COMISIÓN DE LAS COMUNIDADES EUROPEAS

Bruselas, 31.5.2006
COM(2006) 251 final

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

Una estrategia para una sociedad de la información segura – «Diálogo, asociación y potenciación»

{SEC(2006) 656}

ÍNDICE

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

Una estrategia para una sociedad de la información segura – «Diálogo, asociación y potenciación»

1. INTRODUCCIÓN

La Comunicación «i2010 – Una sociedad de la información europea para el crecimiento y el empleo»[1], subrayó la importancia de la seguridad de las redes y de la información para la creación de un espacio único europeo de la información. La disponibilidad, fiabilidad y seguridad de las redes y los sistemas de información son cada vez más esenciales para nuestras economías y para el entramado de nuestra sociedad.

La finalidad de la presente Comunicación es revitalizar la estrategia de la Comisión Europea establecida en 2001 en la Comunicación «Seguridad de las redes y de la información: Propuesta para un enfoque político europeo»[2]. En ella se pasa revista a la situación actual de las amenazas a la seguridad de la sociedad de la información y se determina qué pasos complementarios convendría dar para mejorar la seguridad de las redes y de la información (SRI).

Apoyándose en la experiencia adquirida tanto a nivel de los Estados miembros como de la Comunidad Europea, se pretende seguir desarrollando una estrategia global y dinámica en Europa, basada en una cultura de la seguridad y fundamentada en **el diálogo, la asociación y la potenciación**.

Para afrontar los retos que se plantean a la sociedad de la información en el ámbito de la seguridad, la Comunidad Europea ha elaborado un planteamiento a tres niveles que incluye: las medidas específicas para la seguridad de las redes y de la información, el marco regulador de las comunicaciones electrónicas (que incluye cuestiones relativas a privacidad y protección de datos) y la lucha contra la ciberdelincuencia. Aunque, hasta cierto punto, sea posible desarrollar estos tres aspectos por separado, las numerosas interdependencias existentes justifican una estrategia coordinada. La presente Comunicación expone dicha estrategia y establece un marco que permitirá llevar adelante y perfeccionar un enfoque coherente en relación con la SRI.

En la Comunicación de 2001 se definía la SRI como «*la capacidad de un red o un sistema de información para resistir, con un determinado nivel de confianza, los efectos de accidentes o actos malintencionados que podrían poner en peligro la disponibilidad, autenticidad, integridad y confidencialidad de datos almacenados o transmitidos, y de los servicios relacionados ofrecidos a través de estas redes y sistemas*». En los últimos años, la Comunidad Europea ha llevado a cabo diversas actuaciones destinadas a mejorar la SRI.

---

1 COM(2005) 229 final de 1.6.2005.

2 COM(2001) 298 final de 6.6.2001.

El marco regulador de las comunicaciones electrónicas, cuya revisión se ha emprendido ya, incluye disposiciones relacionadas con la seguridad. En particular, la Directiva sobre privacidad y comunicaciones electrónicas[3] impone a los proveedores de servicios de comunicaciones electrónicas disponibles para el público la obligación de proteger la seguridad de sus servicios. También existen disposiciones contra el *spam*[4] y los programas espía (*spyware*)[5].

La confianza y la seguridad desempeñan también un papel importante en los programas de la Comunidad Europea dedicados a la investigación y al desarrollo. El Sexto Programa Marco de investigación aborda estas cuestiones a través de una amplia gama de proyectos. La investigación relacionada con la seguridad se reforzará en el Séptimo Programa Marco con la creación de un programa europeo de investigación sobre seguridad (ESRP)[6]. Además, el programa sobre la seguridad de Internet apoya los proyectos de creación de redes y el intercambio de mejores prácticas para combatir los contenidos nocivos que circulan por las redes de información.

Como parte integrante de su respuesta a las amenazas a la seguridad, la Comunidad Europea decidió en 2004 crear la Agencia Europea de Seguridad de las Redes y de la Información (ENISA). ENISA contribuye al desarrollo de una cultura de la seguridad de las redes y de la información en beneficio de ciudadanos, consumidores, empresas y organismos del sector público en toda la Unión Europea (UE).

La UE trabaja asimismo activamente en los foros internacionales en los que se abordan estos temas, como la OCDE, el Consejo de Europa o las Naciones Unidas. En la Cumbre Mundial sobre la Sociedad de la Información celebrada en Túnez, la UE prestó su decidido apoyo a los debates sobre la disponibilidad, fiabilidad y seguridad de las redes y de la información. El Programa de Acciones de Túnez[7], que, junto con el Compromiso de Túnez, define nuevos pasos para el debate político sobre la sociedad de la información global según lo han respaldado los líderes mundiales, hace hincapié en la necesidad de seguir luchando contra la ciberdelincuencia y el *spam* al tiempo que se garantiza la protección de la privacidad y la libertad de expresión. En él se señala la necesidad de llegar a un entendimiento común sobre los asuntos relativos a la seguridad en Internet, así como de ampliar la cooperación para facilitar la recopilación y la diseminación de la información relativa a la seguridad, e intercambiar prácticas idóneas entre todas las partes interesadas en las medidas para combatir las amenazas a la seguridad.

2. MEJORAR LA SEGURIDAD DE LA SOCIEDAD DE LA INFORMACIÓN: RETOS CLAVE

Pese a los esfuerzos desplegados a nivel internacional, europeo y nacional, la seguridad sigue planteando difíciles problemas.

---

3 Directiva 2002/58/CE.

4 Se trata de las comunicaciones comerciales no deseadas.

5 Se trata de programas de rastreo implantados sin que el usuario haya sido adecuadamente informado, lo haya consentido o pueda controlarlo.

6 El ESPR se está preparando mediante una Acción preparatoria de investigación sobre seguridad durante el período 2004-2006.

7 *Hacia una asociación mundial para la sociedad de la información: Seguimiento de la Fase de Túnez de la Cumbre Mundial sobre la Sociedad de la Información (CMSI)*, COM(2006) 181 final de 27.4.2006.

En primer lugar, los ataques a los sistemas de información están motivados cada vez en mayor medida por el afán de lucro, más que por el mero deseo de sembrar el caos. Se extraen datos ilegalmente, cada vez más a menudo sin conocimiento del usuario, y el número de variantes (y el ritmo de evolución) del *software* malicioso[8] aumenta con rapidez. El *spam* constituye un buen ejemplo de esta evolución, pues está convirtiéndose en vehículo de virus y de actividades fraudulentas y delictivas, como los programas espía, el *phishing*[9] y otras formas de *software* malicioso. Su difusión se apoya cada vez más en las *botnets*[10], es decir, redes de servidores y PC afectados que actúan de distribuidores sin conocimiento de sus propietarios.

La difusión creciente de los dispositivos móviles (incluidos los teléfonos móviles de 3G, las consolas de videojuegos portátiles, etc.) y de los servicios basados en las redes móviles supondrá la aparición de nuevos retos, al desarrollarse rápidamente los servicios basados en el IP. Con el tiempo, podrían llegar a ser una vía más corriente para efectuar ataques que el ordenador personal, pues este disfruta ya de un nivel importante de seguridad. En realidad, cualquier nuevo tipo de plataforma de comunicación y sistema de información representa de modo inevitable una nueva oportunidad para posibles ataques maliciosos.

Otro acontecimiento significativo es el advenimiento de los «entornos inteligentes», en los que los dispositivos inteligentes apoyados en la tecnología de la computación y las redes estarán por todas partes (p. ej., a través de la RFID[11], el IPv6 y las redes de sensores). Una vida cotidiana totalmente interconectada y puesta en red podría ofrecer interesantes oportunidades, pero crearía al mismo tiempo nuevos riesgos para la seguridad y la privacidad. Aun cuando las plataformas y aplicaciones comunes contribuyan positivamente a la interoperabilidad y a la expansión de las tecnologías de la información y la comunicación (TIC), también pueden acrecentar los riesgos. Por ejemplo, cuanto más se utilice el *software* comercial, más repercusión tendrá el descubrimiento de un punto vulnerable o la existencia de un fallo. La aparición de «monocultivos» en las plataformas y aplicaciones informáticas puede facilitar enormemente el crecimiento y la difusión de amenazas para la seguridad tales como los programas maliciosos y los virus. **La diversidad, la apertura y la interoperabilidad son parte integrante de la seguridad y conviene promoverlas**.

La importancia del sector de las TIC para la economía europea, así como para la sociedad europea en su conjunto, es incontestable. Las TIC constituyen un componente esencial de la innovación, responsable de casi el 40 % del crecimiento de la productividad. Además, este sector tan innovador realiza más de la cuarta parte del esfuerzo europeo de I+D total y desempeña un papel esencial en el crecimiento económico y la creación de puestos de trabajo en toda la economía. Cada vez son más los europeos que viven en una auténtica sociedad basada en la información en la que el uso de las TIC se ha acelerado rápidamente en tanto que función básica de la interacción humana, tanto social como económica. Según Eurostat, el 89 % de las empresas de la UE utilizaban activamente Internet en 2004 y alrededor del 50 % de los consumidores la ha utilizado recientemente[12].

---

8 El denominado *malware*.

9 El *phishing* es una forma de fraude en Internet cuyo propósito es el robo de información valiosa tal como los números de cuenta bancaria o de tarjeta de crédito o los identificadores y contraseñas de los usuarios.

10 Las *botnets,* o redes de robots, son aplicaciones que, instaladas secretamente en una máquina víctima, ejecutan acciones por cuenta de un controlador remoto.

11 Identificación por radiofrecuencias.

12 Eurostat, *Internet activities in the European Union*, 40/2005.

Una violación de la SRI puede tener repercusiones que vayan más allá de la dimensión económica. Preocupa, incluso, el hecho de que los problemas de seguridad puedan desalentar a los usuarios y dificultar la adopción de las TIC, ya que la disponibilidad, la fiabilidad y la seguridad son requisitos previos para garantizar los derechos fundamentales en línea.

Además, dada la creciente conectividad entre las redes, otras infraestructuras críticas (como las de transporte, energía, etc.) cada vez dependen más de la integridad de sus respectivos sistemas de información.

En Europa, empresas y ciudadanos siguen subestimando los riesgos. Esto se debe a varias razones, entre las que la más importante parece ser la escasa visibilidad de la rentabilidad de las inversiones en seguridad en el caso de las empresas, y el desconocimiento de su responsabilidad en la cadena de la seguridad global en el de los ciudadanos.

Pero lo cierto es que, dada la omnipresencia de las TIC y de los sistemas de información, la seguridad de las redes y de la información representa un reto para todos:

- para las **administraciones públicas**, que tienen que afrontar la seguridad de sus sistemas, no sólo para proteger la información del sector público, sino también para dar ejemplo de buenas prácticas al resto de los agentes;

- para las **empresas**, que necesitan abordar la SRI como un activo y un elemento de ventaja competitiva, no ya como un «coste negativo»;

- para los **particulares**, que deben entender que sus sistemas domésticos resultan críticos para el conjunto de la «cadena de la seguridad».

Para poder hacer frente adecuadamente a los problemas que se han descrito, todas las partes interesadas necesitan datos fiables sobre los incidentes y tendencias en materia de seguridad de la información. Sin embargo, no es fácil obtener datos fiables y completos sobre estos incidentes, por razones diversas que van de la rapidez con que se producen los eventos relacionados con la seguridad a la escasa disposición de algunas organizaciones para revelar y hacer públicas las violaciones de la seguridad. Pese a ello, una de las claves para el desarrollo de una cultura de la seguridad es un **mejor conocimiento del problema** planteado.

Es importante que los programas de sensibilización, pensados para resaltar las amenazas a la seguridad, no minen la confianza de los consumidores y usuarios por centrarse exclusivamente en los aspectos negativos de la seguridad. Siempre que sea posible, **debe presentarse la SRI como una ventaja y una oportunidad**, no como un lastre y un coste. Es necesario considerarla un activo para ganar la confianza del consumidor, una ventaja competitiva para las empresas que explotan sistemas de información y un elemento de la calidad del servicio para los prestadores de servicios tanto del sector público como del privado.

El reto más importante para los responsables de formular las políticas es adoptar un enfoque totalizador, en el que se reconozcan los papeles respectivos de las distintas partes interesadas y se garantice una coordinación adecuada de las diversas disposiciones reguladoras y de política pública que afectan directa o indirectamente a la SRI. Los procesos de liberalización, desregulación y convergencia han creado una multiplicidad de agentes entre los distintos grupos de partes interesadas que no facilita precisamente esta tarea. ENISA puede hacer una aportación importante al logro de este objetivo, sirviendo como centro de comunicación de la

información y de cooperación entre todas las partes interesadas, así como de intercambio de prácticas recomendables, tanto en Europa como con el resto del mundo, a fin de contribuir a la competitividad de nuestras industrias de TIC y al buen funcionamiento del mercado interior.

3. HACIA UN ENFOQUE DINÁMICO DE LA SOCIEDAD DE LA INFORMACIÓN SEGURA

Una sociedad de la información segura debe basarse en una **SRI mejorada** y en una **cultura de la seguridad** generalizada. A tal efecto, la Comisión Europea propone un **enfoque dinámico e integrado** que implique a todas las partes interesadas y se base en **el diálogo, la asociación y la potenciación**. Dado que los sectores público y privado desempeñan papeles complementarios en la creación de una cultura de la seguridad, las iniciativas políticas en este campo deben basarse en un **diálogo abierto e incluyente entre las múltiples partes interesadas**.

Este enfoque, junto con las actuaciones asociadas, complementará y enriquecerá el plan de la Comisión para seguir elaborando un marco político dinámico y completo a través de diversas iniciativas en 2006:

(1) Abordar la evolución del *spam* y de amenazas como los programas espía y otros tipos de programas maliciosos en una Comunicación sobre estos temas concretos.

(2) Formular propuestas para mejorar la cooperación entre las autoridades policiales y judiciales y abordar las nuevas formas de actividad delictiva que se sirven de Internet y socavan el funcionamiento de infraestructuras críticas. Tal será el tema de una Comunicación específica sobre la ciberdelincuencia.

Estas iniciativas políticas complementan asimismo la actividad que está planificándose para alcanzar los objetivos del Libro Verde de la Comisión sobre un programa europeo para la protección de infraestructuras críticas (EPCIP)[13], elaborado en respuesta a una solicitud del Consejo de diciembre de 2004. El proceso relacionado con este Libro Verde desembocará probablemente en un plan de acción que combine un marco global para la protección de las infraestructuras críticas junto con las necesarias políticas sectoriales, incluida la referente al sector de las TIC. Esta última examinará, a través de un **diálogo entre las múltiples partes interesadas**, los factores económicos, empresariales y sociales pertinentes que permitirían impulsar la seguridad y la resistencia de las redes y los sistemas de información.

Además, la revisión en 2006 del marco regulador de las comunicaciones electrónicas examinará también elementos que podrían mejorar la SRI, tales como medidas técnicas y organizativas para su adopción por los proveedores de servicios, disposiciones relativas a la notificación de las violaciones de la seguridad y procedimientos y sanciones específicos en relación con el incumplimiento de las obligaciones.

Corresponde básicamente al sector privado ofrecer soluciones, servicios y productos de seguridad a los usuarios finales. Por ello, es de importancia estratégica que la **industria europea sea tanto usuaria exigente** de los productos de seguridad **como proveedora competitiva** de productos y servicios de SRI.

---

[13] COM(2005) 576 final de 17.11.2005.

Es necesario que los gobiernos nacionales puedan identificar y aplicar las mejores prácticas en materia de formulación de políticas, así como demostrar su compromiso con estos objetivos políticos gestionando sus propios sistemas de información de manera segura. Las autoridades públicas, en los Estados miembros y a nivel de la UE, deben desempeñar un papel clave en el proceso de informar adecuadamente a los usuarios para que éstos puedan contribuir a su propia seguridad. La sensibilización sobre las cuestiones relacionadas con la SRI y la entrega de una información apropiada y oportuna, a través de portales en Internet dedicados a la seguridad electrónica, sobre las amenazas, riesgos y alertas, así como sobre las mejores prácticas, debe considerarse prioritaria. A tal efecto, un objetivo importante de ENISA podría ser estudiar si resulta viable la **creación de un sistema europeo multilingüe de comunicación de información y alertas** que se apoyaría en las iniciativas nacionales públicas y privadas ya existentes o previstas y las conectaría.

La dimensión mundial de la seguridad de las redes y de la información reta a la Comisión, tanto a nivel internacional como en coordinación con los Estados miembros, a redoblar sus esfuerzos de **promoción de la cooperación mundial en materia de SRI**, en particular aplicando el programa aprobado en la Cumbre Mundial sobre la Sociedad de la Información (CMSI) en noviembre de 2005.

Por último, la investigación y el desarrollo, especialmente a escala de la UE, contribuirán a crear asociaciones nuevas e innovadoras que impulsen el crecimiento de la industria europea de las TIC en general y de la seguridad de las TIC en particular. La Comisión, por consiguiente, tratará de garantizar la asignación de recursos financieros adecuados a la investigación sobre la SRI y las tecnologías de la seguridad de funcionamiento dentro del 7º Programa Marco de la UE.

3.1. Diálogo

3.1.1. *Como primer paso para profundizar el diálogo entre las autoridades públicas, la Comisión propone la puesta en marcha de un ejercicio de* ***evaluación comparativa de las políticas nacionales relacionadas con la SRI****, incluidas las políticas de seguridad específicas para el sector público. Este ejercicio ayudará a descubrir las prácticas más efectivas, de manera que puedan ser aplicadas más ampliamente en la UE cuando sea posible, y a que las administraciones públicas impulsen las mejores prácticas en materia de seguridad. Los trabajos sobre identificación electrónica, por ejemplo dentro del reciente plan de acción sobre administración electrónica, podrían desempeñar un papel importante al respecto.*

Si se estructuran adecuadamente, los resultados de este ejercicio de evaluación comparativa pondrán de manifiesto cuáles son las **mejores prácticas para sensibilizar a ciudadanos y PYME sobre la necesidad** de afrontar sus particulares retos y requisitos en materia de SRI, así como su capacidad para hacerlo. Debería recurrirse a ENISA para que tomara parte activa tanto en este diálogo como en la consolidación y el intercambio de las mejores prácticas.

3.1.2. *Resulta necesario un* ***debate estructurado entre las múltiples partes interesadas*** *sobre la mejor manera de explotar las herramientas y los instrumentos reguladores existentes para alcanzar un equilibrio social adecuado entre la seguridad y la protección de los derechos fundamentales, entre ellos la privacidad. La Conferencia «i2010, hacia una sociedad de la información europea omnipresente», que organizará la próxima Presidencia finlandesa, y la consulta sobre las consecuencias*

de la RFID para la seguridad y la privacidad, que forma parte de una consulta más general que la Comisión ha puesto en marcha recientemente, contribuirán a alimentar este debate. Además, la Comisión organizará:

- Un acto empresarial destinado a fomentar el compromiso de la industria con la adopción de enfoques efectivos para la implantación de una cultura de la seguridad **en la industria**.

- Un seminario de reflexión sobre cómo sensibilizar acerca de la seguridad y reforzar la confianza de los **usuarios finales** en el uso de las redes y los sistemas de información electrónicos.

3.2. Asociación

3.2.1. *Para poder formular eficazmente una política es imprescindible comprender claramente la naturaleza y el alcance de los retos planteados. Esto exige no solamente disponer de datos económicos y estadísticos fiables y actualizados tanto sobre los incidentes relacionados con la seguridad de la información como con los niveles de confianza de los consumidores y usuarios, sino también de datos actualizados sobre el tamaño y las tendencias de la industria de la seguridad de las TIC en Europa. La Comisión se propone solicitar a ENISA que desarrolle una* ***asociación de confianza con los Estados miembros y las partes interesadas*** *a fin de elaborar un* ***marco adecuado para la recogida de datos****, que incluya procedimientos y mecanismos que permitan recopilar y analizar datos referidos a la totalidad de la UE sobre incidentes relacionados con la seguridad y sobre la confianza de los consumidores.*

Paralelamente, y a la vista de la considerable fragmentación del mercado en la UE y de su especificidad, la Comisión invitará a los Estados miembros, al sector privado y a los investigadores a **establecer una asociación estratégica** para garantizar la disponibilidad de datos sobre la industria de la seguridad de las TIC y sobre las tendencias cambiantes del mercado de productos y servicios en la UE.

3.2.2. A fin de mejorar la capacidad de Europa para hacer frente a las amenazas a la *seguridad de la redes, la Comisión solicitará a ENISA que examine la* ***viabilidad de un sistema europeo de comunicación de información y alerta*** *que facilite la reacción efectiva ante las amenazas actuales y emergentes que afecten a las redes electrónicas. Un requisito de tal sistema será un* ***portal multilingüe de la UE*** *que proporcione información a la medida sobre amenazas, riesgos y alertas.*

3.3. Potenciación

Potenciar el papel de cada uno de los grupos interesados es un requisito previo para sensibilizar sobre los riesgos y necesidades en materia de seguridad a fin de promover la SRI.

3.3.1. *En este contexto, la Comisión invita a los* ***Estados miembros*** *a:*

- Participar proactivamente en los ejercicios de evaluación comparativa de las políticas nacionales de SRI propuestos.

- Promover, en estrecha cooperación con ENISA, campañas de sensibilización sobre las virtudes, beneficios y ventajas asociados a la adopción de unas tecnologías, prácticas y comportamientos efectivos en relación con la seguridad.

- Impulsar el despliegue de servicios de administración electrónica destinados a comunicar y fomentar las buenas prácticas de seguridad, que luego podrían extenderse a otros sectores.

- Estimular la elaboración de programas de seguridad de redes y de la información dentro de los planes de estudio de la educación superior.

3.3.2. *La Comisión invita asimismo a las partes interesadas del* ***sector privado*** *a adoptar iniciativas encaminadas a:*

- Definir adecuadamente las responsabilidades de los productores de *software* y los proveedores de servicios de Internet en relación con el suministro de unos niveles de seguridad adecuados y auditables. Es necesario, en este contexto, apoyar los procesos normalizados que se ajusten a unos niveles de seguridad y unas reglas de mejores prácticas aprobados de común acuerdo.

- Fomentar la diversidad, la apertura, la interoperabilidad, la facilidad de uso y la competencia como elementos clave para impulsar la seguridad y estimular el despliegue de productos, procesos y servicios que favorezcan la seguridad a fin de evitar y combatir la sustracción de la identidad y otros ataques contra la privacidad.

- Difundir las buenas prácticas en materia de seguridad para operadores de redes, proveedores de servicios y PYME como niveles elementales de seguridad y continuidad empresarial.

- Fomentar los programas de formación en el sector empresarial, en particular para las PYME, de manera que se dote a los empleados de los conocimientos y aptitudes necesarios para aplicar con eficacia las prácticas de seguridad.

- Trabajar en favor de unos regímenes de certificación de la seguridad aplicables a productos, procesos y servicios que sean asequibles y respondan a las necesidades específicas de la UE (en particular, en relación con la privacidad).

- Implicar al sector de los seguros en la elaboración de herramientas y métodos apropiados de gestión del riesgo para hacer frente a los riesgos asociados a las TIC y fomentar una cultura de gestión del riesgo en las organizaciones y las empresas (en particular, en las PYME).

4. CONCLUSIONES

Para determinar cuáles son los retos en materia de seguridad que se plantean en relación con los sistemas de información y las redes en la UE y poder afrontarlos es necesario el compromiso pleno de todas las partes interesadas. El enfoque político propuesto en la presente Comunicación trata de alcanzar este objetivo reforzando un **enfoque de participación de las múltiples partes interesadas** que se apoyaría en los intereses mutuos,

identificaría las funciones de cada uno y crearía un marco dinámico de promoción de iniciativas eficaces tanto de los poderes públicos como del sector privado.

La Comisión informará al Consejo y al Parlamento a mediados de 2007 sobre las actividades emprendidas, los primeros resultados y la situación de cada iniciativa, incluidas las de ENISA y las adoptadas en los Estados miembros y en el sector privado. Si procede, propondrá una Recomendación sobre seguridad de las redes y de la información (SRI).