COMISIÓN EUROPEA

Bruselas, 31.3.2011
COM(2011) 163 final

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

sobre la protección de infraestructuras críticas de información

«logros y próximas etapas: hacia la ciberseguridad global»

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

sobre la protección de infraestructuras críticas de información

«logros y próximas etapas: hacia la ciberseguridad global»

1. INTRODUCCIÓN

El 30 de marzo de 2009, la Comisión adoptó una Comunicación sobre la protección de infraestructuras críticas de información, «Proteger Europa de ciberataques e interrupciones a gran escala: aumentar la preparación, seguridad y resistencia»[1], por la que se instauraba un plan (el plan de acción PICI, o de Protección de Infraestructuras Críticas de Información) destinado a fortalecer la seguridad y la resistencia de las infraestructuras vitales de las Tecnologías de la Información y la Comunicación (TIC). El objetivo era estimular y sostener un alto nivel de desarrollo de la capacidad de preparación, seguridad y resistencia, tanto a nivel nacional como europeo. Esta filosofía fue ampliamente respaldada por el Consejo en 2009[2].

El plan de acción PICI se sustentaba en cinco pilares: preparación y prevención, detección y respuesta, mitigación y recuperación, cooperación internacional y criterios relativos a las infraestructuras críticas europeas en el sector de las TIC. En él se expone cómo deben intervenir en cada pilar la Comisión, los Estados miembros y los sectores interesados, con el apoyo de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA).

La Agenda Digital para Europa[3] (ADE), adoptada en mayo de 2010, y las Conclusiones del Consejo[4] correspondientes pusieron de relieve la convicción común de que la confianza y la seguridad son condiciones previas fundamentales para la adopción a gran escala de TIC y, por ende, para el logro de los objetivos de una de las dimensiones de la Estrategia Europa 2020[5], la denominada «crecimiento inteligente». La ADE hace hincapié en la necesidad de que todas las partes interesadas se unan en un esfuerzo conjunto para garantizar la seguridad y la resistencia de las infraestructuras de las TIC, centrándose en la prevención, la preparación y la sensibilización al objeto de desarrollar unos mecanismos eficaces y coordinados que sirvan de respuesta a las formas siempre nuevas y cada vez más sofisticadas de ciberataque y ciberdelincuencia. De este modo se garantiza que sean tenidas en cuenta tanto la dimensión de la prevención como la de la reacción ante este desafío.

En los últimos meses se han tomado las siguientes medidas, anunciadas en la Agenda Digital: en septiembre de 2010 la Comisión adoptó una propuesta de Directiva relativa a los ataques

---

1 COM(2009) 149.

2 Resolución del Consejo, de 18 de diciembre de 2009, relativa a un planteamiento de colaboración en materia de seguridad de las redes y de la información (2009/C 321/01).

3 COM(2010) 245.

4 Conclusiones del Consejo de 31 de mayo de 2010 sobre la Agenda Digital para Europa (10130/10).

5 COM(2010) 2020 y Conclusiones del Consejo Europeo de los días 25 y 26 de marzo de 2010 (EUCO 7/10).

contra los sistemas de información[6]. Su objetivo es intensificar la lucha contra la ciberdelincuencia merced a una aproximación de los ordenamientos jurídicos penales de los Estados miembros y a una cooperación reforzada entre las administraciones judiciales o de otro tipo. Introduce, por otro lado, unas disposiciones destinadas a atender a nuevas formas de ciberataque, en particular los botnets. Como complemento a todo ello, la Comisión ha presentado, de forma paralela, una nueva propuesta de mandato[7] cuyo objetivo es fortalecer y modernizar la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) al objeto de impulsar la confianza en la red, así como su seguridad. El fortalecimiento y modernización de la ENISA ayudará a la UE, los Estado miembros y las empresas a desarrollar sus capacidades y su preparación a la hora de impedir, detectar o responder a los desafíos de la ciberseguridad.

Finalmente, es importante señalar que la ADE, el programa y plan de acción de Estocolmo[8] y la Estrategia de Seguridad Interior de la UE en acción[9] subrayan el compromiso de la Comisión de construir un entorno digital en el que cada europeo pueda desarrollar plenamente su potencial económico y social.

La presente Comunicación pasa revista a los resultados logrados desde la adopción del plan de acción PICI en 2009. Por otro lado, expone las próximas etapas que se han programado para cada acción tanto a nivel europeo como internacional. Se centra además en la dimensión global de los desafíos y en la importancia que reviste impulsar la cooperación entre los Estados miembros y el sector privado a nivel nacional, europeo e internacional al objeto de atender a los factores de interdependencia mutua.

2. UNA SITUACIÓN EN EVOLUCIÓN CONSTANTE

Tanto la evolución de impacto que acompaña al plan de acción PICI[10] como una legión de informes y análisis elaborados por partes interesadas del sector público y el privado ponen de relieve no sólo la dependencia de las TIC que existe en Europa desde el punto de vista social, político y económico, sino también el crecimiento constante en el número, intensidad, sofisticación e impacto potencial de las amenazas que acechan, sean de origen humano o natural.

Están surgiendo amenazas nuevas y más avanzadas tecnológicamente, con una dimensión geopolítica que, de forma cada vez más clara, es de carácter mundial. Estamos presenciando una tendencia hacia el uso de TIC con fines de predominio político, económico y militar, incluida la capacidad ofensiva. La «ciberguerra» y el «ciberterrorismo» son aspectos mencionados a menudo en este contexto.

Además, como ilustran los recientes sucesos acaecidos en la margen meridional del Mediterráneo, algunos regímenes están dispuestos a impedir o perturbar el acceso de sus propios ciudadanos a los medios de comunicación que utilizan las TI (en especial Internet y

6 COM(2010) 517 final.
7 COM(2010) 521.
8 COM(2010) 171.
9 COM(2010) 673.
10 SEC(2009) 399.

comunicación móvil) por razones políticas. Estas intervenciones unilaterales a nivel nacional pueden, sin embargo, tener graves repercusiones en otros lugares del mundo[11].

Para comprender mejor su alcance, estas amenazas podrían agruparse en distintas categorías, según los fines que persigan:

– fines de **explotación**, como es el caso de las «amenazas persistentes avanzadas»[12] de espionaje económico y político (p. ej., GhostNet)[13], los robos de identidad, o los recientes ataques contra el sistema de comercio de derechos de emisión[14] o contra los sistemas de TI de los Estados[15];

– fines de **perturbación**, como la denegación de servicio distribuido o el «spam» generado vía botnets (p. ej., la red Conficker, con más de 7 millones de máquinas, o la red Mariposa, basada en España, con una red de 12,7 millones de máquinas[16]), Stuxnet[17], o el corte de los medios de comunicación;

– fines de **destrucción**; esta es una posibilidad que todavía no se ha presentado pero, vista la omnipresencia creciente de las TIC en las infraestructuras críticas (p. ej., en las redes inteligentes y los sistemas de distribución de agua), no cabe descartarla en los próximos años[18].

3. LA UNIÓN EUROPEA Y EL CONTEXTO MUNDIAL

Todos estos peligros que acechan no son privativos de la Unión Europea, ni pueden ser resueltos por ella aisladamente. La omnipresencia de las TIC y de Internet permite que la comunicación, la coordinación y la cooperación entre los diferentes actores sea más eficaz, eficiente y económica, y da como resultado un dinámico ecosistema de innovación en todos los ámbitos de la vida. Pero el peligro puede surgir de cualquier lugar del mundo y, debido a la interconexión global, repercutir en cualquier lugar del mundo.

Un planteamiento exclusivamente europeo sería insuficiente para hacer frente a las amenazas. Aunque el objetivo de construir un planteamiento coherente y cooperativo en el seno de la UE sigue siendo igual de importante, es necesario integrarlo en una estrategia de coordinación mundial que alcance a todos los actores fundamentales, sean naciones u organizaciones internacionales.

---

11 Comunicación conjunta sobre la Asociación para la democracia y la prosperidad compartida con los países del Mediterráneo meridional - COM(2011) 200 final de 8.3.2011.

12 Es decir, ataques continuados y coordinados contra entidades gubernamentales o del sector público. En el sector privado se está convirtiendo en un problema (véase el informe «RSA 2011 cybercrime trends report».

13 Véanse los informes del proyecto Information Warfare Monitor: «Tracking GhostNet: investigating a Cyber Espionage Network» (2009) y «Shadows in the Cloud: Investigating Cyber Espionage 2.0» (2010).

14 Véase «Q&A» en http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/34&format=HTML&aged=0&language=EN&guiLanguage=fr.

15 Por ejemplo, los recientes ataques contra el Gobierno francés.

16 Véase el proyecto OCDE/IFP sobre los futuros «shocks» mundiales: «Reducing systemic cyber-security risks» (Reducción de los riesgos sistémicos contra la ciberseguridad), de 14 de enero de 2011, en la dirección: http://www.oecd.org/dataoecd/3/42/46894657.pdf.

17 Véase http://www.enisa.europa.eu/media/press-releases/stuxnet-analysis

18 Véase el informe «Global Risks 2011», del Foro económico mundial.

Es necesario realizar un trabajo que nos permita comprender los riesgos que entraña el uso masivo y general de TIC en todos los segmentos de la sociedad. Y, lo que es aún más importante, es necesario concebir estrategias que atiendan, de forma adecuada y efectiva, a la prevención, lucha, mitigación y reacción frente a tales riesgos. La ADE afirma que *«la cooperación entre los agentes pertinentes debe organizarse a nivel mundial, para que sea efectivamente capaz de luchar contra las amenazas a la seguridad y reducirlas»*, y establece como objetivo *«reforzar la **gestión mundial de los riesgos** en el mundo físico y en el digital y llevará a cabo acciones concretas coordinadas internacionalmente contra la delincuencia informática y los ataques a la seguridad»*.

4. APLICACIÓN DEL PLAN DE ACCIÓN PICI: ASPECTOS MÁS IMPORTANTES

Adjunto puede encontrarse el informe completo sobre los logros y las próximas etapas del plan de acción PICI. A continuación se presentan algunos de los aspectos más importantes que caracterizan la situación actual.

4.1. Preparación y prevención

- El **Foro Europeo de Estados miembros** (EFMS) ha realizado progresos significativos; ha alimentado el debate y los intercambios entre las administraciones competentes en materia de buenas prácticas en el terreno de la seguridad y resistencia de las infraestructuras de las TIC. Los Estados miembros reconocen que el EFMS es una importante plataforma de debate e intercambio de buenas prácticas[19]. En sus futuras actividades seguirá recibiendo el apoyo de la ENISA y se centrará en la cooperación entre los equipos de respuesta ante emergencias informáticas (CERT) nacionales/gubernamentales, determinando incentivos económicos y reglamentarios para promover la seguridad y la resistencia (a la vez que respetando las normas vigentes de competencia y ayudas estatales), evaluando el «estado de salud de la ciberseguridad» en Europa, impulsando trabajos a nivel paneuropeo y debatiendo prioridades para promover, a nivel internacional, las cuestiones de seguridad y resistencia.

- La **Asociación público-privada europea de resistencia** (EP3R) fue lanzada con el objetivo de constituir un marco de gobernanza europea para la resistencia de las infraestructuras de TIC. Se propone fomentar la cooperación entre los sectores público y privado en el ámbito de la política estratégica de la UE en materia de seguridad y resistencia. La ENISA desempeñó el cometido de facilitar las actividades de la EP3R y, para dar un seguimiento a la propuesta de la Comisión de modernizar la Agencia, se encargaría de proporcionar un marco sostenible a largo plazo para la EP3R. Ésta serviría a su vez de plataforma para promover, en las esferas internacionales, las cuestiones de política, economía y mercado relevantes para la seguridad y la resistencia con el objetivo, en particular, de fortalecer la gestión mundial de los riesgos de las infraestructuras de las TIC.

---

[19] La respuesta del Gobierno del Reino Unido al Quinto informe de la Comisión de la Unión Europea de la Cámara de los Lores sobre el plan de acción PICI afirma que el EFMS *«ha constituido un éxito y ha colmado una necesidad real de los decisores políticos, la de poder intercambiar experiencias»*.

- Se ha constituido un **conjunto mínimo de capacidades y servicios de referencia**[20], así como las **recomendaciones**[21] correspondientes, para que los CERT nacionales/gubernamentales funcionen de forma efectiva y pasen a ser el factor principal de la preparación, la difusión de información, la coordinación y la respuesta. Estos resultados serán la pieza maestra para establecer, con el apoyo de la ENISA, una red de CERT nacionales/gubernamentales que funcione eficazmente en todos los Estados miembros para 2012. Esta red será la espina dorsal del sistema europeo de intercambio de información y alerta (EISAS) al servicio de ciudadanos y PYME, que se construirá para 2013 a partir de recursos y capacidades nacionales.

4.2. Detección y respuesta

- La ENISA realizó una elaborada hoja de ruta para la creación del sistema europeo de intercambio de información y alerta (**EISAS**) en 2013[22], partiendo de la aplicación de los *servicios básicos* a nivel de CERT nacionales/gubernamentales y de los *servicios de interoperabilidad* de los sistemas nacionales de información y alerta, que quedarían integrados en EISAS. Uno de los principales elementos de esta actividad será una adecuada protección de los datos personales.

4.3. Mitigación y recuperación

- Hasta el momento sólo 12 Estados miembros han organizado ejercicios de respuesta ante incidentes a gran escala de seguridad de las redes y de recuperación en caso de catástrofes[23]. La ENISA ha realizado una **guía de buenas prácticas para ejercicios nacionales**[24] así como unas **recomendaciones**[25] en materia de política de desarrollo de estrategias nacionales con el fin de respaldar las actividades de los Estados miembros, que deben intensificarse.

- El primer **ejercicio paneuropeo sobre incidentes a gran escala de seguridad de las redes** (Cyber Europe 2010) se celebró el 4 de noviembre de 2010 y contó con la participación de todos los Estados miembros, 19 de los cuales tomaron parte activa en el ejercicio, y también de Suiza, Noruega e Islandia. Los próximos ejercicios paneuropeos contarán sin duda con un marco común construido a partir de los planes nacionales de contingencia (pero que a la vez servirá para interconectarlos), facilitando así unos mecanismos y procedimientos de referencia para la comunicación y la cooperación entre Estados miembros.

---

20 Véase: http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-for-national-governmental-certs.

21 Véase http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

22 http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas_roadmap.

23 Fuente: ENISA.

24 Véase: http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises/national-exercise-good-practice-guide/at_download/fullReport.

25 Véase: http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

4.4. Cooperación internacional

- En el EFMS se han debatido y desarrollado unos **principios y directrices europeos sobre resistencia y estabilidad de Internet**[26] La Comisión debatirá y promoverá estos principios con las partes interesadas más relevantes, en particular con el sector privado (a través de la EP3R), de forma bilateral, con los socios internacionales más importantes, como los EE.UU., y de forma multilateral. En este último caso participará, en el marco de sus competencias, en foros tales como el G8, la OCDE, la OTAN (especialmente a través del nuevo concepto estratégico adoptado en noviembre de 2010 y de las actividades del centro de excelencia cooperativo en materia de ciberdefensa), la UIT (en el contexto de la creación de capacidad en el ámbito de la ciberseguridad), la OSCE (a través de su Foro de Cooperación en materia de Seguridad), la ASEAN, Meridian[27], etc. El objetivo es hacer que estos principios y orientaciones constituyan un marco común de compromiso colectivo internacional en torno a la resistencia y estabilidad de Internet a largo plazo.

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

- Las discusiones técnicas en el EFMS llevaron a un **primer borrador de los criterios específicos para el sector de las TIC** para identificar infraestructuras críticas europeas, centrándose en las **comunicaciones móviles y fijas y en Internet**. El debate técnico continuará y se alimentará con las consultas que se realicen con el sector privado acerca del citado borrador, tanto a nivel nacional como europeo (a través de la EP3R). La Comisión debatirá también con los Estados miembros los elementos específicos del sector de las TIC que deban tenerse en cuenta para la revisión de la Directiva sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección[28] en 2012.

5. HACIA EL FUTURO

La ejecución del plan de acción PICI está jalonada de diversos logros, entre ellos el reconocimiento de que es necesario un enfoque cooperativo para la seguridad de las redes y la información, un enfoque en el que participen todas las partes interesadas. Coincide, en líneas generales, con el calendario y las etapas que se programaron en 2009. Con todo, es preciso no darse por satisfechos porque aún queda mucho por hacer, tanto a nivel nacional como europeo, para que todos estos esfuerzos fructifiquen.

Además, es necesario integrar tales esfuerzos en una estrategia de coordinación global y que, de este modo, se extiendan a la esfera internacional, involucrando a los actores pertinentes, y se alcancen otras regiones, países u organizaciones que se enfrentan a problemas similares, y se desarrollen asociaciones de participación que permitan el intercambio de estrategias y el desarrollo de actividades afines, evitando la duplicación de esfuerzos.

Es preciso promover una cultura mundial de la gestión de riesgos. De lo que se trata es de promover acciones coordinadas para impedir, detectar, mitigar y reaccionar frente a todo tipo

---

[26] Véase http://ec.europa.eu/information_society/policy/nis/index_en.htm

[27] El proceso Meridian se propone facilitar a los gobiernos de todo el mundo medios para debatir cómo trabajar juntos a nivel político en el ámbito de la Protección de Infraestructuras Críticas de Información (PICI). Véase http://meridianprocess.org/

[28] Directiva 2008/114/CE del Consejo

de perturbaciones, tanto si son de origen humano como natural, así como para perseguir la ciberdelincuencia. Esto incluye la realización de acciones específicas contra las amenazas a la seguridad y la delincuencia basada en la informática.

A tal efecto **la Comisión**:

- **promoverá principios para la resistencia y la estabilidad de Internet** – es preciso elaborar, en colaboración con otros países, organizaciones internacionales y, en su caso, organizaciones privadas de escala mundial, unos principios internaciones sobre la resistencia y la estabilidad de Internet, utilizando para ello foros y recursos existentes, por ejemplo los de la gobernanza de Internet. Estos principios se convertirían en una herramienta utilizada por todas las partes interesadas para enmarcar sus actividades en el campo de la estabilidad y la resistencia de Internet. A tal efecto pueden servir de base las directrices y principios europeos.

- **construirá asociaciones estratégicas internacionales** - es necesario construir asociaciones estratégicas sobre la base de trabajos ya realizados en ámbitos críticos, como la gestión de ciberincidentes, incluidos la cooperación y realización de ejercicios entre CERT. El compromiso del sector privado, que opera a escala mundial es de importancia primordial. El Grupo de trabajo UE-EE.UU. sobre ciberseguridad y ciberdelincuencia, establecido con ocasión de la cumbre UE-EE.UU. de noviembre de 2010, constituye un paso adelante en la dirección correcta. El Grupo se centrará en la gestión de ciberincidentes, asociaciones público-privadas, política de sensibilización y ciberdelincuencia. Es posible que el Grupo de trabajo estudie además alternativas para integrar en el proceso a otras regiones o países, sobre todo si se enfrentan a problemas similares, para compartir estrategias y actividades y evitar una duplicación del esfuerzo. Se perseguirá el contacto y la coordinación en los foros internacionales, particularmente el G8. Un factor esencial para el éxito sería, en el lado europeo, una buena coordinación entre todas las instituciones de la UE, las agencias pertinentes (en particular la ENISA y Europol) y los Estados miembros.

- **promover la confianza en la computación en nube** - es fundamental profundizar los debates sobre las mejores estrategias de gobernanza para tecnologías emergentes de impacto mundial, tales como la computación en nube. Estos debates deberían tratar, pero sin limitarse a ello, el marco de gobernanza más adecuado para la protección de datos personales. La confianza es fundamental para aprovechar al máximo estas tecnologías[29].

La seguridad es una responsabilidad compartida por todos. Por lo tanto, todos los Estados miembros han de garantizar que sus esfuerzos y las medidas por ellos instauradas contribuyan colectivamente a construir un enfoque coordinado europeo de prevención, detección, mitigación y reacción ante cualquier ciberataque o ciberperturbación. En ese sentido, **los Estados miembros deberían comprometerse a**:

- **reforzar la preparación de la UE estableciendo una red de CERT nacionales/gubernamentales que funcionen eficazmente para 2012.** De igual modo, las

[29] Véanse, por ejemplo, los informes de ENISA «Cloud Computing Information Assurance Framework» (2009), en http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework/at_download/fullReport) y «Security and resilience in governmental clouds» (2011), en http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/).

instituciones de la UE establecerán también un CERT a su nivel para 2012. Todos estos esfuerzos deben servirse del conjunto mínimo de capacidades y servicios de referencia, así como las recomendaciones correspondientes, elaboradas por la ENISA, que seguirá prestando su apoyo a estas iniciativas. Esta actividad anticipará además el desarrollo del sistema europeo de intercambio de información y alerta (EISAS) para el público en general para 2013.

- **elaborar planes de contingencia sobre ciberincidentes para 2012 y efectuar ciberejercicios paneuropeos regulares.** Los ciberejercicios constituyen un elemento importante de cualquier estrategia coherente en materia de planificación de contingencias y recuperación de ciberincidentes, tanto a nivel nacional como europeo. Los ciberejercicios paneuropeos futuros deben basarse en un plan de contingencia europeo en materia de ciberincidentes elaborado a partir de los planes nacionales de contingencia (y que a la vez servirá para interconectarlos). Este plan debe proporcionar los mecanismos y procedimientos de referencia para las comunicaciones entre Estados miembros y, lo que también es importante, un respaldo para la concepción y organización de futuros ejercicios paneuropeos. La ENISA trabajará con los Estados miembros en el desarrollo de este plan de contingencia en materia de ciberincidentes que deberá estar listo para 2012. En el mismo periodo todos los Estados miembros deberán desarrollar planes nacionales de contingencia regulares y ejercicios de respuesta y recuperación.

- **desarrollar esfuerzos coordinados a nivel europeo en foros y debates internacionales en materia de fomento de la seguridad y resistencia de Internet.** Los Estados miembros deben cooperar entre sí y con la Comisión para promover el desarrollo de un enfoque basado en principios o normas en torno al tema de la estabilidad y resistencia global de Internet. El objetivo es fomentar la prevención y preparación a todos los niveles y por parte de todos los interesados, lo que equilibraría la actual tendencia a centrar los debates en aspectos militares o de seguridad nacional.

6. CONCLUSIÓN

La experiencia demuestra que, a la hora de abordar cuestiones de seguridad y resistencia, un enfoque puramente nacional o regional no basta. La cooperación europea se ha desarrollado de forma significativa desde 2009 y se han registrado logros importantes, en particular el ejercicio «Cyber Europe 2010». Con todo, Europa debe continuar sus esfuerzos para construir una estrategia coherente y cooperativa de toda la UE. Es necesario que, en este esfuerzo a largo plazo, una ENISA modernizada preste todo su apoyo a los Estados miembros, las instituciones de la UE y el sector privado.

Para que los esfuerzos europeos tengan éxito, deben inscribirse en un enfoque coordinado a escala mundial. Por ello, la Comisión promoverá debates en materia de ciberseguridad en todos los foros internacionales pertinentes.

Los días 14 y 15 de abril de 2011 tendrá lugar la Conferencia Ministerial PICI, organizada por la Presidencia húngara de la UE. La Conferencia será una oportunidad inmejorable para reforzar el compromiso hacia una mayor cooperación y coordinación entre Estados miembros, tanto a nivel europeo como internacional.

ANEXO

El plan de acción PICI: panorama detallado de los logros y de las siguientes etapas

Los resultados de las actividades desarrolladas en el contexto del plan de acción PICI coinciden en general con el calendario y las etapas que la Comisión programó en 2009. A continuación se exponen los logros obtenidos y la próximas etapas en todos los pilares. En este resumen se tiene en cuenta que algunas actividades se detallaron más en la Agenda Digital para Europa (ADE) y la Estrategia de Seguridad Interior de la UE en acción.

1. **Preparación y prevención**

Capacidades y servicios de referencia para una cooperación paneuropea

Logros

– En 2009 la ENISA, en colaboración con la comunidad de CERT (Computer Emergency Response Team, o Equipo de respuesta ante emergencias informaticas) de Europa desarrollaron y aprobaron un conjunto mínimo de capacidades y servicios de referencia que deben poseer los CERT nacionales/gubernamentales para poder funcionar de forma efectiva en pro de la cooperación paneuropea. Se alcanzó un consenso en torno a una lista de requisitos *sine qua non* en los ámbitos del funcionamiento, la capacidad técnica, los mandatos y la cooperación[30].

– En 2010 la ENISA trabajó con la comunidad de CERT de Europa para convertir los requisitos anteriores, fundamentalmente orientados al funcionamiento, en una serie de recomendaciones de política[31] destinadas a los CERT nacionales/gubernamentales para que pasen a ser el factor principal de la preparación, la difusión de información, la coordinación y la respuesta.

– Hasta la fecha, 20 Estados miembros[32] han desarrollado CERT nacionales/gubernamentales y casi todos los demás tienen previsto hacerlo. Como se anunció en la ADE y se especificó a continuación en la Estrategia de Seguridad Interior, la Comisión ha propuesto medidas para establecer un CERT al servicio de las instituciones europeas para 2012.

Próximas etapas

– La ENISA seguirá prestando su apoyo a los Estados miembros que todavía no hayan instituido CERT nacionales/gubernamentales que se ajusten a los requisitos de referencia anteriormente mencionados con el fin de garantizar que todos los Estados miembros cuenten para finales de 2011 con unos CERT nacionales/gubernamentales que funcionen eficazmente. Esta etapa preparará el terreno para el establecimiento de una red de CERT nacionales/gubernamentales que funcione eficazmente a nivel nacional para **2012**, como se especifica en la ADE.

---

30 Véase: http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-for-national-governmental-certs.

31 Véase: http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

32 Fuente: ENISA.

– La ENISA, con la colaboración de los CERT nacionales/gubernamentales, debatirá si han de ampliarse las «capacidades de referencia» de éstos con el fin de reforzar su apoyo a los Estados miembros a la hora de garantizar la resistencia y estabilidad de las infraestructuras vitales de las TIC, convirtiéndose en la espina dorsal del sistema europeo de intercambio de información y alerta (EISAS) al servicio de los ciudadanos y las PYME, que se construirá con recursos y capacidades nacionales **para 2013**, según se anunció en la Estrategia de Seguridad Interior.

Asociación público-privada europea de resistencia (EP3R)

Logros

– La EP3R fue lanzada en 2009 con el objetivo de constituir un marco de gobernanza europea para la resistencia de las infraestructuras de TIC, que estimularía la cooperación entre el sector público y el privado en torno a objetivos de seguridad y resistencia, requisitos de referencia, buenas prácticas y medidas recomendadas. Como se afirma en la Estrategia de Seguridad Interior, la EP3R *«debería comprometerse con socios internacionales para reforzar la gestión de los riesgos globales de las redes informáticas»*. La ENISA ha facilitado las actividades de la EP3R.

– Se ha consultado a las partes interesadas privadas y públicas para concebir los objetivos, principios y estructura de la EP3R, así como para establecer incentivos que lleven a los actores pertinentes a involucrarse de forma activa[33]. En la propuesta de modernización de la ENISA se determinaron áreas prioritarias para la AP3R[34].

– De forma paralela a la concepción de la estructura de la EP3R, a finales de 2010 se lanzaron tres grupos de trabajo que se encargaban de: a) los bienes, recursos y funciones imprescindibles para la provisión continuada y segura de comunicaciones electrónicas en todos los países; b) los requisitos de referencia para la seguridad y resistencia de las comunicaciones electrónicas; c) las necesidades de coordinación y cooperación y los mecanismos necesarios para prevenir y reaccionar ante perturbaciones a gran escala que afecten a las comunicaciones electrónicas.

– En 2010 la propuesta de la Comisión de modernización de ENISA proporcionó a la EP3R un marco sostenible a largo plazo: en ella se afirmaba que ENISA debería «*apoyar la cooperación entre las partes interesadas públicas y privadas a nivel de la Unión, entre otras cosas promoviendo el intercambio de información y la sensibilización y facilitando sus esfuerzos en relación con el desarrollo y la adopción de normas para la gestión del riesgo y la seguridad de los productos, redes y servicios electrónicos*».

Próximas etapas

– En 2011, la EP3R seguirá fomentando la cooperación entre los actores de los sectores público y privado con el fin de mejorar la seguridad y la resistencia merced a medidas e instrumentos innovadores, así como de determinar las responsabilidades de aquéllos. Aprovechando el impulso y el respaldo prestados por ENISA, los grupos de trabajo de la EP3R comenzarán a entregar sus resultados. Utilizando como base la labor preparatoria

[33] Véase http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/impl_activities/index_en.htm

[34] COM(2010) 521.

efectuada por la Comisión y ENISA, los futuros trabajos abordarán los problemas de ciberseguridad que se plantean para las redes inteligentes.

– EP3R servirá como plataforma de difusión mundial sobre los aspectos de la política, la economía y el mercado relevantes para la seguridad y la resistencia. La Comisión tiene la intención de impulsar la EP3R para que respalde las actividades del Grupo de trabajo UE-EE.UU. sobre ciberseguridad y ciberdelincuencia al objeto de crear un entorno coherente de cooperación entre los sectores público y privado, respetando al mismo tiempo la normativa de ayudas estatales vigente.

– A largo plazo, y en consonancia con la propuesta de nuevo Reglamento de ENISA, se pretende que la EP3R se convierta en una actividad clave la ENISA modernizada.

Foro Europeo de Estados miembros (EFMS)

Logros

– En 2009 se instituyó el EFMS con el fin de fomentar el debate y el intercambio entre las autoridades públicas en materia de buenas prácticas y de compartir objetivos y prioridades políticas en materia de seguridad y resistencia de la infraestructura de TIC, así como beneficiarse directamente del trabajo y del apoyo prestado por la ENISA. El EFMS, que se reúne de forma trimestral, cuenta desde mediados de 2010 con un portal web específico gestionado por la ENISA.

– El EFMS ha efectuado progresos significativos en diferentes campos: a) la fijación de criterios que identifiquen las infraestructuras europeas de las TIC en el contexto de la Directiva sobre la identificación y designación de infraestructuras críticas europeas[35]; b) la determinación de prioridades, principios y directrices europeas para la resistencia y estabilidad de Internet; c) el intercambio de buenas prácticas, en particular en materia de ciberejercicios.

– Los Estados miembros reconocen que el EFMS es una importante plataforma de debate e intercambio de buenas prácticas[36].

Próximas etapas

– En 2011 el EFMS pondrá término a los debates técnicos en torno a los criterios de TIC para las infraestructuras críticas europeas y proporcionará unas orientaciones y prioridades a largo plazo aplicables a los ejercicios paneuropeos a gran escala sobre la seguridad de las redes y la información.

– El EFMS participará nuevamente en debates sobre las prioridades en el ámbito de la divulgación a nivel internacional en materia de seguridad y resistencia, sobre todo en relación con las actividades del Grupo de trabajo UE-EE.UU. sobre ciberseguridad y ciberdelincuencia.

---

35 Directiva del Consejo 2008/114/CE.

36 La respuesta del Gobierno del Reino Unido al Quinto informe de la Comisión de la Unión Europea de la Cámara de los Lores sobre el plan de acción PICI afirma que el EFMS *«ha constituido un éxito y ha colmado una necesidad real de los decisores políticos, la de poder intercambiar experiencias»*.

– Las futuras áreas prioritarias de actividad del EFMS, que contará con el apoyo directo y los recursos de ENISA, serán las siguientes[37]: buscar formas de cooperación efectiva con los CERT nacionales/gubernamentales; promover unos requisitos mínimos en el ámbito de la contratación pública con el fin de fomentar la ciberseguridad; determinar incentivos económicos y reglamentarios para impulsar la seguridad y la resistencia (respetando al mismo tiempo la normativa de ayudas estatales vigente); evaluar el «estado de salud de la ciberseguridad» en Europa.

2. Detección y respuesta

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

Logros

– La Comisión ha financiado dos prototipos, FISHAS y NEISAS, que en la actualidad están arrojando sus resultados finales.

– Partiendo del informe de viabilidad de 2007[38] y del análisis de proyectos pertinentes a nivel nacional y europeo, la ENISA realizó una elaborada hoja de ruta para la creación de EISAS en 2013[39].

Próximas etapas

– En 2011 la ENISA dará su apoyo a los Estados miembros en la ejecución de la hoja de ruta del EISAS y desarrollará los «servicios básicos» que utilizarán los Estados miembros para crear su sistema de intercambio de información y alerta (ISAS) a partir de sus CERT nacionales/gubernamentales.

– En 2012 la ENISA desarrollará los «servicios de interoperabilidad» que permitan a cada ISAS nacional integrarse funcionalmente en el EISAS. La ENISA asistirá también a los Estados miembros en el ensayo de tales servicios a través de una integración progresiva de los sistemas nacionales.

– A lo largo de 2011-2012 la ENISA instará a los CERT nacionales/gubernamentales a integrar la capacidad de ISAS en sus servicios.

3. Mitigación y recuperación

Planificación y ejercicios nacionales de contingencia.

Logros

– A finales de 2010, 12 Estados miembros habían desarrollado un plan nacional de contingencia u organizado ejercicios de respuesta ante incidentes a gran escala de seguridad de las redes y de recuperación en caso de catástrofes[40].

---

37 COM(2010) 251.

38 Véase http://www.enisa.europa.eu/act/cert/other-work/files/EISAS_finalreport.pdf

39 http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas_roadmap

40 Véase: http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises/national-exercise-good-practice-guide/at_download/fullReport.

– Partiendo de experiencias nacionales e internacionales, la ENISA elaboró una guía de buenas prácticas para ejercicios nacionales[41]; organizó en todo el mundo eventos con los Estados miembros y los CERT acerca de los ejercicios nacionales; y, más recientemente, difundió unas recomendaciones en materia de política de desarrollo de estrategias nacionales, en las que los CERT/CSIRT nacionales/gubernamentales desempeñan un papel esencial a la hora de dirigir ejercicios y ensayos nacionales de contingencia con la participación de agentes privados y públicos[42].

Próximas etapas

– La ENISA seguirá prestado su apoyo a los Estados miembros en la elaboración de los planes nacionales de contingencia y la organización de ejercicios periódicos de respuesta ante incidentes a gran escala de seguridad de las redes y de recuperación en caso de catástrofe, como vía hacia una cooperación paneuropea más estrecha.

Ejercicio paneuropeo sobre incidentes a gran escala de seguridad de las redes

Logros

– El primer ejercicio paneuropeo sobre incidentes a gran escala de seguridad de las redes *(Cyber Europe 2010)* se celebró el 4 de noviembre de 2010 y contó con la participación de todos los Estados miembros, 19 de los cuales tomaron parte activa en el ejercicio, y también de Suiza, Noruega e Islandia. El ejercicio fue organizado y evaluado[43] por la ENISA con la participación activa en el equipo de planificación de ocho Estados miembros y el respaldo tecnológico del Centro Común de Investigación (JCR).

Próximas etapas

– En 2011 los Estados miembros emprenderán un debate sobre el objetivo y alcance del próximo ciberejercicio paneuropeo, previsto para 2012. Se considerará la posibilidad de un enfoque con varias fases en el que un grupo menor de Estados miembros llevarían a cabo ejercicios más avanzados, quizá con la participación de socios internacionales. La ENISA seguiría respaldando el proceso.

– La Comisión ofrece su apoyo financiero al proyecto EuroCybex, que en el segundo semestre de 2011 llevará a cabo un ejercicio de simulación.

– Los ciberejercicios constituyen un elemento importante de cualquier estrategia coherente de planificación de contingencias en materia de ciberincidentes, tanto a nivel nacional como europeo. Por lo tanto, los ciberejercicios paneuropeos futuros deben basarse en un plan europeo de contingencia en materia de ciberincidentes elaborado a partir de los planes nacionales de contingencia (y que a la vez servirá para interconectarlos). Este plan debe proporcionar los mecanismos y procedimientos de referencia para las comunicaciones entre Estados miembros y, lo que también es importante, un respaldo para la concepción y organización de futuros ejercicios paneuropeos. La ENISA trabajará con los Estados

41 Véase: http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises/national-exercise-good-practice-guide/at_download/fullReport.

42 Véase: http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations.

43 Véase http://www.enisa.europa.eu/.

miembros en el desarrollo de este plan de contingencia en materia de ciberincidentes que deberá estar listo para 2012. En el mismo periodo todos los Estados miembros deberán desarrollar planes nacionales de contingencia regulares y ejercicios de respuesta y recuperación. La coordinación necesaria para alcanzar este resultado correrá a cargo del EFMS.

Mayor cooperación entre CERT nacionales/gubernamentales.

Logros

– La cooperación entre los CERT nacionales/gubernamentales se ha intensificado. El trabajo de la ENISA en torno a las capacidades de referencia de los CERT nacionales/gubernamentales, a los ejercicios de éstos y los ejercicios nacionales, y a la gestión de ciberincidentes, ha contribuido a fortalecer la cooperación paneuropea entre los CERT nacionales/gubernamentales.

Próximas etapas

– La ENISA seguirá respaldando la cooperación entre los CERT nacionales/gubernamentales. Para ello, en 2011 analizará los requisitos que debe cumplir el canal seguro de comunicación con los CERT y facilitará unas orientaciones sobre ello, incluida una hoja de ruta para su ejecución y desarrollo futuro. La ENISA analizará también las carencias operativas que existen a nivel europeo y presentará un informe de cómo puede reforzarse la colaboración transfronteriza entre los CERT y las partes interesadas, sobre todo en materia de coordinación en la respuesta a los incidentes.

– La ADE insta a los Estados miembros a establecer, para **2012**, una red de CERT a nivel nacional que funcione eficazmente.

4. Cooperación internacional

Resistencia y estabilidad de Internet

Logros

– Partiendo de los trabajos realizados por el EFMS, se han desarrollado unos principios y directrices europeos sobre resistencia y estabilidad de Internet[44].

Próximas etapas

– En 2011 la Comisión: debatirá y promoverá estos principios tanto de forma bilateral con los socios internacionales, en particular los EE.UU., como de forma multilateral con el G8, la OCDE, Meridian y la UIT; consultará con las partes interesadas más relevantes, en particular del sector privado, tanto a nivel europeo (vía la EP3R) como internacional (vía el Foro de gobernanza de Internet y otros foros apropiados); y promoverá el debate con los principales agentes y organizaciones de Internet.

[44] Véase http://ec.europa.eu/information_society/policy/nis/index_en.htm

– En 2012 los socios internacionales harán lo posible para que estos principios y orientaciones constituyan un marco común de compromiso colectivo internacional en torno a la resistencia y estabilidad de Internet a largo plazo.

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

Logros

– Siete Estados miembros[45] participaron en el ciberejercicio norteamericano «Cyber Storm III» como asociados internacionales. La Comisión y ENISA participaron como observadores.

Próximas etapas

– En 2011 la Comisión desarrollará, en el marco del Grupo de trabajo UE-EE.UU. sobre ciberseguridad y ciberdelincuencia, un programa común y una hoja de ruta ante la perspectiva de la celebración de unos ciberejercicios conjuntos/sincronizados transcontinentales en 2012/2013. Se estudiarán las posibilidades para integrar en el proceso a otras regiones o países que conozcan problemas similares para compartir estrategias y actividades.

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

Criterios sectoriales específicos para determinar las infraestructuras críticas europeas de las TIC

Logros

– Los debates técnicos en el EFMS en torno a los criterios sectoriales específicos de las TIC ha llevado al establecimiento de un proyecto de criterios aplicables a las comunicaciones móviles y fijas y a Internet.

Próximas etapas

– El EFMS proseguirá sus estudios técnicos en torno a los criterios sectoriales específicos para las TIC con el fin de completarlos para finales de 2011. De forma paralela está prevista la celebración de consultas con el sector privado acerca del proyecto de criterios para el sector de las TIC, tanto a nivel de determinados Estados miembros como a nivel europeo, vía la EP3R.

– La Comisión debatirá con los Estados miembros los elementos específicos del sector de las TIC que deban tenerse en cuenta para la revisión en 2012 de la Directiva 2008/114/CE sobre la identificación y designación de infraestructuras críticas europeas.

–

[45] FR, DE, HU, IT, NL, SE y UK.