

# GUÍA DE SEGURIDAD (CCN-STIC-810)

# GUÍA DE CREACIÓN DE UN CERT / CSIRT

(BORRADOR)

Edita:



© Editor y Centro Criptológico Nacional, 2011

NIPO: 075-11-053-3

Tirada: 1000 ejemplares

Fecha de Edición: septiembre 2011

TB-Security ha participado en la elaboración y modificación del presente documento y sus anexos.

### **LIMITACIÓN DE RESPONSABILIDAD**

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el **Centro Criptológico Nacional** puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

### **AVISO LEGAL**

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

## PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

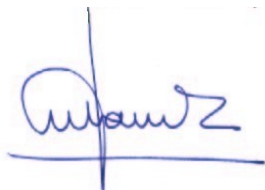
Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia de la serie de documentos CCN-STIC.

Disponer de un marco de referencia que establezca las condiciones necesarias de confianza en el uso de los medios electrónicos es, además, uno de los principios que establece la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 sobre el Esquema Nacional de Seguridad (ENS).

Precisamente el Real Decreto 3/2010 de 8 de Enero de desarrollo del Esquema Nacional de Seguridad fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Septiembre de 2011



Félix Sanz Roldán  
Secretario de Estado  
Director del Centro Criptológico Nacional

## ÍNDICE

<b>1. INTRODUCCIÓN.....</b>	<b>6</b>
<b>2. OBJETO .....</b>	<b>6</b>
<b>3. ESTRATEGIA GENERAL PARA LA PLANIFICACIÓN Y DESARROLLO DE UN CERT .....</b>	<b>7</b>
3.1. TENDENCIAS GUBERNAMENTALES DE SEGURIDAD EN LA SOCIEDAD DE LA INFORMACIÓN.....	7
3.2. ORÍGENES .....	9
3.3. ¿QUÉ ES UN CERT?.....	10
3.4. BENEFICIOS DE LA GESTIÓN CENTRALIZADA A TRAVÉS DE UN CERT.....	11
3.5. ¿POR QUÉ IMPLANTAR UN CERT EN LAS ADMINISTRACIONES PÚBLICAS? .....	12
<b>4. ¿CÓMO CREAR UN CERT? .....</b>	<b>14</b>
4.1. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y LOS CERT .....	14
4.2. PARÁMETROS DE UN CERT .....	15
4.3. DOTACIÓN DE RECURSOS.....	17
4.3.1. RECURSOS HUMANOS.....	17
4.3.2. PLATAFORMA TECNOLÓGICA.....	19
4.3.3. SECURIZACIÓN Y USO APROPIADO DE LOS EQUIPOS .....	19
<b>5. MODELO ORGANIZATIVO .....</b>	<b>21</b>
5.1. MODELO DE ORGANIZACIÓN INDEPENDIENTE.....	21
5.2. MODELO INTEGRADO EN UNA ORGANIZACIÓN PREEXISTENTE.....	21
5.3. MODELO “CAMPUS”.....	21
5.4. MODELO BASADO EN EL VOLUNTARIADO.....	21
<b>6. MISIÓN, COMUNIDAD, AUTORIDAD, COMPETENCIAS.....</b>	<b>22</b>
6.1. MISIÓN.....	22
6.2. COMUNIDAD.....	22
6.3. AUTORIDAD O MODELO DE RELACIÓN CON LA COMUNIDAD .....	23
6.4. ORGANIZACIÓN PATROCINADORA.....	24
<b>7. CATÁLOGO DE SERVICIOS .....</b>	<b>24</b>
7.1. EL PROCESO DE GESTIÓN DE INCIDENTES.....	27
<b>8. ÁMBITOS DE ACTUACIÓN DE LOS CERT.....</b>	<b>28</b>
8.1. CERT PARA EL SECTOR DE LAS PYMES .....	28
8.2. CERT ACADÉMICO .....	28
8.3. CERT COMERCIAL.....	28
8.4. CERT DE PROVEEDOR .....	28
8.5. CERT DEL SECTOR MILITAR.....	28
8.6. CERT PARA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS .....	29
8.7. CERT GUBERNAMENTAL .....	29
8.8. CERT NACIONAL.....	29
8.9. CERT AUTONÓMICO.....	33
<b>9. RESPONSABILIDADES EN EL CIBERESPACIO ESPAÑOL .....</b>	<b>34</b>
9.1. MINISTERIO DE DEFENSA .....	34
9.2. MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO .....	35
9.3. MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA.....	36
9.4. MINISTERIO DEL INTERIOR.....	37
<b>10. CERT NACIONALES.....</b>	<b>38</b>
10.1. CCN-CERT .....	38
10.2. INTECO-CERT .....	38
10.3. IRIS-CERT .....	38
10.4. CSIRT-CV .....	39

10.5. CENTRE DE SEGURETAT DE LA INFORMACIÓ DE CATALUNYA.....	39
10.6. ANDALUCÍA-CERT .....	39
10.7. OTROS CERT .....	39
<b>11. MODELO DE RELACIÓN DE LOS CERT EN ESPAÑA .....</b>	<b>40</b>
11.1. ESQUEMA DE RELACIÓN.....	41
11.2. MECANISMOS DE COORDINACIÓN ENTRE LOS CERT EN ESPAÑA .....	43
11.2.1. COLABORACIÓN NACIONAL .....	45
11.2.2. COLABORACIÓN INTERNACIONAL .....	45
<b>ANEXO A - LEGISLACIÓN Y NORMATIVA APLICABLE .....</b>	<b>49</b>
NORMATIVA Y REGULACIÓN NACIONAL.....	49
LEGISLACIÓN NACIONAL .....	49
NORMATIVA Y LEGISLACIÓN EUROPEA .....	50
ESTÁNDARES Y BUENAS PRÁCTICAS.....	52
GUÍAS CCN-STIC DEL CENTRO CRIPTOLÓGICO NACIONAL .....	52
NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY).....	53
IETF/RFCS (INTERNET ENGINEERING TASK FORCE) .....	53
OTROS ESTÁNDARES UTILIZADOS .....	54
<b>ANEXO B - ENLACES DE INTERÉS .....</b>	<b>55</b>
<b>ANEXO C – REFERENCIAS.....</b>	<b>57</b>

BORRADOR

## 1. INTRODUCCIÓN

1. El uso masivo de las tecnologías de la información en todos los ámbitos de la sociedad, así como la convergencia e interconexión de los sistemas ha venido generando nuevos riesgos y vulnerabilidades en todas las organizaciones que se ven presionadas diariamente por el creciente número de amenazas que ponen en peligro sus activos, en algunos casos, realmente críticos para su funcionamiento. Estas amenazas en el ciberespacio, que en gran medida siguen siendo las mismas que en el mundo físico (fraude, robo, espionaje industrial, terrorismo, sabotaje...) se han visto agravados por la rentabilidad de los ataques automatizados, la acción a distancia y las técnicas de propagación cada día más rápidas y fáciles de emplear. De igual modo, los ataques han ido ganando en complejidad, sigilo y focalización y especialización en los objetivos, siendo, por tanto, más compleja su resolución (la dificultad en hacer frente a amenazas como rookits, troyanos, ataques dirigidos, denegaciones de servicio distribuidas – DDoS – o las botnets, es mucho mayor que las amenazas evidentes como el spam, phishing, virus, gusanos, adware, etc.).
2. El panorama descrito obliga a las organizaciones, bien sean públicas o privadas, a realizar un esfuerzo adicional en preservar la seguridad de sus sistemas y responder a estos nuevos riesgos e incidentes. Una preservación que requiere de una política de seguridad integral y, especialmente, del desarrollo de unos servicios y capacidades operativas específicas en materia de operación y respuesta ante incidentes de seguridad.
3. De este modo, en los últimos años, se han venido desarrollando estructuras orientadas a la operación y gestión de incidentes de seguridad, llamados CERT (*Computer Emergency Response Team*) o CSIRT (*Computer Security Incident Response Team*), como solución más adecuada para dar una respuesta eficaz y eficiente a estos nuevos riesgos.

## 2. OBJETO

4. Esta guía pretende ser un instrumento eficaz que facilite una visión global de todas las implicaciones (no sólo tecnológicas) que conlleva la puesta en marcha de estos equipos de respuesta, tanto en su diseño como en el desarrollo y posterior funcionamiento, especialmente entre las administraciones públicas.
5. Esta guía forma parte del desarrollo del RD 3/2010 del ENS, según se alude en el artículo 37 sobre prestación de servicios de respuesta a incidentes de seguridad en las administraciones públicas, y específicamente, en su punto número 2 sobre el programa desarrollado por el CCN para que las administraciones públicas puedan desarrollar sus propias capacidades de respuesta a incidentes de seguridad.
6. A lo largo de este documento, se desarrolla en sus distintos capítulos: la estrategia general, las experiencias y ámbitos de actuación actuales de los CERT a nivel nacional, la normativa, buenas prácticas y legislación aplicable, la formación e información necesaria, y las herramientas que pueden ser usadas.

### 3. ESTRATEGIA GENERAL PARA LA PLANIFICACIÓN Y DESARROLLO DE UN CERT

#### 3.1. TENDENCIAS GUBERNAMENTALES DE SEGURIDAD EN LA SOCIEDAD DE LA INFORMACIÓN

7. En la actualidad, prácticamente ningún gobierno cuestiona el valor de las Tecnologías de la Información y Comunicaciones (en adelante, TIC) y las ventajas y posibilidades que ofrecen a los ciudadanos. Por este motivo, la mayoría de planes estratégicos gubernamentales contemplan iniciativas que tienen como objetivo contribuir al desarrollo de la Sociedad de la Información, conscientes de que su generalización e implantación depende, en gran medida, del impulso que reciban de las administraciones públicas.<sup>1</sup>
8. A la hora de fomentar el uso de estas nuevas tecnologías, la seguridad y resistencia se presenta como uno de sus ejes fundamentales, imprescindible para conseguir la confianza de los ciudadanos y para eliminar o minimizar los riesgos asociados a su utilización. De hecho, y tal y como recoge el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad<sup>2</sup> en el ámbito de la Administración Electrónica, es preciso crear las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las administraciones públicas fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información. Se debe, por tanto, luchar contra la desconfianza, nacida de la percepción, muchas veces injustificada, de una mayor fragilidad de la información en soporte electrónico, de posibles riesgos de pérdida de privacidad y de la escasa transparencia de estas tecnologías. Una percepción incrementada por el aumento paulatino del número de amenazas y vulnerabilidades y por su difusión, cada vez mayor, en los medios de comunicación.
9. De este modo, las tendencias gubernamentales de los países más avanzados en materia de gestión de la seguridad y lucha contra la delincuencia y el terrorismo, corroborado por entidades supranacionales como la Agencia Europea de Seguridad de las Redes de la Información (ENISA)<sup>3</sup>, la Comisión de la Unión Europea<sup>4</sup>, la Unión Internacional de Telecomunicaciones (UIT)<sup>5</sup> o la OTAN<sup>6</sup>, por citar algunos, apuntan a la creación de organizaciones altamente especializadas, diseñadas con el fin de garantizar la seguridad de los sistemas y redes de información de una nación de los que depende el correcto funcionamiento de la propia sociedad. Organizaciones que, además, sirvan de centro de seguimiento y que cuenten con información fidedigna y utilizables sobre incidentes de seguridad.

<sup>1</sup> En España, y tal y como recoge la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, las administraciones públicas deben desarrollar la administración electrónica en relación con la totalidad de los procedimientos y actuaciones de su competencia.

<sup>2</sup> Boletín Oficial del Estado, viernes 29 de enero de 2010. Nº 25.

<sup>3</sup> En su Informe Anual 2007, ENISA señala a los CERT como "componentes clave en la lucha contra el cibercrimen y la consecución de redes seguras en Europa".

<sup>4</sup> Comunicado de la Comisión de la Unión Europea al Parlamento (Bruselas, 30.03.2009, COM (2009) y Comunicado COM(2011) 163 final. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:ES:PDF>

<sup>5</sup> ITU Study Group Q.22/1 Report on Best Practices for a National Approach to Cybersecurity: a Management Framework for Organizing National Cybersecurity Efforts. <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf>

<sup>6</sup> Creación del NCIRC (National Computer Incident Response Capability), Programa de Ciberdefensa de la OTAN.



10. La mayoría de las iniciativas impulsadas por los gobiernos en materia de estrategia nacional de seguridad de la información (como la Estrategia Española de Seguridad aprobada por el Consejo de Ministros el pasado 24 de junio<sup>7</sup>) presentan una serie de ejes estratégicos análogos, que acaban por configurar un consenso común de los objetivos que se persiguen:
- Coordinar actuaciones centralizadas ante usos nocivos y/o ilícitos de las TIC, abordando los siguientes aspectos:
    - Reducción de vulnerabilidades y amenazas de los sistemas.
    - Protección contra delitos informáticos.
    - Capacidades de prevención, detección, análisis y respuesta temprana ante incidentes.
  - Proteger toda la infraestructura crítica de la información, de la cual depende el correcto funcionamiento del país (telecomunicaciones, energía, transportes, sistema financiero, Administración Pública, etc.).
  - Fomentar la confianza y la seguridad de las redes de telecomunicaciones y de la información que por ellas circula.
  - Divulgar el valor de la seguridad como elemento esencial de una Sociedad de la Información integradora.
  - Comunicar y promocionar las mejores prácticas en seguridad informática para la prevención y respuesta ante incidentes.
  - Fomentar iniciativas que garanticen la estabilidad y la continuidad de las redes.
11. Establecer las relaciones necesarias con organizaciones nacionales e internacionales implicadas en la seguridad, con el fin de colaborar y compartir información que haga frente de modo efectivo a las crecientes amenazas globales.
12. Existe, pues, un convencimiento general de la necesidad de diseñar estrategias comunes a escala nacional e internacional, que minimicen los riesgos y amenazas emergentes provenientes de Internet y, por tanto, transfronterizas e interdependientes de otras infraestructuras.
13. Estas amenazas, que ponen a prueba en muchos casos a las instituciones públicas, están siendo contrarrestadas a través de iniciativas como los Centros de Respuesta ante Incidentes de Seguridad. De hecho, la Comunicación de la Comisión Europea al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, publicada el pasado 31 de marzo de 2011 (véase nota número 4), indica que es fundamental para garantizar la seguridad informática y la protección de las infraestructuras críticas de información crear en el Continente una red de equipos de respuesta a emergencias informáticas gubernamentales o nacionales que funcione correctamente de aquí a 2012.

---

<sup>7</sup> <http://www.lamoncloa.gob.es/ConsejodeMinistros/Enlaces/24062011Enlace2.htm>



### 3.2. ORÍGENES

14. La primera vez que se percibió que la seguridad de las infraestructuras de las TIC podía verse comprometida por un incidente fue en 1988 a causa del gusano “Morris”<sup>8</sup>, creado por el estudiante de Harvard, Robert Tappan Morris, de 23 años, y que se estima afectó a casi el 10% de los sistemas conectados a ARPANET, el antecesor de la actual Internet. El gusano usaba un defecto del sistema operativo Unix para reproducirse hasta bloquear el ordenador, lo que supuso un coste estimado de 15 millones de dólares. Este incidente puso de manifiesto la necesidad de coordinar el trabajo de administradores de sistemas y de gestores TIC de una manera ágil y eficiente, a partir de estructuras organizativas que no tuvieran sólo en cuenta los propios sistemas conectados a Internet.
15. A raíz de este caso la DARPA<sup>9</sup> (Defense Advanced Research Projects Agency) determinó la necesidad de enfocar el problema de modo más organizado y estructurado, y patrocinó la creación del primer Equipo de Respuesta ante Incidentes, el CERT Coordination Center (CERT/CC<sup>10</sup>), ubicado en la Universidad Carnegie Mellon, en Pittsburgh (Pensilvania).
16. Bajo estas mismas siglas comenzaron a formarse otros grupos en distintas universidades norteamericanas encargados de estudiar la seguridad de las redes y ordenadores para proporcionar servicios de respuesta ante incidentes a víctimas de ataques, publicar alertas relativas a amenazas y vulnerabilidades y ofrecer información que ayudara a mejorar la seguridad de estos sistemas. A su vez, empezó a hablarse de CSIRT para completar el concepto de CERT y ofrecer, como valor añadido, los servicios preventivos y de gestión de seguridad. Poco tiempo después, a principios de la década de los noventa, la idea se trasladó a Europa y, gracias al apoyo del programa técnico TERENA<sup>11</sup> empezaron a crearse los primeros CERT en el viejo continente. De hecho, en la actualidad el principal foro europeo de CSIRT es el Trust Introducer<sup>12</sup> de TERENA en el que se colabora, innova y comparte información con el fin de “promover y participar en el desarrollo de unas infraestructuras de información y telecomunicaciones de alta calidad en beneficio de la investigación y la educación”, tal y como recogen sus estatutos. Asimismo, auspicia un grupo de trabajo para promover la cooperación entre CSIRT en Europa, el TF-CSIRT.
17. Así, en 1992 se creó el primer CERT europeo, el SURFnet-CERT, en Holanda<sup>13</sup> y, un año después, en 1993, se creó el BSI-CERT alemán, que en 2001, al pasar a ser una unidad organizativa propia, se transformó en el CERT-Bund<sup>14</sup>.
18. En cuanto a la situación en España, a finales del año 1994, la Universidad Politécnica de Cataluña creó el esCERT-UPC y, un año después, en 1995 se formó el Iris-CERT, el servicio de seguridad de RedIRIS<sup>15</sup>.

<sup>8</sup> [http://en.wikipedia.org/wiki/Morris\\_worm](http://en.wikipedia.org/wiki/Morris_worm) y [http://es.wikipedia.org/wiki/Gusano\\_Morris](http://es.wikipedia.org/wiki/Gusano_Morris)

<sup>9</sup> Agencia de Proyectos de Investigación Avanzada en Defensa, dependiente del Departamento de Defensa de EEUU

<sup>10</sup> <http://www.cert.org>

<sup>11</sup> *Trans-European Research and Education Networking Association* (Asociación Transeuropea de Investigación y Educación de Redes. <https://www.terena.org>)

<sup>12</sup> <http://www.trusted-introducer.nl/>

<sup>13</sup> <http://www.surfnet.nl/nl/Thema/surfcert/Pages/Default.aspx>

<sup>14</sup> [https://www.bsi.bund.de/cln\\_136/DE/Themen/CERTBund/certbund\\_node.html](https://www.bsi.bund.de/cln_136/DE/Themen/CERTBund/certbund_node.html)

<sup>15</sup> Red académica y de investigación nacional que desde enero de 1994 hasta 2003 fue gestionada por el Consejo Superior de Investigaciones Científicas y, a partir de enero de 2004, pasó a integrarse como un departamento con autonomía e identidad propias en el seno de la Entidad Pública empresarial Red.es, adscrita al Ministerio de Industria, Turismo y Comercio).

19. Conviene señalar que, a menudo, y dado que la marca CERT está registrada, se utiliza otra nomenclatura:
- IRT (*Incident Response Team*, Equipo de Respuesta a Incidentes)
  - CIRT (*Computer Incident Response Team*, Equipo de Respuesta a Incidentes Informáticos)
  - CIRC (*Computer Incident Response Capability*, Capacidad de Respuesta a Incidentes Informáticos)
  - SERT (*Security Emergency Response Team*, Equipo de Respuesta a Emergencias de Seguridad)
  - ERI (Equipo de Respuesta a Incidentes)

### 3.3. ¿QUÉ ES UN CERT?

20. Tradicionalmente, se ha definido un CERT como una organización, equipo, unidad o capacidad de un organismo de ofrecer servicios y soporte a un colectivo determinado (denominado “comunidad”) para prevenir, gestionar y responder a los incidentes de seguridad de la información que puedan surgir. Esta definición genérica viene materializándose en un equipo multidisciplinar de expertos que trabaja según unos procesos definidos previamente y que disponen de unos medios determinados para implantar y gestionar, de un modo centralizado, todas y cada una de las medidas necesarias para mitigar el riesgo de ataques contra los sistemas de la Comunidad a la que presta el servicio y responder de forma rápida y efectiva en caso de producirse.
21. No obstante, el concepto de CERT y los servicios que engloban este tipo de estructuras ha ido evolucionando con el paso del tiempo y ampliando sus funciones. No sólo gestionan los incidentes de una organización, sino que también prestan otros servicios complementarios como la asistencia para mitigar riesgos (por ejemplo, mediante la ejecución y/o soporte en la realización de análisis de riesgos o vulnerabilidades), o para la recuperación después de registrar un problema. De hecho, el análisis forense es uno de los servicios que ENISA recomienda incluir a la hora de ampliar los servicios de este tipo de equipos<sup>16</sup>, así como la gestión de las vulnerabilidades.
22. Es decir, si bien el servicio básico de un CERT es el de gestión de incidentes, la mayor parte de ellos hoy en día están evolucionando hacia un modelo integral de gestión de la seguridad en donde se tienen en cuenta todos los elementos técnicos, humanos, materiales y organizativos de un sistema y en donde predominan los servicios proactivos y de alerta temprana. De hecho, cada vez más, ofrecen a sus clientes servicios preventivos (seguridad proactiva, servicios para la mejora de la calidad de la gestión de la seguridad, desarrollo de herramientas de seguridad, detección de intrusiones, sistemas de alerta temprana...), formativos y de concienciación a las personas de su Comunidad (publicación de avisos sobre las vulnerabilidades del software y el hardware en uso, emisión de avisos sobre amenazas como códigos maliciosos o actividades sospechosas o de riesgo, publicación de recomendaciones y buenas prácticas, etc.) o de otro tipo (análisis de riesgos, planes de continuidad y de recuperación ante desastres, evaluación y certificación de productos, etc.).
23. Sirva de ejemplo, la modificación realizada por el US-CERT<sup>17</sup> (CERT del Departamento de Seguridad Nacional de Estados Unidos) del significado de la letra “R”, pasando del tradicional Response a Readiness.

<sup>16</sup> Guía de Buenas Prácticas en la Gestión de Incidentes (2010) <http://www.enisa.europa.eu/act/cert/support/incident-management/files/good-practice-guide-for-incident-management>

<sup>17</sup> <http://www.us-cert.gov/>

### 3.4. BENEFICIOS DE LA GESTIÓN CENTRALIZADA A TRAVÉS DE UN CERT

24. Como ya se ha señalado, la centralización de todas las actividades relativas a la seguridad de la información es una de las tendencias actuales entre aquellas organizaciones (públicas o privadas) que pretenden mantener unas buenas prácticas, cumplir con la normativa vigente y, sobre todo, ser capaces de afrontar los riesgos emergentes a los que están expuestos de un modo sistémico, eficaz y eficiente.
  25. Para afrontar estas amenazas es imprescindible tener un gran conocimiento organizativo, normativo y técnico, y estar continuamente al día en cuestiones de seguridad. De hecho, la operación y mantenimiento de la infraestructura de seguridad y la gestión de los incidentes requieren de un esfuerzo cada día mayor, difícilmente asumible con equipos dispersos y segmentados.
  26. Específicamente, con respecto al cumplimiento normativo, según recoge el RD 3/2010 (ENS) en el artículo 24, 'Incidentes de Seguridad', punto 2, '[...] Se registrarán los incidentes de seguridad que se produzcan y las acciones de tratamiento que se sigan. Estos registros se emplearán para la mejora continua de la seguridad del sistema.', lo que requiere igualmente de un sistema formal de gestión y respuesta a incidentes.
  27. Adicionalmente, en este mismo RD, en su Anexo II de Medidas de Seguridad, dentro del Marco Operacional y la explotación, el punto 4.3.7 relativo a la Gestión de Incidencias especifica: '[...] se dispondrá de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema [...]']'.
  28. La solución de centralizar estos recursos y procesos de forma centralizada en un equipo (CERT) presenta, pues, numerosas ventajas, entre las que destacan:  
Mejora de los tiempos de respuesta en la resolución de incidentes mediante:
    - La centralización de la coordinación de las acciones de contención y respuesta ante incidentes dentro de la organización, como un único punto de contacto.
    - El incremento de la capacidad de coordinación con otros CERT (debe tenerse en cuenta que estos equipos forman parte de grupos y foros internacionales que comparten conocimientos y experiencias, y a los cuales no tiene acceso una organización convencional).
    - Establecerse como centro de excelencia y ofrecer los conocimientos técnicos necesarios para apoyar y asistir a los usuarios que necesitan recuperarse rápidamente de algún incidente de seguridad.
- **Ahorro de costes** al concentrar conocimiento altamente especializado (y, por tanto, costoso) en un sólo centro, desde el que se difundirá posteriormente a toda la Comunidad. Además, esta centralización también mejora la calidad de los servicios típicos de gestión de seguridad (por ejemplo, auditorías) ya que, o bien los lleva a cabo directamente el CERT, o bien será el encargado de centralizar en un único punto la contratación de un tercero (cuenta con la capacidad técnica de seleccionar al mejor contratista o dar los parámetros para identificarlo).
  - Mejora en la calidad de la gestión de la Seguridad de la Información de las organizaciones miembro de la Comunidad, al ofrecerles la función de gestión de incidentes (RD 3/2010, Anexo II de Medidas de Seguridad, punto 4.3.7 relativo a la Gestión de Incidencias) con un elevado grado de especialización y dedicación exclusiva. Esta mejora no derivará forzosamente en una reducción del número de incidentes, – es más, posiblemente aumente su número debido a un procedimiento de detección y respuesta más formal –, pero sí en una

mayor eficacia y eficiencia a la hora de ser detectados, gestionados y resueltos. Los mejores tiempos de respuesta y resolución reducen las pérdidas económicas que conllevan los incidentes de seguridad y el impacto que pueden llegar a tener.

- Aumenta el conocimiento de los miembros de la Comunidad al ofrecerles los contenidos técnicos necesarios para prevenir situaciones de riesgo; para apoyar y asistir en la gestión de algún incidente de seguridad; y para mejorar el grado de sensibilización de sus usuarios finales.
- Puede ofrecer un punto cualificado para gestionar y coordinar las cuestiones normativas y jurídicas asociadas a los incidentes y proteger adecuadamente las evidencias digitales en caso necesario.
- Permite realizar un seguimiento formal de los progresos conseguidos en el ámbito de la seguridad, y establecer sistemas de medición (métricas) del nivel de servicio, calidad, retorno de inversión, etc. asociado a la gestión de las operaciones de seguridad.
- Fomenta la cooperación en la seguridad de las TIC entre los clientes (usuarios) de la comunidad a la que presta servicios, ejerciendo labores de punto central de sensibilización y comunicación entre los miembros de la comunidad.

### 3.5. ¿POR QUÉ IMPLANTAR UN CERT EN LAS ADMINISTRACIONES PÚBLICAS?

29. La Administración Pública (en cualquiera de sus ámbitos) es uno de los sectores más significativos que se encuentra bajo la omnipresencia de las TIC, tanto a nivel organizativo (intervienen directamente en su funcionamiento y en el proceso de control y regulación de otros sectores críticos), como la prestación de servicios públicos orientados hacia y para los ciudadanos. Sobre todo teniendo en cuenta que, el informe E-Government Survey elaborado por Naciones Unidas, en su edición de 2010, sitúa a España como uno de los países que presenta un mayor desarrollo de sus servicios de eAdministración, ocupando el puesto nueve de del ranking mundial. Entre estos servicios, y según un informe de la Fundación Orange<sup>18</sup>, destacan: la obtención de información de las distintas páginas web, la descarga de formularios oficiales y el envío de los mismos ya cumplimentados, la gestión electrónica, presentaciones a licitaciones públicas y, sobre todo, las declaraciones de impuestos a través de Internet (uno de los servicios de Administración Electrónica más utilizado por ciudadanos y empresas).
30. De hecho, y tal y como recoge las disposiciones generales del RD 3/2010 por el que se regula el Esquema Nacional de Seguridad<sup>19</sup>, la necesaria generalización de la Sociedad de la Información es subsidiaria, en gran medida, de la confianza que genere en los ciudadanos la relación a través de medios electrónicos. Para ello, es fundamental una política de seguridad en la utilización de dichos medios que permita la adecuada protección de la información.
31. La finalidad del ENS es, precisamente, la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos. Es decir, que los sistemas de

<sup>18</sup> Informe Anual sobre la Sociedad de la Información en España, 2011

<sup>19</sup> RD 3/2010 de 8 de enero, Regulador del Esquema Nacional de Seguridad:  
<http://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf>



información de las AAPP prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas.

32. La dificultad de preservar los sistemas de la Administración, así como los servicios públicos que ésta ofrece (algunos de ellos críticos para el normal funcionamiento de un país) y la información que sobre ellos circula es, por lo tanto, una de las principales razones para implantar un Equipo de estas características en las administraciones públicas. Máxime teniendo en cuenta que los ataques a la seguridad de las TIC son cada día más complejos y difíciles de detectar<sup>20</sup> y que requieren de una constante actualización y especialización por parte de las personas encargadas de su preservación. Así, entre los cambios producidos se encuentran:

- **Profesionalización y maduración del cibercriminal:** Si bien antes las motivaciones de los atacantes eran la búsqueda de satisfacción personal y prestigio en su entorno, ahora el factor que más los incentiva es el afán de lucro, con organizaciones relacionadas con el robo de información de tarjetas de crédito, blanqueo de dinero o robo de identidades asociado a inmigración ilegal, por ejemplo. Esto queda en evidencia en la progresiva profesionalización y maduración del mercado del cibercrimen, cuyas redes persiguen el rápido beneficio económico y que, en muchas ocasiones, se financian a través de otros negocios ilícitos (“hackers” pagados por delinquentes tradicionales). Esta tendencia ha llevado al aumento de la especialización y diferenciación de los distintos tipos de “hackers”, dando lugar a un auténtico ecosistema económico propio (creadores de código dañino, vendedores de servicios de hacking, spammers, controladores de botnets, gestores de NIC anónimos, ISP ‘colaboradores’, especialistas en blanqueo de dinero electrónico, etc.).
- **Implicación y ataques gubernamentales:** Existe un incremento considerable del hacking político/patriótico que, aunque no suele tener un gran impacto en los sistemas de información, puede provocar un tremendo desprestigio de graves consecuencias.
- Del mismo modo, se conoce la utilización por parte de determinados gobiernos, de grupos criminales o de grupos de hackers especializados, de ataques informáticos para obtener información sensible o clasificada, manejada por los sistemas de información gubernamentales y de empresas nacionales de sectores estratégicos. En el marco de este ciberespionaje las denominadas amenazas persistentes avanzadas (APT –Advanced Persistent Threats-) han pasado a ocupar un primer plano en la preocupación de los estados y las organizaciones gubernamentales<sup>21</sup>. De ahí el continuo desarrollo de estrategias nacionales por parte de un gran número de países con las que se persigue un ciberespacio más seguro.
- **Focalización de los ataques:** Se ha pasado de ataques a escala global a agresiones dirigidas y preparadas con gran antelación contra víctimas muy escogidas (así en las APT, los ataques se realizan de forma sigilosa, de forma muy persistente, modificando las estrategias y desarrollando nuevos tipos de ataques en el caso de que un objetivo se resista a ser penetrado). Es decir, ataques más complejos, sigilosos y personalizados y por lo tanto no detectados (o con poca probabilidad de serlo) por herramientas tradicionales, como antivirus, sistema de detección / prevención de intrusiones, etc. Esto, a su vez, implica una mayor complejidad en la investigación/detección de nuevos ataques (creación de códigos dañinos –

<sup>20</sup> Informe de Amenazas CCN-CERT IA\_01-11. Ciberamenazas 2010 y Tendencias 2011

<sup>21</sup> El ataque denominado “Aurora”, producido en 2010 y destinado a robar información sensible de 30 grandes compañías (entre ellas Google), puso sobre la mesa que el ciberespionaje es una amenaza real contra gobiernos y empresas y que puede llegar a afectar a sistemas de control industrial y a la información crítica de compañías estratégicas.

troyanos– específicamente creados para una víctima, ataques de ingeniería social, etc.).

- **Mayor velocidad:** Los ataques de hoy en día son más complicados en su morfología pero, paradójicamente, algunos de ellos son muy fáciles de realizar: en ocasiones existe muy poco tiempo entre la aparición de una vulnerabilidad de un sistema y la creación y el uso de código dañino para atacarlo (son preocupantes las vulnerabilidades día cero, muy presentes en el mercado clandestino). Además, se trabaja cada vez de forma más activa en la elaboración de herramientas públicas que buscan supuestamente difundir las nuevas vulnerabilidades pero que, en algunos casos, derivan en herramientas automatizadas de ataque a sistemas TIC.
  - **Mayor interconexión:** Actualmente los sistemas de información de las AAPP están fuertemente imbricados entre sí y con los del sector privado. De esta manera, la seguridad tiene un nuevo reto que va más allá del aseguramiento individual de cada sistema. Por ello, cada uno de los sistemas deben tener claro su perímetro y los responsables de cada dominio de seguridad debe coordinarse efectivamente para evitar “tierras de nadie” y fracturas que pudieran dañar la información o los servicios prestados.
33. Debido a la naturaleza de estos ataques, los gestores de incidentes se ven obligados a estar continuamente formados y actualizados: nuevas tecnologías, nuevas técnicas de ataque y defensa, nuevos vectores de ataque, nuevos “scene players”, nuevas vulnerabilidades conocidas, etc. Igualmente, deben mantener el contacto con las últimas técnicas y herramientas disponibles de manera pública (monitorizar foros, conocer herramientas, etc.) para conocer los medios de los que disponen los atacantes potenciales.
34. Bajo esta visión es lógico que la Administración quiera y deba ofrecer mecanismos eficientes para identificar, prevenir y gestionar estos nuevos riesgos de seguridad que pudieran afectar al ciudadano, a las empresas y a las distintas administraciones que prestan servicio a la sociedad, al igual que hace hoy en día con otros servicios de emergencia.
35. Por ello, desde el sector público aparece la necesidad de articular funciones de control de riesgos informáticos a través de CERT que actúen como coordinadores y que garanticen una óptima gestión de la seguridad del territorio y de los miembros de su comunidad.

## 4. ¿CÓMO CREAR UN CERT?

36. Antes de plantear la implantación de la capacidad de respuesta ante incidentes mediante la creación de un CERT, la organización promotora debe considerar los siguientes aspectos:

### 4.1. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y LOS CERT

37. En la práctica, un CERT está constituido por un grupo de expertos que, según unos procedimientos de actuación y comunicación, hacen uso de unos recursos para proporcionar servicios de gestión de incidentes (además de otros no específicamente relacionados con incidentes tal y como ya se ha comentado) a una Comunidad.
38. Lo primero que el patrocinador o promotor debe tener presente es que la creación de un CERT no implica por tanto implantar sólo tecnología, sino adoptar una serie de procesos (compuestos por distintos recursos: humanos, económicos, tecnológicos, etc.), gestionados de acuerdo a unas políticas, normas y procedimientos que persiguen cumplir unos objetivos de negocio concretos.

En un esquema de organización en que la seguridad de la información es madura y se maneja en el marco de un Sistema de Gestión de la Seguridad de la Información (SGSI), el CERT se suele especializar en una función concreta de este SGSI: la de gestión de incidentes.

39. De hecho, esta función cumple plenamente su cometido cuando este SGSI ha alcanzado un cierto grado de madurez, y a su vez la seguridad de la información manejada por el propio CERT se encuentra también beneficiada por la estructuración de la organización de procesos que un SGSI aporta.
40. En el caso de que la entidad no disponga de un sistema de gestión de la seguridad, es recomendable que el CERT cree su propio SGSI.
41. En algunos casos, esta madurez de sus objetivos y modelo de negocio evoluciona hacia el concepto de CSIRT antes mencionado, asumiendo bajo este nuevo modelo, el resto de actividades clave de la gestión de la seguridad, absorbiendo las funciones y responsabilidades de los grupos u oficinas de seguridad previas que conformaban el área de gestión de la seguridad de la información, en muchos casos, dándole forma y entidad propia y segregada del área de TIC.

## 4.2. PARÁMETROS DE UN CERT

42. Entre los distintos factores que contribuyen al éxito de un CERT, se sitúa la proporcionalidad de los recursos con los que se dote con respecto a las expectativas de demanda que genere, al igual que en cualquier otro servicio. Por lo tanto, a la hora de dimensionar correctamente este tipo de equipos deberá considerarse los siguientes parámetros:

- **Tamaño de la Comunidad a la que se da servicio.** Este es el parámetro principal, puesto que a mayor número de miembros se generarán más peticiones de asistencia en gestión de incidentes y de otro tipo.
- **Grado de autoridad sobre los miembros de la Comunidad** y el modelo de relación jerárquica entre ambos. Es relevante si se solicitarán los servicios por propia iniciativa o por imperativo legal, lo que condiciona en este último caso la existencia probable de un mayor volumen de incidentes a gestionar.
- **Servicios ofrecidos y nivel de servicio.** Si se ofrecen servicios en modo 24x7 los 365 días del año se requerirán de muchos más recursos humanos y técnicos que si únicamente se prestan en horario laboral. También hay que considerar los acuerdos de servicio y tiempos de respuesta, como por ejemplo las modalidades de “best effort” (en los que el equipo se compromete a cumplir con las peticiones de su Comunidad, aunque no existe una obligación formal) o de “next business day” (que establece que la petición se atenderá a partir del próximo día laborable), o incluso periodos menores de respuesta.
- **Promoción y comunicación de servicios.** Uno de los parámetros que más influirá será el grado de conocimiento por parte de la Comunidad de los servicios que se ofrecen. Este aspecto implica que la dotación del CERT debe ir progresando a medida que aumente su impacto prestando especial atención a la promoción y comunicación de los nuevos servicios.
- **Proceso de maduración.** Establecer un CERT es un proyecto a largo plazo, que debe ir madurando y ampliándose en la medida que ofrezca valor a su comunidad y se gane su confianza. Normalmente, no se puede considerar completamente implantado hasta al menos dos años después de su inauguración.



- **Plan estratégico.** Es conveniente planificar la correcta evolución del CERT, prestando la adecuada atención a los aspectos de financiación y sostenibilidad a largo plazo, contemplando la entrada progresiva de nuevos servicios, así como de los recursos necesarios para implantarlos, promocionarlos y operarlos.

43. Otras facetas relevantes, aunque en menor medida son:

- La calidad de los controles y, en general, el nivel de madurez de la gestión de la seguridad en los sistemas de información de los miembros de la Comunidad puede influir en el número de incidentes que pueden ocurrir.
- El nivel de exposición a ataques es también relevante. En sectores y actividades concretas tanto públicas como privadas, puede serlo por la importancia de la información manejada por la organización, o la criticidad de esta para la seguridad nacional.

BORRADOR

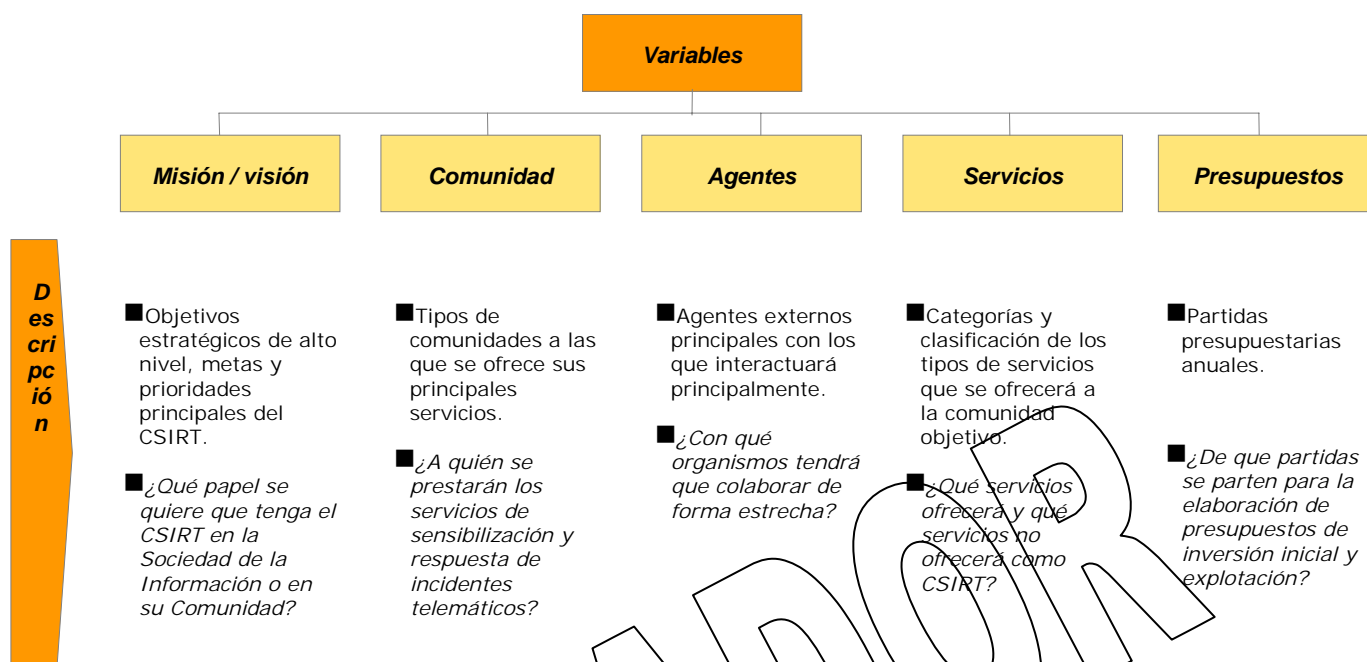


Figura 4.1. Variables para la configuración de un CERT

### 4.3. DOTACIÓN DE RECURSOS

44. Los factores anteriores determinarán los recursos que necesitará el CERT, que se pueden clasificar en dos grupos generales:

#### 4.3.1. RECURSOS HUMANOS

45. Su número evolucionará con el tiempo, aunque en la fase inicial, será necesario contar con las siguientes figuras<sup>22</sup>:
- **Director general/Supervisor** que gestione el equipo.
  - **Personal técnico**, empleados que desarrollan y ofrecen los servicios.
  - **Investigadores**, empleados que llevan a cabo las investigaciones y análisis necesarios.
46. Algunos consultores pueden asistir al director general en sus funciones; entre ellos convendría un experto en leyes que trate con los asuntos jurídicos y proteja las pruebas legales en caso de juicio. El número de personas a contratar depende de la magnitud de los servicios ofrecidos por el CERT y sus recursos económicos pero, en líneas generales, el equipo técnico y operativo debería constar de un director técnico y dos técnicos; y el equipo de investigación de un director de investigación y dos investigadores.

<sup>22</sup> ENISA, Ejercicios CERT Manual

<https://www.enisa.europa.eu/act/cert/support/exercise/files/cert-exercise-handbook-in-spanish>

47. El jefe del equipo CERT debería poseer una formación amplia en el ámbito de la seguridad y experiencia laboral en el proceso de gestión de crisis y recuperación de negocio. Los miembros de un equipo técnico operativo deberían ser expertos en seguridad que puedan proporcionar los servicios especializados del CERT para la gestión y la respuesta a incidentes en el ámbito de las TIC. Los investigadores deberían poseer conocimientos extensos en seguridad TIC y experiencia en proyectos de seguridad.
48. No obstante, de forma más concreta, convendría que todo CERT contase con los siguientes perfiles:
- **Un responsable del equipo** que actúe como punto de contacto con la Comunidad a la que se da servicio y el resto de CERTs con los que se vaya a colaborar.
  - **Un responsable de los sistemas y seguridad de la información.** Este puesto es necesario únicamente en el caso de que el propio CERT sea responsable de la operación, administración y mantenimiento de los sistemas TIC que necesite para su operación. En algunos casos parte de estos sistemas podrán estar compartidos con la organización patrocinadora, aunque continuarán existiendo otros necesariamente bajo la responsabilidad única del CERT: se trataría al menos de las instalaciones para realizar análisis forense y análisis de códigos dañinos.
  - **Un equipo de comunicación o relaciones públicas.** El CERT tendrá que mantener una actividad de comunicación y promoción con la Comunidad para promocionar los servicios que presta y para divulgar conocimiento específico sobre seguridad (si se encuentra dentro de su Catálogo de Servicios). El éxito de un CSIRT depende de la confianza y reconocimiento que logre en su Comunidad. Esto requiere hacer énfasis en la promoción de sus actividades y servicios. El plan de comunicación y promoción debería incluir los siguientes aspectos:
    - Identificación de los medios disponibles.
    - Mecanismos oficiales de divulgación de información del centro – sala de prensa.
    - Participación en eventos y foros especializados.
    - Afiliación a organismos internacionales.
  - **Un equipo de gestión de incidentes.** En esta área es donde resulta más difícil cuantificar los recursos necesarios. Además, dependerá del nivel de servicio que ofrece el CERT en cada uno de ellos y que puede consultarse en el Catálogo de Servicios. El correspondiente a la gestión de incidentes debe ser el más destacado. Si se ofrece una calidad de servicio de 24x7, o bien se espera un número elevado de peticiones de soporte, deberá existir un primer nivel de asistencia a la Comunidad que gestione y filtre inicialmente las notificaciones realizadas, y un segundo nivel especializado que realmente gestione y abra una investigación sobre el incidente, si procede.
  - **El primer nivel** necesita un grado de conocimiento técnico básico especializado en tecnologías TIC suficiente para entender la situación notificada. También deberá caracterizarse por tener gran disponibilidad para trabajar en horario especial y capacidad de trabajo bajo presión.
  - **El segundo nivel,** es donde se encuentran los especialistas que realmente tienen el conocimiento técnico y las habilidades de intercomunicación con otros CERT o miembros de

la comunidad de Internet. Se ha constatado que la calidad del trabajo realizado por un CERT depende en igual medida de los medios de que dispone y del conocimiento técnico de sus miembros, pero también de su capacidad de comunicación e interrelación con otros equipos de respuesta ante incidentes y agentes relevantes en la gestión global de las infraestructuras TIC (como proveedores de servicios de Internet – ISP –, operadores de telecomunicaciones, agentes administrativos de Internet, etc.). Este equipo de personas serán los encargados de analizar, asesorar y, en general, gestionar las situaciones de emergencia que un incidente provoca. Fuera de las situaciones de emergencia, también estarán al cargo de prestar los otros servicios no específicamente de gestión de incidentes (divulgación, análisis de código malicioso, etc.).

- Lo más probable sea que se deba disponer de especialistas en distintas áreas, ya que es difícil que una única persona sea experta en todas las materias de interés para un CERT. El número de recursos necesario en el segundo nivel dependerá del número de incidentes a gestionar, por lo que debe estar preparado para crecer, sobre todo en los primeros estadios de vida del CERT.
- **Un equipo de formación.** Es esencial que el personal del CERT esté adecuadamente formado y actualizado en nuevas tecnologías TIC, nuevas amenazas y técnicas de ataque. Por otra parte, y dependiendo del catálogo de servicios, también es interesante que este conocimiento se transfiera a la Comunidad, especialmente administradores de sistemas, gestores de TIC y usuarios finales, mediante distintos tipos de acciones formativas. Debería existir en el CERT la suficiente capacidad y experiencia pedagógica para poder prestar este tipo de servicio. Esta capacidad puede estar presente en los expertos de segundo nivel, si bien su perfil y exigencias operativas hacen que no sean los perfiles más adecuados, debiéndose buscar por tanto formadores/consultores profesionales.

#### 4.3.2. PLATAFORMA TECNOLÓGICA

49. Se deberá dotar al CERT de los medios técnicos necesarios para poder prestar sus servicios. A nivel general, un CERT requiere de los siguientes sistemas principales:
- Plataforma Internet (Portal)
  - Sistemas de Soporte a Operaciones (Sistemas de tickets, BBDD, etc.)
  - Sistemas de Back-Office (Investigación forense, código dañino, etc.)
50. En esta guía se incluye un capítulo donde se describen las herramientas más comúnmente utilizadas para dichos sistemas.

#### 4.3.3. SECURIZACIÓN Y USO APROPIADO DE LOS EQUIPOS

51. Lo más apropiado es establecer una política de uso de los sistemas en la que se indiquen todas las reglas a las que los miembros del equipo deben atenerse. El primer planteamiento debe partir de si los trabajadores del CERT deben ser sus propios administradores. Hay que plantearse si los equipos pueden ser utilizados para uso personal o no, qué páginas se pueden visitar desde los

sistemas del CERT o qué tipo de software personal se puede descargar o instalar. La política de uso debería incluir también las siguientes cuestiones:

1. Uso apropiado de los equipos.
  2. Copias de seguridad.
  3. Configuraciones de seguridad para software y navegadores, según las guías CCN-STIC.
  4. Buenas prácticas y configuración segura de soluciones cortafuegos, antivirus, proxy, etc.
  5. Instalación de actualizaciones de software y de seguridad.
  6. Acceso remoto a los servicios del CERT para labores de administración y/o soporte de teletrabajadores.
52. También es importante el emplazamiento físico del CERT, no sólo para tener un lugar de trabajo sino también para proteger el acceso al área restringido. Puede incluir las siguientes estancias:
- Oficina general.
  - Área securizada físicamente para reuniones y trabajo sobre incidentes.
  - Acceso seguro para oficinas individuales, trituradoras de papel, faxes e impresoras.
  - Laboratorio de pruebas e instalaciones de formación.
  - Cajas fuertes, etc.
53. Las instalaciones de un CERT, así como su red e infraestructura de telecomunicaciones, tiene que ser diseñada con gran cuidado, no sólo para proteger los sistemas y la información sensible recolectada, sino también al equipo de personas.
54. Se requiere por tanto de un Plan de Seguridad de las instalaciones específico que cumpla con las normativas y buenas prácticas aplicables, especialmente las relativas las instalaciones donde se maneje información sensible o clasificada.
55. Se deberán establecer diversos niveles de acceso, dejando a los más internos la custodia de los activos críticos y confidenciales (salas de almacenamiento de evidencias, salas de proceso de datos o las salas de operación).
56. Estos niveles deberán segregarse físicamente y deberán contar con los adecuados sistemas de control de acceso y vigilancia para garantizar que sólo el personal autorizado pueda acceder.

## 5. MODELO ORGANIZATIVO

57. Existen diversos modelos de funcionamiento para los CERT. Éstos dependerán de la organización patrocinadora y de la Comunidad a la que se atiende. En líneas generales, los modelos se pueden clasificar de la siguiente forma<sup>23</sup>:

### 5.1. MODELO DE ORGANIZACIÓN INDEPENDIENTE

58. Es un CERT extendido que actúa como una organización independiente, con sus propios directivos y empleados. En muchos casos son organizaciones o empresas financiadas por la organización patrocinadora o por los miembros de la Comunidad.

### 5.2. MODELO INTEGRADO EN UNA ORGANIZACIÓN PREEXISTENTE

59. En este modelo el CERT funciona como un departamento de la organización con más o menos autonomía. Generalmente está dirigido por un jefe de equipo responsable de las actividades, que reúne a los técnicos necesarios cuando resuelve incidentes o trabaja en actividades del CSIRT. Puede pedir asistencia especializada a las otras áreas de la organización y en caso que se requiera, incorporar trabajadores propios.

### 5.3. MODELO “CAMPUS”

60. En este modelo se parte de los modelos de algunas universidades y/o redes de investigación, en las cuales existe una sede central y muchas sedes distribuidas con una cierta independencia. En este caso hay un CERT “madre” o principal y unidades o CERTs más pequeños dependientes del primero. Este modelo es ideal para grandes organizaciones con elevada descentralización, como por ejemplo en empresas transnacionales.

### 5.4. MODELO BASADO EN EL VOLUNTARIADO

61. Este modelo generalmente lo constituyen CERT “ad hoc”, donde un grupo de personas (especialistas) se unen para asesorarse, apoyarse entre sí y prestar servicio a una Comunidad de forma voluntaria. Estos CERT dependen en gran parte de la motivación de los participantes. Las redes WARP son un ejemplo de este modelo.

<sup>23</sup> Guía “Cómo crear un CSIRT paso a paso”, de ENISA



## 6. MISIÓN, COMUNIDAD, AUTORIDAD, COMPETENCIAS

62. A la hora de institucionalizarse, un CERT tiene que establecer muy claramente el marco en que deberá desarrollar su actividad. Su éxito a largo plazo dependerá del plan estratégico que se realice. Este plan o marco de referencia consistirá en definir claramente unos conceptos e ideas globales que determinen los objetivos y la evolución del equipo de respuestas ante incidentes. Los distintos elementos que dan la visión estratégica de un CERT son los siguientes:

### 6.1. MISIÓN

63. Objetivos de alto nivel que debe cumplir el CERT y que servirán para poder identificar cuáles son los servicios a ofrecer, a quién se han de ofrecer y qué criterios se deben aplicar para asignar la prioridad a sus actividades. Esta declaración debe ser explícitamente aprobada (firmada, por tanto) por la organización que patrocina su creación y debe ser comunicada al propio equipo del CERT, así como al resto de la Comunidad (tanto de Internet como a la que se da servicio). Algunos CERT han fracasado precisamente por la indefinición de estos objetivos o por la falta de compromiso de la organización patrocinadora.

### 6.2. COMUNIDAD

64. Es el público objetivo o colectivo al que están dirigidos específicamente la mayor parte de los servicios del CERT. Todo equipo de estas características se crea para servir a una Comunidad que puede ser una parte o la totalidad de una organización o incluso de varias organizaciones (en el mundo anglosajón se conoce por "Constituency").
65. Al igual que la misión, la organización patrocinadora del CERT aprobará explícitamente el tipo de Comunidad elegida. Cabe la posibilidad de que una vez concretados los servicios en base a los objetivos establecidos, esta Comunidad se subdivide en varios grupos, a los cuales se les prestará diversos niveles de asistencia. Es decir, no es necesario que todos los miembros de la Comunidad reciban los mismos servicios; pueden existir ciertos segmentos que tengan prioridad y que disfruten de ciertos privilegios a los que el resto no tiene acceso.
66. Por otra parte, no es de extrañar que una misma Comunidad pueda ser atendida por varios CERTs a la vez, aunque muy probablemente cada uno de ellos le ofrecerá un conjunto de servicios distintos. Es importante, por tanto, que el CERT determine correctamente quién pertenece a su Comunidad y en qué servicios está interesado, así como qué CERT le dan asistencia y de qué forma.
67. Asimismo, también puede considerarse a otros actores como parte de la Comunidad de un CERT (otros CERTs locales o internacionales, operadores de redes de comunicaciones, ISP, websites, etc.) con los que compartirá conocimientos y cooperará en la investigación y resolución de incidentes de manera conjunta. En muchos casos, un CERT requerirá de la asistencia o cooperación de otras organizaciones o CERT, con los cuales debe establecer una relación de confianza. En muchos casos estas redes pueden funcionar de manera voluntaria o establecer obligaciones de colaboración recíproca entre sus miembros.



### 6.3. AUTORIDAD O MODELO DE RELACIÓN CON LA COMUNIDAD

68. El modo en el que el CERT se relacione con la Comunidad y el grado de autoridad sobre las intervenciones que realice determinará enormemente el tipo y el nivel de servicios que ofrezca. Existen cuatro tipos de autoridad que un CERT puede tener sobre su Comunidad:
- **Autoridad completa:** el Equipo puede llevar a cabo todas las acciones necesarias para gestionar los incidentes; los miembros de la Comunidad deben implantar las medidas establecidas por el CERT o bien dar facilidades para que su personal las realice.
  - **Autoridad compartida:** el CERT colabora abierta y directamente con los administradores y gestores TIC de la Comunidad en la gestión directa de los incidentes, facilitando información y tomando las decisiones de manera conjunta.
  - **Autoridad nula:** no se tiene ningún tipo de autoridad sobre los miembros de la Comunidad y únicamente actúa como asesor y fuente confiable de información.
  - **Autoridad indirecta:** el equipo del CERT no tiene autoridad directa sobre la Comunidad, pero indirectamente tiene la posibilidad de ejercer presión sobre sus miembros. Este tipo de relación no está explicitada formalmente y se tratan más bien de interrelaciones que han surgido con el paso del tiempo o bien a través de una tercera organización (por ejemplo la organización patrocinadora que apoya abiertamente al CERT).
69. Dentro del modelo de relación entre el CERT y la Comunidad, otro punto a considerar es el modo en el que ambos entran en contacto. De nuevo dependerá de la misión, del tipo de Comunidad, del catálogo de servicios y también del grado de autoridad. En base a estos parámetros, el equipo deberá establecer la manera en la que se realice el contacto inicial. Existen dos modelos:
- **Relación contractual:** antes de la prestación de cualquier tipo de servicio, el CERT y cada miembro de la Comunidad establecen formalmente su relación, indicando:
    - Cuotas y formas de pago (si existen).
    - Aspectos legales respecto a la confidencialidad y la responsabilidad.
    - Acuerdos de nivel de servicio: personas de contacto, mecanismos de comunicación, horario de contacto, tiempos de respuesta, tiempos de resolución, procedimientos de escalado, etc.
  - **Relación informal:** no es necesario que el miembro de la Comunidad establezca un contacto previo con el CERT para disfrutar de ciertas prestaciones. No obstante, es posible que en algunos casos el anonimato completo no sea posible: en algunas circunstancias los administradores de sistemas, los gestores de TIC o simplemente los usuarios finales de una organización miembro de la Comunidad, deberán acceder a determinados servicios previo registro de sus datos de contacto (por ejemplo a través un servicio web).
70. Entre ambos modelos existen puntos intermedios. Puede que un CERT ofrezca algunos servicios bajo el modelo de relación informal y otros que requieran un registro formal de la relación (incluso en casos extremos puede ser obligatoria la firma de documentos que tengan implicaciones legales).

## 6.4. ORGANIZACIÓN PATROCINADORA

71. Obviamente, un CERT no nace espontáneamente sino que está promovido por una organización, pública o privada, que ha detectado la necesidad de proveer a una determinada Comunidad de la capacidad de respuesta ante incidentes de seguridad informática. Esta organización es la que se denomina Organización patrocinadora.
72. Debe indicarse que la relación del CERT, tanto con la organización patrocinadora como con la Comunidad a la que presta servicio, será fundamental en el grado de cumplimiento de los objetivos (determinados en la misión) y en el tipo de autoridad que se establezca.

## 7. CATÁLOGO DE SERVICIOS

73. Finalmente, una vez definidos los aspectos ya citados, el CERT deberá elaborar el Catálogo de Servicios que desea ofrecer a la Comunidad, descritos de forma pormenorizada (incluyendo su extensión, su nivel de asistencia o el modo en el que el cliente tendrá acceso a ellos). Deberá por lo tanto especificar los siguientes aspectos de cada uno de los servicios:
  - **Objetivo:** propósito y naturaleza del servicio.
  - **Definición:** descripción en detalle del alcance del servicio y del grado de profundidad en el que el CERT lo ofrece (por ejemplo: en la gestión de un incidente ¿el CERT llegará a intervenir en los sistemas de un miembro de la Comunidad?).
  - **Funciones:** responsabilidades de cada una de las partes (el CERT, el miembro de la Comunidad, otras partes) en la prestación del servicio.
  - **Nivel de Servicio:** descripción del grado del nivel del servicio.
  - **Parámetros de calidad** que la Comunidad puede esperar obtener del servicio.
  - **Política de comunicación:** explicación del modo en que el CERT se relacionará con cada una de las partes que intervienen en el servicio (el propio equipo, la Comunidad y otras partes). También se detallará el tipo de información que se intercambiará con cada uno.
  - **Prioridades:** grado de prioridad que otorga el CERT al servicio. Este aspecto está directamente relacionado con los puntos “Nivel de Servicio” y “Parámetros de Calidad”. Las consideraciones tenidas en cuenta constituirán una imagen de lo que debe esperar obtener la Comunidad del CERT a nivel de servicios.
74. Los servicios que un CERT puede ofrecer se suelen agrupar en tres categorías<sup>24</sup>: servicios reactivos, proactivos y los denominados “de valor añadido” o “de gestión de la calidad de la seguridad”.

<sup>24</sup> Los puntos descritos en esta sección se encuentran desarrollados en las siguientes guías: CCN-STIC 403 “Gestión de Incidentes de Seguridad”; “Handbook for Computer Security Incident Teams”, del CERT/CC; “Cómo crear un CSIRT paso a paso”, de ENISA; “A Collection of good practices for CERT quality assurance”, de ENISA y “CERT-in-a-box”, del GOVCERT.NL

Servicios Reactivos	Servicios Proactivos	Servicios de Gestión de la Calidad de la Seguridad
<ul style="list-style-type: none"> <li>Alertas y advertencias</li> <li>Tratamiento de incidentes</li> <li>Análisis de incidentes</li> <li>Respuesta a incidentes <i>in situ</i></li> <li>Apoyo a la respuesta a incidentes</li> <li>Coordinación de la respuesta a incidentes</li> <li>Tratamiento de vulnerabilidades</li> <li>Análisis de vulnerabilidades</li> <li>Respuesta a vulnerabilidades</li> <li>Coordinación de la respuesta a la vulnerabilidad</li> <li>Asistencia remota a vulnerabilidades e incidentes</li> </ul>	<ul style="list-style-type: none"> <li>Comunicados y anuncios</li> <li>Observatorio de tecnología</li> <li>Evaluaciones o auditorías de la seguridad</li> <li>Configuración y mantenimiento de la seguridad</li> <li>Desarrollo de herramientas de seguridad</li> <li>Servicios de detección de intrusos</li> <li>Difusión de información relacionada con la seguridad</li> <li>Programas de gestión de listas de configuración segura de sistemas TIC</li> <li>Monitorización de redes</li> </ul>	<ul style="list-style-type: none"> <li>Análisis de riesgos</li> <li>Continuidad del negocio y recuperación ante desastres</li> <li>Consultoría de seguridad</li> <li>Sensibilización</li> <li>Educación / Formación</li> <li>Evaluación o Certificación de productos</li> </ul>

Figura 7-1.: Lista de servicios tradicionales de un CERT.

	CCN-CERT	CERTA	CPNI	CERT-Bund	GOVCERT	US-CERT	CERT.br
	(ESP)	(FR)	(UK)	(DE)	(NL)	(USA)	(BR)
<b>CONTENIDOS</b>							
Inform. del CERT	✓	✓	✓	✓	✓	✓	✓
FAQ	✓		✓			✓	✓
Misión y objetivos	✓	✓		✓	✓	✓	✓
Información contacto	✓	✓	✓		✓	✓	✓
Eventos	✓					✓	
Documentos	✓	✓	✓	✓	✓	✓	✓
Herramientas	✓		✓				✓
Avisos vulnerabilidades	✓	✓	✓			✓	✓
Noticias/ Notas de seguridad	✓	✓	✓		✓	✓	✓
Indicadores /estadística	✓					✓	✓
Enlaces (sitios relacionados)	✓	✓	✓			✓	✓
<b>FUNCIONALIDADES</b>							
Novedades	✓					✓	
Mapa del sitio	✓		✓	✓			✓
Multilingüe	Sí (inglés + cooficiales)			Sí (inglés)	Sí (inglés)		Sí (inglés)
Motor de búsqueda	✓	✓		✓	✓	✓	✓
Base de conocimiento de vulnerabilidades	✓					✓	
Reporte online de incidentes	✓					✓	
Zona de acceso restringido	✓					✓	
Listas de distribución por correo	✓					✓	✓
Publicación por RSS	✓	✓				✓	

Figura 7.2.: Ejemplos de servicios prestados por algunos CERT. Fuente: elaboración propia y FIRST

## 7.1. EL PROCESO DE GESTIÓN DE INCIDENTES

75. Dado que la capacidad de gestión y respuesta a incidentes es la actividad principal de un CERT, el proceso de gestión de incidentes es el proceso clave de éste. Un CERT deberá desarrollar un proceso formal y coherente de gestión de incidentes que incluya los siguientes pasos:
- Detección de eventos que puedan reflejar actividades maliciosas de acuerdo a los niveles de prioridad y criterios de detección reflejados previamente por los responsables del área de gestión de incidentes. Estos eventos pueden haber sido resultado de una investigación inicial (monitorización de redes) o de las notificaciones recibidas de distintas fuentes (entre otras la propia Comunidad a la que se presta el servicio).
  - Discernimiento entre eventos interesantes, irrelevantes y falsos positivos.
  - Registro de casos en un sistema de gestión de incidentes (ticketing) con una información mínima: identidad del informante, fecha y hora de la llamada, miembro de la Comunidad a la que hace referencia, descripción de la situación notificada, etc.
  - En una segunda fase (segundo nivel) y una vez identificado un incidente, comenzará la fase de triaje en la que se debería determinar:
    - Confirmar que no es un falso positivo,
    - Correlar la información recibida con el resto de información del sistema de gestión,
    - Crear un nuevo incidente o enlazar el ticket en otro ya existente,
    - Asignar el ticket al POC afectado sin enviarle aún información,
    - Clasificar el incidente según una clasificación establecida previamente,
    - Priorización del incidente.
  - Una vez identificado un incidente, y adecuadamente clasificado y priorizado, se procederá al Registro y Notificación del mismo a las partes afectadas (miembros de la Comunidad y/o otras organizaciones externas)
  - En una cuarta fase, y una vez notificadas las partes afectadas por un incidente, se realizará el seguimiento del mismo y su cierre final. En dicho seguimiento se colaborará en la contención de los daños, erradicación de las causas o efectos adversos e implantación o mejora de controles de seguridad para la prevención de nuevos incidentes del mismo tipo. De igual modo, se colaborará con las entidades afectadas para la pronta notificación de incidentes de gran envergadura que se extendieran fuera del ámbito de la Comunidad.
76. No obstante, para un desarrollo en profundidad de este apartado se puede consultar la Guía CCN-STIC 403<sup>25</sup> de Gestión de Incidentes de Seguridad Informáticos.

<sup>25</sup> Guía de Seguridad de las TIC (CCN-STIC) Gestión de Incidentes de Seguridad Informáticos

## 8. ÁMBITOS DE ACTUACIÓN DE LOS CERT

77. En la actualidad existen en todo el mundo más de 250 CERT<sup>26</sup> pertenecientes a los distintos ámbitos de la sociedad y de diferentes organizaciones (públicas y privadas). En términos generales, estos equipos se clasifican atendiendo a su Comunidad, diferenciándose entre:

### 8.1. CERT PARA EL SECTOR DE LAS PYMES

78. Por el tamaño de las empresas es poco viable que las organizaciones clasificadas en este segmento puedan implementar de forma individual las funciones de un CERT. Surge, por tanto, la necesidad de aunar esfuerzos y ofrecer los servicios de un único CERT a varias PYMES (por parte de un equipo público o privado). Un ejemplo es el creado en España por el Instituto Nacional de Tecnologías de la Comunicación, sociedad anónima estatal adscrita al Ministerio de Industria, el INTECO-CERT, que dirige sus servicios a PYMES y ciudadanos.

### 8.2. CERT ACADÉMICO

79. El área de responsabilidad de este tipo de equipos se circunscribe a entidades académicas. Su tamaño puede variar: desde CERT interacadémicos (por ejemplo IRIS-CERT), a equipos dedicados a una escuela, facultad o instituto, pasando por CERT a cargo de toda una universidad (como por ejemplo esCERT-UPC en su origen). La dimensión de la Comunidad condicionará los servicios que ofrezcan, el modo en que lo hagan y su grado de intervención directa en el campo.

### 8.3. CERT COMERCIAL

80. Estos centros prestan distintos servicios a cambio de una contraprestación económica. Habitualmente utilizan acuerdos de servicios específicos con cada miembro (cliente) de su Comunidad.

### 8.4. CERT DE PROVEEDOR

81. Se centra en los productos o servicios específicos de un proveedor. Su objetivo es proveer servicios y soluciones para eliminar o reducir el impacto negativo de las vulnerabilidades de estos productos o servicios, ya sea un producto tecnológico o un servicio TIC como, por ejemplo, los servicios de telecomunicaciones.

### 8.5. CERT DEL SECTOR MILITAR

82. Prestan servicios a organizaciones militares con responsabilidades en infraestructuras TIC necesarias con fines de defensa. Su Comunidad está conformada por las instituciones militares y de entidades estrechamente relacionadas con éstas como, por ejemplo, del Ministerio de Defensa.

<sup>26</sup> En julio de 2011 estaban afiliados al FIRST (Forum of Incident Response and Security Teams) un total de 247 equipos, una cifra que será sensiblemente mayor.



## 8.6. CERT PARA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

83. Los CERT de este sector se centran principalmente en la protección de las infraestructuras críticas y de las infraestructuras críticas de la información (Administración, Centrales y redes de energía, Tecnologías de la información y las comunicaciones, Sistema Financiero y Tributario, Sector sanitario, Espacio, Instalaciones de Investigación, Alimentación, Agua, Transportes, Industria Nuclear e Industria Química)<sup>27</sup>.

## 8.7. CERT GUBERNAMENTAL

84. Bajo esta denominación se sitúan los equipos cuyo principal objetivo es asegurar la infraestructura TIC de un Gobierno/Estado y los servicios ofrecidos a la población (al fin y al cabo es a los gobiernos a los que compete en última instancia garantizar la seguridad y el bienestar de los ciudadanos<sup>28</sup>). La Comunidad a la que están dirigidos son las administraciones públicas y sus distintos organismos. A su vez, esta Comunidad puede dar servicio, de acuerdo a cada país y/o CERT particular (y a la organización que los patrocina), a la administración local, autonómica, central o a todas ellas. Estos CERT gubernamentales generalmente forman parte y están patrocinados por instituciones del Estado.
85. De acuerdo a la forma en que un país ordena su funcionamiento, estos equipos pueden combinarse. Por ejemplo, en un CERT militar puede ser parte de un CERT gubernamental, mientras en otro, el CERT militar es independiente.
86. Muchos gobiernos están tratando de agrupar y coordinar sus iniciativas o sus CERT bajo una estrategia común para lograr una mayor eficiencia y efectividad en la respuesta ante incidentes y gestión de crisis. Esto ha llevado a la búsqueda de modelos de colaboración y alianzas entre CERT, tanto dentro del propio Estado, como entre el sector público y privado. Estos esfuerzos de coordinación son el primer paso hacia la conformación de un CERT Nacional.
87. En el caso de España, el CCN-CERT es el CERT Gubernamental, según se recoge en el RD 3/2010 (ENS) en sus artículos 36, Capacidad de respuesta a incidentes de seguridad de la información, y 37, Prestación de servicios de respuesta a incidentes de seguridad a las Administraciones Públicas.

## 8.8. CERT NACIONAL

88. Este es un equipo con responsabilidad general de coordinación sobre todos los sectores y tiene una amplia responsabilidad sobre prácticamente todos los puntos tratados anteriormente. Este centro funciona como punto focal de contacto tanto en el entorno nacional como para requerimientos internacionales. ENISA, en un documento elaborado en diciembre de 2009, donde se establecen las capacidades básicas que debe tener un CERT nacional/gubernamental<sup>29</sup>, ofrece una definición informal de CERT Nacional, como aquel que actúa como el Punto Nacional de Contacto (POC) con otros CERT nacionales y/o internacionales. De hecho, podría considerarse como “CERT del último recurso”, por su papel de coordinación. En muchos casos el CERT nacional también actúa como CERT gubernamental o tiene su origen en él. De igual modo, señala

<sup>27</sup> Sectores recogidos en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas en España.

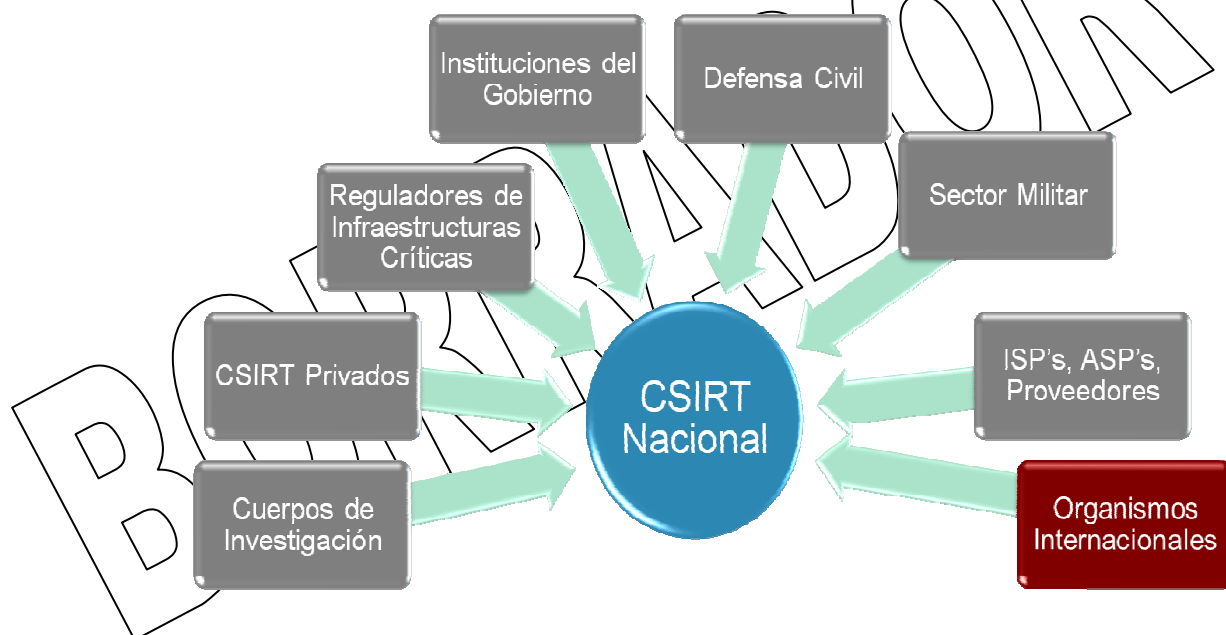
<sup>28</sup> Comunicado de la Comisión de la Unión Europea al Parlamento (Bruselas, 30.03.2009, COM (2009)

<sup>29</sup> Baseline capabilities for national / governmental CERT (diciembre de 2009). ENISA



el documento, el CERT nacional de facto suele ser aquel que ha sido establecido primero por un Gobierno y actúa como contacto con otros países.

89. En la mayoría de los casos, estos CERT atienden a la comunidad de CERT en su país, y asumen la responsabilidad de coordinación de otros CERT en el ámbito nacional. Los CERT nacionales generalmente han evolucionado de los CERT gubernamentales como una consecuencia lógica de la ampliación de sus servicios. Así, por ejemplo, la Unión Europea ha señalado en diversas ocasiones la necesidad de contar con Equipos nacionales o gubernamentales de respuesta a incidentes de seguridad (sin decantarse por una u otra definición) que dispongan de una base común en términos de capacidad y que actúen como catalizadores nacionales de los interesados y de su capacidad para realizar actividades públicas. Esta “gran capacidad de alerta temprana y respuesta a incidentes”<sup>30</sup> debería participar de manera efectiva en la cooperación transfronteriza y en el intercambio de información con otras organizaciones existentes, como el EGC Group o Grupo de CERT gubernamentales europeos. (Véase capítulo 6.7 “Organizaciones Internacionales”).



**Figura 8.1. CSIRT Nacional, como centro de coordinación**

90. Cada CSIRT es único, en el sentido de que establece sus operaciones, su organización y su imperativo legal para satisfacer las necesidades de su país y su comunidad. Frente a esto, todos los CSIRT tienen un objetivo común, mantener seguras las redes de sus países. De este modo podemos concluir que, aunque cada CSIRT utiliza herramientas y procedimientos diferentes, todos comparten el mismo objetivo. Esto es así según la Autoridad Regulatoria de las Comunicaciones finlandesa, que en 2008 llevó a cabo un estudio basado en entrevistas y análisis a once CSIRT nacionales<sup>31</sup>. Según este informe, las capacidades encontradas en todos los CSIRT estudiados, serían:

<sup>30</sup> Comunicado de la Comisión de la Unión Europea al Parlamento (Bruselas, 30.03.2009, COM (2009)

<sup>31</sup> Los datos de este estudio han sido extraídos a partir del análisis de 11 CSIRTs nacionales europeos: CERTA (Francia), CERT-Bund (Alemania); CERT Estonia (Estonia); CERT-FI (Finlandia); CERT-Hungary (Hungría); CSIRT-UK (Reino Unido); DK-CERT (Dinamarca); GovCERT.NL (Holanda); NorCERT (Noruega); SITIC (Suecia) y SWITCH-CERT (Suiza). Más información acerca del estudio en Anexo B – Referencias.

<sup>31</sup> <https://eu2009.pts.se/Documents/PTS%20Resilience%20Conference%20-%20Erka%20Koivunen.pdf?epslanguage=en-GB>

- Designar un punto de contacto para la coordinación de la respuesta a incidentes.
  - Construir y mantener una red de contactos extensa, tanto nacional como internacional.
  - Monitorización de la situación actual y mejora de la concienciación.
91. Este mismo documento señala que la constitución de un CERT nacional/gubernamental no es la única medida a tener en cuenta en una estrategia de ciberseguridad completa por parte de un Estado, pero sí una parte importante de la misma, teniendo en cuenta, además, que este tipo de equipos deberían asumir, además, la responsabilidad de la Protección de las Infraestructuras Críticas de Información (CIIP).
92. Para concretar todo lo dicho con anterioridad, acudiremos de nuevo al documento elaborado por ENISA, que divide en cuatro grupos las aptitudes que un CERT Nacional debe reunir en un primer momento, creadas a partir del consenso y estudio de los CERT existentes en los estados miembros.

- **Catálogo de Servicios:** Cubre los servicios que el equipo proporciona a su Comunidad o utiliza para su propio funcionamiento interno. La única categoría de servicios que un CERT Nacional, según el documento de ENISA anteriormente mencionado, debe ofrecer a su Comunidad en un primer momento es la Gestión, Análisis y Comunicación de Incidentes. Como máxima prioridad se aconseja que el equipo ofrezca avisos y alertas, así como comunicados, tanto reactivos como proactivos.

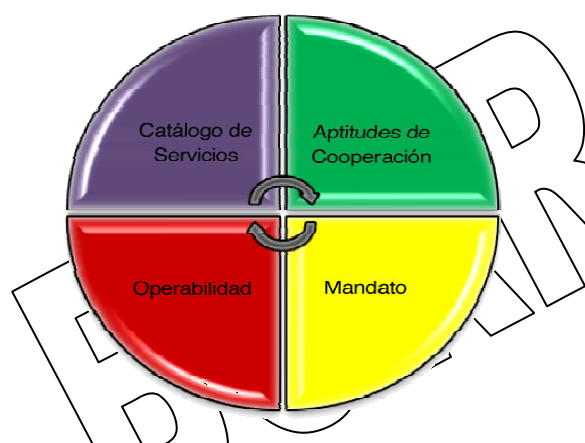


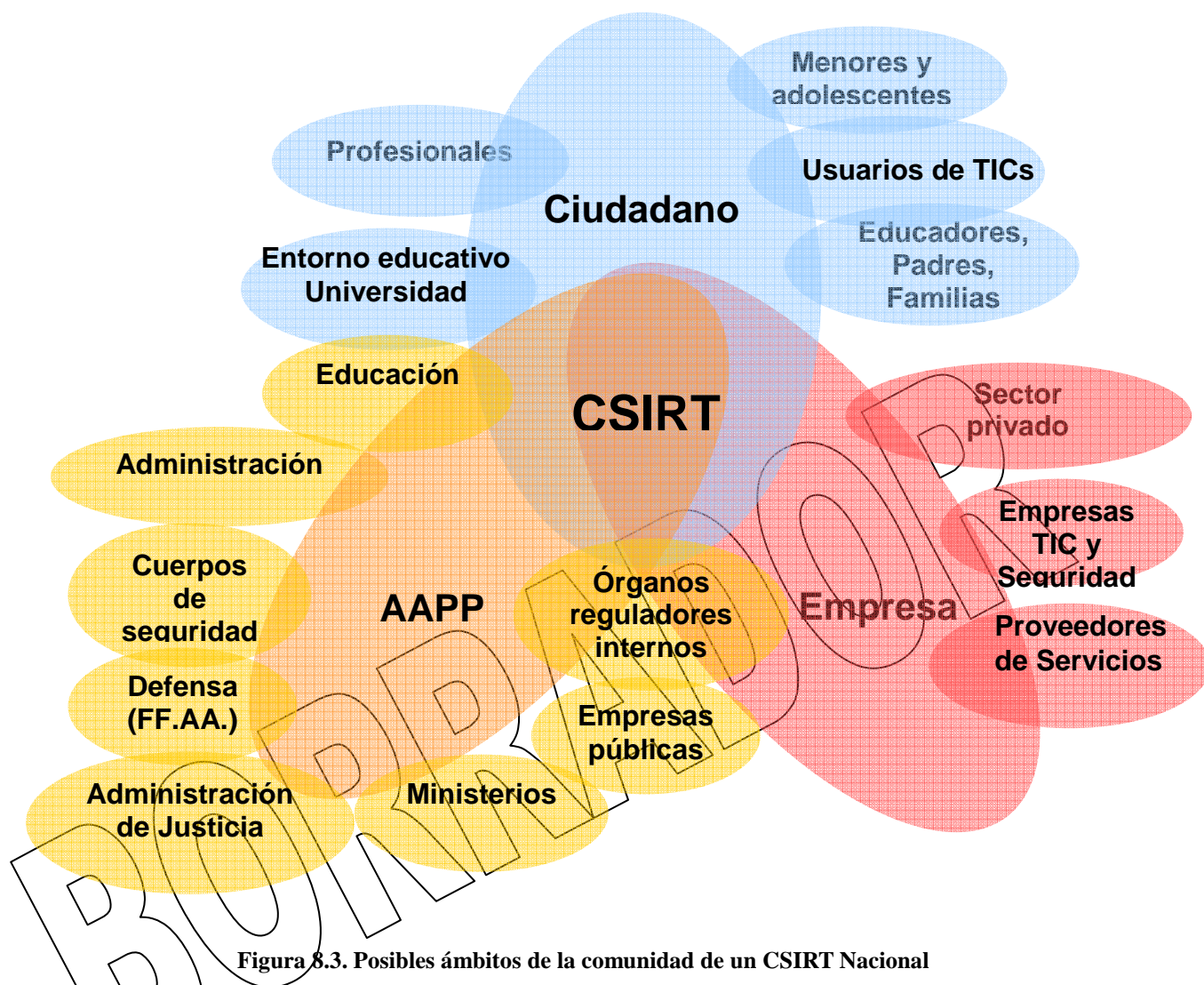
Figura 8-2 Aptitudes básicas del CERT Nacional. Fuente: ENISA

- El intercambio de información relativa a la seguridad, tanto de carácter inmediato para amenazas o emergencias cercanas, como a medio y largo plazo para reforzar la concienciación, es un recurso de gran valor añadido para la Comunidad del CERT que, además, supone relativamente poco esfuerzo. Notificaciones de seguridad y otras informaciones exclusivas refuerzan, al mismo tiempo, la visibilidad del CERT, aumentando su posicionamiento en cuanto a confianza y capacidades. La guía aconseja que, en un primer momento, el CERT opte por externalizar servicios de menor inmediatez.
- **Mandato / marco de trabajo:** Cubre la autoridad y la justificación que el gobierno respectivo le otorga al equipo para poder desarrollar sus funciones. Es crucial la existencia de una orden oficial que adjudique al CERT Nacional la labor de representar al equipo en las comunidades de CERT y a nivel nacional para proteger las Infraestructuras Críticas del país. ENISA recomienda que no sea el CERT Nacional quien se haga cargo de todos los incidentes a nivel nacional, sino que estudie el panorama de CERT existente y trate de integrarse en él, maximizando la eficiencia en las comunicaciones y el intercambio de información.
- **Aptitud operativa/Operabilidad:** Cubre los requisitos técnicos y operacionales que el equipo debe cumplir. Asimismo, ENISA aconseja que el número mínimo de integrantes para implantar un CERT no baje de 6 a 8 personas ocupadas a tiempo completo. Entre ellos deben figurar un jefe de equipo y un gestor de incidentes senior. El CERT debe estar disponible

24/7/365 tanto para su Comunidad como para cooperar con socios nacionales e internacionales. Es crucial cumplir un tiempo de respuesta mínimo en la respuesta a incidentes.

- **Capacidades de Cooperación:** Incluye los requisitos relativos al intercambio de información con otros equipos y que no se vean satisfechas con las otras tres categorías. Además de dotar al CERT con equipos tecnológicos y humanos, uno de los activos más valiosos de los que dispondrá para desarrollar sus funciones en general y específicamente las de cooperación, será el conocimiento de sus miembros. Conocimiento y reputación serán las piedras angulares para crear y reforzar la confianza del CERT. ENISA aconseja una integración temprana en las comunidades de CERT nacionales e internacionales. Algunos retos a los que se enfrentan los CERT en esta mayor coordinación e integración a nivel nacional e internacional, que exigen de grandes esfuerzos y recursos, son:

- La normalización de la información intercambiada, y el uso de estándares abiertos.
- La utilización de terminologías parecidas en los distintos estados.
- El establecimiento de esquemas de respuesta similares.
- La clasificación de la información sensible.
- El uso de mecanismos seguros de comunicación.



## 8.9. CERT AUTONÓMICO

93. Son aquellos Equipos desarrollados e implantados por los gobiernos de distintas comunidades autónomas cuyas responsabilidades son diferentes, pudiéndose referir a los sistemas de la administración autonómica y/o local, así como tener otras misiones de asistencia a empresas y ciudadanos. En este caso, y a fecha de publicación de esta Guía, se habían creado y reconocido el CSIRT-CV, de la Generalitat Valenciana; el CESICAT (CERT de la Generalitat de Catalunya) y estaban en fase de despliegue/desarrollo el Andalucía-CERT.

## 9. RESPONSABILIDADES EN EL CIBERESPACIO ESPAÑOL

94. La preocupación por la ciberseguridad y por los sistemas de información no es nueva en nuestro país. Tampoco lo es la apuesta por la Sociedad de la Información y por la necesidad de compaginarla con la seguridad de las TIC y la confianza que se debe generar en el ciudadano para conseguir su desarrollo pleno. Así, durante los últimos años, la legislación y los diferentes organismos públicos han ido adaptándose a los nuevos retos y amenazas provenientes de Internet, con todo tipo de medidas.
95. En nuestro país, la dirección y coordinación de las políticas de Seguridad de la Información recaen principalmente en los siguientes ministerios: Ministerio de Defensa, Ministerio de Industria, Turismo y Comercio y Ministerio de Política Territorial y Administración Pública.
96. En relación con la lucha contra la delincuencia electrónica, y la protección de las infraestructuras críticas, cabe también destacar el Ministerio del Interior y en especial las tareas llevadas a cabo por las unidades de ciberseguridad y delitos informáticos de los diferentes Cuerpos y Fuerzas de Seguridad del Estado, incluidos los cuerpos de seguridad autonómicos y locales, así como por el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC).

### 9.1. MINISTERIO DE DEFENSA

97. Corresponde al Ministerio de Defensa el ejercicio de todas las competencias y atribuciones que le confiere el ordenamiento jurídico como órgano encargado de la ordenación, coordinación y ejecución de las directrices generales del Gobierno sobre política de defensa. Este Ministerio dispone de un elevado número de sistemas clasificados y gestiona diversos sistemas de intercambio de información y mando y control con OTAN. Como órgano superior, de la Secretaría de Estado de Defensa cuenta, además, con los siguientes otros organismos adscritos:

- **Centro Nacional de Inteligencia**

El Centro Nacional de Inteligencia, CNI, regulado por la Ley 11/2002, de 6 de mayo, tiene como principal misión proporcionar al Presidente del Gobierno y al Gobierno de la nación las informaciones, análisis, estudios o propuestas que permitan prevenir y evitar cualquier peligro, amenaza o agresión contra la independencia o integridad territorial de España, los intereses nacionales y la estabilidad del Estado de derecho y sus instituciones.

Aunque depende orgánicamente del Ministerio de Defensa, en la seguridad de la información clasificada y en el ámbito de la ciberdefensa tiene encuadrados a organismos que tienen misiones que afectan a todas las administraciones públicas. Entre otras funciones del Centro, tal y como fija la citada Ley, se encuentran: coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las tecnologías de la información en ese ámbito, informar sobre la adquisición coordinada de material criptológico y formar al personal, propio o de otros servicios de la Administración, especialista en este campo para asegurar el adecuado cumplimiento de las misiones del Centro. De igual forma, el CNI debe de velar por el cumplimiento de la normativa relativa a la protección de la información clasificada.

- **Centro Criptológico Nacional**

El CCN fue creado en el año 2004, a través del Real Decreto 421/2004, adscrito al Centro Nacional de Inteligencia. A su vez, a él están adscritos el Organismo de Certificación (OC) del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la



Información (ENECSTI) y la Capacidad de Respuesta a Incidentes de Seguridad de la Información en la Administración Pública, CCN-CERT. Dicho RD determina la misión, funciones y ámbito de competencia del CCN

#### ▪ CCN-CERT

Creado a finales de 2006, en el seno del Centro Criptológico Nacional, la Capacidad de Respuesta a Incidentes del CCN, CCN-CERT, tiene como principal objetivo contribuir a la mejora del nivel de seguridad de los sistemas de información de las administraciones públicas españolas (general, autonómica y local). Tiene responsabilidades en ciberataques sobre sistemas clasificados, sistemas de las distintas administraciones públicas y, en coordinación con el CNPIC, sobre sistemas que gestionen infraestructuras críticas. Proporciona el estado de la amenaza en ciberseguridad para Presidencia del Gobierno.

Además, y siendo el CERT Gubernamental/Nacional de España, tiene entre sus potestades, recogidas en el Real Decreto 3/2010 en el que se desarrolla el Esquema Nacional de Seguridad, el coordinar con otras administraciones públicas, la promoción y creación de capacidades de respuesta a incidentes, teniendo él asignado el papel de coordinador público estatal.

Los servicios que el CCN-CERT prestará a las Administraciones Públicas, siguiendo este RD, se establecen de la siguiente forma:

- Soporte y coordinación para el tratamiento de vulnerabilidades y la resolución de incidentes de seguridad que tengan la Administración General del Estado, las Administraciones de las comunidades autónomas, las entidades que integran la Administración Local y las Entidades de Derecho público con personalidad jurídica propia vinculadas o dependientes de cualquiera de las administraciones indicadas.
- Investigación y divulgación de las mejores prácticas sobre seguridad de la información entre todos los miembros de las Administraciones públicas. Con esta finalidad, las series de documentos CCN-STIC (Centro Criptológico Nacional-Seguridad de las Tecnologías de Información y Comunicaciones), elaboradas por el Centro Criptológico Nacional, ofrecerán normas, instrucciones, guías y recomendaciones para aplicar el Esquema Nacional de Seguridad y para garantizar la seguridad de los sistemas de tecnologías de la información en la Administración.
- Formación destinada al personal de la Administración especialista en el campo de la seguridad de las tecnologías de la información, al objeto de facilitar la actualización de conocimientos del personal de la Administración y de lograr la sensibilización y mejora de sus capacidades para la detección y gestión de incidentes.
- Información sobre vulnerabilidades, alertas y avisos de nuevas amenazas a los sistemas de información, recopiladas de diversas fuentes de reconocido prestigio, incluidas las propias.

## 9.2. MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

98. Este Ministerio, a través de su Secretaría de Estado de Telecomunicaciones y Sociedad de la Información, tiene entre otras misiones, la de relacionarse con los operadores de telecomunicaciones, la gestión de nombres del dominio .es, la capacidad de dictar normas sobre interceptación legal de comunicaciones y el desarrollo de la Sociedad de la Información con el plan AVANZA. En dicho Plan, en su Anexo I, se menciona el desarrollo de una red de centros de seguridad cuyo principal objetivo sea crear una infraestructura básica de centros de alerta y

respuesta ante incidentes de seguridad que atienda a las demandas específicas de los diferentes segmentos de la sociedad. Sectores críticos, agencias gubernamentales, Administración Pública, PYMES, grandes corporaciones y ciudadanos deberían recibir, según el citado Plan, el adecuado asesoramiento por parte de estos centros. En este sentido, se habla de la creación de centros de seguridad y de establecer los procedimientos y protocolos que permitan coordinar sus funciones y actuaciones. En este mismo texto se adelanta la creación de un CERT para la Administración/Gubernamental.

#### ▪ Red.es

Red.es es la Entidad Pública Empresarial adscrita al MITyC encargada de impulsar el desarrollo de la Sociedad de la Información en España y ejecutar proyectos en el marco del Plan Avanza de acuerdo a las prioridades estratégicas de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI), trabajando con Comunidades Autónomas, Diputaciones, Entidades Locales y el sector privado en materia de tecnologías de la información y comunicaciones.

#### ▪ RedIris

Red que cuenta con unas 250 instituciones afiliadas, principalmente Universidades y Organismos Públicos de Investigación, que llegan a formar parte de esta comunidad mediante la firma de un acuerdo de afiliación. Los servicios de comunicaciones que RedIRIS ofrece a la comunidad académica y científica española, requieren el soporte de una infraestructura básica de transporte adaptada tecnológicamente a las necesidades de los centros e instituciones usuarias.

#### ▪ INTECO

El Instituto Nacional de Tecnologías de la Comunicación (INTECO) tiene como misión impulsar y desarrollar proyectos de innovación relacionados con el sector de las Tecnologías de la Información y la Comunicación (TIC) y en general, en el ámbito de la Sociedad de la Información, que mejoren la posición de España y aporten competitividad, extendiendo sus capacidades tanto al entorno europeo como al latinoamericano.

### 9.3. MINISTERIO DE POLÍTICA TERRITORIAL Y ADMINISTRACIÓN PÚBLICA

99. Este Ministerio<sup>32</sup> preside el Consejo Superior de Administración Electrónica y, a través de éste, debe promover la colaboración y cooperación con las comunidades autónomas y las entidades locales para la puesta en marcha de servicios públicos interadministrativos. Para ello preside la conferencia sectorial de las AAPP que reúne a todas las CCAA y la conferencia nacional de la Administración local (para ayuntamientos de más de 140.000 habitantes). Además debe impulsar las actividades de cooperación de la Administración General del Estado con la Unión Europea, con las organizaciones internacionales y, especialmente, con Iberoamérica, en materia de tecnologías de la información y Administración electrónica, en colaboración con el Ministerio de Asuntos Exteriores y de Cooperación. Por otro lado, gestiona la red SARA<sup>(33)</sup>.

<sup>32</sup> Funciones han sido desarrolladas por el anterior Ministerio de Administraciones Públicas y posteriormente en el Ministerio de Presidencia. En la última remodelación del gobierno de octubre de 2010 estas competencias se han traspasado al Ministerio de Política territorial y Administración Pública

<sup>33</sup> Sistemas de Aplicaciones y Redes para las Administraciones (SARA). Artículo 43. Ley 11/2007 de 22 junio. Acceso de los ciudadanos a los servicios públicos. Establece la interconexión de las diferentes Administraciones para intercambio de información y servicios y para la interconexión con la Unión Europea y otros Estados miembros. [www.ctt.map.es/web/proyectos/redsara](http://www.ctt.map.es/web/proyectos/redsara)



100. Del Ministerio de la Presidencia emanó en su día el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

## 9.4. MINISTERIO DEL INTERIOR

101. La Secretaría de Estado de Seguridad es el organismo que, en este Ministerio, tiene competencia en el ciberespacio a través del Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), y de las unidades encargadas de la ciberdelincuencia y en las Fuerzas y Cuerpos de Seguridad del Estado.

### ▪ CNPIC

Tras la aprobación en diciembre de 2004 por parte del Consejo Europeo, de un Programa Europeo de Protección de Infraestructuras Críticas (PEPIP), La Secretaría de Estado de Seguridad puso en marcha el Plan Nacional de Protección de Infraestructuras (PPI) y el Catálogo Nacional de Infraestructuras Estratégicas, cuya custodia pertenece al Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC), creado mediante un acuerdo en Consejo del Ministros de fecha 2 de noviembre de 2007. Dicho catálogo es el instrumento que contiene toda la información y valoración de las Infraestructuras estratégicas del país, entre las que se hallan incluidas aquellas clasificadas como Críticas o Críticas Europeas según el reglamento de la Directiva de la UE 2008/114/CE, del 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.

Posteriormente, se publicó la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras que fijan y el Real Decreto 704/2011, de 29 de mayo, por el que se aprueba el reglamento para la protección de las IC, en donde se regulan las obligaciones tanto del Estado como de los Operadores de dichas infraestructuras.

La citada Ley menciona doce los sectores estratégicos acogidos a esta categoría:

- Centrales y redes de energía
- Tecnologías de la información y las comunicaciones
- Sistema Financiero y Tributario (por ejemplo, banca, valores e inversiones)
- Sector sanitario
- Espacio
- Instalaciones de Investigación
- Alimentación
- Agua (embalses, almacenamiento, tratamiento y redes)
- Transportes (aeropuertos, puertos, instalaciones intermodales, ferrocarriles y redes de transporte público, sistemas de control del tráfico)
- Industria Nuclear
- Industria Química
- Administración (servicios básicos, instalaciones, redes de información, activos, y principales lugares y monumentos nacionales)

El Centro Criptológico Nacional (CCN) apoya al CNPIC en el tratamiento de los ciberataques sobre infraestructuras críticas y en la actualización de información sobre vulnerabilidades SCADA e incidentes de seguridad informáticos relacionados con infraestructuras críticas.

## 10. CERT NACIONALES

102. A partir de las actuaciones llevadas a cabo por los citados ministerios y por otras organizaciones tanto público como privadas, en España han ido surgiendo distintas iniciativas de Equipos de Respuesta a Incidentes:

### 10.1. CCN-CERT



103. El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN), dependiente del Centro Nacional de Inteligencia (CNI). Este servicio se creó en 2006 como CERT gubernamental español y su principal objetivo es contribuir a la mejora del nivel de seguridad de los sistemas de la información de las tres administraciones públicas existentes en España (general, autonómica y local) y coordinar, a nivel público estatal, los distintos equipos de respuesta, tal y como recoge el RD 3/2010 (ENS) en sus artículos 36 y 37.

104. Tiene responsabilidades, como ya se ha citado, en ciberataques clasificados, sistemas de las distintas administraciones públicas y, en coordinación con el CNPIC, sobre sistemas que gestionen infraestructuras críticas. Proporciona

### 10.2. INTECO-CERT



105. El Centro de Respuesta a Incidentes en Tecnologías de la Información para PYMES y Ciudadanos (INTECO-CERT) nació a mediados de 2007 con la misión de prestar servicio a PYMES y ciudadanos en materia de seguridad. Sirve de apoyo al desarrollo del tejido industrial nacional y ofrece los servicios clásicos de un Centro de Respuesta a Incidentes, dando soluciones reactivas a incidentes de seguridad informáticos, servicios de prevención frente a posibles amenazas y servicios de información, concienciación y formación en materia de seguridad.

### 10.3. IRIS-CERT



106. El servicio de seguridad de RedIRIS (IRIS-CERT) tiene como finalidad la detección de problemas que afecten a la seguridad de las redes de centros de RedIRIS, así como la actuación coordinada con estos centros para poner solución a estos problemas. También se realiza una labor preventiva, avisando con tiempo de problemas potenciales, ofreciendo asesoramiento a los centros, organizando actividades de acuerdo con los mismos, y ofreciendo servicios complementarios.

#### 10.4. CSIRT-CV

107. Centro de Seguridad TIC de la Comunidad Valenciana, puesto en marcha por esta autonomía en 2007, dentro de su plan estratégico de telecomunicaciones avanzadas denominado Avantic. Su Comunidad son los ciudadanos, PYMES y Administración Pública de la Comunidad Valenciana, ofreciendo especial atención a esta última.



#### 10.5. CENTRE DE SEGURETAT DE LA INFORMACIÓ DE CATALUNYA



108. Es el organismo ejecutor del Plan Nacional de impulso de la Seguridad TIC aprobado por el gobierno de la Generalitat de Cataluña el 17 de marzo de 2009. Este plan se estructura en torno a cuatro objetivos estratégicos: Ejecutar la estrategia de seguridad TIC establecida por el Gobierno de la Generalitat, soporte a la protección de las infraestructuras críticas TIC nacionales, promoción de un tejido empresarial catalán sólido en seguridad TIC e incrementar la confianza y protección de la ciudadanía catalana en la sociedad de la información.

#### 10.6. ANDALUCÍA-CERT

109. Centro especializado y orientado a la prevención, detección y respuesta a incidentes y amenazas de seguridad en el ámbito de la administración, el sector empresarial y la ciudadanía de la Comunidad Autónoma de Andalucía. Su desarrollo está contemplado en la política de seguridad de las TIC en la Junta de Andalucía (aprobada por Decreto en enero de 2011)<sup>34</sup>.

#### 10.7. OTROS CERT

110. Existen otros CERT y centros operativos de seguridad que ofrecen servicios a otros sectores. Entre ellos cabe mencionar: e-la Caixa-CSIRT, es-CERT (Universidad Politécnica de Cataluña) Mapfre CCG-CERT, S21Sec-CERT, TB-Security-CERT....

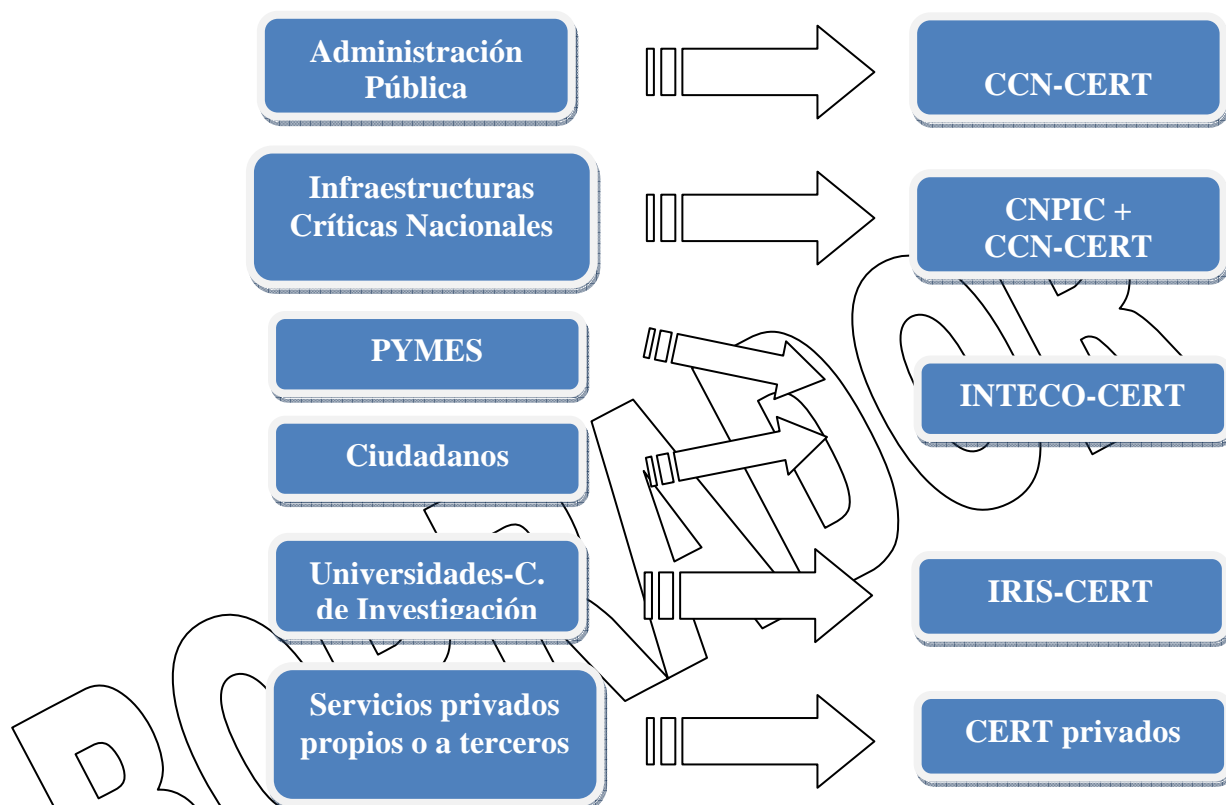
<sup>34</sup> Boletín Oficial de la Junta de Andalucía de 18/01/2011 <http://www.juntadeandalucia.es/boja/boletines/2011/11/d/2.html>

## 11. MODELO DE RELACIÓN DE LOS CERT EN ESPAÑA

111. Debido a la naturaleza integradora e interdependiente de la Sociedad de la Información, los incidentes de seguridad no dejan de ser una responsabilidad compartida, que afecta a gobiernos, empresas y todo tipo de organizaciones e incluso usuarios individuales. De hecho, el alcance de la seguridad de la información es tan amplio, que afecta a cualquier agente que desarrolle, posea, provea, gestione o utilice sistemas de información y redes de comunicaciones en general.
112. Si al alcance mencionado, se suma la naturaleza transnacional y la disparidad en el origen de los ciberataques, podemos concluir que los centros o equipos encargados de responder y mitigar los incidentes de seguridad están obligados a entenderse, compartir objetivos (independientemente de su oferta y la Comunidad a la que presta servicios) y, sobre todo, coordinarse y colaborar, tanto en el ámbito estatal como internacional. No en vano, la tendencia general apunta a una proliferación creciente en cuanto al número de CERT, por lo que, a medida que aumente su número se incrementará la necesidad de coordinación entre ellos, especialmente en la gestión y resolución de incidentes.
113. Entre las ventajas de una estrecha colaboración entre este tipo de Equipos se encuentran:
- Incremento del alcance de actuación mediante la coordinación de incidentes con otros centros, con un efecto multiplicador evidente de cara a cada Comunidad
  - Aprovechamiento de sinergias y economías de escala en aspectos concretos como las fuentes de información, infraestructuras comunes de información, publicación de alertas y amenazas, etc.
  - Intercambio de buenas prácticas entre todas las partes interesadas
  - La agilidad, flexibilidad y rapidez en el escalado de problemas de seguridad, compartiendo fuentes y contactos entre los distintos equipos.
  - Apoyo operativo a la actuación de otros centros
  - Respuestas más rápidas y eficaces ante los incidentes, impidiendo su propagación y mitigando sus daños
  - Diseño conjunto de protocolos de actuación que permitan coordinar y reaccionar con rapidez ante emergencias.
  - Realización de ejercicios conjuntos que permitan conocer las capacidades de reacción y las distintas hipótesis posibles en un ciberataque, así como la mejor respuesta al mismo
  - Campañas de divulgación y sensibilización comunes.
  - Conocimiento personal entre los miembros de los equipos que facilita una mejor actuación en los casos urgentes.
114. Para que ello ocurra deben darse marcos de colaboración lo suficientemente amplios y flexibles como para que, respetando las competencias y ámbitos de actuación particulares de cada CERT, puedan optimizarse las operaciones de cada centro aprovechando sinergias y economías de escala con otras iniciativas.

## 11.1. ESQUEMA DE RELACIÓN

115. En la actualidad en España, la distribución de competencias a nivel estatal se basa principalmente en una asignación de las mismas por comunidades de usuarios, según la siguiente distribución:



**Fig. 10.1 Distribución de competencias de los distintos CERT a nivel estatal por Comunidades<sup>35</sup>**

116. Ante este panorama de Equipos de Respuesta, y siguiendo las recomendaciones de las principales organizaciones internacionales es necesaria la implantación de un modelo de colaboración en el que se desarrolle la figura del Coordinador Nacional en materia de ciberseguridad o, siguiendo con la nomenclatura utilizada, la implantación de un CERT Nacional. Así lo recomiendan las principales organizaciones internacionales (UIT, ENISA, OTAN...) y así lo recogen la inmensa mayoría de las Estrategias de Ciberseguridad hechas públicas hasta la fecha a lo largo y ancho del planeta, entre otras, la española, que señala en su capítulo IV la necesidad de adoptar un enfoque integral de ciberseguridad, citando el papel del CCN-CERT como principal organismo de prevención y respuesta frente a las ciberamenazas<sup>36</sup>.
117. Por su parte, la Unión Internacional de Telecomunicaciones, UIT, recomienda<sup>37</sup> que “el Estado cree o identifique un CSIRT nacional/gubernamental que sirva de piedra angular para la seguridad del ciberespacio y la protección de las infraestructuras de la información esencial, y cuya misión principal abarque esfuerzos de prevención, advertencia, respuesta y recuperación

<sup>35</sup> Los CERT autonómicos creados hasta la fecha abarcan todas las comunidades señaladas, salvo los servicios privados

<sup>36</sup> <http://www.lamoncloa.gob.es/ConsejodeMinistros/Enlaces/24062011Enlace2.htm>

<sup>37</sup> ITU Study Group Q.22/1 Report on Best Practices for a National Approach to Cybersecurity: a Management Framework for Organizing National Cybersecurity Efforts. Chapter 4 <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf>

(reduciendo el riesgo y minimizando el impacto) y facilite la colaboración entre las entidades gubernamentales, nacionales y locales, así como con el sector privado, el sector académico y la comunidad internacional”.

118. Del mismo modo, la Unión Europea, en diversos dictámenes y comunicados de la Comisión al Parlamento Europeo<sup>38</sup>, exhorta a las naciones a la creación de equipos de respuesta a incidentes nacionales. En el último, hecho público en marzo de 2011, la Comisión señala que ENISA seguirá prestando su apoyo a los Estados miembros que todavía no hayan instituido CERT nacionales/gubernamentales con el fin de garantizar que todos los Estados miembros cuenten para finales de 2011 con unos CERT nacionales/gubernamentales que funcionen eficazmente. El objetivo es establecer una red de CERT nacionales/gubernamentales<sup>39</sup> en Europa.
119. Por tanto, y siguiendo este modelo, el CCN-CERT, como CERT gubernamental tendría las siguientes funciones:
- **Coordinador e impulsor de la ciberseguridad en todo el Estado**, definiendo las líneas estratégicas y buenas prácticas de la seguridad de la información (Guías CCN-STIC, Esquema Nacional de Seguridad, etc.)
  - **Coordinador a nivel nacional** de todos los Equipos de Respuesta que presten sus servicios a las administraciones públicas, desarrollando el ENS, desplegando un sistema de alerta temprana y de protección de las redes de las AAPP y sus interconexiones, apoyo al CNPIC en los incidentes de seguridad relacionados con las infraestructuras críticas, etc. Todo ello sin perjuicio de que cada centro fije su propia estrategia, en virtud de sus competencias.
  - **Promotor de la interacción entre todos los CERT nacionales** (tanto públicos como privados), a partir de la creación de grupos de trabajo y relaciones de confianza, facilitando el intercambio de información y de servicios entre todos. La constitución del Foro CSIRT.es (del que se hablará más adelante) es un buen ejemplo de ello.
  - **Promotor y punto de referencia para la constitución de otros Equipos** que puedan surgir, tanto a nivel general, autonómico o local. Así lo recoge el Plan Avanza, cuando señala que el CCN-CERT será el encargado de informar, formar y facilitar herramientas para que las distintas administraciones públicas puedan desarrollar sus propios CERT, permitiendo a este equipo actuar de catalizador y coordinador de CERT cuya Comunidad (o parte de ella) sea la Administración. En este mismo sentido, el RD 3/2010 por el que se regula el Esquema Nacional de Seguridad, señala que el CCN-CERT actuará sin perjuicio de las capacidades de respuesta a incidentes de seguridad que pueda tener cada Administración y de la función de coordinación a nivel nacional e internacional del CCN.
  - **Punto de contacto internacional en organismos**, programas internacionales y grupos de equipos de respuesta en los que se comparten objetivos, procedimientos e información sobre la seguridad<sup>40</sup>.

<sup>38</sup> COM (2009) 149 FINAL (2010/C 255/18) Dictamen c/255 de 22/09/2010

<sup>39</sup> COM(2011) 163 final. Comunicado, 31.3.2011

<sup>40</sup> El CCN-CERT interviene en las reuniones del NCIRC de la OTAN (*NATO Computer Incident Response Capability*), asiste a grupos de trabajo de la Unión Europea (ENISA), es miembro del FIRST, del Trusted Introducer de TERENA y del EGC.



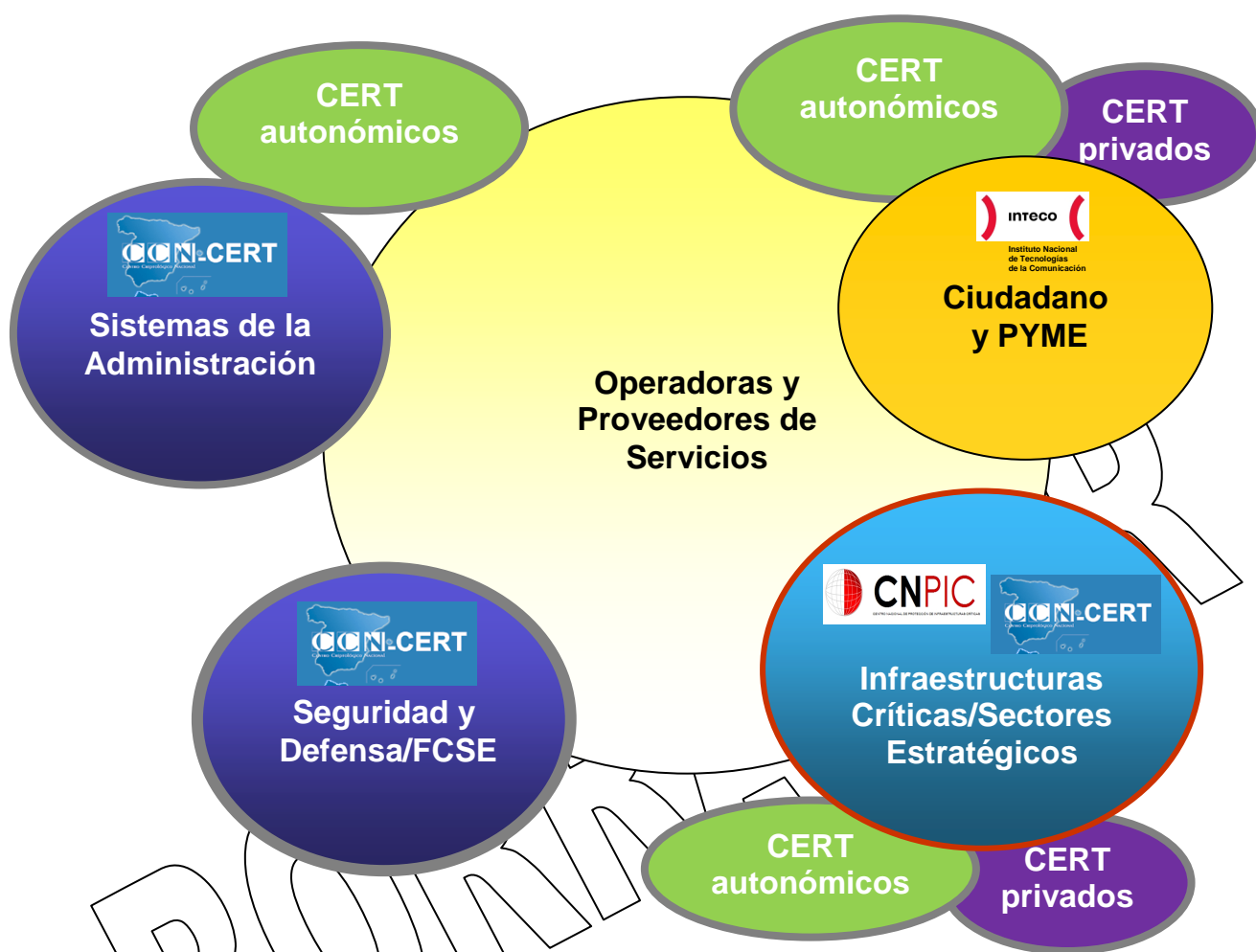


Figura 11-2: Centros coordinadores de cada Comunidad

## 11.2. MECANISMOS DE COORDINACIÓN ENTRE LOS CERT EN ESPAÑA

120. Establecido un modelo de relación y dada la importancia de la cooperación entre los diferentes CERT en materia de ciberseguridad, el siguiente paso consiste en el establecimiento de los mecanismos de coordinación que permitan, entre otros objetivos:

- Establecer marcos de colaboración
- Propiciar la coordinación y cooperación a nivel nacional e internacional.
- Prevenir, detectar y responder a la ciberdelincuencia y al uso indebido de las TIC en modelos de cooperación entre gobiernos y el sector privado.
- Definir puntos de contacto para intervenir y resolver incidentes en tiempo real y desarrollar una red cooperativa entre estos puntos de contacto de forma que se comparta información y tecnologías para intervenir en caso de incidentes de seguridad.
- Fijar pautas de coordinación en la resolución de incidentes que afectan a más de una Comunidad.

121. Para garantizar el cumplimiento de los objetivos anteriores es preciso establecer los mecanismos que permitan definir un marco de colaboración multilateral que establezca entre otros, los siguientes parámetros:

- Autoridades, regulación, competencias y requerimientos de cada uno de los CERT.
- Prioridades de la gestión de operaciones.
- Servicios de soporte a la resolución de incidentes.
- Sistema de gestión de incidentes.
- Estandarización de sistemas de gestión de emergencias.
- Protocolos de ayuda mutua.
- Grupos de coordinación regional.
- Desarrollo de planes de objetivos comunes.
- Tipos de incidentes y niveles de coordinación, mejora en el intercambio de información de alertas, vulnerabilidades, amenazas y eventos detectados por cada CERT u organización (sea pública o privada) para obtener una visión de conjunto de las amenazas que se produzcan.
- Gestión de redes seguras a Internet y establecimiento de canales seguros para el intercambio de información entre el sector público y privado
- Acuerdos de sistemas de alerta temprana, con sensores de detección de intrusiones
- Marcos de actuación a nivel de administración local y autonómica.
- Marcos de actuación con CERT privados y centros no gubernamentales, a través de acuerdos de colaboración.

### 11.2.1. COLABORACIÓN NACIONAL



122. Un ejemplo de esta colaboración entre equipos de estas características es la creación en el año 2008 del Foro CSIRT.es<sup>41</sup>, una asociación independiente y sin ánimo de lucro compuesto por equipos de respuesta a incidentes de seguridad informáticos cuyo ámbito de actuación es la comunidad de usuarios que operan dentro del territorio español. El Foro CSIRT está formado hasta la fecha por los Equipos de Respuesta:

- CCN-CERT
- CESICAT-CERT
- CSIRT-CV
- ESCERT-UPC
- e-laCaixa CSIRT
- INTECO-CERT
- IRIS-CERT

123. Entre sus principales objetivos se encuentra el promover la cooperación entre los CSIRT españoles existentes, tanto en el terreno de la respuesta a incidentes como en el desarrollo de proyectos conjuntos que contribuyan a la mejora de la seguridad tanto en su ámbito de actuación como en la comunidad española. De igual modo, sus miembros comparten información sobre incidentes de seguridad, patrones de ataque y cualquier otro tipo de información que se considere de utilidad.



124. Otro ejemplo de coordinación entre equipos es el Foro ABUSES<sup>42</sup>, en el que los equipos de seguridad de organismos y empresas se relacionan con los principales proveedores de servicios de Internet

### 11.2.2. COLABORACIÓN INTERNACIONAL

125. En el ámbito internacional también existen foros de colaboración entre los organismos responsables de la gestión de incidentes de los distintos países. Los más significativos son los siguientes:

- ENISA

<sup>41</sup> [www.csirt.es](http://www.csirt.es)

<sup>42</sup> <http://www.abuses.es/>

European Network and Information Security Agency, ENISA<sup>43</sup> fue creada siguiendo la Regulación (EC) No 460/2004 del Parlamento y el Consejo Europeo del 10 de marzo de 2004. Comenzó a funcionar en Creta en el 2005 y es el órgano comunitario que trabaja para las instituciones europeas y los estados miembros, aconseja y apoya la creación de CERT nacionales que cooperen entre sí para asegurar una protección efectiva de los Sistemas Europeos (redes, infraestructuras, etc.). De igual forma, ayuda a prevenir y responder a problemas relacionados con la Seguridad de la Información y las Redes. También asesora a la Comisión Europea en la creación, actualización y desarrollo de leyes comunitarias en materia de seguridad de la información.

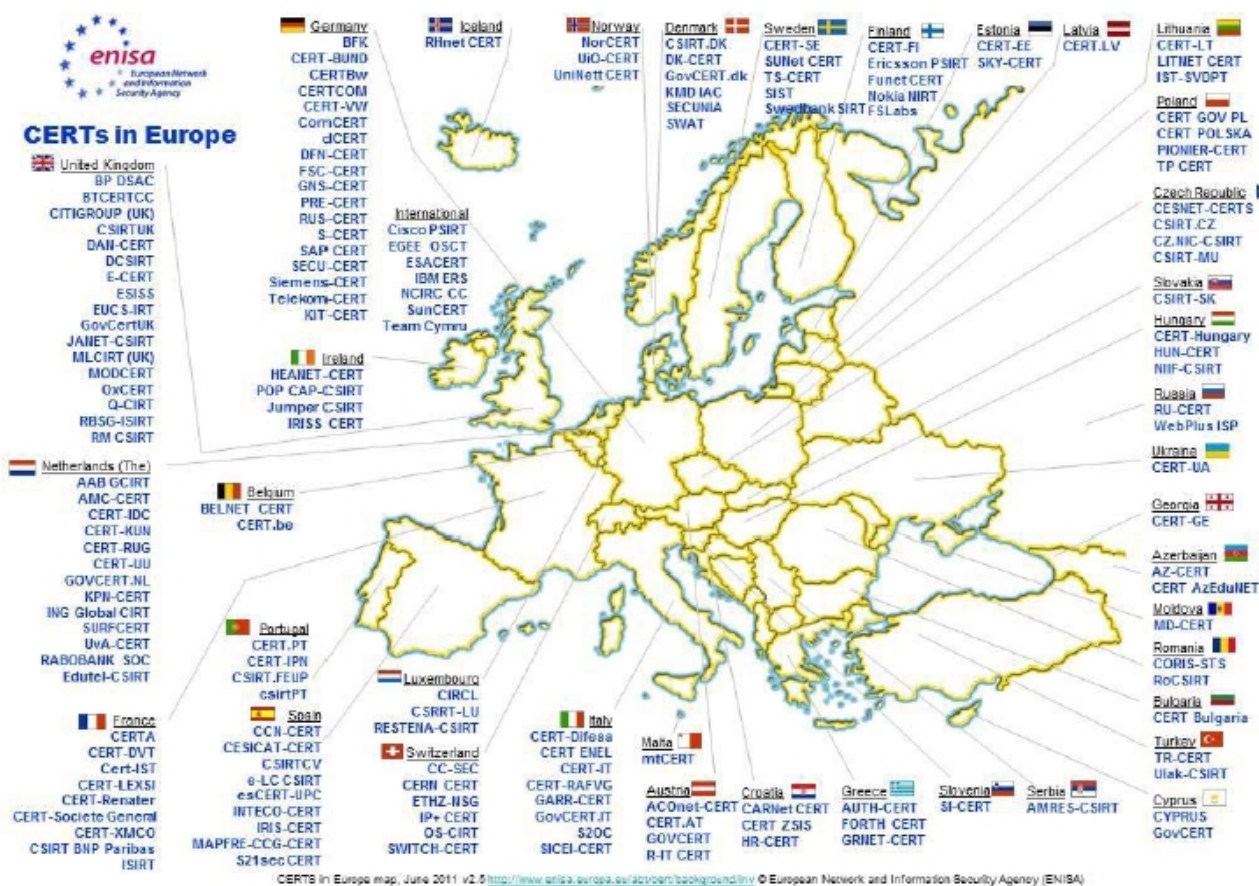


Figura 11-4. Mapa CERT en Europa<sup>44</sup>

#### ▪ FIRST

FIRST (Foro para Equipos de Respuesta a Incidentes y Seguridad)<sup>45</sup> es una de las primeras organizaciones globalmente reconocida en respuesta a incidentes. Su principal objetivo es promover la cooperación y coordinación en la prevención de incidentes, así como compartir información entre sus miembros y la Comunidad en su conjunto. A través de sus miembros de

<sup>43</sup> <http://www.enisa.europa.eu/>

<sup>44</sup> <http://www.enisa.europa.eu/act/cert/background/inv/files/inventory-of-cert-activities-in-europe>

<sup>45</sup> <http://www.first.org>

pleno derecho, FIRST constituye una “red de confianza” para la respuesta a incidentes globales. En la actualidad cuenta con 218 miembros de 48 países distintos, repartidos por los cinco continentes. Los grupos españoles reconocidos son: CCN-CERT, INTECO-CERT, Iris-CERT, e-La Caixa-CERT, esCERT-UPC, CESICAT-CERT, TB-Security-CERT, Mapfre-CCG-CERT y S21Sec-CERT.

### ▪ TRUST INTRODUCER

Trusted Introducer for CSIRT in Europe<sup>46</sup>, es un grupo de trabajo creado por TERENA que promueve la colaboración entre CSIRT a nivel Europeo. Su principal objetivo es proporcionar un foro (TF-CSIRT) donde sus miembros puedan intercambiar experiencias y conocimientos en un entorno de confianza. La red Trusted Introducer se comenzó a gestar en septiembre de 2000 y, en la actualidad el número de colaboradores asciende a más de 70. Entre ellos se encuentra el CCN-CERT, que se unió en enero de 2008.

### ▪ EGC Group

European Government CERT (EGC) Group es un grupo informal de Equipos de Respuesta Gubernamentales que está desarrollando una cooperación eficaz en materia de respuesta a incidentes entre sus miembros, basándose en la similitud de los grupos y el conjunto de problemas entre CSIRT gubernamentales en Europa.

Su constitución se produjo en noviembre de 2001<sup>47</sup> por la necesidad de alcanzar una nivel mayor de confianza y de capacidades operacionales a nivel internacional para tratar incidentes a gran escala, con CERT involucrados en políticas nacionales o en la protección de las infraestructuras críticas nacionales, ante el gran número de CSIRT a nivel mundial involucrados en la gestión de incidentes (muchos sin ser capaces de dar una respuesta a incidentes a escala internacional).

Los miembros que componen el EGC Group son:

- Austria - GovCERT.AT
- Dinamarca - Danish\_GovCERT
- Finlandia - CERT-FI
- Francia - CERTA
- Alemania - CERT-Bund
- Hungría - CERT-Hungary
- Holanda - GOVCERT.NL
- Noruega - NorCERT
- España - CCN-CERT
- Suecia - CERT-SE
- Suiza - GovCERT.ch
- Reino Unido - CSIRTUK
- Reino Unido - GovCertUK y CSIRT UK



Figura11-5. Miembros del European Government CERTs Group (EGC)

### ▪ NCIRC de OTAN

<sup>46</sup> <http://www.trusted-introducer.org/>

<sup>47</sup> [http://www.egc-group.org/fact\\_sheet.pdf](http://www.egc-group.org/fact_sheet.pdf)



Siguiendo las decisiones tomadas en las reuniones de Praga (2002) y Estambul (2004), la OTAN comenzó a implementar su Capacidad de Respuesta a Incidentes de Seguridad TIC, el NCIRC (NATO Computer Incident Response Capability), con sede en Bruselas.

- **Financial ISAC**

FS-ISAC<sup>48</sup>, siglas en inglés de Financial Services - Information Sharing and Analysis Center, es el único foro para la colaboración frente a amenazas de seguridad del sector financiero. Cuando se dan incidentes, la alerta temprana y el consejo de expertos pueden significar la diferencia entre continuidad de negocio y catástrofe empresarial de gran impacto. Los miembros de este foro reciben notificaciones e información fidedigna específicamente diseñada para ayudar a proteger los sistemas y activos críticos frente a las amenazas físicas y de ciberseguridad.

BORRADOR

---

<sup>48</sup> <http://www.fsisac.com/>



## ANEXO A - LEGISLACIÓN Y NORMATIVA APLICABLE

### NORMATIVA Y REGULACIÓN NACIONAL

126. El lógico y adecuado funcionamiento de cualquier CERT pasa por la definición del Marco Legislativo, que implica definir e identificar las leyes aplicables para la organización que tienen relación con la seguridad de los Sistemas de Información y del Marco Normativo, que conlleva definir e identificar las normas y estándares de seguridad de la información que aplican en cada caso.
127. Como ya se ha mencionado, la actividad principal de un CERT es la gestión de incidentes de seguridad en la Red o en los sistemas de información. Cualquiera de estos incidentes en Internet implica un riesgo que conlleva la vulneración de derechos de mayor o menor alcance, normalmente, y con mayor trascendencia en el ámbito penal.
128. Cualquier solución de seguridad debe contribuir a cumplir con los criterios básicos de la seguridad, es decir: confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad (criterios CIDTA). Igualmente, el desarrollo de cualquier estrategia de seguridad deberá tener en cuenta tanto el respeto de los derechos individuales, como la coordinación y cooperación en el manejo de información y la protección de infraestructuras críticas en un contexto territorial transnacional e indeterminado.
129. Cualquier CERT debe contar con un marco jurídico específico y apropiado que permita configurar tanto su personalidad jurídica, como sus relaciones con los miembros de su propia Comunidad y aquellas que se deriven con terceros (otros CERT públicos y privados, o nacionales e internacionales). Hay que tener siempre presente que la gestión de incidentes puede dar lugar a situaciones jurídicas especiales que traspasan el derecho nacional del Estado, lo que exige la fijación de normas que determinen su funcionamiento en condiciones de protección adecuada, generación de confianza y seguridad (por otra parte, significarán además una clara garantía del trabajo eficaz que realice el CERT).
130. Por otro lado, la actuación del CERT ha de integrarse en el marco de las leyes nacionales y comunitarias y éstas, a su vez, deben marcar las directrices sobre las responsabilidades legales del CERT.
131. Con todas estas salvedades, y a modo de orientación y con carácter no exhaustivo, podemos enumerar como normativa aplicable a los CERT de ámbito estatal, en el marco de la legislación nacional, las normas que se muestran a continuación y que se pueden consultar siguiendo los enlaces adjuntados en los anexos.

### LEGISLACIÓN NACIONAL

- **Derechos fundamentales:**
  - **Constitución Española 1978:** Artículos 18.3, 18.4, 20, 55, 105,b).
- **Privacidad de las personas:**
  - **RD 1.720/2007 de 21 de diciembre** Reglamento de desarrollo de LO 15/1999
  - **LO 15/1999, de 13 de diciembre**, de protección de datos de carácter personal
  - **LO 10/1995, de 23 de noviembre** del Código Penal, artículos 197 al 278, 400 y 536
- **Seguridad y defensa nacional:**

- O.M. 76/2006 de 29 de mayo sobre Política INOFOSEC en el Ministerio de Defensa
- **Ley 11/2002 de 6 de mayo** reguladora del CNI Y **RD 421/2004** sobre el CCN
- **O.M. 1/1982 de 25 de enero**. Normas de Protección de Materias Clasificadas
- **Ley 9/1968 de Secretos Oficiales** y **Decreto 242/1969 de 20 de febrero** de Reglamento.
- **Administración Pública:**
  - **RD 3/2010 de 8 de enero**, regulador del Esquema Nacional de Seguridad en el ámbito de la administración electrónica.
  - **Ley 11/2007, de 22 de junio**, de acceso de los ciudadanos a los servicios públicos
  - **Ley 59/2003, de 19 de diciembre**, de firma electrónica
  - **Ley 30/1992, de 26 de noviembre**, del régimen jurídico de las administraciones públicas y del procedimiento administrativo común
- **Infraestructuras Críticas**
  - **Ley 8/2011 de 28 de abril** por la que se establecen medidas para la protección de las infraestructuras críticas
  - **Real Decreto 704/2011 de 20 de mayo** por el que se aprueba el Reglamento de protección de las infraestructuras críticas
- **Prestadores de servicios de telecomunicaciones**
  - **Ley 32/2003, de 3 de noviembre** general de telecomunicaciones
  - **Ley 34/2002, de 11 de julio**, de servicios de la sociedad de la información y de comercio electrónico.
  - **Ley 25/2007, de 18 de octubre**, de conservación de datos relativos a los comunicaciones electrónicas y a las redes públicas de comunicaciones  
<http://www.boe.es/boe/dias/2007/10/19/pdfs/A42517-42523.pdf>
  - **Ley 56/2007, de 28 de diciembre**, de medidas de impulso de la sociedad de la información
  - **RD 424/2005, de 15 de abril**, por el que se aprueba el reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios

## NORMATIVA Y LEGISLACIÓN EUROPEA

132. Cuando hablamos de seguridad informática, resulta imprescindible aproximarse a la protección jurídica que ofrecen las normas internacionales, puesto que la trasgresión de los derechos en Internet no tiene fronteras.
133. A nivel europeo existe un amplio acuerdo sobre la necesidad de armonizar las normas nacionales legales de los estados miembros y mejorar la cooperación judicial y policial, pero existen todavía muchos obstáculos que impiden el logro de resultados concretos. Sin embargo, esta necesidad

(cuyo fin último es el desarrollo de la Sociedad Información) es una prioridad de primer orden, de la mayor parte de las instituciones nacionales e internacionales.

134. Se expone a continuación una relación sobre distintas iniciativas, comunicaciones y directivas que, desde distintos ámbitos pretenden esta armonización en las legislaciones de los estados miembros de la UE:

▪ **Privacidad de las personas**

- **Comunicación** de la Comisión al Parlamento Europeo y al Consejo sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad (PET). **COM/2007/228**.
- **Directiva 2006/24/CE** del Parlamento Europeo y del Consejo de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.
- Directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales.
- **Reglamento (CE) No 45/2001** del Parlamento Europeo y del Consejo de 18 de diciembre de 2000 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.
- **Directiva 1995/46/CE** del Parlamento Europeo y del Consejo de 24 de Octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de esos datos.

▪ **Protección de Infraestructuras Críticas**

- Comunicación de la comisión al parlamento europeo, al consejo, al comité económico y social europeo y al comité de las regiones. **Com/2005/662 final**: disposiciones de la comisión sobre el sistema de alerta temprana general "ARGUS".
- Comunicación de la comisión sobre un programa europea para la protección de infraestructuras críticas. **Com/2006/786 final**.
- Propuesta de directiva del consejo del 12.12.2006, **Com/2006/787 final** sobre la identificación y designación de las infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.
- Decisión del consejo de 12 de febrero de 2007 por la que se establece para el período 2007-2013 el programa específico «prevención, preparación y gestión de las consecuencias del terrorismo y de otros riesgos en materia de seguridad», integrado en el programa general «seguridad y defensa de las libertades» (2007/124/ce, euratom).
- **Directiva 2008/114/ce del consejo de 8 de diciembre** de 2008 sobre la identificación y designación de infraestructuras críticas europeas y evaluación de la necesidad de mejorar su protección.
- **Comunicación de la comisión del 30.3.2009** Com (2009) 149 final al parlamento europeo, al consejo, al comité económico y social europeo y al comité de las regiones sobre protección de infraestructuras críticas de la información.

▪ **Seguridad de la Sociedad de la Información**

- Comunicación de la comisión al parlamento europeo, al consejo, al comité económico y social europeo y al comité de las regiones sobre la lucha contra el spam, los programas espía y los programas maliciosos [com (2006) 688]
  - Comunicación de la comisión al parlamento europeo y al consejo, de lucha contra el crimen cibernético [com (2007) 267]
  - Reglamento (ce) no 460/2004 del parlamento europeo y del consejo de 10 de marzo de 2004 por el que se crea la agencia europea de seguridad de las redes y de la información.
- **Cooperación penal internacional**
- Convenio sobre cibercriminalidad. budapest, 23.xi.2001

## ESTÁNDARES Y BUENAS PRÁCTICAS

135. El establecimiento de un marco de referencia es un aspecto clave para que el personal de un CERT lleve a cabo su tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad. De hecho, y como ya se ha mencionado en el capítulo 7 (Servicios CERT), dentro de los servicios proactivos y de gestión de este tipo de equipos suelen elaborarse y difundir normas, instrucciones, guías o recomendaciones para que los responsables de seguridad dispongan de la suficiente información para desempeñar con criterio su trabajo. Esta documentación debe ser actualizada permanentemente para hacer frente a los riesgos y amenazas en continuo cambio.
136. Entre los distintos estándares y buenas prácticas con las que se puede contar, destacan:

## GUÍAS CCN-STIC DEL CENTRO CRIPTOLÓGICO NACIONAL

137. Una de las funciones más destacables que el Real Decreto 421/2004 asigna al CCN, es la 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. Precisamente, estas Guías CCN-STIC inspiraron el contenido del RD 3/2010, del ENS, y a su vez se recogen en su artículo 29, en donde se establece la elaboración y difusión, por parte del CCN, de las correspondientes guías de seguridad de las tecnologías de la información y las comunicaciones para el mejor cumplimiento de lo establecido en el Esquema.
138. Estos documentos se dividen en nueve series que son ampliadas y actualizadas anualmente, de tal forma que en el año 2011 el CCN cuenta con 153 Guías (a las que hay que sumar 21 que están pendientes de publicar). De ellas, la serie 800 es de nueva instauración, ya que se creó para cumplir con lo establecido en el Esquema Nacional de Seguridad, según el Real Decreto 3/2010 anteriormente mencionado.
- **Serie 000 Políticas.** Desarrollo del RD 421/2004.
  - **Serie 100 Procedimientos STIC.** Establecen el marco común de actuación en los procesos de acreditación, certificación TEMPEST, gestión de material de cifra y de cualquier otro campo que se considere.
  - **Serie 200 Normas STIC.** Son reglas generales que deben seguirse, o a las que se deben ajustar las conductas tareas o actividades de las personas y Organizaciones en relación con la

protección de la información cuando es manejada por un Sistema.

- **Serie 300 Instrucciones Técnicas STIC.** Atienden a un objetivo de seguridad específico, y serán eminentemente técnicas. Establecen los requisitos de seguridad generales a implantar en un Sistema.
- **Serie 400 Guías Generales.** Son recomendaciones a los responsables de seguridad relativas a temas concretos de la seguridad de las TIC (redes inalámbricas, telefonía móvil, cortafuegos, herramientas de seguridad...).
- **Serie 500 Guías entornos Windows.** Estas guías establecen las configuraciones mínimas de seguridad de los diferentes elementos basados en la tecnología Windows.
- **Serie 600 Guías otros entornos.** Estas guías establecen las configuraciones mínimas de seguridad de otras tecnologías (HP-UX, SUN-SOLARIS, LINUX, equipos de comunicaciones,...).
- **Serie 800 Esquema Nacional de Seguridad.** Estas guías establecen las políticas y procedimientos para la implementación de las medidas contempladas en el RD 3/2010.
- **Serie 900 Informes Técnicos.** Estas guías de carácter técnico recogen el resultado y las conclusiones de un estudio o evaluación teniendo por objeto facilitar el empleo de algún producto o aplicación de seguridad.

## NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY)

139. Agencia federal no regulatoria, perteneciente al Departamento de Comercio de EEUU. Fue fundada en 1901 y su misión es promover la innovación y la competitividad industrial en los EEUU.

- **NIST SP 800-61 “Computer Security Incident Handling Guide”**  
<http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf>. Buenas prácticas y procedimientos para la gestión de incidentes.
- **NIST SP 800-83 “Guide to Malware Incident Prevention and Handling”**  
<http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf>
- **NIST SP 800-86 “Guide to Integrating Forensic Techniques into Incident Response”**  
<http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf>

## IETF/RFCs (INTERNET ENGINEERING TASK FORCE)

140. Es una amplia y abierta comunidad internacional de diseñadores de redes, operadores, fabricantes e investigadores preocupados por la evolución de la arquitectura de Internet y por facilitar su operatividad. Los resultados de sus trabajos y las aportaciones de sus miembros se publican en documentos denominados RFCs (Request for Comments, o Solicitud de Comentarios), que se usan comúnmente como estándares de referencia en la industria. A continuación se describen los más interesantes:

- **RFC2350 “Expectations for Computer Security Incident Response”**  
<http://www.ietf.org/rfc/rfc2350.txt>. Incluye un modelo que puede ser usado por los CERT para comunicar esta información a los miembros de su Comunidad, así como los servicios que los miembros deberían ciertamente esperar de un CERT. En el capítulo 7.1 de este informe, se describe la experiencia de implantación del CCN-CERT siguiendo el modelo planteado por el RFC2350.
- **RFC3227 “Guidelines for evidence collection and archiving”**  
<http://www.ietf.org/rfc/rfc3227.txt>. Buenas prácticas para la recolección y archivado de



evidencias digitales producidas en un incidente.

- **RFC 3067 “Incident Object Description and Exchange Format (IODEF)”**  
<http://www.ietf.org/html.charters/HISTORY/inch-charter.2006-07-12.15.html>. Define un formato común de descripción de objetos y procedimientos de intercambio para compartir la información necesaria para gestionar incidentes entre CERT.
- **RFC 4765 “The Intrusion Detection Message Exchange Format”**  
<http://www.ietf.org/rfc/rfc4765.txt>. Define el formato de datos y procedimientos de intercambio para compartir información de interés para los sistemas de detección y respuesta de intrusiones y para los sistemas de gestión que tienen que interaccionar con ellos.

## OTROS ESTÁNDARES UTILIZADOS

- **Common Vulnerabilities and Exposure – CVE**  
<http://cve.mitre.org/>. CVE® es un diccionario, internacional y de uso gratuito para el público, de vulnerabilidades y exposiciones públicamente conocidas para la seguridad de la información. Los identificadores comunes de CVE permiten el intercambio de datos entre productos de seguridad y proporcionan una línea base para evaluar la cobertura de herramientas y servicios.
- **Common Vulnerability Scoring System (v2) – CVSS**  
<http://www.first.org/cvss/cvss-guide.html>. CVSS proporciona un marco abierto para comunicar características e impactos de las vulnerabilidades en las TIC. CVSS permite a responsables TIC, proveedores de boletines de vulnerabilidades, vendedores de aplicaciones y seguridad, así como a investigadores, beneficiarse de la adopción de un lenguaje común para la valoración de vulnerabilidades.
- **OASIS: Application Vulnerability Description Language (AVDL)**  
<http://www.oasis-open.org/committees/download.php/7145/AVDL%20Specification%20V1.pdf>  
AVDL es un estándar XML que permite a entidades (como aplicaciones, organizaciones o instituciones) comunicar información sobre vulnerabilidades en las aplicaciones web de forma estándar.
- **OASIS: Common Alerting Protocol (CAP)**  
[http://www.oasis-open.org/committees/download.php/15135/emergency-CAPv1.1-Corrected\\_DOM.pdf](http://www.oasis-open.org/committees/download.php/15135/emergency-CAPv1.1-Corrected_DOM.pdf). CAP es un estándar XML general y simple que permite el intercambio de información de alertas y avisos públicos sobre todo tipo de redes y sistemas de alerta, de forma estándar. Se pretende convertir en uno de los estándares básicos para el desarrollo de soluciones de Protección de Infraestructuras Críticas.



## ANEXO B - ENLACES DE INTERÉS

- **Unión Europea**
  - ENISA: [http://ec.europa.eu/information\\_society/eeurope/i2010/index\\_en.htm](http://ec.europa.eu/information_society/eeurope/i2010/index_en.htm)
  - European ePractice: <http://www.epractice.eu/>
  - OECD Anti-Spam Toolkit: <http://www.oecd-antispam.org/>
- **Equipos y/o foros de CERT:**
  - European Cooperation of Abuse Fighting Teams (E-COAT). <http://www.e-coat.org/>
  - European Government CERT (EGC) Group. <http://www.egc-group.org/>
  - CERT - Coordination Center. <http://www.CERT.org/>
  - FIRST, Forum for Incident Response and Security Team. <http://www.first.org/>
  - Terena/TF-CSIRT. <http://www.terena.nl/tech/task-forces/tf-csirt/>
  - Trusted Introducer (TI). <http://www.trusted-introducer.nl/>
  - Warning, Alerting and Reporting Points (WARPs). <http://www.warp.gov.uk/>
  - APCERT-Asia Pacific Computer Emergency Response Teams. <http://www.apCERT.org/>
  - European CSIRT Directory. <http://www.ti.terena.org/teams/>
- **Enlaces a Organismos de estandarización y recursos relacionados:**
  - 1) **ISO - International Organisation for Standardization.** <http://www.iso.org>
    - Familia de estándares ISO/IEC 27000: Information technology - Security techniques - Information security management systems (ISMS).
    - Security Techniques: Information Security Incident Management (ISO/IEC TR 18044).
  - 2) **ITU/UIT International Telecommunications,** Agenda de 'Ciberseguridad': <http://www.itu.int/cybersecurity/>. Warning and Incident Response: <http://www.itu.int/ITU-D/cyb/cybersecurity/wwir.html>
  - CAIF - Common Advisory Interchange Format.** <http://CERT.uni-stuttgart.de/projects/caif/> y <http://www.caif.info/>. CAIF es un formato basado en XML para almacenar e intercambiar anuncios de seguridad de forma normalizada. Proporciona un conjunto de elementos básicos, pero completo, diseñado para describir los aspectos principales de un asunto relacionado con la seguridad. Estos elementos permiten agrupar información de manera multilingüe y para distintos tipos de lectores-objetivo.
  - 3) **SecDEF - Security Description and Exchange Format.** <http://www.secdef.org/> Iniciativa de la Central Sponsor for Information Assurance (CSIA, Reino Unido), para evolucionar varios estándares internacionales de intercambio de datos estructurados, basados en XML. Su audiencia objetivo son los CERT y otros equipos de gestión de incidentes.

- 4) **VEDEF - Vulnerability and Exploit Description and Exchange Format**  
<http://www.vedef.org>. Iniciativas SecDEF, llevada a cabo por un Grupo de Trabajo Europeo (Task Force) sobre Equipos de Respuesta a Incidentes, TF-CSIRT, y presidido por la CSIA. Los miembros de este grupo de trabajo provienen del National Infrastructure Security Coordination Centre (NISCC) y han estado trabajando en este proyecto con socios de USA y Japón.

- **Enlaces a organizaciones sectoriales:**

**EICTA** : European Information & Communications Technologie Industry Association  
<http://www.eicta.org/story.asp?level2=8&level1=2&level0=1>

**EuroISPA** : European Internet Services Providers Association  
<http://www.euroispa.org/>

BORRADOR

## ANEXO C – REFERENCIAS

- [Ref.-1] **Boletín Oficial del Estado**  
23 de junio de 2007  
L 11/2007, de 22 de junio  
<http://www.boe.es/boe/dias/2007/06/23/pdfs/A27150-27166.pdf>
- [Ref.-2] **Boletín Oficial del Estado**  
29 de enero de 2010  
RD 3/2010, de 8 de enero  
<http://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf>
- [Ref.-3] **ENISA**  
Informe Anual 2007  
[http://www.enisa.europa.eu/media/key-documents/enisa-general-reports/enisa\\_general\\_report\\_2007-1.pdf](http://www.enisa.europa.eu/media/key-documents/enisa-general-reports/enisa_general_report_2007-1.pdf)
- [Ref.-4] **Comisión de la Unión Europea**  
30 de marzo de 2009  
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:ES:PDF>
- [Ref.-5] **Unión Internacional de Telecomunicaciones (UIT)**  
Enero 2008  
Study Group Q.22/1  
<http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf>
- [Ref.-6] **La Moncloa**  
24 de junio de 2011  
Estrategia Española de Seguridad  
<http://www.lamoncloa.gob.es/ConsejodeMinistros/Enlaces/24062011Enlace2.htm>
- [Ref.-7] **DARPA Defense Advanced Research Projects Agency**  
<http://www.darpa.mil/>
- [Ref.-8] **CERT CC**  
Carnegie Mellon University's Software  
<http://www.cert.org/cert/>
- [Ref.-9] **Asociación Transeuropea de Investigación y Educación de Redes**  
10 y 11 de junio de 1999  
<http://www.terena.org/about/tech/ToR.html>
- [Ref.-10] **Trusted Introducer**  
<http://www.trusted-introducer.nl/>
- [Ref.-11] **SURFnet-CERT**  
<http://www.surfnet.nl/nl/Thema/surfcert/Pages/Default.aspx>
- [Ref.-12] **BSI-Bundesamt für Sicherheit in der Informationstechnik**

Febrero de 2001  
Congreso: “El Estado Eficiente”  
[https://www.bsi.bund.de/cln\\_136/DE/Themen/CERTBund/certbund\\_node.html](https://www.bsi.bund.de/cln_136/DE/Themen/CERTBund/certbund_node.html)

[Ref.-13] **RedIRIS**

Catálogo de Servicios  
<http://www.rediris.es/cert/servicios/iris-cert>

[Ref.-14] **ENISA**

24 de febrero de 2010  
Guía de Buenas Prácticas en la Gestión de Incidentes  
<http://www.enisa.europa.eu/act/cert/support/incident-management/files/good-practice-guide-for-incident-management>

[Ref.-15] **Fundación Orange**

Informe Anual 2011 sobre la Sociedad de la Información en España  
[http://fundacionorange.es/fundacionorange/analisis/eespana/e\\_espana11.html](http://fundacionorange.es/fundacionorange/analisis/eespana/e_espana11.html)

[Ref.-16] **BOE**

RD 3/2010 de 8 de enero, Regulador del Esquema Nacional de Seguridad  
<http://www.warp.gov.uk/>  
<http://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf>

[Ref.-16] **CCN-CERT**

Abril 2011  
Informe de Amenazas CCN-CERT IA\_01-11. Ciberamenazas 2010 y Tendencias 2011  
<http://www.ccn-cert.cni.es>

[Ref.-17] **ENISA**

Febrero de 2010  
Ejercicios CERT Manual  
<https://www.enisa.europa.eu/act/cert/support/exercise/files/cert-exercise-handbook-in-spanish>

[Ref.-18] **ENISA**

Diciembre de 2006  
Guía “Cómo crear un CSIRT paso a paso”  
<https://www.enisa.europa.eu/act/cert/support/guide/files/csirt-setting-up-guide-in-spanish>

[Ref.-19] **Centro Criptológico Nacional**

Guía CCN-STIC 403 “Gestión de Incidentes de Seguridad”  
[https://www.ccn-cert.cni.es/index.php?option=com\\_wrapper&view=wrapper&Itemid=188&lang=es](https://www.ccn-cert.cni.es/index.php?option=com_wrapper&view=wrapper&Itemid=188&lang=es)

[Ref.-20] **CERT Coordination Center**

“Handbook for Computer Security Incident Teams”  
Abril 2003  
[www.cert.org/archive/pdf/csirt-handbook.pdf](http://www.cert.org/archive/pdf/csirt-handbook.pdf)

- [Ref.-21] **ENISA**  
“A Collection of good practices for CERT quality assurance”
- [Ref.-22] **ENISA**  
Baseline capabilities for national / governmental CERT. V.1.0  
Diciembre de 2009
- [Ref.-23] **Computer Emergency Response Team for the Dutch Government – GOVCERT.NL**  
“CERT-in-a-box”  
12 de septiembre de 2005  
<http://www.govcert.nl/render.html?it=69>
- [Ref.-24] **Forum of Incident Response and Security Teams – FIRST**  
Julio de 2011  
<http://www.first.org/>
- [Ref.-25] **Software Engineering Institute Carnegie Mellon. CERT-CC**  
26 de noviembre de 2002  
CSIRT Services  
<http://www.cert.org/csirts/services.html>
- [Ref.-26] **National Finland CERT – CERT-FI**  
22 de octubre de 2009  
National and Governmental CSIRTs in Europe  
[http://www.cert.fi/attachments/certiedostot/5kiBC9Qy0/National\\_and\\_Governmental\\_CSIRTs\\_in\\_Europe.pdf](http://www.cert.fi/attachments/certiedostot/5kiBC9Qy0/National_and_Governmental_CSIRTs_in_Europe.pdf)  
<https://eu2009.pts.se/Documents/PTS%20Resilience%20Conference%20-%20Erka%20Koivunen.pdf?epslanguage=en-GB>
- [Ref.-27] **Comisión Europea**  
30 de marzo de 2009  
Comunicado de la Comisión de la Unión Europea al Parlamento  
(Bruselas, 30.03.2009, COM (2009)
- [Ref.-28] **Ministerio de Industria, Turismo y Comercio**  
Plan Avanza 1 y 2  
<http://www.planavanza.es>
- [Ref.-29] **Centro Nacional de Protección de Infraestructuras Críticas**  
Abril 2011  
*Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.*  
<https://www.ccn-cert.cni.es/publico/InfraestructurasCriticaspublico/Ley82011-de28deabril-PIC.pdf>
- [Ref.-30] **Diario Oficial de la Unión Europea**  
8 de diciembre de 2008  
Directiva 2008/114/CE del Consejo sobre identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección  
<http://eur->

[lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:ES:PDF](http://lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:ES:PDF)

[Ref.-31] **European Government CERT Group (EGC)**

15 de diciembre de 2008

“Fact Sheet”

[http://www.egc-group.org/fact\\_sheet.pdf](http://www.egc-group.org/fact_sheet.pdf)

[Rf.-32] **Foro CSIRT.es**

<http://www.csirt.es>

BORRADOR