I

(Resoluciones, recomendaciones, orientaciones y dictámenes)

RESOLUCIONES

CONSEJO

RESOLUCIÓN DEL CONSEJO

de 22 de marzo de 2007

sobre una estrategia para una sociedad de la información segura en Europa

(2007/C 68/01)

EL CONSEJO DE LA UNIÓN EUROPEA,

ADOPTA LA PRESENTE RESOLUCIÓN Y

SE CONGRATULA POR

La 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», presentada el 31 de mayo de 2006.

DESTACA

La Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la lucha contra el spam, los programas espía y los programas maliciosos, presentada el 15 de noviembre de 2006.

RECUERDA

1. La Resolución del Consejo de 28 de enero de 2002 relativa a un enfoque común y a acciones específicas en materia de seguridad de las redes y de la información ([1]).

2. La Resolución del Consejo de 18 de febrero de 2003 sobre un enfoque europeo orientado hacia una cultura de seguridad de las redes y de la información ([2]).

3. Las Conclusiones del Consejo de 8 y 9 de marzo de 2004 relativas a comunicaciones no solicitadas de prospección comercial directa o «spam» y las Conclusiones del Consejo de 9 y 10 de diciembre de 2004 relativas a la lucha contra el «spam».

4. Las Conclusiones del Consejo Europeo de marzo de 2005 por lo que respecta a la renovación de la estrategia de Lisboa y las Conclusiones del Consejo Europeo de marzo de 2006, en las que insta a la Comisión y a los Estados miembros a aplicar resueltamente la nueva Estrategia i2010.

5. El marco reglamentario comunitario en el ámbito de las comunicaciones electrónicas ([3]) y, en particular, las disposiciones en relación con la seguridad, la protección de la intimidad y la confidencialidad de las comunicaciones, que han contribuido a garantizar un alto nivel de protección de los datos personales y de la intimidad de las personas y de la integridad y seguridad de las redes públicas de comunicación.

6. El Reglamento (CE) nº 460/2004, de 10 de marzo de 2004, del Parlamento Europeo y del Consejo por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información ([4]).

7. El Programa de Acciones de Túnez y el Compromiso de Túnez de la Cumbre Mundial sobre la Sociedad de la Información (CMSI) ponen de manifiesto que hay que seguir luchando contra la ciberdelincuencia y el correo basura, al tiempo que se garantiza la protección de la intimidad y la libertad de expresión, y seguir promoviendo, desarrollando y aplicando en cooperación con todas las partes interesadas una cultura global en materia de seguridad informática.

8. Las conclusiones de la Presidencia de la Conferencia anual europea sobre la sociedad de la información: «i2010 — Hacia una sociedad de la información europea omnipresente», que se celebró en Espoo, Finlandia, los días 27 y 28 de septiembre de 2006.

([1]) DO C 43 de 16.2.2002, p. 2.
([2]) DO C 48 de 28.2.2003, p. 1.
([3]) Directivas 2002/58/CE (Directiva sobre la protección de la intimidad en las comunicaciones electrónicas), 2002/20/CE (Directiva sobre la autorización) y 2002/22/CE (Directiva sobre el servicio universal). DO L 201 de 31.7.2002, p. 37, DO L 108 de 24.4.2002, p. 21 y DO L 108 de 24.4.2002, p. 51, respectivamente.
([4]) DO L 77 de 13.3.2004, p. 1.

SUBRAYA A ESTE RESPECTO QUE:

1. Nuestras sociedades están cambiando rápidamente hacia una nueva fase de desarrollo, una sociedad de la información omnipresente, en la que las actividades cotidianas de los ciudadanos se basarán cada vez más en la utilización de las tecnologías de la información y de las comunicaciones (TIC) y en redes de comunicaciones electrónicas; la seguridad de las redes y de la información debe considerarse como un factor clave para que este desarrollo se lleve a cabo con éxito.

2. La confianza es un factor clave para el éxito de la nueva sociedad de la información; la confianza también está relacionada con las experiencias de los usuarios y con el deber de respetar su intimidad; por consiguiente, la seguridad de las redes y de la información no debe considerarse simplemente como un aspecto técnico.

3. La seguridad de las redes y de la información es un elemento fundamental en la creación del espacio europeo de información, que forma parte de la iniciativa i2010 y contribuye de esta forma al cumplimiento de la Estrategia renovada de Lisboa; las TIC son también un elemento clave de innovación, crecimiento económico y empleo en toda la economía.

4. Ya se están desarrollando las nuevas tecnologías que nos llevarán a la sociedad de la información omnipresente; la aparición de tecnologías pioneras (tales como redes inalámbricas de alta velocidad, dispositivos de identificación por radiofrecuencia, redes de sensores) y de servicios de alto contenido e innovadores (tales como la televisión por Internet, la telefonía Internet, la televisión móvil y otros servicios móviles) requieren niveles adecuados de seguridad de las redes y de la información ya desde el comienzo de la fase de desarrollo para que lleguen a tener realmente valor comercial; la rápida adopción de nuevas innovaciones prometedoras es muy importante para el desarrollo de la sociedad de la información y la competitividad de Europa; los organismos oficiales y las empresas deben adoptar las nuevas tecnologías y servicios emergentes en cuanto sean seguros desde el punto de vista práctico para acelerar su uso generalizado.

5. Para la UE es importante desde el punto de vista estratégico que la industria europea sea un usuario exigente y al mismo tiempo un proveedor competitivo de redes y de productos y servicios de seguridad; debe promoverse la diversidad, apertura e interoperabilidad como partes integrantes de la seguridad.

6. El conocimiento y las aptitudes en el ámbito de la seguridad de las redes y de la información deben pasar a formar parte de la vida cotidiana de cada persona y de las distintas partes interesadas de la sociedad; se han llevado a cabo campañas de sensibilización tanto a nivel nacional como de la UE, pero aún queda trabajo en este ámbito, en particular, por lo que se refiere a los usuarios finales y a las pequeñas y medianas empresas (PYME); deberá prestarse especial atención a los usuarios con necesidades específicas o escasamente concienciados con respecto a la seguridad de las redes y de la información; todas las partes interesadas deben ser conscientes de que forman parte de una cadena de seguridad global y deberían estar facultados para actuar como tales; temas relativos a la seguridad de las redes y de la información deberían incluirse en toda formación relacionada con las TIC.

7. La creación de la Agencia Europea de Seguridad de las Redes y de la Información ha sido un paso muy importante en los esfuerzos de la UE para responder a los retos que plantea la seguridad de las redes y de la información; el Reglamento (CE) nº 460/2004 define el ámbito de aplicación, los objetivos, las funciones y la duración de la Agencia.

8. Los recursos destinados a investigación y desarrollo (I+D) e innovación, tanto a nivel nacional como comunitario, constituyen uno de los elementos fundamentales para reforzar el nivel de seguridad de las redes y de la información de los nuevos sistemas, aplicaciones y servicios; debería intensificarse el esfuerzo a nivel europeo en los ámbitos de la investigación y la innovación en relación con la seguridad, en particular, a través del Séptimo programa marco y del Programa marco para la competitividad y la innovación; también habría que realizar esfuerzos en pro de medidas destinadas a la difusión y promoción de la explotación comercial de los resultados, incluida la evaluación de su utilidad para la comunidad en su conjunto, lo que contribuirá a mejorar la capacidad de los proveedores europeos para suministrar soluciones de seguridad que respondan a las necesidades específicas del mercado europeo.

9. La sociedad de la información omnipresente aporta grandes beneficios, pero supone al mismo tiempo un considerable reto y crea, por lo tanto, un nuevo entorno de riesgos potenciales; las amenazas a la seguridad y a la intimidad, incluso a través de la interceptación y explotación ilícitas de datos están siendo cada vez más graves, tienen objetivos más definidos y pretenden lograr un beneficio económico; las nuevas respuestas a las amenazas emergentes y ya existentes deben crearse de forma innovadora e incluir temas relacionados con la complejidad de los sistemas, errores, accidentes e instrucciones confusas; debe fomentarse más la creación y desarrollo a nivel nacional de organismos de respuesta a situaciones de emergencia en el ámbito informático dirigidos a las distintas partes interesadas así como la cooperación entre dichos organismos y con otras partes interesadas pertinentes.

10. La normalización y la certificación de productos, servicios y sistemas de gestión, en particular los suministrados por instituciones existentes, merece especial atención por parte de la política de la UE de seguridad de las redes y de la información como medio para difundir las buenas prácticas y profesionalidad en el ámbito de la seguridad de las redes y de la información; la adopción a su debido tiempo de posibles nuevas normas abiertas e interoperativas sería beneficioso, en particular, para las nuevas tecnologías emergentes tales como los dispositivos de identificación por radiofrecuencia y la televisión móvil; deberían estimularse las actividades de los organismos europeos de normalización en este ámbito.

11. Habida cuenta de que las redes y los sistemas de información electrónicos desempeñan un papel cada vez más importante en el funcionamiento global de infraestructuras esenciales, su disponibilidad e integridad resultan imprescindibles para la seguridad y calidad de vida de los ciudadanos, y de las administraciones y empresas, así como para el funcionamiento general de las sociedades.

12. La cooperación y unos planteamientos pragmáticos son más necesarios que nunca; las diferentes partes interesadas deberían determinar y reconocer sus funciones, responsabilidades y derechos respectivos.

Y POR CONSIGUIENTE INVITA A LOS ESTADOS MIEMBROS A:

1. Apoyar los programas de formación y a mejorar la sensibilización en relación con la seguridad de las redes y de la información, por ejemplo, mediante campañas de información sobre la seguridad de las redes y de la información, destinadas a todos los ciudadanos, usuarios y sectores de la economía, en particular, las PYME y los usuarios finales con necesidades especiales o escasamente sensibilizados; para antes de 2008 podría elegirse una fecha común como día europeo de sensibilización (por ejemplo: «día de la seguridad de las redes y de la información») que cada Estado miembro celebraría cada año de forma voluntaria.

2. Incrementar la contribución a favor de la Investigación y Desarrollo en el ámbito de la seguridad y mejorar las posibilidades de utilización y la difusión de los resultados consiguientes; fomentar el desarrollo de asociaciones innovadoras para incentivar el crecimiento del sector europeo relacionado con la seguridad de las TIC y mejorar la rápida utilización de nuevas tecnologías y servicios de seguridad de las redes y de la información para darles un impulso comercial.

3. Prestar la debida atención a la necesidad de prevenir y luchar contra amenazas nuevas y existentes contra la seguridad de las redes de comunicación electrónica, incluida la interceptación y explotación ilícita de datos, reconocer y abordar los riesgos relacionados con dichas amenazas y promover, cuando proceda en cooperación con la Agencia Europea de Seguridad de las Redes y de la Información, intercambios efectivos de información y cooperación entre los organismos y agencias pertinentes a nivel nacional; comprometerse a luchar contra el spam, los programas espía y los programas maliciosos, en particular mediante una mejora de la cooperación entre las autoridades competentes a nivel nacional e internacional.

4. Reforzar su cooperación mutua en el marco de i2010, con el fin de determinar prácticas efectivas e innovadoras para mejorar la seguridad de las redes y de la información y ampliar la difusión de dichas prácticas a toda la UE para que se utilicen sobre una base voluntaria.

5. Fomentar la continua mejora de los organismos nacionales de respuesta en caso de emergencia informática.

6. Promover un entorno que anime a los proveedores de servicios y a los operadores de redes a prestar servicios fiables a sus clientes y garantizar la capacidad de adaptación y ofrecer a los consumidores posibilidades de elección de servicios y soluciones en el ámbito de la seguridad; promover y, llegado el caso, exigir a los operadores de redes y a los proveedores de servicios que garanticen a sus clientes un nivel adecuado de seguridad de las redes y de la información.

7. Proseguir el debate estratégico en el marco del grupo de alto nivel i2010, tomando en consideración el desarrollo en curso de la sociedad de la información, y garantizar un enfoque coherente en las diferentes dimensiones: normativa, corregulación, investigación y desarrollo y administración electrónica, además de la comunicación y la formación.

8. En consonancia con el Plan de acción i2010 sobre administración electrónica, desarrollar servicios permanentes de administración electrónica, promover soluciones interoperables de gestión de la identidad y emprender todos los cambios adecuados en la organización del sector público; el sector oficial y las administraciones públicas deberían servir como ejemplo de buenas prácticas en la promoción de servicios seguros de administración pública para todos los ciudadanos.

SE CONTRATULA DE LA INTENCIÓN DE LA COMISIÓN DE:

1. Seguir desarrollando a nivel de la UE una estrategia global y dinámica en el ámbito de la seguridad de las redes y de la información. El planteamiento global propuesto por la Comisión resulta de especial importancia.

2. Considerar el tema de la seguridad de las redes y de la información como un objetivo de la revisión del marco reglamentario europeo relativo a las comunicaciones electrónicas.

3. Seguir desempeñando su papel con el fin de lograr una mayor concienciación sobre la necesidad de un compromiso político general en la lucha contra el spam y los programas espía y programas maliciosos; incrementar el diálogo y la cooperación con terceros países, en particular, mediante acuerdos con terceros países, inclusive por lo que respecta al spam y los programas espía y programas maliciosos.

4. Reforzar la participación de la Agencia Europea de Seguridad de las Redes y de la Información en la Estrategia para una sociedad de la información segura en Europa recogida en la presente Resolución, atendiendo a los objetivos y funciones establecidos en el Reglamento (CE) nº 460/2004 estrechando la cooperación y las relaciones de trabajo con los Estados miembros y las partes interesadas.

5. Desarrollar en el marco de i2010, en cooperación con los Estados miembros y todas las partes interesadas, en particular, con expertos en materia de estadísticas y de seguridad de la información de los Estados miembros, indicadores adecuados para llevar a cabo encuestas comunitarias sobre aspectos relacionados con la seguridad y la confianza.

6. Alentar a los Estados miembros a estudiar en el marco de un diálogo entre las múltiples partes interesadas los factores económicos, empresariales y sociales con el objetivo de desarrollar una política específica para el sector de las TIC que mejore la seguridad y la capacidad de adaptación de las redes y de los sistemas de información, como posible contribución al Programa europeo sobre protección de infraestructuras esenciales previsto.

7. Proseguir sus esfuerzos, de forma coordinada con los Estados miembros, para promover el diálogo con los interlocutores y organizaciones pertinentes a nivel internacional para fomentar la cooperación mundial en el ámbito de la seguridad de las redes y de la información, en particular, mediante la aplicación de las líneas de actuación de la cumbre mundial sobre la sociedad de la información y una información periódica al Consejo a este respecto.

Y HACE UN LLAMAMIENTO A:

1. La Agencia Europea de Seguridad de las Redes y de la Información para que siga trabajando en estrecha cooperación con los Estados miembros, la Comisión y demás partes interesadas pertinentes, con el fin de realizar sus funciones y objetivos establecidos en el Reglamento (CE) nº 460/2004, y asista a la Comisión y los Estados miembros en sus esfuerzos por respetar sus obligaciones en el ámbito de la seguridad de las redes y de la información y, de esta forma, contribuir a la aplicación y ulterior desarrollo de la Estrategia para una sociedad de la información segura en Europa, recogida en la presente Resolución.

2. Todas las partes interesadas para que mejoren la seguridad de sus programas y la seguridad y capacidad de adaptación de las redes y sistemas de información, atendiendo a la Estrategia para una sociedad de la información segura recogida en la presente Resolución, y para que participen en un debate estructurado con las distintas partes interesadas sobre cómo utilizar mejor los medios y los instrumentos normativos disponibles.

3. Las empresas para que adopten una actitud positiva con respecto a la seguridad de la información y de las redes con el fin de crear productos y servicios más avanzados y seguros, considerando la inversión en dichos productos y servicios como una ventaja competitiva.

4. Los fabricantes y proveedores de servicios para que integren, según proceda, requisitos de seguridad, protección de la intimidad y confidencialidad en sus diseños de productos y servicios y en el desarrollo de infraestructuras, aplicaciones y programas de redes, y apliquen y supervisen las soluciones de seguridad.

5. Las partes interesadas para que cooperen y creen entornos experimentales para probar y poner en práctica nuevas tecnologías y servicios de forma segura y adopten en su momento las nuevas tecnologías y servicios seguros una vez comercializadas.

6. Todas las partes interesadas para que emprendan nuevos esfuerzos en la lucha contra el spam y demás prácticas maliciosas en línea, y cooperen activamente con las autoridades competentes a nivel nacional e internacional.

7. Los proveedores de servicios y el sector de las TIC para que se concentren en mejorar la seguridad, la protección de la intimidad y la utilidad de los productos, procesos y servicios para obtener fiabilidad, prevenir y combatir los robos de identidad y otras intromisiones en la intimidad.

8. Los operadores de redes, proveedores de servicios y sector privado para que compartan y apliquen buenas prácticas de seguridad y fomenten una cultura de análisis y gestión de riesgos en las organizaciones y empresas mediante programas de formación adecuados y el desarrollo de planes de emergencia y poniendo a disposición de sus clientes soluciones de seguridad como parte de los servicios que prestan.