Implantación de un CSIRT 70
4.9.1 Definición del planteamiento de comunicación con los clientes y usuarios 70
Análisis DAFO (SWOT) 71
Análisis PEST 73
Canales de comunicación 75
4.9.2 Declaración de la Misión 77
4.9.3 Desarrollo del Plan de Negocio y Servicios 77
Definir el modelo financiero 77
4.9.4 Definición del organigrama estructural 80
Modelo de negocio independiente 82
Modelo "incrustado" 83
Modelo campus 84
El modelo voluntario 85
4.9.5 Contratación del personal adecuado 85
Descripción de características para personal técnico general 86
4.9.6 Utilización y equipamiento de la oficina del CSIRT 88
Fortalecer el edificio 88
4.9.7 Desarrollo de una política de seguridad de la información 91
Nacionales 91
Europea 92
Internacional 92
Estándares 93

4.9.8 Buscando la cooperación con otros CSIRT's y posibles iniciativas nacionales 94

V. Descripción del proyecto. 95

5. Descripción del Proyecto 96

5.1 Gestión de incidencias y denuncias. 99
5.1.1 Recibir denuncias e incidencias 102
5.1.2 Evaluación de los casos 104
Identificación 104
Relevancia 104
Clasificación 104
Triage 107
5.1.3 Acciones 108
Iniciar un ticket de incidencia 108
Ciclo de vida de los casos 108
Informe del manejo de una Incidencia 109
Archivar 109
5.2 Modelo organizativo de los Centros 110
5.3 Modelo económico 112

VI. Conclusión 113

6. Conclusión 114

VII. Referencias 117

I. Resumen Ejecutivo

Según la conferencia Intergubernamental de Emergencia en Telecomunicaciones, **un desastre o emergencia es todo aquello que altera el funcionamiento de la sociedad, poniendo en peligro generalizado la vida de las personas, su salud, su propiedad y/o su medio ambiente, siendo la causa que lo produce de múltiples índoles.** Por lo tanto la asistencia a un desastre incluye la **PREVENCIÓN, PREDICCIÓN, PREPARACIÓN y RESPUESTA** para mitigar el mismo.

Los ataques en la red deben dejar de considerarse privados/sectoriales o institucionales para ser **considerados dentro de la emergencia ciudadana,** particularmente en aquellas instituciones en las que puedan **vulnerarse gravemente los derechos de los ciudadanos** como es el caso de la administración de la Justicia y la Sanidad por el tipo de información confidencial que gestionan.

En estos casos es más importante la prevención y predicción que propiamente el manejo de la emergencia que por otra parte esta estandarizada por FIRST o forum para la incidencia y respuesta del equipo de seguridad.

De ahí que según nuestra opinión hayan de ser considerados los grupos gubernamentales policiales, de la administración o civiles que lleven a cabo la labor de inspección y sanción en los colectivos de riesgo que no

cuenten con un análisis de riesgo en condiciones, con unas medidas de seguridad y con un plan de respuesta a las emergencias.

Este aspecto sobrepasa la ley de protección de datos y las Agencia Nacional o Autonómica de protección de datos y aunque los criterios de Seguridad Normalización y Conservación de los sistemas de información utilizables por las administraciones publicas (criterios SNC) tienen su propia legislación, publicada en el BOE de 23 de junio de 2003 y que es la Resolución de 26 de mayo de 2003, de la Secretaría de Estado para la Administración Pública y varios programas como MARGERIT del MAP y Pilar del Centro Nacional de Inteligencia no es visible para el ciudadano la existencia de **Centros de Alerta Tecnológica**, salvo quizás el de la Brigada de Investigación Tecnológica de la Policía Nacional, que el ciudadano asocia con otro tipo de delitos informáticos y en el entorno universitario de la red IRIS o IRIS-CERT que igualmente el ambiente universitario asocia al aviso de ataques y virus informáticos para la red académica

Nuestra propuesta plantea un modelo de estructura para el ciudadano en el ámbito de la Comunidad Autónoma de Canarias, que coordine una respuesta rápida a incidencias en seguridad de la información, tanto para violaciones a nivel individual como a grandes grupos sociales, independientemente del ámbito donde se generen las incidencias e integrado a los organismos de inteligencia, policiales, de seguridad, de la Administración y Comunidades Autónomas, de manera tal que se cubra

un déficit en la atención de las emergencias producidas por vulneración de información sensible, personal o colectiva, o que ponga en riesgo la integridad de los servicios prestados a la población.

II. Introducción

El siguiente gráfico provisto por el CERT/CC (figura 1) ilustra los problemas en seguridad de información.

En el gráfico indica como la complejidad de las herramientas que están disponibles para la vulneración de los sistemas de soporte de información o procesos, sean sensibles o no, asciende de manera progresiva, mientras que el conocimiento necesario para utilizar (o incluso crear) dichas herramientas, desciende de manera exponencial, haciendo cada vez más fácil su uso por parte de personas malintencionadas no necesariamente expertas en sistemas informáticos. A menor requerimiento de conocimiento, mayor daño se puede provocar.

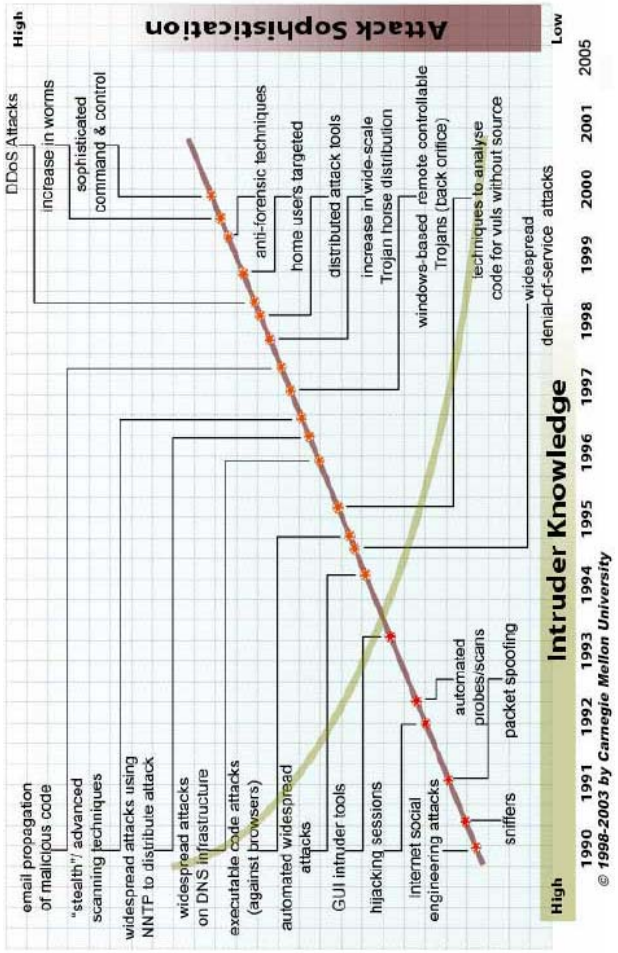

Figura 1. Complejidad de los ataques vs. Conocimiento necesario para ejecutarlo

Múltiples son los tipos de ataques que pueden sufrir los sistemas de información. La figura 2 muestra un ejemplo cómo se puede coordinar un ataque masivo contra redes e infraestructuras de servicios, provocando una negación de un determinado servicio.

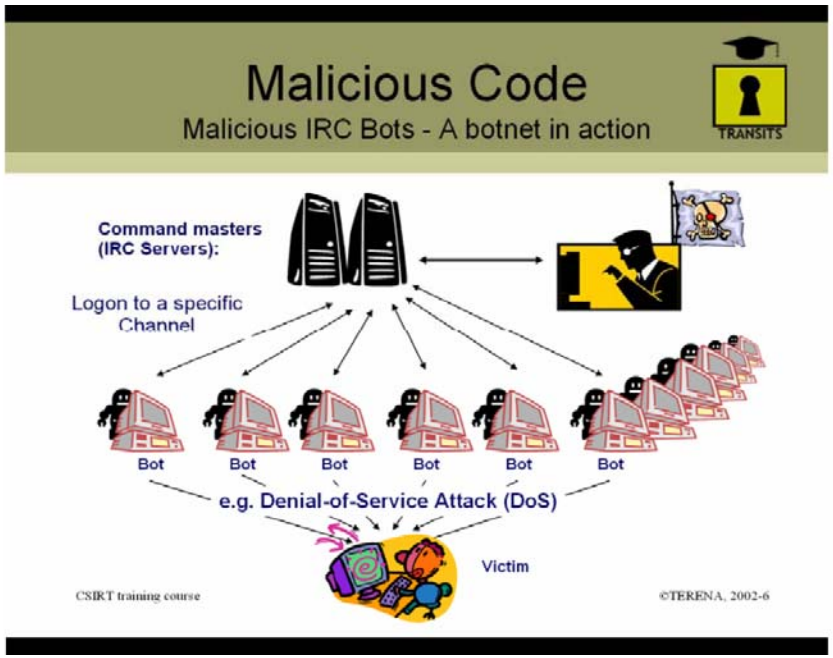

Figura 2. negación de servicios (DoS). (TERENA ©)

Como ejemplos de casos que demuestran el grado crítico de violación en la seguridad de información podemos citar los siguientes:

Ejemplo de ataques a red informática bancaria.

Con la expansión de los servicios bancarios en Internet, el fraude a entidades bancarias y clientes de éstas se ha venido incrementando aceleradamente durante los últimos años. De acuerdo con Consumer Sentinel[1] Hasta el 31 de diciembre de 2006, la usurpación de identidad para cometer fraudes en la Red ocupaba el primer lugar de quejas de los usuarios, tal como se puede observar en la tabla 1:

1	Usurpación de identidad	36%
2	Compras por catálogo	7%
3	Premios y loterías	7%
4	Servicios de Internet	6%
5	Acciones en Internet	5%
6	Gestión de divisas	3%
7	Gestión de créditos y préstamos	2%
8	Revistas y club de compradores	1%
9	Servicios telefónicos	1%
10	Salud	1%
11	Oportunidades de Negocios y trabajo en casa	1%
12	Viajes, vacaciones y resorts	1%
13	Suministros y servicios de oficina	1%
14	Becas y subvenciones	1%
15	Agencias de empleo	1%
16	Inversiones	1%
17	Otras quejas compiladas	2%

Tabla 1. Categorías de fraude en Internet y porcentaje de queja de los usuarios (fuente Consumer Sentinel, www.consumer.gov).

La penetración de Internet en Técnicas como el *phising* es común hoy en día. Es frecuente oír cómo los usuarios son bombardeados con correos electrónicos fraudulentos que buscan acceder ilegalmente a la información personal y de sus cuentas bancarias.

Técnicas de *hacking social* aplican técnicas similares de engaño, realizando contacto telefónico o personal con el usuario y logrando que éste aporte información sensible que puede ser utilizada para cometer fraude.

Finalmente mediante la técnica de *pharming*, los delincuentes informáticos logran redirigir a sus ordenadores la información sensible que los usuarios aportan a sitios aparentemente certificados (portales bancarios, sitios de e-comercio, etc.) sin que éstos se den cuenta que tal acción se está cometiendo en ese momento.

Ejemplo en planta generadora de electricidad

En agosto de 2003, el gusano informático *SQL*/*Slammer* afectó por espacio de cinco horas las redes privadas de ordenadores de la planta nuclear de Davis-Besse, Ohio (EE.UU.), deshabilitando los servicios de monitorización de seguridad del complejo. Aunque la situación no desencadenó un accidente grave, incidentes como este llevaron a la administración del gobierno de los EE.UU en 2005 a emitir una ley federal que obliga a las plantas de producción y distribución de energía eléctrica a reforzar la seguridad contra intrusiones y ataques maliciosos a sus

redes. Ataques coordinados sobre la producción y distribución de energía eléctrica implicarían la negación de servicio del suministro eléctrico poniendo en riesgo no sólo operaciones comerciales o administrativas, sino también a vidas humanas.

Ejemplo en ámbito asistencial y sanitario

En el entorno asistencial y sanitario, la protección de la información adquiere una dimensión y relevancia tal que la no intervención urgente en los casos de vulneración de la información puede poner en riesgo muy alto la intimidad, la salud o la vida de los pacientes o del personal sanitario. Un caso específico es lo relacionado con La Historia Clínica Electrónica (HCE) [1]. La HEC es una herramienta que permite integrar toda la información de datos muy sensibles de cada paciente y prestar un servicio de salud más eficaz y eficiente. La violación de los derechos de privacidad y confidencialidad de tales datos por terceros implicaría un ataque directo a la intimidad del individuo. Estadistas, políticos, jueces, empresarios, profesionales, gente común: todos serían vulnerables ante la exposición de sus datos personales o de sus familiares. El daño producido tendría características irreversibles, influyendo no sólo sobre la persona o familiares relacionados, sino incluso sobre decisiones que podrían afectar el normal desenvolvimiento de sociedades enteras.

La complejidad en la atención de los incidentes de seguridad de la información es tanta como la variedad de los posibles ataques que se puedan realizar sobre ésta. Nuestro enfoque constituye una primera

aproximación a lo que sería necesario definir para enfrentar tales incidencias, basados en procedimientos y estándares de seguridad ya definidos en entornos específicos de tratamiento de datos, como por ejemplo en el ámbito de la Sanidad y la Salud y los centros de respuestas a emergencias en sistemas de redes.

Como en todos los casos de atención de desastres y emergencias, la definición de una centros de atención de incidencias en seguridad de la información no puede ser un punto de decisión opcional en aquellos organismos donde se gestionan datos sensibles o donde la negación de operaciones basadas en la información ponga en riesgo la prestación de servicios esenciales para el ciudadano. Tampoco consideramos como opcional la integración de dichos centros dentro de una supra-estructura de respuesta inmediata a las emergencias en seguridad de información tal como propone el presente trabajo, pues en la comunicación eficiente entre los distintos colectivos de riesgo reside la efectividad de las soluciones a las incidencias.

III. Antecedentes

3.1 Estándares de confidencialidad y seguridad de los datos

Varios son los elementos a tener en cuenta en la seguridad electrónica de los datos cuya lista de estándares se especifica a continuación:

a. UNE/ISO/IEC 17799:2005 Código de buenas prácticas para la gestión de la seguridad informática.

1-Política de seguridad

2-Aspectos organizativos

3-Clasificación y control de los elementos activos

4-Seguridad ligada a los trabajadores/publico.

5-Seguridad física y del entorno

6-Gestión de Operaciones y comunicaciones

7-Control de acceso a la información y al sistema

8-Puesta al día y mantenimiento.

9-Plan de continuidad

10-Adecuación a la legislación.

b. UNE/ISO/IEC **15408 Criterio Común.** Information technology- Security techniques- Evaluation criteria for IT security.

c. UNE 71502:2004 Information system security management.

d. ISO/IEC **15443** Information system security techniques. (35 **evaluation methods**)

e. ISO/IEC **18014** Time stamping

f. ISO/IEC 27004 Information Security Management measurements.

g. ISO/IEC 27001:2005 Information Security management systems-Requirements. La norma ISO 27001 (hasta ahora certificable en España mediante la UNE 71502 y el BS 7799-2:2002) nace con la finalidad de establecer las bases de un SGSI (Sistema de Gestión de la Seguridad de la Información o gestión del riesgo) utilizando como marco de referencia el Código de Buenas Prácticas en Gestión de la Seguridad de la Información de la norma UNE-ISO/IEC 17799:2005.

h. ISO/IEC-TR 15446:2004 *Information Technology- Security techniques*- Es una guía practica para especificar modelos y perfiles de protección. y

i. ISO/TS-17090 *Security on health informatics* o Seguridad en la Informática medica. Son las especificaciones técnicas para la seguridad de los sistemas sanitarios.

La figura 3 ilustra un resumen y relación de los estándares listados.

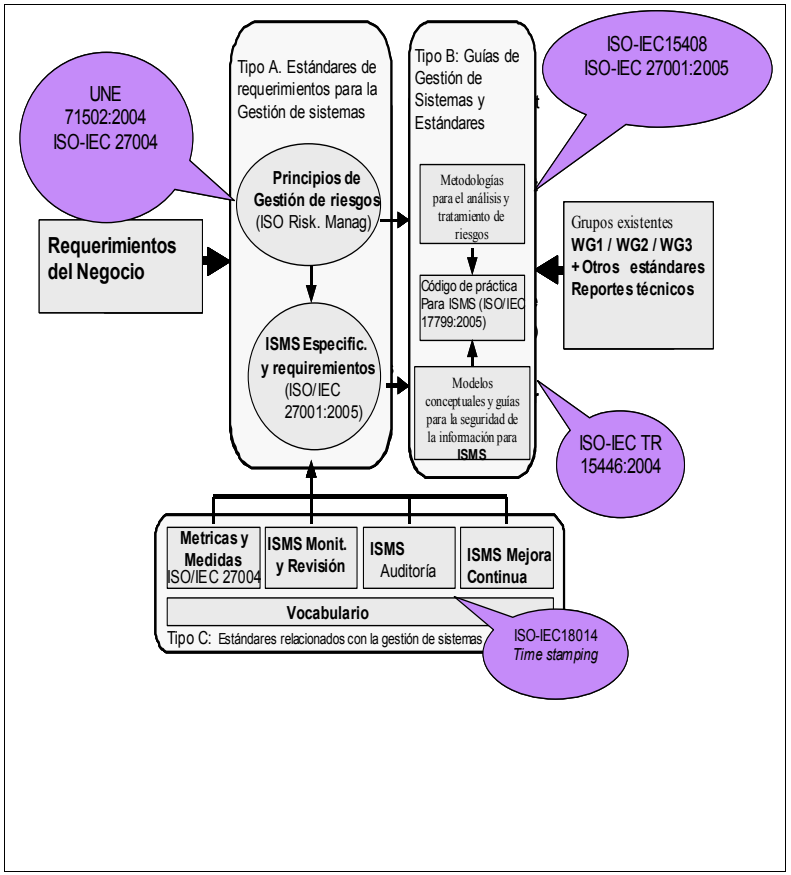

Figura 3. Estándares relacionados con los procesos de seguridad y privacidad.

Ley Orgánica de Protección de Datos (LOPD)

El objeto de la LOPD 15/1999 se encuentra en su artículo 1 donde se define para "garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar".

La influencia de la Ley es sobre todo dato de carácter personal registrado en cualquier medio, sea electrónico o no, que permita su posterior tratamiento o uso, sean datos provenientes del sector público o privado.

La Ley rige tanto los ficheros contentitos de información sensible así como los procesos automatizados o no que tratan tales datos. Para su aplicación a los ficheros manuales la Ley estableció un plazo transitorio que se inició en octubre de 1995 y finaliza en octubre de 2007.

La LOPD se aplica a todo tratamiento de información realizado en territorio español o cuando el responsable de dicho tratamiento le sea aplicable la legislación española vigente aun cuando el tratamiento de los datos se realice fuera del territorio español.

Reglamento de Medidas de Seguridad (RMS)

El RMS es un marco de referencia neutral desde el punto de vista tecnológico, lo que lo protege de la obsolescencia.

El RMS especifica los niveles y medidas mínimas de seguridad deben adoptar para la gestión de ficheros, dejando en manos del responsable de los mismos el establecer los mecanismos para conseguir dichos niveles de protección.

El reglamento obliga a:

- Definir una política de seguridad, especificando cuales son los recursos protegidos y los objetivos de seguridad que se deben conseguir para cada uno de ellos.
- el establecimiento de los procedimientos adecuadas para asegurar que las medidas se ponen en práctica
- La fijación de responsabilidades de todos aquellos que tratan datos de carácter personal en relación con el mantenimiento de las medidas de seguridad adoptadas;
- La puesta en marcha de un registro de incidentes que permita conocer las violaciones o los intentos de violación de la seguridad que se han producido;
- La formación de todas las personas implicadas; la comprobación sistemática y periódica del cumplimiento de lo establecido en la política de seguridad y,
- La actualización de las políticas y medidas cuando cambios en el

sistema o en la organización así lo aconsejen.

El RMS se fundamenta sobre dos principios: el concepto de nivel de seguridad y la existencia obligatoria de un “Documento de Seguridad” que contenga los elementos que ayudan a definir la política de seguridad de cada organización.

Dentro de las políticas de seguridad se prevé categorizar los ficheros que contienen datos de carácter personal en tres niveles, según la sensibilidad de los datos que contienen:

- nivel básico
- nivel medio
- nivel alto

Las medidas de seguridad que se definan para un nivel deben incluir obligatoriamente las medidas del nivel inmediatamente anterior.

Los ficheros que contenga datos personales de cualquier tipo deben asignárseles las medidas correspondientes al nivel básico.

En caso que tales ficheros contengan datos producto de infracciones administrativas, penales, financieras, crediticia, información patrimonial, tributaria, le corresponde a los ficheros las medidas de nivel medio.

Ficheros con datos personales especialmente protegidos por la legislación europea (datos ideología, religión, raciales, de salud o vida

sexual), o ficheros relacionados con investigaciones policiales, les es aplicable las medidas de nivel alto.

Como se expresa en [2], "además de las disposiciones relativas a cada uno de los niveles mencionados, existen una serie de aspectos generales que deben ser tenidos en cuenta. En primer lugar, **las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local, sin que la utilización de redes públicas de telecomunicaciones puedan servir como excusa para disminuir las garantías de seguridad**". También existe una previsión similar respecto del trabajo fuera de los locales en dónde esté ubicado el fichero. En ella se establece que este tipo de tratamiento debe ser expresamente autorizado por el responsable y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado. De la misma manera, las reglas de seguridad deberán aplicarse también a los ficheros creados con carácter temporal, debiendo éstos borrarse una vez que dejen de resultar necesarios para el fin con el que fueron creados."

Es importante insistir en que el RMS, establece la obligatoriedad de realizar una auditoria al menos cada 2 años para verificar que se han establecido las medidas de índole técnica y organizativa necesarias para garantizar la seguridad que deben reunir los ficheros automatizados, los centros de tratamiento, locales, equipos, sistemas, programas y las

personas que intervengan en el tratamiento de datos de carácter personal.

El servicio auditoria LOPD/LSSI-CE que consiste en realizar revisiones del estado de los ficheros con datos de carácter personal y de las medidas aplicadas debe quedar en manos de una auditoria externa. Esta auditoria permite a las organizaciones cumplir con la legislación.

En este servicio se analiza el registro de los ficheros, las medidas implantadas, así como la posible existencia de nuevos ficheros.

3.2 Organismos e Iniciativas para la atención de incidencias en seguridad de la información

En la actualidad es frecuente encontrar múltiples organismos que incorporan dentro de sus organizaciones centros de atención de emergencias en materia de seguridad de la información y/o seguridad ciudadana. Como ejemplos podemos citar ciertas iniciativas: los centros de respuesta a incidentes de seguridad informáticos (CSIRT[4]) que se encuentran en diversos centros, tales como hospitales, universidades, organismos de militares y de defensa, proveedores de servicios de telecomunicaciones, etc.; otras como la de las Brigadas de Investigación Tecnológica, organismo policial creado para enfrentar la creciente actividad delictiva que utiliza los medios de la sociedad de la información para la ejecución de delitos contra las personas y la propiedad. Finalmente, la Agencia Española de Protección de Datos (AEPD), que

ejerce su acción administrativa y sancionadora sin importar el medio con el cual se ejerce el delito sobre los datos e información de los ciudadanos.

3.2.1 Iniciativa CSIRT Europea (TERENA TF-CSIRT)[1]

El TF-CSIRT (*Task Force*) promociona la colaboración entre los CSIRT's de Europa. Sus objetivos principales son: actuar de plataforma para el intercambio de experiencias y conocimiento, establecer servicios pilotos para la comunidad de CSIRT's en Europa y ayudar los nuevos CSIRT's establecerse

• Actuar de plataforma para el intercambio de experiencias y conocimiento

• Establecer servicios pilotos para la comunidad de CSIRT's en Europa

• Promocionar estándares y procedimientos estándar para responder a incidencias en seguridad de la información.

• Ayudar a los nuevos CSIRT's establecerse y ayudar a la formación de personal.

Las actividades del TF-CSIRT se concentran en Europa y los países colindantes, en cumplimiento con los Términos de referencia aprobados por TERENA Technical Committee del 15 Septiembre 2004.

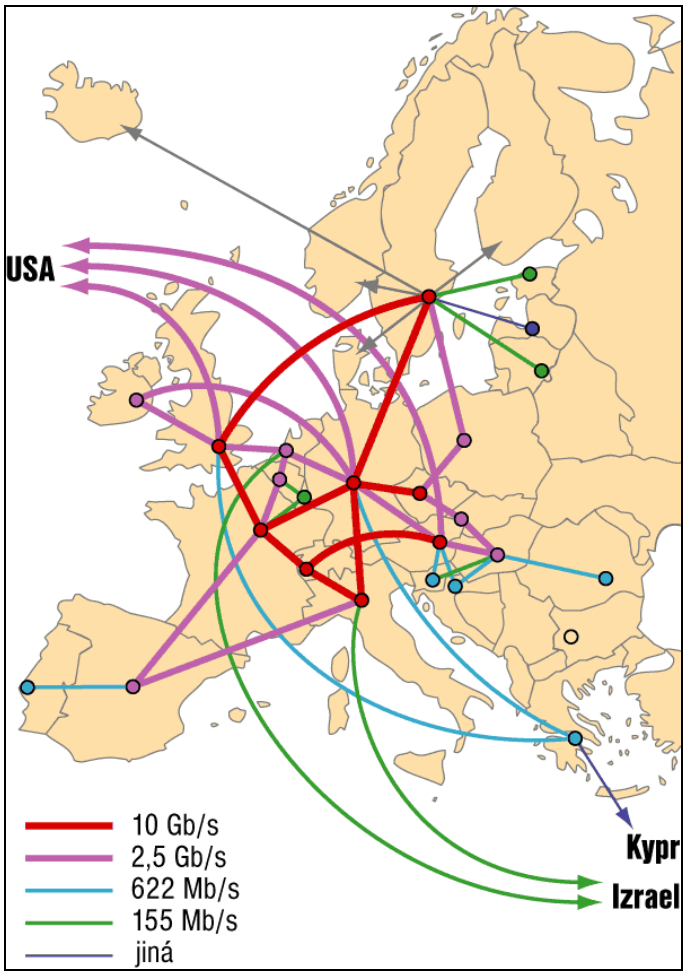

Figura 4. Esquema de interconexión red europea (fuente: www.arcert.gov.ar/tc/presentaciones/lunes/IniciativasRegionales-Europa.pdf)

3.3 Iniciativa CSIRT Global (FIRST)[6]

FIRST es la primera organización y líder global reconocido en respuestas a incidencias.

FIRST reúne diversos equipos de organizaciones gubernamentales, comerciales y educativas. Promociona la cooperación y coordinación para la prevención de incidencias, para estimular la rápida reacción, y para promocionar el intercambio de información entre sus miembros y la comunidad en general. Además de su papel como red de confianza, FIRST también proporciona servicios de valor añadido.

Los siguientes han sido los primeros miembros de FIRST:

- Air Force Computer Emergency Response Team (AFCERT)
- CERT® Coordination Center (CERT/CC)
- Defense Communication Agency/Defense Data Network (DCA/DDN)
- Department of Army Response Team
- Department of Energy's Computer Incident Advisory Capability, Lawrence Livermore National Laboratory (DOE's CIAC)
- Goddard Space Flight Center
- NASA Ames Research Center Computer Network Security Response Team (NASA ARC CNSRT)
- NASA Space Physics Analysis Network (SPAN CERT)
- Naval Computer Incident Response Team (NAVCIRT)
- National Institute of Standards and Technology Computer Security Resource and Response Center (CSRC)
- SPAN-France

En la actualidad integran a FIRST más de 180 miembros, entre los cuales se pueden citar la iniciativa europea DANTE (Delivery of Advanced Network Technology to Europe, Ltd.) encargada de proveer interconexión a las distintas redes académicas y de investigación, e IRIS-CERT.

3.4 IRIS-CERT[7]

La RedIRIS (figura 5) corresponde a la infraestructura de red de la comunidad académica y de investigación en España. Creada en 1991 y financiada por el Plan I+D+I, es un organismo autónomo dentro de la entidad pública empresarial Red.es. Cuenta con cerca de 250 centros afiliados que permanecen en contacto permanente con RedIRIS a través de sus personas de enlace.

El IRIS-CERT ofrece los servicios de seguridad y detección de problemas en las redes de los centros afiliados a la RedIRIS, incluídos universidades y centros de investigación, realizando labores tanto reactivas como preventivas. IRIS-CERT es miembro de FIRST desde 1997 y participa activamente en el TF-TERENA.

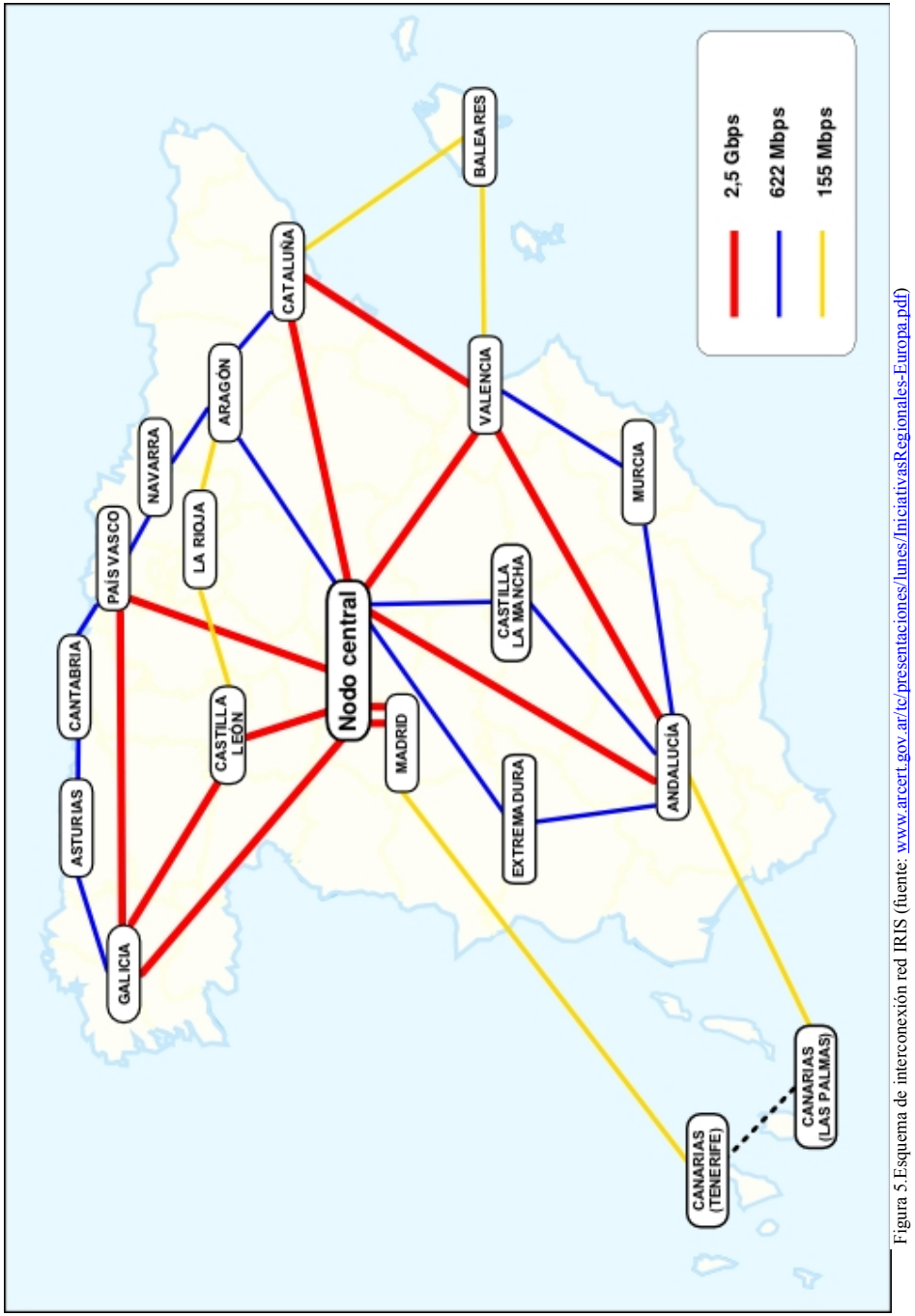

Figura 5.Esquema de interconexión red IRIS (fuente: www.arcert.gov.ar/tc/presentaciones/lunes/IniciativasRegionales-Europa.pdf)

3.5 Brigada de Investigación Tecnológica (BIT) – Policía Nacional[8]

Es un ente dependiente de la Comisaría General de Policía Judicial, que a su vez depende de la Dirección General de Policía y de la Guardia Civil y ésta del Ministerio del Interior.

La Brigada de Investigación Tecnológica es la Unidad policial que responde a nivel nacional a las nuevas formas de delincuencia que utilizan como medio Internet, infraestructura de telecomunicaciones o cualquier medio electrónico de soporte de la información: pornografía infantil; fraudes bancarios, fraudes en el uso de las comunicaciones, ataques cibernéticos, piratería.

Su misión es obtener las pruebas, perseguir a los delincuentes y ponerlos a disposición judicial.

La figura 6 muestra la ubicación de la BIT en el contexto de la organización de la comisaría de la policía Nacional.

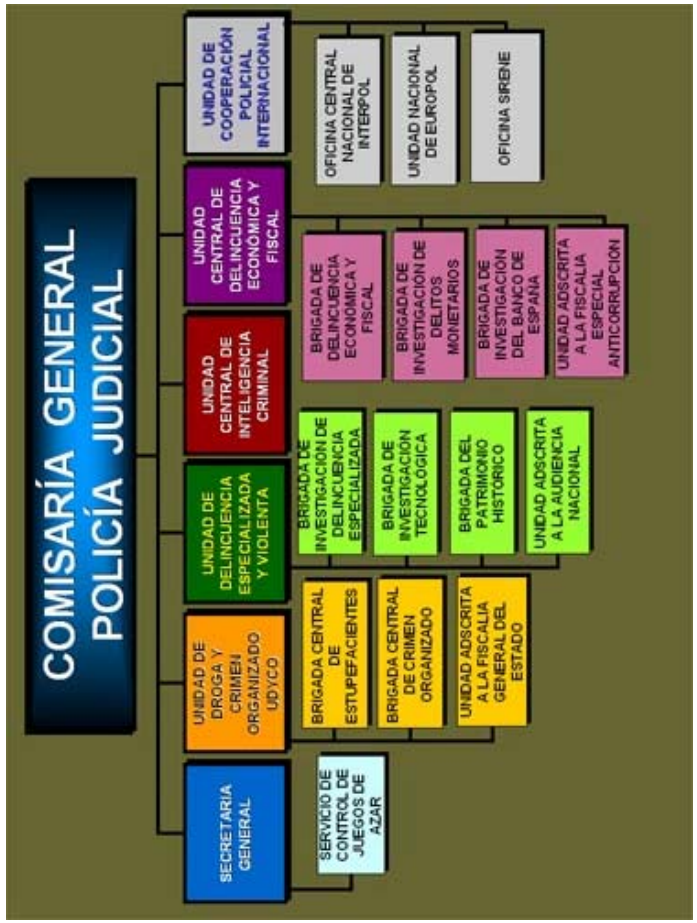

Figura 6. Organigrama de la CGPJ (fuente: http://www.policia.es)

3.6 Agencia Española de Protección de Datos[9]

La Agencia Española de Protección de Datos es el organismo nacional que vela por el cumplimiento de la legislación sobre protección de datos y el control de su aplicación, especialmente en lo relacionado con los derechos de información, acceso, rectificación, oposición y cancelación de datos.

Entre sus funciones específicas tenemos:

- Atender a sus peticiones y reclamaciones.
- Información de los derechos reconocidos en la Ley.
- Promover campañas de difusión a través de los medios.
- Emitir autorizaciones previstas en la Ley.
- Requerir medidas de corrección.
- Ordenar, en caso de ilegalidad, el cese en el tratamiento y la cancelación de los datos.
- Ejercer la potestad sancionadora.
- Recabar ayuda e información que precise.
- Autorizar las transferencias internacionales de datos.
- Informar los Proyectos de normas de desarrollo de la LOPD.
- Informar los Proyectos de normas que incidan en materias de protección de datos.
- Dictar Instrucciones y recomendaciones de adecuación de los tratamientos a la LOPD.
- Dictar recomendaciones en materia de seguridad y control de acceso a los ficheros.

- Tutelar los derechos y garantías de los abonados y usuarios en el ámbito de las comunicaciones electrónicas, incluyendo el envío de comunicaciones comerciales no solicitadas realizadas a través de correo electrónico o medios de comunicación electrónica equivalente.

3.7 Centro Criptológico Nacional[10]

El Centro Criptológico Nacional (CCN), es el responsable de coordinar las acciones que involucren el uso de procedimientos cifrados o códigos dentro del ámbito de la Administración del Estado, responsabilizándose por la seguridad de las tecnologías de la información utilizadas dentro de ese marco. Es un organismo dependiente de el Centro Nacional de Inteligencia (CNI).

El Director del CCN es la autoridad de certificación de la seguridad de las tecnologías de la información (http://www.oc.ccn.cni.es) y autoridad de certificación criptológica (http://www.ccn.cni.es). Asimismo es responsable de velar por el cumplimiento de la normativa relativa a la protección de la información clasificada en los aspectos de los sistemas de información y telecomunicaciones, de acuerdo a lo señalado en el artículo 4.e) y f) de la Ley 11/2002, de 6 de mayo.

De acuerdo con la página Web del CCN (http://www.ccn.cni.es/), este realiza las funciones de:

- Elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración. Las

acciones derivadas del desarrollo de esta función serán proporcionales a los riesgos a los que esté sometida la información procesada, almacenada o transmitida por los sistemas.

- Formar al personal de la Administración especialista en el campo de la seguridad de los sistemas de las tecnologías de la información y las comunicaciones.

- Constituir el organismo de certificación del Esquema nacional de evaluación y certificación de la seguridad de las tecnologías de información, de aplicación a productos y sistemas en su ámbito.

- Valorar y acreditar la capacidad de los productos de cifra y de los sistemas de las tecnologías de la información, que incluyan medios de cifra, para procesar, almacenar o transmitir información de forma segura.

- Coordinar la promoción, el desarrollo, la obtención, la adquisición y puesta en explotación y la utilización de la tecnología de seguridad de los sistemas antes mencionados.

- Velar por el cumplimiento de la normativa relativa a la protección de la información clasificada en su ámbito de competencia.

- Establecer las necesarias relaciones y firmar los acuerdos pertinentes con organizaciones similares de otros países, para el desarrollo de las funciones mencionadas.

IV. Marco Teórico

4.1 Centros de Atención de Emergencias Cibernéticas (CSIRT)

Un CSIRT es un equipo de expertos en seguridad cuyo principal trabajo es responder a incidencias de Seguridad Informática (SI) proporcionando los servicios necesarios para resolver las incidencias y ayudar a su clientela a recuperarse[4].

Sus siglas vienen del inglés **C***omputer* **S***ecurity* **I***ncident* **R***esponse* **T***eam*, un acrónimo usado en lugar del término reconocido y registrado CERT® (**C***omputer* **E***mergency* **R***esponse* **T***eam*)[11].

Además de los servicios reactivos, un CSIRT ofrece servicios preventivos, tales como emisión de notificaciones a los usuarios de la red monitorizada, informes periódicos sobre vulnerabilidades de los sistemas informáticos, intentos de fraude a través de correo electrónico, SPAM's, etc. De esta forma sus clientes y usuarios pueden tomar las medidas correctivas del caso para proteger a sus sistemas y minimizar el uso malintencionado con o sobre los mismos.

4.2 Ámbitos de los CSIRT

A continuación una lista de los posible ámbitos en donde se puede establecer un centro de atención de incidencias de seguridad de la información:

4.2.1 CSIRT Académico

Un CSIRT en el sector académico proporciona servicios CSIRT a instituciones académicas y educativas, como universidades o unidades de investigación, y a sus servicios online en el campus universitario.

Clientes y usuarios*:* típicamente, personal y estudiantes universitarios.

4.2.2 CSIRT Comercial

Un CSIRT comercial proporciona servicios comerciales a sus clientes y usuarios. En el caso de un proveedor de servicios de Internet (*ISP*), el CSIRT proporciona principalmente servicios contra abusos a sus clientes y usuarios finales (*Dial-in*, *ADSL*) y servicios CSIRT a sus clientes profesionales.

Clientes y usuarios: Los CSIRT's Comerciales suelen proporcionar servicios a clientes y usuarios que pagan por ellos.

4.2.3 CSIRT CIP/CIIP

Los CSIRT's especializados en este sector se dedican a la **P**rotección de **I**nformación **C**rítica (CIP en inglés) y/o la **P**rotección de **I**nfraestructura y **I**nformación **C**rítica (CIIP). Suele tener una estrecha cooperación con un departamento CIIP gubernamental. Cubre todos los sectores críticos del país y protege a los ciudadanos de ese país.

Clientes y usuarios: Gobierno, negocios críticos de IT y ciudadanos.

4.2.4 CSIRT Gubernamental

Un CSIRT gubernamental proporciona servicios a agencias gubernamentales y en algunos países a los ciudadanos.

Clientes y usuarios: El Gobierno y agencias relacionadas con él; en algunos países proporcionan servicios de alerta a los ciudadanos (p.ej. Bélgica, Hungría, Los Países Bajos, Reino Unido o Alemania).

4.2.5 CSIRT Interno

Proporciona servicios solamente a su organización anfitriona. Muchas organizaciones bancarias y de telecomunicaciones tienen sus propios CSIRT's internos. No suelen mantener un sitio Web para el público.

Clientes y usuarios: Personal interno y el departamento de Tecnología de la Información (*IT*) de la organización

4.2.6 CSIRT Sector Militar

Proporciona servicios a organizaciones militares y se responsabiliza de la infraestructura IT necesaria para los propósitos de defensa.

Clientes y usuarios: Personal de instituciones militares o entidades estrechamente relacionadas, p.ej. con el Departamento de Defensa

4.2.7 CSIRT Nacional

Tiene un enfoque nacional, considerado como el **P**unto **d**e **C**ontacto del país (*PdC*). En algunos casos el CSIRT del Gobierno también actúa como el PdC nacional (como UNIRAS en el Reino Unido).

Clientes y usuarios: No suele tener clientes y usuarios directos, ya que el CSIRT nacional solo juega un papel intermediario para todo el país.

4.2.8 CSIRT de las Pequeñas y Medianas Empresas (PyMEs)

Es un CSIRT auto-organizado que proporciona servicios a su propio negocio u otro grupo de usuarios similar.

Clientes y usuarios: Podrían ser los PyMEs y su personal, o grupos especiales como una "Asociación de Pueblos y Municipios" de un país.

4.2.9 CSIRT para mayoristas de productos informáticos

Apoyar productos específicos de ventas en masa. Normalmente, su objetivo es desarrollar y proporcionar soluciones para eliminar vulnerabilidades y mitigar sus efectos potencialmente negativos.

Clientes y usuarios: Propietarios de productos informáticos.

4.2.10 CSIRT en Sanidad

Un CSIRT en Sanidad proporciona servicios a centros de Salud donde se maneja información y procesos sensibles como por ejemplo, incidencias sobre el acceso a información de historias clínicas electrónicas.

Clientes y usuarios: Centros asistenciales y de salud.

4.3 Servicios ofrecidos por un CSIRT

Dentro de los servicios que ofrecen un CSIRT podemos clasificarlos en servicios reactivos (aquellos que se efectúan en respuesta a un incidente detectado) o proactivos (los que se realizan en prevención de incidentes, tales como los anuncios periódicos sobre vulnerabilidades). Adicionalmente los CSIRT pueden realizar actividades de informática forenses tales como la gestión de artefactos (elementos o trazas lógicas dejadas por el intruso o aplicación *malware* en los sistemas afectados), así como de supervisión de la calidad de los sistemas de su clientela.

La tabla 2 muestra un resumen de los principales servicios que puede prestar un CSIRT[4]:

Servicios Reactivos
• **Alertas y Advertencias** (servicio fundamental)
• **Gestión de Incidencias** (servicio fundamental)
• **Análisis de Incidencias** (servicio fundamental)
• **Apoyo de Respuesta a Incidencias** (servicio fundamental)
• **Coordinación de Respuesta a Incidencias** (servicio fundamental)
• Respuesta a Incidencias en el sitio
• Gestión de vulnerabilidades
• Análisis de vulnerabilidades
• Respuesta a vulnerabilidades
• Coordinación de respuesta a vulnerabilidades

Tabla 2. Servicios ofrecidos por un CSIRT

Servicios Proactivos
• **Anuncios** (servicio fundamental)
• Vigilancia de la tecnología
• Auditorias o Evaluaciones de la seguridad
• Configuración y Mantenimiento de la Seguridad
• Desarrollo de la herramientas para la Seguridad
• Servicios de Detección de Intrusos
• Distribución de Información relacionada con la Seguridad

Tabla 2 (cont.) . Servicios ofrecidos por un CSIRT

Gestión de Artefactos
• Análisis de Artefacto
• Respuesta a Artefacto
• Coordinación de Respuesta al Artefacto

Tabla 2 (cont.) . Servicios ofrecidos por un CSIRT

Supervisión de Calidad en la Seguridad
• Análisis de Riesgos
• Continuidad del negocio y recuperación de desastres.
• Asesoramiento sobre Seguridad
• Desarrollo de conciencia (sensibilización)
• Formación
• Evaluación o Certificación de Productos

Tabla 2 (cont.) . Servicios ofrecidos por un CSIRT

Los CSIRT pueden clasificarse por el ámbito sobre el cual ejercen su acción. Así, tenemos CSIRT's gubernamentales, nacionales, académicos, militares, internos (aquellos que funcionan dentro de una empresa ofreciéndoles sus servicios de seguridad), para proveedores de productos informáticos, para PyME's, etc. Dependiendo del entorno donde funcione, el CSIRT tendrá definido aparte de su conjunto mínimo de servicios, unas funciones propias de las actividades para las cuales se definió el CSIRT.

En el caso de un CSIRT definido para la seguridad de la información ciudadana, el ámbito de acción correspondería a toda la comunidad bajo la cual tiene influencia el organismo de seguridad que la atiende, pudiendo ser esta una comunidad local y pequeña hasta el ámbito nacional.

4.4 Servicios Reactivos

Los servicios reactivos están diseñados para responder a incidencias detectadas, sea por notificación o por evaluación de los registros informáticos de los sistemas.

4.5 Alertas y Advertencias

Las notificaciones y alertas se realizan con la finalidad de informar a los clientes y usuarios sobre novedades que puedan afectar la integridad de sus sistemas, o sobre prácticas fraudulentas que puedan poner en peligro la privacidad de información sensible.

La información puede crearse en el CSIRT o puede ser redistribuida procedente de los proveedores, otros CSIRT's, expertos en seguridad o otras grupos de usuarios.

4.5.1 Gestión de Incidencias

La gestión de incidencias conlleva la recepción, clasificación y atención urgente (*triage*), la respuesta a solicitudes y informes, y el análisis de incidencias y eventos.

Determinadas actividades de respuesta pueden incluir:

• Tomar medidas para proteger sistemas y redes afectadas o amenazadas por actividad de intrusos

• Proporcionar soluciones y estrategias mitigantes por notificaciones o alertas relevantes

• Buscar actividad de intrusos en otras partes de la red

• Filtrar el tráfico de la red

• Reconstruir los sistemas

• Actualizar o reparar los sistemas

• Desarrollar otras respuestas o estrategias alternativas

Dado que las actividades del manejo de incidencias se implementan de varias maneras por diferentes tipos de CSIRT's, estos servicios se clasifican según el tipo de actividad y el tipo de ayuda requerida.

4.5.2 Análisis de Incidencia

El análisis de incidencias es un examen de toda la información disponible incluida cualquier evidencia o artefacto relacionado con la incidencia o evento. El propósito del análisis es determinar el ámbito de la incidencia, la extensión del daño causado, la naturaleza de la incidencia, y las estrategias o alternativas disponibles. El CSIRT puede emplear los resultados del análisis de vulnerabilidad y de artefacto (descrito más abajo) para entender y proporcionar el análisis más actualizado de lo ocurrido en un sistema determinado.

El CSIRT correlaciona la actividad de las incidencias para determinar si hay interrelaciones, tendencias, patrones o huellas/rastros del intruso (*intruder signatures*).

Dos sub-servicios que pueden realizarse como parte del análisis de incidencias, según su misión, objetivos y procesos, son:

- Recogida de Evidencia Forense

- Seguimiento de ruta (Tracking/Tracing)

Recogida de evidencias forenses

La recogida, preservación, documentación y el análisis de evidencias en un sistema informático comprometido para determinar cambios en el sistema y para ayudar en la reconstrucción de los eventos que condujeron a la incidencia. Esta recogida de información y evidencias deben hacerse de manera que documente una cadena comprobable de custodia, admisible en un juzgado bajo las leyes de la evidencia. Las tareas involucradas en la recogida de evidencias forenses incluyen (pero no se limitan a): hacer una copia bit-a-bit del disco duro del sistema afectado; registrar los cambios en el sistema como nuevos programas, archivos, servicios y usuarios; examinar los procesos activos y puertos abiertos; buscar posibles troyanos y root toolkits (categoría de software malicioso que sustituye programas del sistema operativo para obtener privilegios de acceso). El personal del CSIRT que realice esta función puede tener que actuar como testigo experto en un proceso judicial.

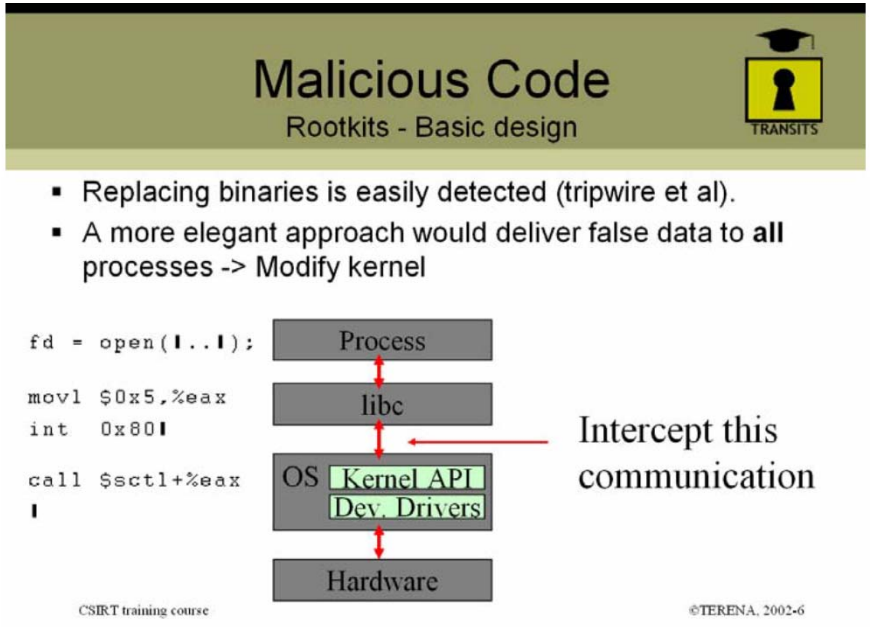

Figura 7. Estructura básica de un root kit (TERENA©)

La figura 7 muestra la estructura básica de un rootkit. Código comprometido del núcleo del sistema operativo actúa como puerta trasera para los intrusos informáticos.

Seguimiento de ruta (Tracking/Tracing)

Esta actividad supone el rastreo para determinar los orígenes del intruso o identificar los sistemas de acceso del intruso. Puede involucrar determinar cómo el intruso entró en los sistemas afectados y las redes relacionadas, qué sistemas se usaron para el acceso, dónde se originó el ataque, y qué otros sistemas y redes se usaron como parte del ataque. También puede involucrar tratar de determinar la identidad del intruso. Este trabajo podría hacerse solo, pero normalmente requiere trabajar con la policía, proveedores de servicios Internet u otras organizaciones.

4.5.3 Apoyo a Respuesta a Incidencias

El CSIRT ayuda y guía a la(s) victima(s) del ataque recuperarse mediante de teléfono, correo electrónico, fax, o documentación. Puede involucrar ayuda técnica en la interpretación de datos recogidos, proporcionar información de contactos, o transmitir pautas sobre estrategias de mitigación y recuperación. No involucra acción directa *in situ* como la del apartado anterior. En su lugar, el CSIRT proporciona las pautas a seguir de forma remota, así que el personal puede realizar la recuperación de forma autónoma.

4.5.4 Coordinación de Respuesta a Incidencias

El CSIRT coordina los esfuerzos de las partes involucradas en la incidencia. Esto normalmente incluye a las víctimas del ataque, otros

sitios de la red involucrados, y cualquier sitio en la red que requiera ayuda para el análisis del ataque. También puede incluir las partes que proporciona apoyo IT a la victima, como los ISP, otros CSIRT's, o administradores de sistema y de red en el sitio donde está implantado el CSIRT. El trabajo de coordinación puede involucrar recoger información de contactos, notificar sitios de su posible relación con el ataque (como víctima o fuente), recoger estadísticas sobre el número de sitios afectados, y facilitar el intercambio y análisis de la información.

Parte de este trabajo puede involucrar la notificación y colaboración con los asesores legales, departamentos de recursos humanos o relaciones públicas. También incluiría la coordinación con la policía.

Este servicio no involucra la respuesta directa *in situ*.

4.5.5 Respuesta a Incidencias *in situ*

El CSIRT proporciona ayuda directa para que los clientes y usuarios se recuperen de la incidencia. El CSIRT físicamente analiza los sistemas afectados y lleva a cabo la reparación y recuperación de los sistemas, en lugar de responder sólo por teléfono o correo electrónico. Este servicio abarca todas las acciones necesarias a nivel local si se sospecha que haya ocurrido una incidencia. Si el CSIRT no esta localizado en el sitio afectado, miembros del equipo tienen que desplazarse al sitio y realizar el trabajo allí. En otros casos puede que ya hay un equipo en el sitio que proporcione la respuesta a la incidencia como parte rutinaria de su trabajo. Este es el caso que se produce cuando el manejo de incidencias

forma parte del trabajo normal de administradores del sistema, la red o de la SI en el lugar en donde el CSIRT está establecido.

4.5.6 Gestión de Vulnerabilidades

La gestión de una vulnerabilidad conlleva la recepción de información e informes sobre vulnerabilidades de hardware y software; análisis de la naturaleza, mecánica y efectos de las vulnerabilidades; y el desarrollo de estrategias de respuesta para detectar y reparar las vulnerabilidades. El manejo de vulnerabilidades se implementa de varias maneras por los diferentes tipos de CSIRT, así que este servicio se clasifica según el tipo de actividad y de ayuda requeridas.

4.5.7 Análisis de Vulnerabilidad

El CSIRT realiza análisis técnico y examen de vulnerabilidades en el hardware o software. Este incluye la verificación de vulnerabilidades sospechadas y el examen técnico de vulnerabilidades del hardware o software para determinar dónde se localiza y cómo puede ser explotada. El análisis puede incluir la verificación del código fuente, utilizando un programa depurador (*debugger*) para determinar dónde ocurre la vulnerabilidad, o intentar reproducir el problema en un sistema de pruebas.

4.5.8 Respuesta a Vulnerabilidades

Este servicio involucra la determinación de la respuesta apropiada para mitigar o reparar la vulnerabilidad. Puede involucrar desarrollar o investigar parches informáticos (*patches*), soluciones definitivas (*fixes*) o soluciones parciales (*workarounds*). También involucra notificar a otros de la estrategia de mitigación, posiblemente mediante la creación o distribución de notificaciones o alertas. Este servicio puede incluir la realización de la respuesta con la instalación de parches informáticos, soluciones definitivas o parciales.

4.5.9 Coordinación de la respuesta a vulnerabilidades

El CSIRT notifica a las partes de la empresa o la clientela acerca de la vulnerabilidad y comparte información sobre cómo arreglar la vulnerabilidad o mitigar sus efectos. El CSIRT verifica que la estrategia se ha implementada con éxito. Este servicio puede involucrar la comunicación con mayoristas, otros CSIRT's, expertos técnicos, clientes y con los individuos o grupos que fueron los primeros en descubrir o informar de la vulnerabilidad. Las actividades incluyen realizar el análisis de la vulnerabilidad o el informe sobre la vulnerabilidad; coordinar la agenda de publicación de documentos correspondientes, parches informáticos o soluciones parciales; y sintetizar los análisis técnicos hechos por las diferentes partes. Este servicio también puede incluir el mantenimiento de un archivo público o privado o una base de

conocimiento de información acerca de la vulnerabilidad y las correspondientes estrategias de respuesta.

4.6 Servicios Proactivos

Estos servicios son diseñados para mejorar la infraestructura y procesos de seguridad de la clientela antes de que se detecte cualquier incidencia o evento. Los objetivos principales son evitar la incidencias y reducir su impacto y expansión cuando ocurran.

4.6.1 Anuncios

Esto incluye (pero no se limita a) anunciar alertas de intrusión, advertencias sobre vulnerabilidades y notificaciones sobre la seguridad informática. Tales anuncios informan a los clientes y usuarios de novedades con impacto de medio a largo plazo, como vulnerabilidades recientemente encontradas o herramientas de intrusión.

Los anuncios permiten que los clientes y usuarios puedan proteger sus sistemas y redes contra estos problemas antes de que sean explotadas.

4.6.2 Vigilancia de la tecnología (*Technology Watch*)

El CSIRT monitoriza, controla y observa novedades técnicas, actividades de intrusos y tendencias relacionadas para ayudar identificar futuras amenazas. Los temas a repasar pueden incluir normas legales y administrativas, amenazas sociales o políticas y tecnologías emergentes.

Este servicio involucra leer listas de correo electrónico de seguridad, sitios Web de seguridad y noticias actuales y artículos de revistas técnicas en los campos de la ciencia, la política y el gobierno para extraer la información relevante para la seguridad de los sistemas y redes de sus clientes. Este puede incluir comunicarse con otras partes autoridades en estos campos para asegurar la obtención de la mejor y más exacta información o interpretación.

El resultado de este servicio puede ser un anuncio, unas pautas o recomendaciones dirigidas a mejorar la seguridad informática a medio o largo plazo.

4.6.3 Auditorías o Evaluaciones de la Seguridad

Este servicio proporciona un repaso detallado y análisis de la infraestructura de seguridad de una organización, basándose en los requerimientos definidos por la organización o por otros estándares de la industria que sean aplicables. También puede involucrar un repaso de las prácticas de seguridad de la organización. Existen muchos diferentes tipos de auditorias o evaluaciones posibles, incluidas:

Repaso de la Infraestructura

Manualmente se repasan las configuraciones del hardware y software, de los enrutadores (*routers*), cortafuegos (*firewalls*), servidores y dispositivos de escritorio para asegurar que cumplen con las políticas de seguridad y las configuraciones estándar de la organización o con las prácticas recomendadas de la industria.

Repaso de Prácticas Recomendadas

Entrevistar a los empleados y administradores de sistemas y redes para determinar si sus prácticas de seguridad cumplen con las políticas de seguridad de la organización o con los estándares específicos de la industria

Detección de Vulnerabilidades

Emplear programas de detección de vulnerabilidades (*scanners*) o de virus para determinar qué sistemas o redes son vulnerables.

Prueba de Penetración

Con esto se comprueba la seguridad de un sitio mediante un ataque planificado a sus sistemas y redes. Se requiere la aprobación de la dirección superior antes de realizar tales auditorías o evaluaciones. Algunas de estas estrategias pueden ser prohibidas por la política de la organización.

Este servicio puede involucrar el desarrollo de un conjunto de prácticas contra las cuales se dirigen las pruebas o evaluaciones, junto con el desarrollo de un conjunto de habilidades o requerimientos de certificación para el personal que realiza las pruebas, evaluaciones, auditorías o repasos. Este servicio puede ser subcontratado a un tercero o administrado por un proveedor de servicios de seguridad que tenga el conocimiento apropiado en la administración de tales auditorías o evaluaciones.

4.6.4 Configuración y Mantenimiento de la Seguridad

Este servicio identifica o proporciona la pautas apropiadas sobre cómo configurar y mantener con seguridad las herramientas, aplicaciones y la infraestructura informática en general empleada por la clientela del CSIRT o por el mismo CSIRT. Además de proporcionar estas pautas, el CSIRT puede realizar actualizaciones de la configuración y del mantenimiento de las herramientas y servicios de seguridad, como los Sistemas de Detección de Intrusiones (IDS - *Intrusion Detection Systems*), detección (*scanning*) en redes o monitorización de sistemas, filtros, adaptadores (*wrappers*), cortafuegos, redes privadas virtuales (VPN), o mecanismos de autenticación. El CSIRT incluso puede proporcionar estos servicios como parte de su función principal. El CSIRT también puede configurar y mantener los servidores, ordenadores de sobremesa, portátiles, asistentes personales digitales (PDA's), y otros dispositivos inalámbricos, según las pautas de seguridad. Este servicio incluye transmitir a la dirección cualquier problema relacionado con las configuraciones o el empleo de herramientas y aplicaciones que el CSIRT considera vulnerables a ataques.

4.6.5 Desarrollo de herramientas para la Seguridad

Este servicio incluye el desarrollo de nuevas herramientas específicas para su clientela que son requeridas o deseadas por la clientela o por el mismo CSIRT. Este puede incluir, por ejemplo, el desarrollo de parches

de seguridad para software personalizado utilizados por la clientela o distribuciones de software seguro que pueden utilizarse para restaurar los sistemas de anfitriones comprometidos. También puede incluir el desarrollo de herramientas o archivos de comandos (*scripts*) que amplían las capacidades funcionales de las herramientas de seguridad existentes, como un nueva extensión (*plug-in*) para un detector de vulnerabilidades o redes, archivos de comando que facilitan el uso de tecnologías de encriptación, o mecanismos automatizados de distribución de parches.

4.6.6 Servicios de Detección de Intrusos

Los CSIRT's que realizan este servicio examinan los archivos de auditoría de los IDS, analizan e inician una respuesta a cualquier evento que sobrepasa el umbral definido, o emiten alertas según el acuerdo sobre el nivel de servicio predefinido o estrategia de elevar los problemas a una instancia superior para su solución (*escalation*). La detección de intrusos y el análisis de los archivos de auditoría de seguridad asociados no es tarea fácil. No sólo hay que determinar dónde situar los elementos de detección en el contexto, sino hay que recoger y luego analizar grandes cantidades de datos capturados. En muchos casos se requieren herramientas o habilidades especiales para sintetizar e interpretar la información para identificar las falsas alarmas, ataques o eventos en la red y para implementar estrategias para eliminar o minimizar tales eventos. Algunas organizaciones prefieren subcontratar para esta función a terceros con

experiencia comprobada, como los proveedores de servicios de seguridad.

4.6.7 Distribución de Información relacionada con la Seguridad

Este servicio proporciona a los clientes y usuarios una colección completa de información útil y fácil de encontrar que ayuda mejorar la seguridad. Tal información podría incluir:

• Informes de pautas e información sobre contactos para el CSIRT
• Archivos de alertas, advertencias y otros anuncios
• Documentación sobre prácticas óptimas actuales
• Consejos sobre seguridad informática general
• Políticas, procedimientos y listas de verificación.
• Desarrollo de parches e información de distribución
• Enlaces con proveedores mayoristas
• Estadística actual y tendencias en informes sobre incidencias
• Otra información que puede mejorar las prácticas de seguridad en general

Esta información puede ser desarrollada y publicada por el CSIRT o por otras partes de la organización (IT, recursos humanos o relaciones con los medios), y puede incluir información procedente de fuentes externos como otros CSIRT's, proveedores y expertos en seguridad.

4.7 Gestión de Artefactos

Un artefacto es cualquier archivo u objeto que se encuentra en un sistema y que puede estar relacionado con la intrusión o ataque a sistemas y redes, o que es usado para superar las medidas de seguridad.

Los artefactos pueden incluir (pero no se limitan a) los virus, troyanos, gusanos (*worms*), comandos para la explotación de vulnerabilidades (*exploit scripts*), y sustitutos *malware* de aplicaciones críticas del sistema (*toolkits*).

La gestión de artefactos involucra la recepción de copias o información acerca de artefactos empleados en los ataques por intrusos, el reconocimiento y otras actividades no autorizadas o negativas.

Una vez recibido, el artefacto se examina. Esto incluye el análisis de su naturaleza, la mecánica, la versión y el uso. Luego, requiere el desarrollo de una estrategia de respuesta para detectar, quitar y defenderse de ataques de este artefacto. Dado que las actividades del manejo de artefactos se implementan de varias maneras por diferentes tipos de CSIRT's, este servicio se clasifica según el tipo de actividad y el tipo de ayuda.

4.7.1 Análisis del artefacto

El CSIRT realiza un examen técnico y análisis de cualquier artefacto encontrado en un sistema. El análisis puede incluir la identificación del tipo de archivo y la estructura del artefacto, comparando el nuevo artefacto con los existentes o con otras versiones del mismo artefacto

para determinar similitudes diferencias, o ingeniería inversa o desensamblaje del código para determinar el propósito y la función del artefacto.

4.7.2 Respuesta al artefacto.

Este servicio involucra determinar las medidas apropiadas para detectar y eliminar los artefactos de un sistema, además de prevenir que se instalen. Esto puede involucrar la creación de firmas que se adjuntan al software antivirus o al IDS.

4.7.3 Coordinación de la respuesta a artefactos

Este servicio involucra compartir y sintetizar los resultados de análisis y estrategias de respuesta referente al artefacto con otros investigadores, CSIRT's, proveedores o expertos en seguridad informática. Las actividades incluyen notificar a otros y sintetizar los análisis técnicos procedentes de diversas fuentes. Las actividades también incluyen mantener un archivo público o privado de los artefactos conocidos y su impacto, además de las estrategias de respuesta.

4.7.4 Servicios de la Calidad de la Seguridad

Los servicios que se encuentran en esta categoría no son únicamente para el manejo de incidencias ni de los CSIRT's en particular. Son muy conocidos y establecidos, diseñados para mejorar la seguridad general de

las organizaciones. Aprovechándose de la experiencia de proporcionar servicios reactivos y preactivos antes descritos, un CSIRT puede aportar perspectivas únicas para estos servicios de calidad. Estos servicios son diseñados para incorporar la retroalimentación y las lecciones aprendidas durante las respuestas a incidencias, vulnerabilidades y ataques. Incorporar tal experiencia en los servicios tradicionales y establecidos puede mejorar los esfuerzos de seguridad de la organización a largo plazo. Dependiendo de las estructuras y responsabilidades de la organización, un CSIRT puede proporcionar estos servicios o participar como parte de un esfuerzo más amplio del equipo organizacional.

4.7.5 Análisis de Riesgos

Los CSIRT's pueden añadir valor al análisis y evaluaciones de riesgos. Esto puede mejorar la capacidad de la organización de evaluar amenazas reales, realizar evaluaciones realistas de los riesgos para información valiosa y de las estrategias de protección y respuesta. Los CSIRT's que realizan este servicio llevarían o apoyarían los análisis de riesgo para la seguridad de la información en nuevos sistemas y procesos de negocio o evaluarían las amenazas y ataques contra los bienes y sistemas de sus clientes.

4.7.6 Planificación de la Recuperación post-desastre y Continuidad de Negocio

Basado en eventos pasados y predicciones para el futuro sobre incidencias y tendencias en la seguridad, se sabe que las incidencias tienen cada vez más potencial para causar graves perjuicios para las operaciones comerciales. Por tanto, la planificación debería considerar la experiencia y recomendaciones de los CSIRT's sobre las mejores maneras de responder a tales incidencias para asegurar la continuidad de las operaciones de negocio. Los CSIRT's que realizan este servicio están involucrados en la continuidad del negocio y en la planificación de la recuperación post-desastres para los eventos relacionados con amenazas y ataques contra la seguridad informática.

4.7.7 Asesoramiento sobre la Seguridad

Los CSIRT's pueden proporcionar consejos y pautas sobre las mejores prácticas de seguridad a implementar para las operaciones comerciales de sus clientes y usuarios. Un CSIRT que realiza este servicio esta involucrado en la preparación de recomendaciones o la identificación de requerimientos para la compra, adquisición y instalación de nuevos sistemas, dispositivos de red, aplicaciones de software o procesos comerciales para toda la empresa. Este servicio incluye proporcionar consejos y asistencia en el desarrollo de políticas de seguridad para la organización o la clientela. Este servicio también puede involucrar aportar testimonios o consejos a departamentos gubernamentales o legislativos.

4.7.8 Desarrollo de la Conciencia (sensibilización).

Los CSIRT's pueden identificar las áreas donde sus clientes y usuarios necesitan más información y consejos para cumplir con las prácticas de seguridad aceptadas y con la política de seguridad de la organización. Elevar la conciencia en seguridad de los usuarios no sólo mejora su comprensión de estas cuestiones sino que les ayuda a realizar sus operaciones diarias de una manera más segura. Con esto se puede reducir el número de ataques con éxito y aumentar la probabilidad de que los clientes puedan detectar e informar sobre estos ataques, así reduciendo el tiempo de recuperación y eliminando o minimizando pérdidas.

Los CSIRT's que realizan este servicio buscan oportunidades para incrementar el nivel de conciencia sobre la seguridad, valiéndose de artículos, pósteres, publicaciones periódicas, sitios Web, u otras fuentes de información que explican las mejores prácticas de seguridad y proporcionan consejos sobre las precauciones indicadas.

Las actividades pueden incluir celebrar reuniones y seminarios para mantener los clientes informados sobre procedimientos actuales de seguridad y sobre las amenazas para los sistemas de la organización.

4.7.9 Educación/Formación

Con este servicio el CSIRT proporciona información a clientes y usuarios sobre seguridad informática mediante seminarios, talleres, cursos y tutoriales. Los temas podrían incluir consejos sobre informes de incidencias, métodos apropiados de respuesta, herramientas de respuesta a incidencias, métodos de prevención de incidencias y otra información necesaria para proteger, detectar, informar y responder a incidencias de seguridad informática.

4.7.10 Evaluación o Certificación de Productos

Para este servicio, el CSIRT puede llevar a cabo evaluaciones de productos sobre herramientas y aplicaciones u otros servicios para asegurar la seguridad de los productos y su cumplimento con las prácticas de seguridad de la organización. Las herramientas y aplicaciones pueden ser de código fuente abierto o comerciales. Este servicio puede ser proporcionado como una evaluación o mediante un programa de certificación dependiendo de los estándares aplicados por la organización o por el CSIRT.

4.8 Relaciones con otros centros de atención de emergencias

Originalmente la “Web de confianza” de los centros estaba basada en las relaciones personales de los miembros del *staff* de los CSIRTs implicados. Sin embargo el crecimiento de la red y los cambios del personal hacen impracticable esta política. La presentación de un

miembro por parte de un CSIRT no es ya factible ni digno de confianza. Servicios específicos de inducción de confianza para gestionar este problema como el *Trusted Introducer* (TI)[12] o introductor de confianza es una iniciativa de los CSIRTs Europeos.

4.9 Implantación de un CSIRT

La implantación de un CSIRT implica el análisis de la clientela, principalmente para seleccionar los canales de comunicación correctos:

- Definición del planteamiento de comunicación con los clientes y usuarios
- Definición de la declaración de funciones (*mission statement*)
- Desarrollo del Plan de Negocios y Servicios
- Definición de la estructura de organización
- Contratación del personal adecuado
- Utilización y equipamiento de la oficina del CSIRT
- Definición de la política de Seguridad de Información
- Búsqueda de la cooperación entre otros CSIRT’s y posibles iniciativas nacionales

4.9.1 Definición del planteamiento de comunicación con los clientes y usuarios

La teoría de la Dirección proporciona varios posibles planteamientos para abordar el problema de analizar un grupo de interés. En este documento describimos dos: el análisis DAFO (inglés: *SWOT*) y el análisis PEST.

*Análisis DAFO (*SWOT*)*

Este es una herramienta de planificación empleado para evaluar las **D**ebilidades (***W****eaknesses*), **A**menazas (***T****hreats*), **F**ortalezas (***S****trengths)* y **O**portunidades (***O****pportunities*) inherentes al proyecto, negocio o cualquier otra situación que requiera tomar una decisión. La técnica se atribuye a Albert S. Humphrey, que dirigió un proyecto de investigación en la Universidad de Stanford en las décadas de los ´60 y ´70, empleando datos de la revista "Fortune 500 companies".

Ejemplos de criterios	**Fortalezas**	**Debilidades**	Ejemplos de criterios
Ventajas de la propuesta Capacidades Ventajas Competitivas Recursos, Activos, Gente Experiencia, Conocimiento Disponibilidad de datos Aspecto financiero, retorno de la inversión Mercadeo: sensibilización, logros Aspectos Innovadores Lugar geográfico Precio, valor Certificaciones, estandarización Infraestructura de IT, Comunicaciones Aspectos culturales Plan de carrera profesional en la organización Valores, ética			Desventajas de la propuesta Carencia de capacidad Debilidad en competitividad Reputación adversa Finanzas Vulnerabilidades Tiempos, fin de plazos, presión Flujo de caja Cadena de suministro, continuidad Confiabilidad de los datos, plan, pronósticos Liderazgo, compromiso, moral del personal Acreditaciones, no cumplimiento de estándares Infraestructura IT, comunicaciones Plan de desarrollo profesional, de sucesión
Ejemplos de criterios	**Oportunidades**	**Amenazas**	Ejemplos de criterios
Nuevos Mercados, horizontal, vertical Vulnerabilidades de la competencia Tendencias de la industria o sociales Desarrollo tecnológico, IT, comunicaciones Influencias globales Exportaciones, importaciones Tácticas, nuevos contratos, sorpresas Desarrollo de negocios, productos Información y desarrollo Socios comerciales, distribución Volúmenes Economía local Influencia de la moda, temporada			Efectos políticos, locales Legislación Efectos ambientales Desarrollo de IT Nuevos servicios o ideas Competencia Demanda del mercado Socios Obstáculos a encarar Debilidades no superables Pérdida de recursos humanos claves Superación de reveses financieros Efectos de la temporada, clima

Figura 8 Análisis DAFO (SWOT)

Análisis PEST

El análisis **PEST** pretende entender las circunstancias **P**olíticas, **E**conómicas, **S**ocio-culturales y **T**ecnológicas del futuro ámbito del trabajo del CSIRT. Ayuda a determinar si la planificación está de acorde con el ámbito y evitar actuaciones basadas en suposiciones erróneas.

Política

- Cuestiones Ecológicas/medioambientales
- Legislación actual del mercado doméstico
- Legislación futura
- Legislación Europea/internacional
- Órganos Reguladores y procesos
- Políticas gubernamentales
- Período y posible cambio de gobierno
- Políticas de comercio
- Financiación, ayudas e iniciativas
- Grupos de presión para el mercado doméstico
- Grupos de presión internacionales

Económica

- Situación de la economía doméstica
- Tendencias de la economía doméstica
- Tendencias de la economía extranjera

- Asuntos generales de impuestos
- Impuestos específicos para productos/servicios
- Estacionalidad/tiempo
- Ciclos del mercado y comercio
- Factores de industrias específicas
- Rutas del mercado y tendencias de distribución
- Motivadores de Clientes/usuarios finales
- Tasas de cambio y de intereses

Social

- Tendencias en el estilo de vida
- Demografía
- Actitudes y opiniones de los consumidores
- Opiniones de los medios de comunicación
- Cambios legales que afectan factores sociales
- Imagen de la marca, compañía y tecnología
- Patrones de compras entre consumidores
- Modelos sociales y de moda
- Eventos e influencias importantes
- Acceso y tendencias de compras
- Factores religiosos/étnicos
- Publicidad

Tecnológica

- Desarrollo de tecnología competitiva
- Financiación de la investigación

- Tecnologías asociadas/dependientes
- Tecnología/soluciones de respuesta
- Madurez de la tecnología
- Madurez y capacidad de la manufactura
- Información y comunicaciones
- Mecanismos y tecnología de consumidores
- Legislación sobre la tecnología
- Potencial de Innovación
- Acceso, licencias, patentes referentes a la tecnología
- Cuestiones de Propiedad intelectual

Tanto DAFO como PEST proporcionan una visión global y estructurada de las necesidades de los clientes y usuarios. Los resultados son utilizados para complementar la propuesta de negocio y ayudar a conseguir financiación para la creación del CSIRT.

Canales de comunicación

Un tema importante a incluir en el análisis es la posible distribución de información y comunicación o cómo comunicarse con los clientes y usuarios.

Si es posible, deberían considerarse las visitas personales realizadas con regularidad. Está comprobado que las reuniones cara-a-cara facilitan la cooperación y una relación más abierta.

Normalmente los CSIRT's emplean un conjunto de canales de comunicación. Los siguientes resultaron útiles en la práctica y deben considerarse:

- Un sitio Web público
- Área restringida para usuarios online.
- Formularios Web para informar sobre incidencias
- Listas de correo electrónico
- Correo electrónico personalizado
- Teléfono / Fax
- Mensajes SMS
- Correo ordinario
- Informes mensuales/anuales

Además de emplear estos métodos para facilitar el manejo de incidencias (y recibir informes de la clientela, coordinar esfuerzos con otros equipos y apoyar a la víctima), muchos CSIRT's publican sus advertencias en la red públicamente y utilizan sus listas de correo electrónico.

Si es posible, la información debería distribuirse de manera segura. Los correos electrónicos, por ejemplo, pueden firmarse digitalmente con un PGP, y la información sensible en forma encriptada.

4.9.2 Declaración de la Misión

La **declaración de la misión** describe las funciones básicas de la organización en la sociedad y los productos y servicios que proporcionará a los clientes y usuarios. Comunica claramente la existencia y función del nuevo CSIRT.

Es aconsejable que sea una declaración compacta pero no demasiado cerrada ya que no suele modificarse durante varios años.

La declaración de la misión es muy importante y constituye un paso necesario para iniciar el CSIRT.

4.9.3 Desarrollo del Plan de Negocio y Servicios

El resultado del análisis aporta una buena visión global de las necesidades y las supuestas debilidades de la clientela, y se toma como entrada para la definición del plan de negocios y servicios a prestar.

Definir el modelo financiero

La definición del modelo financiero lleva a la pregunta: ¿Qué servicios son indicados y rentables?

La lista de servicios debe adaptarse al presupuesto, así que es más realista empezar con planear las cuestiones monetarias.

Modelo de Costes

Los dos factores que más influyen en los costes son el número de horas de servicio y el número (y calidad) de personal

(empleados). ¿Es necesario proporcionar un servicio 24/7 de respuesta a incidencias SI y apoyo técnico? ¿O sólo trabajará en horas de oficina?

Dependiendo de la disponibilidad deseada y el equipamiento de oficina (¿se puede trabajar desde casa?), ¿puede ser interesante trabajar con un programa rotativo de guardias presenciales o localizables (no-presenciales).

Una posibilidad es ofrecer los servicios pro y reactivos en horas de oficina. Fuera de estas horas, sólo se ofrecen servicios reactivos, p.ej. en caso de desastres importantes. Éstos serían atendidos por un miembro del equipo que esté de guardia localizable.

Otra opción es buscar colaboración con otros equipos CSIRT internacionales. Ya existen ejemplos de cooperación *Following-the-Sun* que funcionan. Por ejemplo la cooperación entre equipos europeos y americanos resultó beneficiosa y compartieron sus respectivas capacidades. El CSIRT Sun Microsystems tienen múltiples sucursales localizados en diferentes husos horarios alrededor del mundo (todos siendo miembros del mismo equipo) y realiza servicios 24/7 mediante jornadas de guardia que cubren todas las horas.

Este sistema limita los costes porque los equipos sólo trabajan horas normal de oficina y también proporciona sus servicios a la “parte dormida” del mundo.

Se recomienda analizar con la clientela la necesidad de prestar servicios 24/7. Las alertas y advertencias emitidas de noche no tienen mucho sentido si el receptor sólo las leerá a la mañana siguiente. El horario de trabajo influye enormemente en el número de empleados y el equipamiento requerido, y por tanto en los costes.

Modelo de Ingresos

Cuando se sepan los costes, el siguiente paso es pensar en posibles fuentes de ingreso para la financiación del proyecto. He aquí algunas posibilidades:

Uso de recursos existentes

Siempre hay que valorar los recursos ya presentes en otras partes de la compañía (p.ej. personal ya empleado en el departamento de IT) con los conocimientos necesarios. Probablemente se puede llegar a un acuerdo con la dirección para que tales personas puedan trabajar en el CSIRT durante al menos la fase inicial, o que ellas estén disponibles para apoyar al CSIRT de forma *ad hoc*.

Cuota de socios

Otra posibilidad es vender los servicios a la clientela mediante una cuota periódica (anual o trimestral) para socios. Servicios

adicionales podrían ser cobrados por su utilización puntual, por ejemplo, servicios de consultoría o auditorias de SI.

Otro escenario posible: servicios para la clientela interna son proporcionados de forma gratuita pero los servicios a clientes externos tendrían que ser de pago.

Otra idea es publicar boletines de información y notificaciones en el sitio Web público y tener una sección “solo para miembros” con información específica, detallada y personalizada.

Se ha comprobado en la práctica que la “Suscripción por servicio CSIRT” solo proporciona financiación limitada, sobre todo en la fase inicial de implantación. Hay, por ejemplo, costes fijos para el equipo humano y el equipamiento técnico que tienen que financiarse con carácter previo. La financiación de estos costes a través de la venta de servicios CSIRT es problemática y requiere un análisis financiero muy detallado para definir el equilibrio entre costes e ingresos.

Subsidios

Actualmente muchos gobiernos tienen fondos para proyectos de SI. Contactar con el Ministerio del Interior podría ser un buen comienzo. Combinar diferentes modelos de financiación también es posible.

4.9.4 Definición del organigrama estructural

La estructura organizacional de un CSIRT depende en gran medida de la estructura existente en la organización anfitriona y de la clientela.

También depende de la accesibilidad de expertos a contratar de forma permanente o ad hoc.

Un CSIRT típico define los siguientes papeles dentro del equipo:

General

- Gerente General

Personal

- Gerente de la oficina
- Contable
- Asesor experto en Comunicación
- Asesor Legal

Equipo Técnico Operativo

- Jefe del Equipo Técnico
- Técnicos CSIRT, que proporcionan los servicios.
- Investigadores

Asesores Externos

- Contratados cuando se necesitan

Es de gran ayuda tener a bordo un especialista legal, sobre todo al principio. Cuesta dinero pero al final ahorra tiempo y evita problemas legales.

Según la variedad de expertos dentro de la clientela, y también cuando el CSIRT tiene una alta consideración en los medios, resulta muy útil tener a bordo un experto de la comunicación. Estos expertos "traducen"

cuestiones difíciles y altamente técnicas en mensajes fácilmente comprensibles para los clientes y usuarios o medios. También proporciona retroalimentación acerca de la clientela y pueden actuar como traductores y facilitadores entre el equipo y la clientela.

Lo siguiente contiene ejemplos de modelos organizacionales en uso por unos CSIRT's operativos.

Modelo de negocio independiente

El CSIRT se establece como organización independiente, con su propia dirección y empleados.

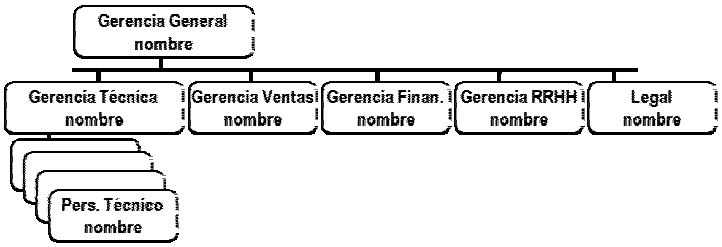

Figura 9. CSIRT. Modelo de Negocio Independiente

Modelo "incrustado"

El CSIRT se crea dentro de la organización existente, y utiliza un departamento IT existente. Está dirigido por un Jefe de Equipo encargado de dirigir las actividades del CSIRT. Esta persona contacta con los técnicos necesarios para resolver las incidencias y puede contar con asistencia especializada dentro de la organización.

Este modelo puede adaptarse para afrontar situaciones específicas a medida que surgen. En este caso el equipo tendrá un número fijo de empleados a jornada completa o *Full Time Equivalents* (FTE). El puesto de atención al cliente ante incidencias de SI (*abuse desk*) en un ISP p. ej. es claramente un trabajo a jornada completa para una o más personas.

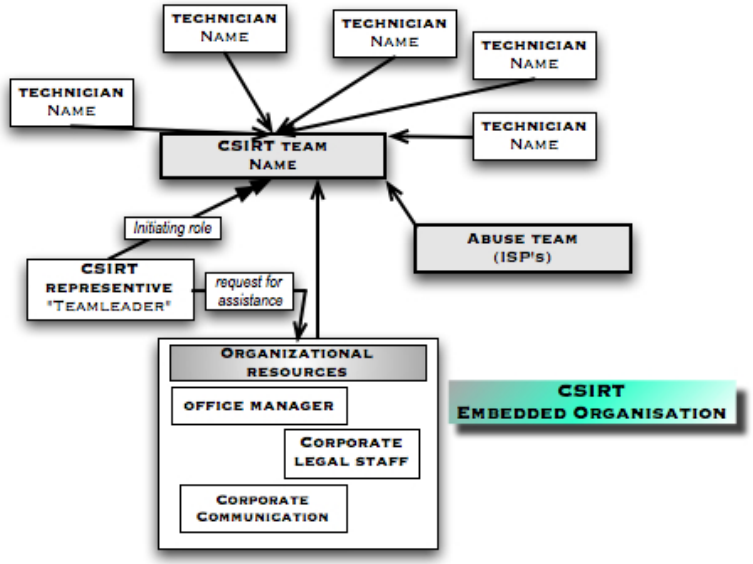

Fig. 10. Modelo Organizacional "Incrustado"

Modelo campus

Este modelo es típico de los CSIRT's académicos y de investigación. La mayoría de tales organizaciones consisten en varias universidades y dependencias del campus situadas en diferentes lugares, extendiéndose por toda una región o incluso un país (como en el caso de los NREN's o *National Research Networks*). Normalmente independientes, estas organizaciones tienen sus propios CSIRT's, a menudo bajo el control de un CSIRT 'madre' o central. Este CSIRT coordina y actúa de PoC para el mundo exterior y suele proporcionar los servicios claves además de distribuir información sobre incidencias a los equipos del campus. Algunos CSIRT's proporcionan los servicios claves y colaboran con otros equipos del campus, así reducen los costes generales.

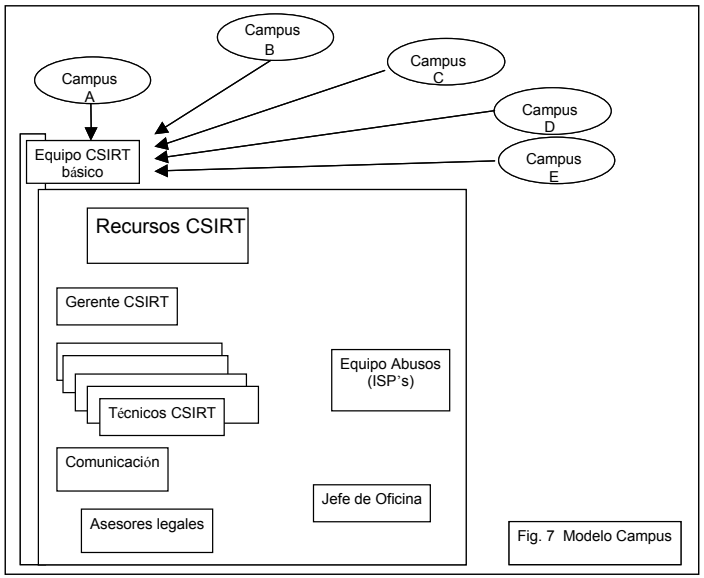

Figura 11. Modelo Campus

El modelo voluntario

Este modelo consta de un grupo de personas (especialistas) que se juntan para proporcionar consejos y apoyo mutuo (y a otros) de manera voluntaria. Es una comunidad que depende en gran medida de la motivación y entrega de los participantes.

4.9.5 Contratación del personal adecuado

Habiendo decidido los servicios y el nivel de apoyo a proporcionar, y tras elegir un modelo de organización, el siguiente paso es encontrar la personas cualificadas para realizar el trabajo.

Es casi imposible dar cifras concretas de cuántos técnicos se necesitarán, pero los siguientes valores claves han resultado útiles:

- Para dos servicios claves de la distribución de boletines de advertencias además de resolver las incidencias: un mínimo de **4** FTE (Empleados 8/5)
- Para el servicio completo de CSIRT durante horas de oficina (8/5) y mantenimiento de sistemas: un mínimo de **6 - 8** FTE.
- Para una jornada 24/7 con un equipo completo (2 turnos para cubrir las horas de cierre de oficina), un mínimo de unos **12** FTE.

Estas cifras incluyen bajas por enfermedad, vacaciones, etc. Es necesario revisar los convenios sindicales de los trabajadores. Las horas trabajadas fuera del horario laboral de oficina pueden involucrar gastos extras.

Descripción de características para personal técnico general

Personal

- Flexible, creativo y con buen espíritu de equipo
- Fuertes habilidades analíticas
- Habilidad de explicar tecnicismos con palabras fácilmente comprensibles para el cliente.
- Buen sentido de la confidencialidad y de trabajo según procedimientos.
- Buenas habilidades organizativas.
- Resistencia al estrés
- Buenas habilidades de comunicación y redacción
- Abierto y dispuesto a aprender

Competencias técnicas

- Amplio conocimiento de la tecnología y protocolos de Internet.
- Conocimiento de sistemas Linux y Unix (dependiendo de los sistemas informáticos de la clientela)

• Conocimiento de Windows (dependiendo de los sistemas informáticos de la clientela)

• Conocimiento de los sistemas informáticos que componen la infraestructura de la red (enrutadores, *switches*, DNS, *proxys*, correo electrónico, etc.)

• Conocimiento de aplicaciones de Internet (SMTP, HTTP(s), FTP, *telnet*, SSH, etc.)

• Conocimiento de amenazas de Seguridad (*DDoS, Phishing, Defacing, sniffing*, etc.)

• Conocimiento de evaluación de riesgos e implementaciones prácticas.

Competencias Adicionales

• Dispuesto a trabajar 24/7 o a realizar guardias localizables (dependiendo del modelo de servicio)

• Máxima distancia de desplazamiento (en caso de emergencia, disponibilidad de acudir a la oficina; máximo tiempo de desplazamiento)

• Nivel de educación institucional

• Experiencia en el campo de la SI

4.9.6 Utilización y equipamiento de la oficina del CSIRT

Fortalecer el edificio

Los CSIRT's suelen manejar información muy confidencial y es recomendable que ellos controlen la seguridad física del edificio, pero esto depende de la infraestructura y la política existente de la compañía anfitriona. Los gobiernos, p.ej., utilizan esquemas de clasificación y son muy estrictos en cuestiones acerca de cómo manejar la información confidencial. Revise el tema con su propia compañía/institución sobre las reglas y políticas locales.

El nuevo CSIRT dependerá de la compañía anfitriona para aprender sus normas, políticas y otras cuestiones legales.

A continuación hay una lista corta de aspectos básicos para el espacio físico de un CSIRT.

Reglas generales para el edificio

• Emplee controles de acceso

• La oficina CSIRT, al menos, sólo será accesible al personal CSIRT.

• Monitorización de las oficinas y entradas con cámaras.

• Archivar información confidencial en taquillas bajo llave o en cajas fuertes.

• Emplee sistemas seguros de IT.

Reglas generales para el equipamiento IT

• Emplee equipamiento que sepa utilizar el personal

• Fortalezca todos los sistemas

• Parchee y actualice todos los sistemas antes de conectarlos al Internet

• Emplee software de seguridad (cortafuegos, antivirus, anti-spyware, etc.)

Mantenimiento de los canales de comunicación

• Sitio Web público

• Área restringida a usuarios online.

• Formularios Web para informar de incidencias

• Correo electrónico (soporte PGP / GPG / S/MIME)

• Software para la lista de correo electrónico.

• Un teléfono dedicado para la clientela: Teléfono, Fax, SMS

Sistema(s) de seguimiento de registros (Record tracking)

• Una base de datos de contactos con información acerca de los miembros del equipo, otros equipos, etc.

• Herramientas CRM (*Customer Relationship Management*)

• Sistema de etiquetas numeradas (*tickets*) para la administración de incidencias

Empleo de estilo formal en escritos y correspondencias

• Correo electrónico estándar y boletines de avisos

• Correo ordinario

• Informes mensuales o anuales

• Formularios de Informes sobre incidencias.

Otros puntos

• Prevea canales alternativos de comunicación en caso de ataques

• Prevea la posibilidad de contar con varias conexiones para Internet

4.9.7 Desarrollo de una política de seguridad de la información

Según el tipo de CSIRT, este tendrá una política a medida para la seguridad de la información.

Además de describir el estado deseado de los procesos operativos y administrativos, tal política ha de estar ajustada a la legislación y los estándares vigentes, sobre todo los referente a la responsabilidad legal del CSIRT. Los CSIRT's suelen estar sujetos a las leyes y regulaciones nacionales, a menudo puestas en marcha dentro del contexto de la legislación europea (usualmente Directivas) y de otros acuerdos internacionales. Los estándares no son necesariamente vinculantes, pero pueden ser mandatarios, recomendados por ley o por regulaciones.

A continuación, una breve lista de posibles leyes de SI y políticas.

Nacionales

- Diversas leyes sobre IT, telecomunicaciones y medios de comunicación
- Leyes sobre la protección de datos y la privacidad
- Leyes y regulaciones sobre retención de datos
- Legislación sobre finanzas, contabilidad y dirección de compañías
- Códigos de conducta para la dirección de compañías y de IT

Europea

- Directivas sobre las firmas electrónicas (1993/93/EC)
- Directivas sobre la protección de datos (1995/46/EC) y la privacidad en las comunicaciones electrónicas (2002/58/EC)
- Directivas sobre redes de comunicación electrónica y servicios (2002/19/EC – 2002/22/EC)
- Directivas sobre la Ley de Compañías (p.ej. la Directiva Nº 8 de la Ley de Compañías)

Internacional

- Acuerdo de Basilea II (especialmente referente a la administración de riesgo operativo)
- Convención del Consejo de Europa sobre Cibercrimen.
- Convención del Consejo de Europa sobre Derechos Humanos (artículo 8 sobre la privacidad)
- Estándares Internacionales de Contabilidad, que rigen hasta cierto punto el control de IT)

Estándares

• British Standard BS 7799 (Seguridad de la Información)

• Estándares Internacionales ISO2700x (Sistemas de Administración para la Seguridad de la Información)

• El IT-Grundschutzbuch alemán, el EBIOS francés y otras variaciones nacionales.

Es necesario consultar con un asesor legal para asegurar que el CSIRT actúa de acuerdo con la legislación nacional e internacional.

Las preguntas más básicas acerca de cómo manejar la información son:

• ¿Cómo se etiqueta o clasifica la información que entra?

• ¿Cómo se maneja esta información, sobre todo referente a la exclusividad?

• ¿Cuál es tu política de protección de datos para revelar información, sobre todo si la comunica a otros equipos o sitios Web.

• ¿Hay consideraciones legales a tomar en cuenta referentes al manejo de la información?

• ¿Tiene una política de encriptación de datos para proteger la exclusividad e integridad de archivos y/o la comunicación, sobre todo por correo electrónico?

• Esta política ¿Incluye posibles límites legales, como depósito de claves u obligación de des-encriptación en caso de procedimientos judiciales?.

4.9.8 Buscando la cooperación con otros CSIRT's y posibles iniciativas nacionales

Es recomendable contactar con otros CSIRT's cuanto antes. Suelen ser abiertos y dispuestos a ayudar a los nuevos equipos.

El *Inventory of CERT activities in Europe* de ENISA es un buen punto de partida para buscar otros CSIRT's en el país y para actividades de cooperación entre los CSIRT's nacionales.

V. Descripción del proyecto.

Nuestra propuesta plantea la creación de una estructura para el ciudadano que coordine las acciones a ejecutar en caso de emergencias en seguridad de la información, que integre a los distintos organismos policiales, de seguridad, de la Administración y Comunidades Autónomas, cubriendo un déficit en la atención de las emergencias o catástrofes producidas por vulneración de información sensible, personal o colectiva, o que ponga en riesgo la integridad de los servicios prestados a la población.

Dicha organización integraría los diferentes centros existentes de alertas tecnológicas de los diferentes ámbitos dentro de una estructura orientada a la respuesta rápida de las emergencias a catástrofes o emergencias en seguridad de la información, así como los organismos responsables de la seguridad ciudadana, inteligencia, judiciales, administrativos, etc., relacionados con la gestión y protección de la información sensible y procesos que dependen de ella.

Cada centro de respuesta a emergencias estaría en relacionado tanto en estructura como en procedimientos y ejecución de acciones con un centro que encauza las acciones a ser tomadas por motivos de alguna emergencia. Los centros no sólo se comunican información a nivel técnico, sino a nivel administrativo, legal o judicial, de forma que las

incidencias puedan ser resueltas perentoriamente y detectar los posibles responsables de las acciones delictivas en caso que éstas se produzcan.

A figura 12 muestra un esquema de la estructura jerárquica de respuesta inmediata a emergencias o catástrofes en seguridad de la información.

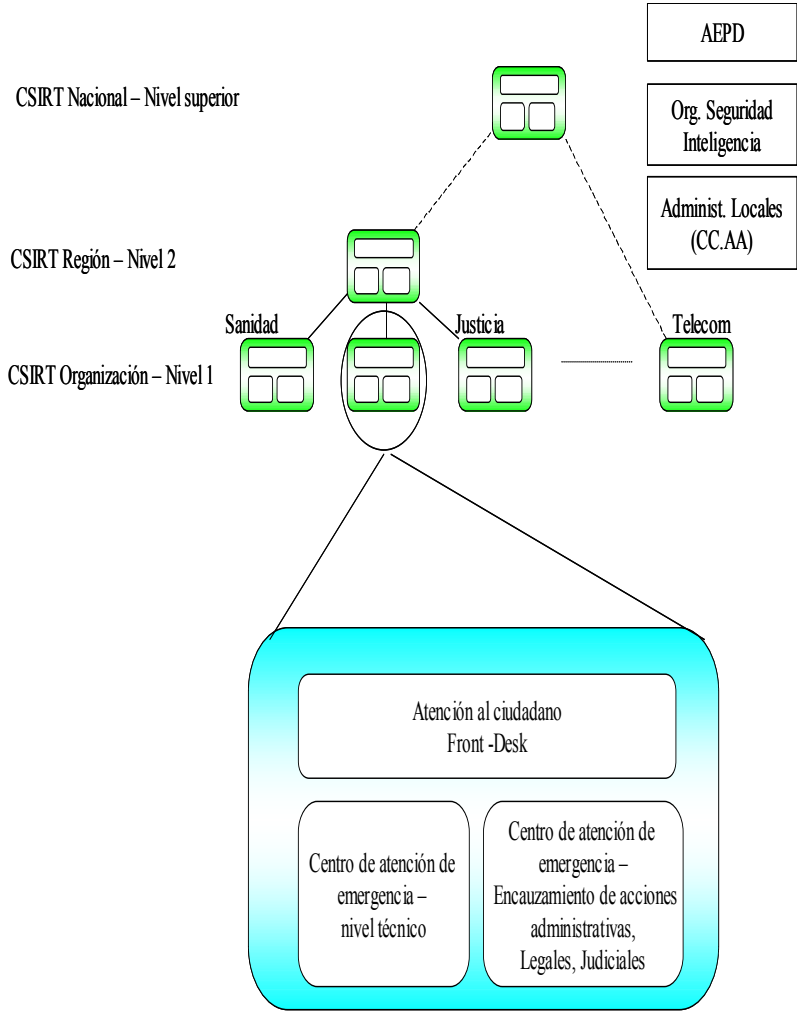

Figura 12. Estructura de respuesta rápida a emergencias y catástrofes en seguridad de la información

En el caso de organismos con competencias delegadas, tal el caso de administraciones locales de las comunidades autónomas (por ejemplo, Sanidad, Justicia, etc.) sus centros de alertas estarían coordinados por un centro embebido directamente dentro de la estructura jerárquica de la administración local. Esto facilitaría el correcto y eficaz encauzamiento de las acciones de emergencia de los distintos niveles (técnico, administrativo, legal, etc.) . Dicho centros locales, así como centros de organismos con alcance más allá del ámbito local (proveedores de telecomunicaciones, bancos, mayoristas, etc.) estarían en coordinación con el centro a nivel nacional.

La información dentro de la estructura propuesta fluye según los casos de incidencias que se presenten: la detección de un fallo en la seguridad local de la información puede representar un caso masivo de vulneración de la información, de las infraestructuras de soporte de la misma o de los procesos relacionados. Por ello el análisis, filtrado y reporte inmediato de las incidencias a los centros superiores de coordinación es requerida para activar los protocolos de actuación en casos de emergencias. Los centros coordinadores "tensarían la red" informando a los restantes centros a involucrar en la respuesta a la emergencia.

5.1 Gestión de incidencias y denuncias.

Para la gestión de incidencias existe un procedimiento estandarizado que es aplicado en los CSIRT[4] . Este esquema modificado en forma adecuada permite la incorporación de las denuncias como elemento de

entrada (*input*) al flujo de procesos de incidencias original. La figura 13 muestra el flujo de procesos modificado para la recopilación de incidencias y denuncias sobre violaciones de información.

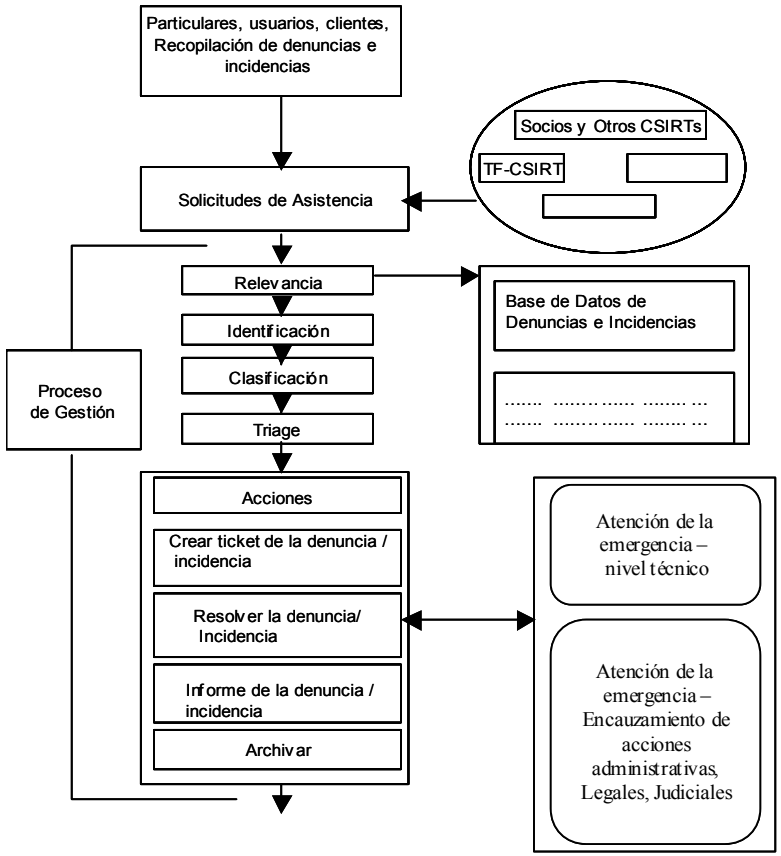

Figura 13. Flujo de procesos para la recopilación de incidencias y denuncias sobre violaciones de información

Los procesos se explican a continuación, tomando como base la descripción general hecha en la sección 4 del marco teórico.

5.1.1 Recibir denuncias e incidencias

Las denuncias / incidencias llegan al Centro a través de su *front-desk* desde diferentes canales, sea por denuncia en persona, teléfono, internet, fax, etc. Cada detalle debe ser registrado enseguida en seguida, mientras se recibe el informe. A continuación un ejemplo de formato de recogida de información:

Ejemplo de FORMULARIO DE Registro de denuncia / incidencia El asterisco * indica información requerida. **Información personal o institucional del afectado** Nombre / Organización /Responsable 1. Nombre*:
2. Código de identificación*:
3. Representante (en el caso de Organizaciones)
4. Tipo de Sector:
5. País*:
6. Ciudad*:
7. E-Mail*:
8. Teléfono*:
9. Otra:

Ejemplo de FORMULARIO DE Registro de denuncia / incidencia (Cont.)
El asterisco * indica información requerida.
Información o sistemas afectados
10. Descripción de los sistemas (número de ordenadores, nombre y direcciones IP de los dispositivos, función de cada dispositivo, modelos, sistemas operativos)
11. Información o procesos vulnerados (registros, archivos, bases de datos, software, ...)
12. Protocolo/puerta:
Incidencia
13. Número de referencia #:
14. Tipo de Incidencia:
15. Incidencia Empezó:
16. Esta es una incidencia activa: SI NO
17. Hora y Método de Detección:
18. Conocimiento de alguna vulnerabilidad, artefactos, acciones sospechosas.
19. Contramedidas que se hayan llevado a cabo.
20. Descripción detallada*.

5.1.2 Evaluación de los casos

Durante este paso se revisa la autenticidad y relevancia de la denuncia / incidencia y luego es clasificada.

Identificación

Para prevenir cualquier acción innecesaria es necesario revisar la identidad y fiabilidad del informador. Ejemplo:

1. ¿Es conocido el informante?
2. ¿Hay motivos para dudar de la fiabilidad de la fuente?
3. ¿Ha seguido los pasos regulares en el planteamiento del caso?
4. ¿Hay inconsistencias o puntos no claros que hagan dudar de la información dada?

Cada centro debe tener su política de verificación de la identidad y veracidad de la fuente de información, de manera de no generar trabajo adicional o alarmas innecesarias que pongan en duda la efectividad de los procedimientos del centro.

Relevancia

Si el incidente se origina dentro del ámbito de acción del centro, se procesa . Si no, se remite al centro de atención correspondiente.

Clasificación

Se prepara el *triage* y se clasifica la severidad del caso. Un listado posible de incidencias que pueden afectar a las personas/organismos en cuanto a vulneración de su información o procesos se presenta a en la tabla 3.

Categoría del incidente	Sensibilidad	Descripción
Usurpación de identidad	Alta	Usurpación de la identidad del ciudadano para sacar provecho material o intelectual, uso indebido de la información de cuentas bancarias, sistemas críticos, etc.
Información vulnerada	Alta	Intento de destrucción o destrucción, corrupción o divulgación de información corporativa o propiedad intelectual.
Negación de servicio	Alta	Ataque DoS o DdoS, negación de información, acceso, operación, servicios básicos.
Actividad delictiva	Alta	Robo, fraude, seguridad de personas, pornografía infantil. Incidentes informáticos de naturaleza criminal, que involucran el cumplimiento de la ley, investigaciones globales o prevención de pérdidas.

Tabla 3. Clasificación de incidencias.

Categoría del incidente	Sensibilidad	Descripción
Activos vulnerados	Media	Sistema vulnerado (cuenta de administrador, troyano, *rootkit*), dispositivo de red, aplicación cuenta de usuario . Incluye sistemas infectados con malware donde el *hacker* tiene el control del sistema.
Hacking interno	Depende del caso	Reconocimientos del terreno o actividades sospechosas que se originan desde el interior de redes corporativas, privadas o institucionales, excluyendo malware.
Hacking externo	Depende del caso	Reconocimientos del terreno o actividades sospechosas que se originan desde el exterior de redes corporativas, privadas o institucionales, excluyendo malware.
Malware	Depende del caso	Un virus o gusano que típicamente afecta a múltiples dispositivos en red. No incluye los servidores u ordenadores que están siendo activamente controlados por un *hacker* vía troyanos u orificios (*backdoors*)..
Correo electrónico	Depende del caso	Correos electrónicos forjados, SPAM, y otros eventos de seguridad relacionado con el correo electrónico.

Tabla 3. Clasificación de incidencias.

Categoría del incidente	Sensibilidad	Descripción
Consultas	Depende del caso	Consulta de seguridad no relacionada con algún incidente confirmado.
Incumplimiento de políticas	Depende del caso	▪ Intercambiar material ofensivo, intercambiar/poseer material con derechos reservados de autor. ▪ Violación deliberada de la política de seguridad de información. ▪ Uso inapropiado de activos de organismos o empresas, tales como ordenadores, red o aplicaciones. ▪ Subvertir de controles de acceso.

Tabla 3. Esquema de clasificación de incidencias

Triage

Una forma de hacer más eficiente el uso de recursos, especialmente cuando éstos son escasos, es hacer *triage*. De esta forma se puede atender mayor número de personas con la misma cantidad de recursos al hacer una evaluación inicial de los casos. Este método es empleado en urgencias por el personal médico o en emergencias. Generalmente el

personal más experimentados se asigna a las labores de triage, al disponer de mayor experiencia en el uso y gestión de los recursos.

El *triage provee de:*

Información del estado actual de todos las casos reportados

- Casos abiertos o cerrados
- Número y Tipos de casos
- Acciones pendientes
- Número y tipos de acciones realizadas

Con el triage se puede identificar posibles problemas y priorizar el trabajo, estimar las tendencias de los casos entrantes y elaborar estadísticas.

5.1.3 Acciones

Luego del triage, los casos de colocan en una cola de solicitudes dentro de una herramienta de manejar denuncias / incidencias. Generalmente, los pasos que siguen son los siguientes:

Iniciar un ticket de incidencia

Un número del ticket se asigna para referirse al caso / incidencia en el futuro.

Ciclo de vida de los casos

La gestión de las denuncias / incidencias debe seguir los pasos diseñados por cada organismo o institución para su solución y proveer a las partes tengan toda la información que les sea necesaria. Por ejemplo, en el caso

de vulneración de la información en sistemas informáticos, los pasos que se siguen en la resolución de la incidencia son básicamente cuatro: análisis, búsqueda de información sobre contactos, ayuda técnica a los afectados y coordinación / comunicación con otros centros de atención de alertas. Estos pasos se aplican reiteradamente en un ciclo hasta que se termina de resolver la denuncia / incidencia.

Informe del manejo de una Incidencia

El informe de las denuncias / incidencias se realizan con la finalidad habitual de informar a los directores o superiores sobre la gestión realizada sobre el caso. Adicionalmente, el informe puede ser útil para hacer manuales de buenas prácticas o lecciones aprendidas de mucha utilidad para la gestión de comunicación y aprendizaje con el personal menos experimentado.

Archivar

Todos los registros del caso deben ser adecuadamente archivados para su preservación en el tiempo, de acuerdo con las políticas y estándares definidos a tal propósito dentro del ámbito del centro.

5.2 Modelo organizativo de los Centros

Dadas las características de sensibilidad de la información que se maneja en cada centro y por estar en una red de atención de emergencias 24 x 7, éstos deberían ser definidos como centros inmersos dentro de cada organización que atienden, estando representados por una dirección que comparta toda las responsabilidades técnicas, administrativas o legales de la organización anfitriona.

Es de notar que cada organismo con responsabilidad de gestión de información o procesos informáticos sensibles debería poseer un centro de atención de emergencias tipo CSIRT / CERT que preste los servicios elementales de soportes a las incidencias que le ocurren en sus sistemas. En cada caso, esta estructura organizativa podría ampliarse (en cuanto a funciones o personal del centro) de manera que cubra los requerimientos de comunicación y encauzamiento de casos hacia los centros coordinadotes correspondientes.

Por ejemplo, ante la necesaria y urgente intervención de organismos policiales ante un evento de emergencia, el centro afectado debe encauzar perentoriamente la incidencia a su correspondiente e inmediato centro de coordinación, digamos el centro de alerta de la brigada de investigación tecnológica de la policía nacional, de manera que éste informe, tome las acciones y asigne el personal correspondiente para el tratamiento de la incidencia.

La prestación de servicios reactivos por parte de todos los centros de atención dentro de la estructura de respuesta rápida debe realizarse 24 x 7, pudiendo dejar los servicios preventivos a ser prestados en horarios normales de oficina.

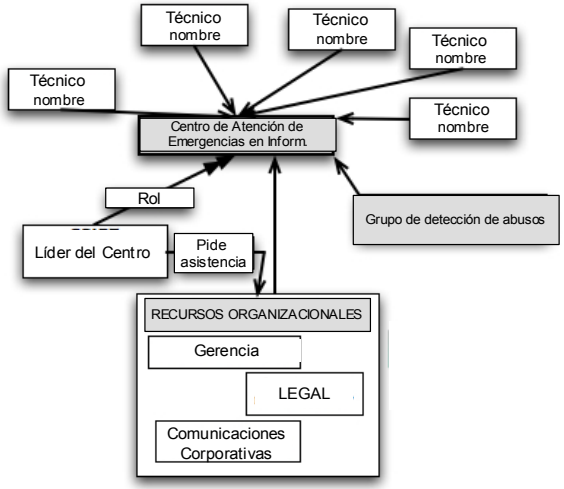

Figura 14. Ejemplo de centro de alertas incrustado dentro de una organización (fuente ENISA).

5.3 Modelo económico

Cada centro perteneciente a la estructura de atención de emergencias podría mantener su actual fuente de financiamiento para ejecutar sus acciones en forma coordinada.

No obstante, dependiendo de la infraestructura de información que pueda llegar a definirse para lograr un servicio de coordinación y atención de catástrofes en seguridad de información, se puede estudiar la posibilidad de obtener subsidios gubernamentales o la utilización de recursos de infraestructura oficial para la implantación del modelo.

Modelos económicos mixtos pueden ser adoptados, especialmente en aquellos casos que la infraestructura de información es compartida entre diferentes organizaciones. Por ejemplo, en una comunidad autónoma como Canarias, no es infrecuente que varias instituciones (gobierno, universidad, sanidad….) compartan las redes de hardware aunque se gestionen en redes virtuales independientes.

VI. Conclusión

Actualmente los ataques a la información y procesos, sean en la Red o en cualquier infraestructura deben dejar de considerarse como privados/sectoriales o institucionales para ser considerados dentro de las emergencias ciudadanas, particularmente en aquellas instituciones en las que puedan vulnerarse gravemente los derechos de los ciudadanos como por ejemplo la administración de Justicia y la Sanidad por el tipo de información confidencial que gestionan.

No debemos olvidar que según la conferencia intergubernamental de Emergencia en telecomunicaciones, un desastre o emergencia es todo aquello que altera el funcionamiento de la sociedad, poniendo en peligro generalizado la vida de las personas, su salud, su propiedad y/o su medio ambiente, siendo la causa que lo produce de múltiples índole. Por lo tanto la asistencia a un desastre incluye la prevención, predicción, preparación y respuesta para mitigar el mismo.

Los casos donde se maneja información muy sensible, es más importante la prevención y predicción que propiamente el manejo de la emergencia que por otra parte ya hemos visto estandarizada por el FIRST o forum para la incidencia y respuesta del equipo de seguridad.

De ahí que según nuestra opinión hayan de ser considerados los grupos gubernamentales policiales, de la administración o civiles que lleven a cabo la labor de inspección y sanción en los colectivos de riesgo que no cuenten con un análisis de riesgo en condiciones, con unas medidas de seguridad y con un plan de respuesta a las emergencias.

Este aspecto sobrepasa la ley de protección de datos y las Agencia Nacional o Autonómica de Protección de Datos y aunque los criterios de Seguridad Normalización y Conservación de los sistemas de información utilizables por las administraciones publicas (criterios SNC)[13] tienen su propia legislación, publicada en el BOE de 23 de junio de 2003 y que es la Resolución de 26 de mayo de 2003, de la Secretaría de Estado para la Administración Pública y varios programas como:

- el MARGERIT, elaborados por el Consejo superior de informática y
- el PILAR desarrollado por el Centro Nacional de Inteligencia que realiza un análisis de la gestión de riesgos siguiendo los criterios del MARGERIT.

Para el ciudadano común, la existencia de **Centros de Alerta Tecnológica** no es muy evidente, salvo quizás el de la Brigada de Investigación Tecnológica de la Policía Nacional, que el ciudadano asocia con otro tipo de delitos informáticos y en el entorno universitario de la red IRIS o IRIS-CERT que igualmente el ambiente universitario asocia al aviso de ataques y virus informáticos para la red académica.

El modelo de organización de las instituciones del Estado es definitivamente un factor que se debe tomar en cuenta para el diseño de una Red de atención de emergencias en seguridad de la información tal como la propuesta. Citando un caso específico, el de la Sanidad esta en España, esta se encuentra totalmente descentralizada y que por lo tanto debería tener un CERT-Sanitario en cada comunidad autónoma claramente visible para que el ciudadano tuviera confianza en su salud electrónica. Si tenemos en cuenta que en una comunidad autónoma no es infrecuente que varias instituciones (gobierno, universidad, sanidad….) compartan las redes de hardware aunque se gestionen en redes virtuales independientes, es evidente el grado de complejidad que adquiere la estructuración de estos centros de alertas.

Sin embargo, en el espíritu de nuestra propuesta, cada centro existente que monitorice la infraestructura de red estaría en capacidad teórica de convertirse en un CERT y tan solo tendría que proceder a la estandarización de los modelos y registros de alertas y el flujo de información y atención de incidencias de las mismas.

VII. Referencias

[1] Consumer Sentinel Report. Federal Trade Commision. Febrero 2007. Disponible en: http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf

[2] Aced, E., Normativa actual sobre protección de datos personales", Proceedings XIII Winter Course – AmI@Medicine, Catai Ed. 2004., Tenerife, pp: 66-76.

[3] O. Ferrer-Roca, Telepathology. In Ferrer-Roca O, Sosa-Iudicissa M. Ed., Handbook of Telemedicine. Amsterdam: IOS-Press, 1998, pp: 70-5.

[4] CSIRT Setup Guide: http://www.enisa.europa.eu/cert_guide

[5] TERENA TF-CSIRT: http://www.terena.org/activities/tf-csirt/

[6] Forum of Incident Response and Security Team: http://www.first.org

[7] RedIRIS: http://www.rediris.es

[8] Policía Nacional – Brigada de Investigación Tecnológica: http://www.policia.es/bit/index.htm

[9] Agencia Española de Protección de Datos: http://www.agpd.es

[10] Centro Criptológico Nacional: http://www.cni.es/castellano/index.html

[11] Carnegie & Mellon CERT: http://www.cert.org

[12] TI o Trusted Introducer http://www.trusted-introducer.nl/

[13] Criterios SNC http://www.csi.map.es//csi/pg5c10.htm

[14] EISSP [En línea, rev. Febrero 2007]. Disponible en: http://www.enisa.europa.eu/ENISA%20CERT/pages/04_03.htm#03

[15] TRANSITS: http://www.enisa.europa.eu/ENISA%20CERT/Páginas/04_02_02.htm#11

[16] DAF: [En línea, rev. Febrero 2007]. Disponible en: http://www.enisa.europa.eu/ENISA%20CERT/pages/04_03.htm#02