I

(Resoluções, recomendações e pareceres)

RESOLUÇÕES

CONSELHO

RESOLUÇÃO DO CONSELHO

de 18 de Dezembro de 2009

sobre uma abordagem de colaboração europeia no domínio da segurança das redes e da informação

(2009/C 321/01)

O CONSELHO DA UNIÃO EUROPEIA,

I. TENDO EM CONTA:

1. A comunicação da Comissão, de 31 de Maio de 2006, intitulada «Estratégia para uma sociedade da informação segura» — «Diálogo, parcerias e maior poder de intervenção» que envolve os Estados-Membros e as partes interessadas do sector privado.

2. A comunicação da Comissão, de 12 de Dezembro de 2006, sobre o «Programa Europeu de Protecção das Infra-Estruturas Críticas (PEPIC)» que visa melhorar a protecção das infra-estruturas críticas na UE e criar um enquadramento da UE para tal protecção.

3. A directiva do Conselho, de 8 de Dezembro de 2008, relativa à identificação e designação das infra-estruturas críticas europeias e à avaliação da necessidade de melhorar a sua protecção.

4. A Resolução do Conselho, de 22 de Março de 2007, sobre a estratégia para uma sociedade da informação segura na Europa.

5. As conclusões do Conselho, de 19 e 20 de Abril de 2007, sobre um programa europeu de protecção das infra-estruturas críticas.

6. A comunicação da Comissão, de 30 de Março de 2009, relativa à protecção das infra-estruturas críticas da informação.

7. O debate em curso, incluindo as consultas públicas pertinentes, sobre o futuro da Agência Europeia para a Segurança das Redes e da Informação (ENISA) e o seu papel na protecção das infra-estruturas críticas da informação.

8. As conclusões da Presidência sobre a protecção das infra-estruturas críticas da informação extraídas da Conferência Ministerial que decorreu em Talin a 27 e 28 de Abril de 2009.

9. Os objectivos da competitividade e do crescimento enunciados na Estratégia de Lisboa e os trabalhos actualmente em curso para a rever.

10. As medidas de segurança propostas na revisão do quadro regulamentar das redes e serviços de comunicações electrónicas.

11. Na perspectiva da eficácia de uma futura política no domínio da segurança das redes e da informação, a presente resolução presume que ainda não se chegou a nenhuma conclusão sobre as eventuais alterações necessárias ao regulamento «ENISA». Como a Comissão está a reexaminar o futuro da referida política, a presente resolução não deve condicionar os resultados desse reexame que se prendam com eventuais alterações ao regulamento «ENISA» na pendência da publicação dos resultados da Comissão.

II. REGISTANDO O SEGUINTE:

1. Dada a importância das infra-estruturas e dos serviços de comunicações electrónicas como base da actividade socioeconómica, a segurança das redes e da informação contribui para valores e objectivos importantes na sociedade, como sejam a democracia, a privacidade, o crescimento económico, a livre circulação de ideias, e bem assim a estabilidade económica e política.

2. Os sistemas, as infra-estruturas e os serviços das tecnologias da informação e da comunicação, incluindo a internet, desempenham um papel fundamental para a sociedade, e a sua perturbação pode causar avultados prejuízos económicos, realçando a importância de se dispor de medidas para aumentar a protecção e a resiliência que assegurem a continuidade dos serviços críticos.

3. Os incidentes de segurança podem abalar a confiança dos utilizadores. Embora as perturbações graves das redes e dos sistemas de informação possam ter importantes repercussões socioeconómicas, os problemas e transtornos quotidianos também podem abalar a confiança do público nas redes e nos serviços tecnológicos.

4. O cenário de ameaças tem vindo a evoluir e a aumentar, o que faz com que seja mais necessário do que nunca oferecer aos utilizadores finais, às empresas e aos governos infra-estruturas de comunicações electrónicas que sejam robustas e resilientes por defeito, e identificar os incentivos adequados para que os fornecedores o façam atempadamente.

5. É necessário reforçar e integrar a segurança das redes e da informação em todas as políticas e sectores da sociedade, bem como enfrentar o desafio de assegurar competências suficientes, tanto através de acções nacionais como europeias, e sensibilizar os utilizadores das tecnologias da informação e da comunicação (TIC).

6. Para a realização e o funcionamento do mercado interno, é necessária uma cooperação transfronteiras entre os proprietários das redes e os fornecedores dos serviços, já que eventuais perturbações num Estado-Membro também podem afectar outros Estados-Membros e toda a UE.

7. Os novos padrões de utilização, como a computação em nuvem e o *software* fornecido a título de serviço (*software-as-a-service*), acentuam ainda mais a importância de que se reveste a segurança das redes e da informação.

8. A segurança das redes e da informação serve o objectivo de todas as partes, em todos os sectores da sociedade, para poderem confiar nos sistemas de informação, pelo que é necessária uma abordagem intersectorial e transfronteiras.

9. Com a crescente utilização das TIC na sociedade, a segurança das redes e da informação constitui um pré-requisito para a prestação de serviços públicos fiáveis e seguros, como a administração pública electrónica.

10. A ENISA tem potencialidades para consolidar o importante papel que já desempenha na segurança das redes e da informação.

III. SUBLINHA QUE:

1. É necessário um nível elevado de segurança das redes e da informação na UE para apoiar:

   a) As liberdades e os direitos dos cidadãos, incluindo o direito à privacidade;

   b) Uma sociedade eficaz em termos de qualidade no tratamento da informação;

   c) A rendibilidade e o crescimento do comércio e da indústria;

   d) A confiança dos cidadãos e das organizações no tratamento da informação e nos sistemas das TIC.

2. O sector das TIC é vital para a maioria dos sectores da sociedade, fazendo com que a segurança das redes e da informação seja responsabilidade conjunta de todas as partes interessadas, nas quais se incluem os operadores, os prestadores de serviços, os fornecedores de *hardware* e *software*, os utilizadores finais, os organismos públicos e os governos nacionais.

IV. RECONHECE:

1. A importância de haver a nível europeu uma comunidade de segurança das redes e da informação, activa e conhecedora, que contribua para uma maior colaboração entre os Estados-Membros e o sector privado.

2. As vantagens de uma utilização harmonizada de normas internacionais de segurança em toda a UE para efeitos da segurança das redes e da informação.

3. A necessidade de se dispor de uma abordagem de colaboração europeia no domínio da segurança das redes e da informação na cena internacional, visto que se trata de um desafio à escala global.

4. A importância de que se reveste para os Estados-Membros e para as instituições da UE a existência de dados estatísticos fiáveis sobre o estado de segurança das redes e da informação na Europa.

5. A necessidade de aumentar a consciencialização e os instrumentos de gestão de risco de todas as partes interessadas.

6. A importância da intensificação de esforços entre os Estados-Membros no sentido de haver uma maior consciencialização, intercâmbios de boas práticas e orientações que os norteiem.

7. A importância de modelos multilaterais como as parcerias entre os sectores público e privado, assentes num modelo ascendente e de longo prazo, com o intuito de atenuar os riscos identificados, sempre que uma abordagem deste género represente uma mais-valia para ajudar a garantir um nível elevado de resiliência das redes.

8. O papel crucial desempenhado pelos prestadores ao oferecerem à sociedade infra-estruturas de comunicações electrónicas robustas e resilientes.

9. A utilidade de se realizarem exercícios na Europa no domínio da segurança das redes e da informação que podem proporcionar valiosos ensinamentos aos operadores das redes, aos fornecedores de serviços e aos governos.

10. Que equipas nacionais ou governamentais de resposta informática de emergência (CERT) ou outros mecanismos de intervenção que respondam às ameaças e reduzam as vulnerabilidades podem contribuir para um elevado nível de resiliência e capacidade para resistir e resolver perturbações das redes e dos sistemas de informação.

11. A importância que assume a exploração de efeitos, riscos e perspectivas estratégicos para criar equipas de resposta informática de emergência (CERT) para as instituições da UE e reflectir sobre o papel que a ENISA possa futuramente vir a desempenhar nesta matéria.

12. O trabalho até agora desenvolvido pela ENISA no domínio da segurança das redes e da informação e a necessidade de continuar a transformá-la num organismo eficiente com claros benefícios para a segurança das redes e da informação a nível europeu.

V. SALIENTA O SEGUINTE:

1. Para fazer face aos desafios actuais e futuros, é fundamental uma estratégia europeia reforçada e holística para a segurança das redes e da informação, em que os papéis da Comissão Europeia, dos Estados-Membros e da ENISA estejam claramente definidos.

2. Após a consulta e a análise adequadas, deve ponderar-se no processo legislativo a modernização e o reforço da ENISA com um mandato que assegure flexibilidade e supervisão por parte dos Estados-Membros e da Comissão, bem como um papel eficiente para a representação dos intervenientes do sector privado. O mandato da ENISA deve ter em conta o quadro regulamentar das redes e serviços de comunicações electrónicas, estar em consonância com as ambições enunciadas na Agenda de Lisboa e incluir objectivos relacionados com a investigação, a inovação, a competitividade, o crescimento económico e a garantia de confiança.

3. A ENISA poderá apoiar o papel que incumbe, respectivamente, à Comissão e aos Estados-Membros, na definição e execução das políticas, em particular fazendo a ponte entre tecnologia e política, e deverá colaborar estreitamente com os Estados-Membros e as demais partes interessadas para assegurar que as suas actividades estejam em consonância com as prioridades da UE.

4. A ENISA, no âmbito de um mandato revisto, deverá constituir o centro de competência da UE em questões de segurança das redes e da informação relacionadas com a UE. Como tal, ao definirem e executarem políticas que possam ter repercussões neste domínio, as instituições europeias devem pedir parecer à ENISA e tê-lo eminentemente em conta.

5. Se lhe for solicitado, a ENISA poderá também ajudar os Estados-Membros a melhorar as respectivas capacidades no domínio da segurança das redes e da informação e a sua aptidão para fazer face aos incidentes de segurança.

VI. CONVIDA OS ESTADOS-MEMBROS A:

1. Prosseguirem os trabalhos para aumentar a confiança dos utilizadores finais nas TIC através de campanhas de sensibilização.

2. Organizarem exercícios nacionais e/ou participarem em exercícios periódicos europeus no domínio da segurança das redes e da informação, tendo presente a necessidade de um planeamento exaustivo em virtude da complexidade do domínio e da participação do sector privado. Se lhe for solicitado, a ENISA poderá ajudar os Estados-Membros nesta matéria. O âmbito e a dimensão geográfica dos exercícios deverá evoluir naturalmente com o tempo e basear-se nos riscos reconhecidos.

3. Criarem equipas de resposta informática de emergência (CERT) nos Estados-Membros que ainda não desenvolveram essa capacidade e reforçar a cooperação, a nível europeu, entre este tipo de equipas nacionais. A ENISA poderá ajudar os Estados-Membros nesta matéria.

4. Envidarem mais esforços no ensino, na formação e em programas de investigação no domínio da segurança das redes e da informação para garantir que na UE existam as competências técnicas e os profissionais necessários, e aumentar o profissionalismo de quem trabalha neste domínio.

5. Reagirem conjuntamente em caso de incidentes transfronteiriços e a melhorarem a sua capacidade para o fazerem de forma adequada, para o que é necessário um maior diálogo entre os decisores envolvidos, especialmente no que toca às questões de confidencialidade.

VII. CONVIDA A COMISSÃO A:

1. Apoiar os Estados-Membros, se for caso disso, na aplicação da presente resolução.

2. Informar periodicamente o Parlamento Europeu e o Conselho sobre iniciativas tomadas a nível da UE relacionadas com a segurança das redes e da informação.

3. Em colaboração com a ENISA, dar início a uma campanha de sensibilização do público europeu e dos intervenientes privados sobre a importância da gestão adequada dos riscos no tocante à segurança das redes e da informação.

4. Continuar, em colaboração com os Estados-Membros, a identificar incentivos para que os fornecedores de infra-estruturas de comunicações electrónicas ofereçam infra-estruturas robustas e resilientes aos utilizadores finais, às empresas e aos governos.

5. Em colaboração com os Estados-Membros, desenvolver métodos que permitam uma avaliação comparativa a nível da UE das repercussões socioeconómicas dos incidentes e da eficácia das medidas de prevenção.

6. Incentivar e melhorar os modelos multilaterais que deverão ter um indiscutível valor acrescentado, beneficiando os utilizadores finais e a indústria.

7. Apresentar uma estratégia holística em matéria de segurança das redes e da informação, que inclua ([1]) propostas sobre um mandato reforçado e flexível para a ENISA, bem como a supervisão reforçada por parte dos Estados-Membros e da Comissão.

8. Proceder a uma análise, em colaboração com os Estados-Membros, das equipas de resposta informática de emergência (CERT) para identificar os domínios em que é preconizada uma maior cooperação.

9. Prosseguir a investigação no sentido de uma abordagem comum ou interoperável para as instituições da UE na aquisição de sistemas e serviços seguros no domínio das TIC.

VIII. APELA À ENISA PARA QUE:

1. Continue a apoiar activamente os Estados-Membros, a Comissão Europeia e as demais partes interessadas pertinentes na execução das políticas europeias no domínio da segurança das redes e da informação e do plano de acção relativo à protecção das infra-estruturas críticas da informação.

2. Colabore com os Estados-Membros, a Comissão e os organismos de estatística no desenvolvimento de um quadro de dados estatísticos sobre o estado de segurança das redes e da informação na Europa.

IX. CONVIDA AS PARTES INTERESSADAS A:

1. Intensificar esforços para aumentar o nível de segurança das redes e da informação, em particular no que respeita ao fornecimento de produtos e serviços fiáveis, dignos de confiança e de fácil utilização.

2. Informar correctamente os utilizadores sobre os riscos de segurança associados aos produtos e serviços e o modo como se podem proteger.

3. Tomar todas as medidas técnicas e organizacionais para salvaguardar a continuidade, integridade e confidencialidade das redes e dos serviços de comunicações electrónicas.

4. Continuar a trabalhar na normalização da segurança das redes e da informação para tentar encontrar soluções harmonizadas e interoperáveis.

5. Participar com os Estados-Membros em exercícios destinados a proporcionar respostas adequadas às situações de emergência.

([1]) A Comissão sugere que se adite aqui o termo «eventualmente».