COMISIÓN DE LAS COMUNIDADES EUROPEAS

Bruselas, 30.3.2009
COM(2009) 149 final

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES

sobre protección de infraestructuras críticas de información

«Proteger Europa de ciberataques e interrupciones a gran escala: aumentar la preparación, seguridad y resistencia»

{SEC(2009) 399}
{SEC(2009) 400}

(presentada por la Comisión)

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES

sobre protección de infraestructuras críticas de información

«Proteger Europa de ciberataques e interrupciones a gran escala: aumentar la preparación, seguridad y resistencia»

1. INTRODUCCIÓN

Las tecnologías de la información y la comunicación (TIC) se entrecruzan cada vez más en nuestras actividades diarias. Algunos de estos sistemas, servicios, redes e infraestructuras TIC —para abreviar, las infraestructuras TIC— forman una parte vital de la economía y la sociedad europeas, sea porque proporcionan bienes y servicios fundamentales, sea porque constituyen los cimientos de otras infraestructuras críticas. En general se consideran infraestructuras críticas de información (ICI)[1] ya que su alteración o destrucción afectaría gravemente a funciones sociales fundamentales. Como ejemplos de este tipo de situaciones cabe citar los ciberataques a gran escala dirigidos contra Estonia en 2007 y la rotura de cables transcontinentales en 2008.

En 2008, el Foro Económico Mundial estimó que las probabilidades de que las ICI sufran una avería importante en los próximos diez años oscila entre el 10 y el 20 %, con un coste económico mundial de aproximadamente 250 000 millones de dólares[2].

La presente Comunicación se centra en la prevención, la preparación y el conocimiento, y define un plan de medidas inmediatas para potenciar la seguridad y resistencia de las ICI. Esta atención es coherente con el debate iniciado a petición del Consejo y el Parlamento Europeo con el fin de abordar los problemas y prioridades de la política de seguridad de las redes y de la información, así como los instrumentos más apropiados que se precisan a escala de la UE para hacerles frente. Las medidas propuestas son asimismo complementarias de las encaminadas a prevenir, combatir y llevar a juicio las actividades delictivas y terroristas cuyo objetivo sean las ICI, y actúan de manera sinérgica con los esfuerzos comunitarios presentes y futuros sobre investigación en el ámbito de la seguridad de las redes y de la información, así como con las iniciativas internacionales en este ámbito.

2. CONTEXTO

La presente Comunicación desarrolla la política europea de potenciar la seguridad de la sociedad de la información y la confianza en ella. Ya en 2005, la Comisión[3] destacó la urgente necesidad de coordinar los esfuerzos para cimentar la confianza de los interesados en los servicios y comunicaciones electrónicos. Con este fin, en 2006 se adoptó una estrategia

---

1 El documento COM(2005) 576 final propone una definición de ICI.
2 «Global Risks» 2008.
3 COM(2005) 229.

para una sociedad de la información segura[4]. Sus elementos principales, entre ellos la seguridad y resistencia de las infraestructuras TIC, se ratificaron en la Resolución 2007/C 68/01 del Consejo. No obstante, parecen insuficientes la propiedad y la aplicación por los interesados. Asimismo, esta estrategia potencia el papel, a niveles tácticos y operativos, de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), fundada en 2004 para contribuir a los objetivos de garantizar un nivel elevado y eficaz de seguridad de las redes y de la información en la Comunidad y fomentar una cultura sobre este particular en beneficio de los ciudadanos, consumidores, empresas y administraciones de la UE.

En 2008, el mandato de la ENISA se prorrogó sin cambios hasta marzo de 2012[5]. Al mismo tiempo, el Consejo y el Parlamento Europeo exigieron «*más debates sobre el futuro de la ENISA y sobre la dirección general de los esfuerzos europeos en pos de una mayor seguridad de las redes y de la información*». Para respaldar esos debates, la Comisión puso en marcha, el pasado mes de noviembre, una consulta en línea[6], cuyo análisis se dará a conocer en breve.

Las actividades programadas en la presente Comunicación se realizan al amparo del Programa Europeo para la Protección de Infraestructuras Críticas (PEPIC)[7] y en paralelo con él. Un elemento clave del PEPIC es la Directiva[8] sobre la identificación y designación de infraestructuras críticas europeas[9], en la que se señala que el sector de las TIC será un sector prioritario en el futuro. Otro elemento importante del PEPIC es la Red de información sobre alertas en infraestructuras críticas (CIWIN)[10].

En cuanto al aspecto normativo, la propuesta de la Comisión sobre la reforma del marco regulador común de las redes y los servicios de comunicaciones electrónicas[11] incluye nuevas disposiciones sobre seguridad e integridad, en concreto para potenciar las obligaciones de los operadores a fin de asegurar que se adoptan las medidas adecuadas para hacer frente a riesgos determinados, garantizar la continuidad de la provisión de servicios y notificar fallos de seguridad[12]. Este planteamiento está encaminado a aumentar la seguridad y resistencia de las ICI. El Parlamento Europeo y el Consejo apoyan estas disposiciones.

Las actuaciones propuestas en la presente Comunicación complementan las medidas vigentes y futuras, en el ámbito de la cooperación policial y judicial para prevenir, combatir y llevar a juicio las actividades delictivas y terroristas cuyo objetivo sean las infraestructuras TIC, tal como se contempla, entre otros actos, en la Decisión marco del Consejo sobre ataques a los sistemas de información[13] y la actualización prevista de dicha Decisión[14].

Esta iniciativa tiene en cuenta las actividades de la OTAN sobre política común de ciberdefensa, esto es, la Autoridad de Gestión de la Ciberdefensa y el Centro de Excelencia para la Ciberdefensa Cooperativa.

---

4 COM(2006) 251.
5 Reglamento (CE) nº 1007/2008.
6 http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=4464
7 COM(2006) 786 final.
8 2008/114/CE.
9 http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/gena/104617.pdf
10 COM(2008) 676 final.
11 COM(2007) 697, COM(2007) 698, COM(2007) 699.
12 Artículo 13 de la Directiva marco.
13 2005/222/JHA.
14 COM(2008) 712.

Por último, se hace el debido repaso de la evolución de la política internacional, en particular de los principios del G8 sobre protección de infraestructuras críticas de información[15]; la Resolución 58/199 de la Asamblea General de la ONU «Creación de una cultura mundial de seguridad cibernética y protección de las infraestructuras de información esenciales» y la reciente Recomendación de la OCDE sobre la protección de infraestructuras críticas de información.

3. BAZAS EN JUEGO

3.1. Las infraestructuras críticas de información son fundamentales para el crecimiento económico y social de la UE

La función económica y social del sector y de las infraestructuras TIC se subraya en varios informes sobre la innovación y el crecimiento económico publicados recientemente, como la Comunicación que lleva por título «Revisión intermedia de la iniciativa i2010»[16], el informe del Grupo Aho[17] y los informes económicos anuales de la Unión Europea[18]. La OCDE hace hincapié en la importancia de las TIC y de Internet «*para estimular el rendimiento económico y el bienestar social, así como para intensificar la capacidad de las sociedades para mejorar la calidad de vida de los ciudadanos de todo el mundo*»[19]. Además, recomienda la adopción de estrategias que refuercen la confianza en la infraestructura de Internet.

El sector de las TIC es fundamental para todos los segmentos de la sociedad. Las empresas dependen de él tanto para las ventas directas como para la eficiencia de los procesos internos. Las TIC son un componente crítico de la innovación y aproximadamente el 40 % del crecimiento de la productividad se debe a ellas[20]. Asimismo, son un elemento imprescindible para la realización de las tareas de los gobiernos y las administraciones públicas: la utilización de la administración electrónica a todos los niveles, junto con aplicaciones nuevas, como soluciones innovadoras relacionadas con la salud, la energía y la participación política, hacen que el sector público dependa en gran medida de las TIC. Por último, los ciudadanos dependen cada vez más de las TIC y hacen un uso de ellas cada vez mayor en sus actividades diarias: intensificar la seguridad de las ICI haría que aumentase la confianza de los ciudadanos en las TIC, gracias, entre otras cosas, a una mejor protección de los datos personales y la privacidad.

3.2. Riesgos para las infraestructuras críticas de información

Sucede con frecuencia que los riesgos provocados por el hombre, por desastres naturales o por fallos técnicos no se comprenden del todo ni se analizan suficientemente, por lo que el nivel de conciencia de los interesados es insuficiente para concebir salvaguardias y contramedidas eficaces.

Los ciberataques han alcanzado un nivel de complejidad inaudito. Experimentos sencillos se están convirtiendo en complejas actividades que se realizan para sacar provecho o por

---

15 http://www.usdoj.gov/criminal/cybercrime/g82004/G8_CIIP_Principles.pdf

16 COM(2008) 199 final.

17 http://ec.europa.eu/invest-in-research/action/2006_ahogroup_en.htm

18 «The EU economy: 2007 review» http://ec.europa.eu/economy_finance/publications/publication10130_en.pdf

19 http://www.oecd.org/dataoecd/1/29/40821707.pdf

20 http://epp.eurostat.ec.europa.eu/ - Science and Technology/Information Society

motivos políticos. Los ciberataques a gran escala que han sufrido recientemente Estonia, Lituania y Georgia son los ejemplos de una tendencia general que han recibido la mayor cobertura informativa. El enorme número de virus, gusanos y demás formas de *malware*, la expansión de *botnets* y el continuo aumento de correo no deseado confirman la gravedad del problema[21].

La gran dependencia de las ICI, su interconexión transfronteriza y su interdependencia de otras infraestructuras, su vulnerabilidad y las amenazas a las que se hallan expuestas, hacen que aumente la necesidad de abordar su seguridad y resistencia desde una perspectiva sistémica como primera línea de defensa contra los fallos y los ataques.

3.3. Seguridad y resistencia de las infraestructuras críticas de información para fomentar la confianza en la sociedad de la información

Con el fin de garantizar la máxima utilización de las infraestructuras TIC y aprovechar de ese modo todas las oportunidades económicas y sociales que ofrece la sociedad de la información, es preciso que todas las partes interesadas tengan un elevado nivel de confianza en ellas. Ello depende de diversos elementos, el más importante de los cuales es garantizarles un elevado nivel de seguridad y resistencia. Diversidad, franqueza, interoperabilidad, usabilidad, transparencia, rendición de cuentas, auditabilidad de los diferentes componentes y competencia son fuerzas impulsoras básicas para desarrollar la seguridad y estimular el empleo de productos, procesos y servicios que aumenten la seguridad. Como ha señalado ya la Comisión[22], es una responsabilidad compartida: ningún interesado tiene los medios por sí solo para garantizar la seguridad y resistencia de todas las infraestructuras TIC y asumir todas las responsabilidades que llevan aparejadas.

Aceptar esas responsabilidades exige un planteamiento y una cultura de gestión de los riesgos que permitan responder a las amenazas conocidas y anticiparse a las desconocidas que se presenten en el futuro, sin reaccionar de manera exagerada ni sofocar la aparición de servicios y aplicaciones innovadoras.

3.4. Problemas que se le plantean a Europa

Además de todas las actividades relacionadas con la aplicación de la Directiva sobre la identificación y designación de infraestructuras críticas europeas, y de manera complementaria a todas esas actividades, en particular la determinación de criterios específicos del sector de las TIC, es preciso abordar diversos problemas de gran envergadura para fortalecer la seguridad y resistencia de las ICI.

3.4.1. Planteamientos nacionales desiguales y descoordinados

Aunque los problemas y las cuestiones que hay que abordar tienen elementos comunes, las medidas y regímenes adoptados para garantizar la seguridad y resistencia de las ICI, así como el nivel de conocimientos y preparación, difieren de un Estado miembro a otro.

Con un planteamiento puramente nacional se corre el riesgo de ver surgir la fragmentación y la ineficiencia en Europa. Las diferencias existentes entre los planteamientos nacionales y la falta de cooperación transfronteriza sistemática reducen considerablemente la eficacia de las

---

[21] COM(2006) 688 final.
[22] COM(2006) 251 final.

medidas nacionales de protección, entre otros motivos porque, debido a la interconexión de las ICI, un nivel escaso de seguridad y resistencia de las ICI de un país puede hacer que aumenten la vulnerabilidad y los riesgos de las de otro.

Para superar esta situación, es necesario un esfuerzo europeo que aporte valor añadido a las políticas y programas nacionales impulsando un mejor conocimiento y una comprensión común de los problemas, estimulando la adopción de prioridades y objetivos políticos compartidos, fortaleciendo la cooperación entre los Estados miembros e integrando las políticas nacionales en una dimensión más global y europea.

3.4.2. Necesidad de un nuevo modelo de gobernanza europea para las ICI

Aumentar la seguridad y resistencia de las ICI plantea problemas de gobernanza especiales. Si bien la elaboración de las políticas relacionadas con las ICI compete en última instancia a los Estados miembros, su aplicación depende de la intervención del sector privado, que posee o controla un buen número de ellas. Por otro lado, los mercados no siempre ofrecen incentivos suficientes para que el sector privado invierta en la protección de las ICI al nivel que los gobiernos exigirían normalmente.

Para solucionar este problema de gobernanza, han aparecido asociaciones público-privadas a escala nacional como modelo de referencia. Con todo, y a pesar del consenso existente en cuanto a la conveniencia de que también hubiera asociaciones público-privadas a escala europea, estas no se han materializado todavía. Un marco para la gobernanza de carácter europeo e integrado por múltiples interesados, en el que la ENISA pudiera desempeñar una función destacada, podría fomentar la participación del sector privado en la determinación de objetivos estratégicos de carácter público y de medidas y prioridades operativas. Este marco permitiría acortar la distancia entre la elaboración de políticas a escala nacional y la realidad operativa sobre el terreno.

3.4.3. Capacidad europea limitada de alerta temprana y respuesta a los incidentes

Los mecanismos utilizados para la gobernanza serán verdaderamente eficaces solo si todos los participantes disponen de información fidedigna que les permita actuar. Ello es especialmente importante en el caso de los gobiernos, a los que compete en última instancia garantizar la seguridad y el bienestar de los ciudadanos.

Ahora bien, los procesos y prácticas utilizados para el seguimiento y la comunicación de los incidentes relacionados con la seguridad de las redes difieren considerablemente de un Estado miembro a otro. Algunos carecen de una organización de referencia que sirva de centro de seguimiento y, lo que es más importante, la cooperación entre los Estados miembros y el intercambio entre ellos de datos fidedignos y utilizables sobre incidentes de la seguridad está poco desarrollada: bien es informal, bien se limita a intercambios bilaterales o a intercambios multilaterales restringidos. Además, la simulación de incidentes y la realización de ejercicios para probar la capacidad de respuesta son aspectos estratégicos para poder aumentar la seguridad y resistencia de las ICI, en concreto centrándose en estrategias y procesos flexibles con los que hacer frente a la imprevisibilidad de las posibles crisis. En la UE, los ejercicios de ciberseguridad están aún en fase embrionaria y los que implican saltar las fronteras nacionales son muy limitados. Como han puesto de manifiesto acontecimientos recientes[23], la ayuda

[23] http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/large_scale/

mutua es un elemento fundamental para lograr una respuesta adecuada a las amenazas y ataques a gran escala contra las ICI.

Para poder contar con una gran capacidad europea de alerta temprana y respuesta a los incidentes es preciso disponer de equipos nacionales o gubernamentales de respuesta a incidentes de seguridad de la información (CERT) que funcionen correctamente, esto es, que dispongan de una base común en términos de capacidad. Estos organismos deben actuar como catalizadores nacionales de los interesados y de su capacidad para realizar actividades públicas (incluidas las relacionadas con los sistemas de difusión de información y alertas que lleguen a los ciudadanos y a las PYME) y deben participar de manera efectiva en la cooperación transfronteriza y en el intercambio de información, posiblemente impulsando organizaciones existentes, como el *EGC Group* o Grupo de CERT gubernamentales europeos[24].

3.4.4. Cooperación internacional

El auge de Internet en tanto que ICI básica exige prestar una atención especial a su resistencia y estabilidad. Internet, gracias a su diseño distribuido y redundante, ha demostrado ser una infraestructura muy sólida. Ahora bien, su espectacular crecimiento ha dado lugar a una creciente complejidad física y lógica y a la aparición de nuevos usos y servicios: es razonable poner en duda la capacidad de Internet para resistir el número cada vez mayor de perturbaciones y ciberataques.

La divergencia de puntos de vista sobre el carácter crítico de los elementos que componen Internet explica en parte la diversidad de opiniones gubernamentales expresadas en foros internacionales y las impresiones, a menudo contradictorias, sobre la importancia de este asunto. Ello puede dificultar una prevención, preparación y capacidad de recuperación apropiadas con respecto a las amenazas que se ciernen sobre Internet. Por ejemplo, las consecuencias del paso del IPv4 al IPv6 deben evaluarse también desde el punto de vista de la seguridad de las ICI.

Internet es una red de redes mundial y muy extendida, cuyos centros de control no se adaptan necesariamente a las fronteras nacionales. Ello exige un planteamiento específico y selectivo, con el fin de garantizar su resistencia y estabilidad, basado en dos medidas convergentes. La primera, lograr un consenso general sobre las prioridades europeas con respecto a la resistencia y estabilidad de Internet, en términos de normativa pública y de utilización operativa. La segunda, hacer participar a la comunidad mundial en la creación de un conjunto de principios, que reflejen los valores esenciales europeos, sobre la resistencia y estabilidad de Internet, en el marco de nuestro diálogo y cooperación estratégicos con terceros países y organizaciones internacionales. Estas actividades deben apoyarse en el reconocimiento por parte de la Cumbre Mundial sobre la Sociedad de la Información[25] de la importancia capital de la estabilidad de Internet.

---

[24] http://www.egc-group.org/

[25] Agenda de Túnez para la Sociedad de la Información, http://www.itu.int/wsis/docs2/tunis/off/6rev1.html

4. EL CAMINO HACIA ADELANTE: HACIA UNA MAYOR COORDINACIÓN Y COOPERACIÓN COMUNITARIAS

Debido a la dimensión comunitaria e internacional del problema, un planteamiento comunitario integrado que aumente la seguridad y resistencia de las ICI complementaría y añadiría valor a los programas nacionales y a los regímenes bilaterales y multilaterales vigentes de cooperación entre Estados miembros.

Los debates sobre las estrategias públicas que se han sucedido tras los acontecimientos ocurridos en Estonia dejan entrever que los efectos de ataques similares pueden limitarse con medidas preventivas y una actuación coordinada durante la propia crisis. Un intercambio de información más estructurado y la utilización de buenas prácticas en la UE podrían facilitar considerablemente la lucha contra las amenazas transfronterizas.

Es preciso reforzar los instrumentos de cooperación existentes, incluida la ENISA, y, en caso necesario, crear nuevas herramientas. Es fundamental un planteamiento de varios niveles en el que intervengan diversos interesados y que discurra a escala europea, pero respetando y complementando íntegramente las competencias nacionales.

Es necesaria una comprensión profunda del entorno y las limitaciones. Por ejemplo, la naturaleza distribuida de Internet, en la que los nodos externos pueden utilizarse como vectores de ataque —p. ej., *botnets*—, es motivo de preocupación. No obstante, esta naturaleza distribuida es un componente básico de estabilidad y resistencia y puede ayudar a que la recuperación sea más rápida que si se tratase de procedimientos descendentes y excesivamente formalizados. Ello requiere análisis prudente y caso por caso de las estrategias públicas y los procedimientos operativos que haya que aplicar.

El horizonte temporal también es importante. Resulta evidente la necesidad de actuar ya y de reunir rápidamente los elementos precisos para crear un marco que permita solucionar los problemas actuales y se incardine en la futura estrategia para la seguridad de las redes y de la información.

Para hacer frente a estos problemas se proponen cinco pilares:

(1) Preparación y prevención: garantizar la preparación a todos los niveles.

(2) Detección y respuesta: proporcionar suficientes mecanismos de alerta temprana.

(3) Mitigación y recuperación: fortalecer los mecanismos comunitarios de defensa de las ICI.

(4) Cooperación internacional: fomentar internacionalmente las prioridades comunitarias.

(5) Criterios para el sector de las TIC: apoyar la aplicación de la Directiva sobre la identificación y designación de infraestructuras críticas europeas[26].

[26] Directiva 2008/114/CE del Consejo.

5. PLAN DE ACCIÓN

5.1. Preparación y prevención

Base de las capacidades y servicios para una cooperación paneuropea. La Comisión insta a los Estados miembros y los interesados a:

- Definir, con la ayuda de la ENISA, un nivel mínimo de capacidades y servicios para los CERT nacionales o gubernamentales y operaciones de respuesta a los incidentes en apoyo a la cooperación paneuropea.

- Garantizar que los CERT nacionales o gubernamentales actúan como componente fundamental de la capacidad nacional de preparación, intercambio de información, coordinación y respuesta.

Fecha objetivo: finales de 2010 para acordar normas mínimas; finales de 2011 para establecer CERT nacionales o gubernamentales que funcionen bien en todos los Estados miembros.

Asociación público-privada europea de resistencia.

- La Comisión fomentará la cooperación entre los sectores público y privado sobre objetivos de seguridad y resistencia, requisitos básicos, buenas prácticas normativas y medidas. El objetivo principal de la asociación público-privada europea de resistencia será la dimensión europea desde perspectivas estratégicas (buenas prácticas normativas) y tácticas u operativas (utilización industrial). La asociación público-privada europea de resistencia debe basarse en las iniciativas nacionales existentes y las actividades operativas de la ENISA, complementándolas.

Fecha objetivo: finales de 2009 para elaborar un plan de asociación público-privada europea de resistencia; mediados de 2010 para establecer una asociación público-privada europea de resistencia; finales de 2010 para que la asociación dé sus primeros resultados.

Foro europeo para el intercambio de información entre los Estados miembros.

- La Comisión establecerá un foro europeo para que los Estados miembros intercambien información y buenas prácticas normativas sobre seguridad y resistencia de las ICI. Esta iniciativa aprovechará los resultados de las actividades de otras organizaciones, en particular la ENISA.

Fecha objetivo: finales de 2009 para la puesta en marcha del foro; finales de 2010 para obtener los primeros resultados.

5.2. Detección y respuesta

Sistema europeo de intercambio de información y alerta (EISAS).

- La Comisión apoya la creación y utilización de un sistema europeo de intercambio de información y alerta, que llegue a los ciudadanos y las PYME y se base en información de

los sectores nacional y privado y en sistemas para compartir alertas. La Comisión apoya financieramente dos proyectos prototipo complementarios[27]. Se pide a la ENISA que evalúe los resultados de estos proyectos y de otras iniciativas nacionales y elabore un plan para fomentar la creación y utilización de sistemas europeos de intercambio de información y alerta.

Fecha objetivo: finales de 2010 para la conclusión de los proyectos prototipo; finales de 2010 para la elaboración del plan encaminado a lograr un sistema europeo.

5.3. Mitigación y recuperación

Planificación y ejercicios nacionales de contingencia.

- La Comisión insta a los Estados miembros a elaborar planes nacionales de contingencia y organizar ejercicios periódicos de respuesta ante incidentes a gran escala de seguridad de las redes y de recuperación de desastres, como vía hacia una cooperación paneuropea más estrecha. Se podrá pedir a los CERT o los CSIRT nacionales o gubernamentales que dirijan pruebas y ejercicios de planificación de contingencias nacionales en los que participen interesados de los sectores público y privado. Se pide la participación de la ENISA para apoyar el intercambio de buenas prácticas entre los Estados miembros.

Fecha objetivo: finales de 2010 para realizar al menos un ejercicio nacional en cada Estado miembro.

Ejercicios paneuropeos sobre incidentes a gran escala de seguridad de las redes.

- La Comisión apoyará financieramente la realización de ejercicios paneuropeos sobre incidentes de la seguridad de Internet[28], que también podrán constituir la plataforma operativa para la participación paneuropea en ejercicios internacionales sobre incidentes de seguridad de las redes, como la US Cyber Storm o cibertormenta estadounidense.

Fecha objetivo: finales de 2010 para la concepción y ejecución del primer ejercicio paneuropeo; finales de 2010 para la participación paneuropea en ejercicios internacionales.

Mayor cooperación entre CERT nacionales o gubernamentales.

- La Comisión insta a los Estados miembros a intensificar la cooperación entre CERT nacionales o gubernamentales, impulsando y ampliando asimismo los mecanismos de cooperación existentes, como el EGC[29]. Se precisará del activo papel de la ENISA para estimular y apoyar la cooperación paneuropea entre los CERT nacionales o gubernamentales, que deberá traducirse en una mejor preparación, una mayor capacidad europea para reaccionar y responder a los incidentes, y en ejercicios paneuropeos o regionales.

---

27 En el Programa comunitario «*Prevención, preparación y gestión de las consecuencias del terrorismo y de otros riesgos en materia de seguridad*» http://ec.europa.eu/justice_home/funding/cips/funding_cips_en.htm

28 Véase *supra*, nota 27.

29 Véase *supra*, nota 24.

Fecha objetivo: finales de 2010 para duplicar el número de organismos nacionales que participen en el ECG; finales de 2010 para que la ENISA elabore documentos de consulta que apoyen la cooperación paneuropea.

5.4. Cooperación internacional

Resistencia y estabilidad de Internet. Se contemplan tres actividades complementarias:

- Prioridades europeas sobre resistencia y estabilidad de Internet a largo plazo. La Comisión dirigirá un debate europeo, en el que participarán todos los interesados públicos y privados pertinentes, para determinar las prioridades de la UE con respecto a la resistencia y estabilidad de Internet a largo plazo.

Fecha objetivo: finales de 2010 para establecer las prioridades de la UE sobre componentes y cuestiones relacionados con Internet.

- Principios y directrices sobre resistencia y estabilidad de Internet (a escala europea). La Comisión trabajará con los Estados miembros para establecer directrices sobre resistencia y estabilidad de Internet, prestando especial atención, entre otras cuestiones, a las medidas correctivas regionales, los acuerdos de asistencia mutua, las estrategias coordinadas de recuperación y continuidad, la distribución geográfica de los recursos críticos de Internet, las salvaguardias tecnológicas en la arquitectura y protocolos de Internet, y la replicación y diversidad de servicios y datos. En la actualidad, la Comisión ya financia un grupo operativo sobre resistencia del sistema de nombres de dominio que, junto con otros proyectos pertinentes, ayudará a lograr el consenso[30].

Fecha objetivo: finales de 2009 para elaborar un plan europeo de principios y directrices sobre resistencia y estabilidad de Internet; finales de 2010 para acordar el primer borrador de tales principios y directrices.

- Principios y directrices sobre resistencia y estabilidad de Internet (a nivel mundial). La Comisión trabajará con los Estados miembros para elaborar un plan de fomento de los principios y directrices a escala mundial. Se potenciará la cooperación estratégica con terceros países, principalmente mediante diálogos sobre la sociedad de la información, como vehículo para alcanzar un consenso mundial[31].

Objetivo: principios de 2010 para elaborar un plan de cooperación internacional sobre principios y directrices de seguridad y resistencia; finales de 2010 para elaborar el primer borrador de principios y directrices reconocidos internacionalmente que se examinará con terceros países y en los foros pertinentes, entre ellos el Foro para la Gobernanza de Internet.

Ejercicios mundiales sobre recuperación y mitigación de incidentes a gran escala de Internet.

- La Comisión insta a los interesados europeos a reflexionar sobre el modo práctico de hacer extensivos a escala mundial los ejercicios que se realizan al amparo del pilar de mitigación y recuperación, apoyándose en planes de contingencia y capacidades regionales.

30 Véase *supra*, nota 27.
31 COM(2008)588 final.

Fecha objetivo: finales de 2010 para que la Comisión proponga un marco y un plan para apoyar la participación europea en ejercicios mundiales de recuperación y mitigación de incidentes a gran escala de Internet.

5.5. Criterios relativos a infraestructuras críticas europeas en el sector de las TIC

Criterios específicos del sector de las TIC. Basándose en la actividad inicial realizada en 2008, la Comisión:

- Seguirá elaborando, en cooperación con los Estados miembros y todos los interesados pertinentes, criterios para caracterizar las infraestructuras críticas europeas del sector de las TIC. Con ese fin, se extraerá la información pertinente de un estudio específico que se acaba de iniciar[32].

Fecha objetivo: primer semestre de 2010 para que la Comisión establezca los criterios relativos a las infraestructuras críticas europeas del sector de las TIC.

6. CONCLUSIONES

La seguridad y resistencia de las ICI son la primera línea de defensa contra los fallos y los ataques. Mejorar esos factores en toda la UE es fundamental para aprovechar plenamente las ventajas de la sociedad de la información. Con el fin de lograr este ambicioso objetivo se propone un plan de acción que permita fortalecer la cooperación táctica y operativa a escala europea. El éxito de estas actuaciones depende de su eficacia para apoyarse en las actividades de los sectores público y privado, beneficiándolas a su vez, y del compromiso y total participación de los Estados miembros, las instituciones europeas y los interesados.

Con esa finalidad, los días 27 y 28 de abril de 2009 se celebrará una conferencia ministerial para debatir con los Estados miembros las iniciativas propuestas y dejar constancia del compromiso de estos con el debate sobre una política de seguridad de las redes y de la información modernizada e intensificada en Europa.

Por último, la mejora de la seguridad y resistencia de las ICI es un objetivo a largo plazo, cuya estrategia y medidas requieren evaluaciones periódicas. Por esta razón, dado que dicho objetivo es coherente con el debate general sobre el futuro de la política de seguridad de las redes y de la información en la UE después de 2012, la Comisión iniciará un ejercicio de evaluación a finales de 2010, con el fin de hacer balance de la primera fase de actuaciones y señalar y proponer más medidas, según convenga.

[32] Véase *supra*, nota 27.