

**PT**

**PT**

**PT**



COMISSÃO EUROPEIA

Bruxelas, 30.9.2010  
COM(2010) 521 final

2010/0275 (COD)

Proposta de

**REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO**

**relativo à Agência Europeia para a Segurança das Redes e da Informação (ENISA)**

{SEC(2010) 1126}

{SEC(2010) 1127}

## EXPOSIÇÃO DE MOTIVOS

### 1. CONTEXTO DA PROPOSTA

#### 1.1. Contexto político

A Agência Europeia para a Segurança das Redes e da Informação (ENISA) foi criada em Março de 2004, por um período inicial de cinco anos, pelo Regulamento (CE) n.º 460/2004<sup>1</sup>, tendo como principal objectivo «*garantir na [União] um nível de segurança das redes e da informação elevado e eficaz, [...] com vista a desenvolver uma cultura de segurança das redes e da informação em benefício dos cidadãos, dos consumidores, das empresas e das organizações do sector público da União Europeia, contribuindo assim para o normal funcionamento do mercado interno*». O Regulamento (CE) n.º 1007/2008<sup>2</sup> prolongou o mandato da ENISA até Março de 2012.

O prolongamento do mandato da ENISA em 2008 lançou igualmente um debate sobre o rumo geral dos esforços europeus no sentido da segurança das redes e da informação (SRI), para o qual a Comissão contribuiu lançando uma consulta pública sobre os possíveis objectivos de uma política reforçada em matéria de segurança das redes e da informação a nível da União. Essa consulta pública decorreu entre Novembro de 2008 e Janeiro de 2009 e reuniu cerca de 600 contribuições<sup>3</sup>.

Em 30 de Março de 2009, a Comissão adoptou uma Comunicação relativa à protecção das infra-estruturas críticas da informação<sup>4</sup>, centrada na protecção da Europa contra ataques informáticos e perturbações nas redes através da melhoria da prontidão, da segurança e da resiliência, com um plano de acção que apelava à intervenção da ENISA, principalmente em apoio dos Estados-Membros. O plano de acção foi aprovado, nas suas linhas gerais, na Conferência Ministerial sobre protecção das infra-estruturas críticas da informação, realizada em Tallin, na Estónia, em 27 e 28 de Abril de 2009<sup>5</sup>. As conclusões da Conferência da Presidência da União Europeia sublinharam a importância de «*mobilizar o apoio operacional*» da ENISA; declaram que a ENISA «*proporciona um instrumento valioso para apoiar os esforços de cooperação a nível da UE neste domínio*» e apontam para a necessidade de se repensar e reformular o mandato da Agência «*para melhor dar resposta às prioridades e necessidades da UE; para conseguir uma capacidade de resposta mais flexível; para desenvolver aptidões e competências; e para apoiar a eficiência operacional e o impacto*

---

<sup>1</sup> Regulamento (CE) n.º 460/2004 do Parlamento Europeu e do Conselho, de 10 de Março de 2004, que cria a Agência Europeia para a Segurança das Redes e da Informação (JO L 77 de 13.3.2004, p. 1).

<sup>2</sup> Regulamento (CE) n.º 1007/2008 do Parlamento Europeu e do Conselho, de 24 de Setembro de 2008, que altera o Regulamento (CE) n.º 460/2004 do Parlamento Europeu e do Conselho, de 10 de Março de 2004, que cria a Agência Europeia para a Segurança das Redes e da Informação, no que respeita à duração da agência (JO L 293 de 31.10.2008, p. 1).

<sup>3</sup> O relatório resumido dos resultados da consulta pública intitulada «Para uma política reforçada de segurança das redes e da informação na Europa» encontra-se apenso à Avaliação de Impacto que acompanha a presente proposta, enquanto Anexo 11.

<sup>4</sup> COM(2009) 149 de 30.3.2009.

<sup>5</sup> Documento de Discussão: [http://www.tallinnciip.eu/doc/discussion\\_paper\\_-\\_tallinn\\_ciip\\_conference.pdf](http://www.tallinnciip.eu/doc/discussion_paper_-_tallinn_ciip_conference.pdf)

Conclusões da Presidência: [http://www.tallinnciip.eu/doc/EU\\_Presidency\\_Conclusions\\_Tallinn\\_CIIP\\_Conference.pdf](http://www.tallinnciip.eu/doc/EU_Presidency_Conclusions_Tallinn_CIIP_Conference.pdf).

geral da Agência» por forma a torná-la «um trunfo permanente para cada Estado-Membro e para a União Europeia em geral».

Após a discussão no Conselho Telecomunicações de 11 de Junho de 2009, em que os Estados-Membros manifestaram o seu apoio ao prolongamento do mandato da ENISA e ao aumento dos seus recursos, tendo em conta a importância da segurança das redes e da informação e a complexidade crescente dos desafios nesta matéria, o debate foi concluído sob a Presidência sueca da União. A Resolução do Conselho de 18 de Dezembro de 2009<sup>6</sup> reconhece o papel e o potencial da ENISA, assim como a necessidade de «continuar a transformá-la num organismo eficiente». Além disso, sublinha a necessidade de modernizar e reforçar a Agência para que ajude a Comissão e os Estados-Membros a acabarem com o distanciamento entre tecnologia e políticas, servindo de centro especializado da União em matérias relacionadas com a segurança das redes e da informação.

## 1.2. Contexto geral

As tecnologias da informação e das comunicações (TIC) tornaram-se a espinha dorsal do conjunto da economia e da sociedade na União Europeia. As TIC são vulneráveis a ameaças que já não se limitam às fronteiras nacionais e que mudaram com a evolução das tecnologias e do mercado. Tendo as TIC uma dimensão planetária e estando estreitamente interligadas e interdependentes em relação a outras infra-estruturas, não é possível garantir a sua segurança e resiliência com abordagens puramente nacionais e descoordenadas. Ao mesmo tempo, os desafios a que a segurança das redes e da informação está sujeita evoluem rapidamente. As redes e os sistemas informáticos têm de ser eficazmente protegidos contra todas as espécies de perturbações e falhas, incluindo ataques de origem humana.

As políticas em matéria de segurança das redes e da informação (SRI) ocupam um papel central na Agenda Digital para a Europa<sup>7</sup>, uma iniciativa emblemática no âmbito da estratégia UE 2020, destinada a explorar e desenvolver o potencial das TIC e traduzir esse potencial em crescimento sustentável e inovação. A Agenda Digital tem como prioridades promover a adesão às TIC e aumentar a confiança na sociedade da informação.

A ENISA foi inicialmente criada para assegurar um nível elevado e eficaz de protecção das redes e da informação na União. A experiência adquirida com a Agência, bem como os desafios e as ameaças actuais, acentuaram a necessidade de modernizar o seu mandato de modo a torná-lo mais apto a responder às necessidades da União Europeia decorrentes:

- da diversidade de abordagens nacionais de resposta aos desafios que constantemente evoluem;
- da inexistência de modelos colaborativos na execução das políticas em matéria de SRI;
- do nível insuficiente de preparação, também devido à capacidade limitada da Europa em matéria de alerta precoce e de resposta;
- da falta de dados europeus fiáveis e do pouco conhecimento dos novos problemas;

---

<sup>6</sup> Resolução do Conselho de 18 de Dezembro de 2009 sobre uma abordagem de colaboração europeia no domínio da segurança das redes e da informação (JO C 321 de 29.12.2009, p. 1), <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:321:0001:0004:EN:PDF>.

<sup>7</sup> COM(2010) 245 de 19.5.2010.

- do baixo nível de sensibilização para os riscos e desafios a que a segurança das redes e da informação está sujeita;
- do desafio de integrar os aspectos da segurança das redes e da informação nas políticas, de forma a combater com maior eficácia o cibercrime.

### **1.3. Os objectivos políticos**

O objectivo geral do regulamento proposto é permitir à União, aos Estados-Membros e às partes interessadas desenvolverem um elevado grau de capacidade e preparação para prevenirem, detectarem e responderem com mais eficácia aos problemas de segurança das redes e da informação. Será um modo de contribuir para criar confiança, que está na base do desenvolvimento da sociedade da informação, melhorar a competitividade das empresas europeias e garantir que o mercado interno funcione eficazmente.

### **1.4. Disposições em vigor no domínio da proposta**

A presente proposta complementa as iniciativas regulamentares e não regulamentares em matéria de segurança das redes e da informação tomadas a nível da União para aumentar a segurança e a resiliência das TIC:

- O plano de acção lançado pela Comunicação relativa à protecção das infra-estruturas críticas da informação previu o estabelecimento de:
  - (1) Um fórum europeu de Estados-Membros destinado a promover o debate e o intercâmbio de boas práticas políticas tendo em vista partilhar objectivos e prioridades políticas sobre a segurança e a resiliência da infra-estrutura TIC, também beneficiando directamente do trabalho e do apoio fornecido pela Agência.
  - (2) Uma parceria público-privada europeia para a resiliência, que constitui o quadro flexível de governação à escala europeia para a resiliência da infra-estrutura TIC, que visa intensificar a cooperação entre o sector público e o privado na mira da consecução dos objectivos em termos de segurança e resiliência, requisitos de base, assim como boas práticas e medidas políticas.
- O Programa de Estocolmo, adoptado pelo Conselho Europeu em 11 de Dezembro de 2009, promove políticas que garantam a segurança das redes e permitam uma reacção mais rápida em caso de ataques informáticos na União.
- Estas iniciativas contribuem para dar efeito à Agenda Digital para a Europa. As políticas em matéria de segurança das redes e da informação desempenham um papel central na parte da estratégia focada na promoção da confiança e da segurança na sociedade da informação. Além disso, apoiam as medidas e a política da Comissão em matéria de protecção da privacidade (nomeadamente “desde a concepção”) e dos dados pessoais (revisão do quadro), a rede de cooperação para a defesa do consumidor, a gestão da identidade e o programa «Para uma Internet mais segura».

## 1.5. Desenvolvimentos da política actual em matéria de segurança das redes e da informação relacionados com a proposta

Vários dos desenvolvimentos em curso na política de SRI, nomeadamente os anunciados na Agenda Digital para a Europa, beneficiam do apoio e da especialização da ENISA. Por exemplo:

- Reforço da cooperação em matéria de política de segurança das redes e da informação através da intensificação das actividades do **Fórum Europeu dos Estados-Membros (EFMS)**, o que, com o apoio directo da ENISA, contribuirá para:
  - definir modos de estabelecimento de uma rede europeia eficaz através da cooperação transfronteiras entre as equipas nacionais / governamentais de resposta a emergências informáticas (CERT);
  - identificar os objectivos e as prioridades a longo prazo para exercícios pan-europeus em larga escala sobre incidentes de segurança das redes e da informação;
  - Impulsionar a introdução de requisitos mínimos nos contratos públicos para promover a segurança e a resiliência dos sistemas e redes públicos;
  - definir incentivos económicos e regulamentares em favor da segurança e da resiliência;
  - avaliar o estado da segurança das redes e da informação na Europa.
- Reforço da cooperação e da constituição de parcerias entre os sectores público e privado, através do apoio à **Parceria Público-Privada Europeia para a Resiliência (EP3R)**. A ENISA tem um papel cada vez mais importante na facilitação das reuniões e actividades da EP3R. Os próximos passos desta parceria incluirão:
  - A discussão de medidas e instrumentos inovadores para melhorar a segurança e a resiliência, tais como:
    - (1) requisitos básicos de segurança e resiliência, em particular nos contratos públicos de produtos ou serviços TIC, para criar condições equitativas, garantindo ao mesmo tempo um nível adequado de preparação e prevenção;
    - (2) estudo das questões ligadas à responsabilidade dos operadores económicos, nomeadamente quando instauram requisitos mínimos de segurança;
    - (3) incentivos económicos ao desenvolvimento e à adopção de práticas de gestão de riscos e de processos e produtos de segurança;
    - (4) avaliação de riscos e mecanismos de gestão para avaliar e gerir os grandes incidentes numa base de entendimento comum;
    - (5) cooperação entre o sector público e o sector privado na eventualidade de incidentes em grande escala;
    - (6) organização de uma **cimeira empresarial** dedicada aos obstáculos económicos e aos factores indutores de segurança e de resiliência.

- Aplicação prática dos requisitos de segurança do pacote regulamentar das comunicações electrónicas, domínio no qual é necessária a competência especializada e a assistência da ENISA para:
  - dar apoio aos Estados-Membros e à Comissão, tendo em conta os pontos de vista do sector privado, se for caso disso, no estabelecimento de um quadro de regras e procedimentos para implementar as disposições em matéria de notificação de violações da segurança (constantes do artigo 13.º, alínea a), da Directiva-Quadro revista);
  - criar um fórum anual onde os organismos nacionais competentes em matéria de segurança das redes e da informação / autoridades reguladoras nacionais e as partes interessadas do sector privado discutirão os ensinamentos colhidos e partilharão as boas práticas na aplicação das medidas regulamentares para a segurança das redes e da informação.
- Facilitação de **exercícios de preparação no domínio da cibersegurança em toda a UE** com o apoio da Comissão e a contribuição da ENISA, tendo em vista dar a esses exercícios, numa fase posterior, uma dimensão internacional.
- **Criação de uma CERT (equipa de resposta a emergências informáticas) para as instituições da UE.** A acção-chave 6 da Agenda Digital para a Europa prevê que a Comissão apresente medidas que visem «instaurar uma política reforçada e de alto nível em matéria de segurança das redes e da informação, incluindo [...] medidas que permitam reagir mais rapidamente em caso de ataques informáticos, incluindo uma CERT para as instituições europeias»<sup>8</sup>. Para tal, será necessário que a Comissão e as outras instituições da União analisem as possibilidades e criem uma equipa de resposta a emergências informáticas à qual a ENISA possa fornecer apoio técnico e conhecimentos especializados.
- Mobilização dos Estados-Membros e apoio aos mesmos na ultimação e, se necessário, na criação de **CERT nacionais/governamentais com vista a estabelecer uma rede de equipas perfeitamente operacional que cubra toda a Europa.** Esta actividade será igualmente fundamental para desenvolver futuramente um sistema europeu de partilha de informações e de alerta (EISAS, sigla inglesa) para os cidadãos e as PME, a construir com recursos e capacidades nacionais até ao final de 2012.
- **Sensibilização** para os desafios da segurança das redes e da informação, que incluirá:
  - A colaboração da Comissão com a ENISA com vista a delinear orientações para a promoção de normas, boas práticas e uma cultura de gestão de riscos em matéria de segurança das redes e da informação. Será elaborada a primeira série de orientações.

---

<sup>8</sup> Da Resolução do Conselho de 18 de Dezembro de 2009 sobre uma abordagem de colaboração europeia no domínio da segurança das redes e da informação também consta o seguinte: «O Conselho [...] reconhece [...] 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.»

- A organização, pela ENISA, em cooperação com os Estados-Membros, do «**mês europeu da segurança das redes e da informação para todos**», que incluirá concursos nacionais / europeus em matéria de cibersegurança.

### **1.1. Coerência com outras políticas e com os objectivos da União**

Ao melhorar o nível de preparação e de reacção aos desafios da segurança das redes e da informação, a proposta é coerente com as políticas em vigor e com os objectivos da União Europeia e totalmente conforme com o objectivo de contribuir para o bom funcionamento do mercado interno.

## **2. RESULTADOS DAS CONSULTAS E DA AVALIAÇÃO DE IMPACTO**

### **2.1. Consulta das partes interessadas**

Esta iniciativa política é o resultado de uma ampla discussão orientada numa perspectiva inclusiva e de respeito pelos princípios da participação, abertura, responsabilização, eficácia e coerência. O amplo processo que teve lugar incluiu uma avaliação da Agência em 2006/2007, seguida de recomendações por parte do conselho de administração da ENISA, duas consultas públicas (em 2007 e em 2008–2009) e uma série de *workshops* sobre matérias relacionadas com a segurança das redes e da informação.

A primeira consulta pública foi lançada em articulação com a Comunicação da Comissão relativa à avaliação intercalar da ENISA. Centrou-se no futuro da Agência, decorreu de 13 de Junho a 7 de Setembro de 2007 e reuniu um total de 44 contribuições em linha e ainda duas apresentadas por escrito. As respostas provieram de uma variedade de intervenientes e partes interessadas dos Estados-Membros, incluindo ministérios, entidades reguladoras, associações industriais e de consumidores, instituições académicas, empresas e simples cidadãos.

As respostas chamaram a atenção para uma série de questões interessantes sobre a evolução do cenário de ameaças; a necessidade de clarificar e introduzir maior flexibilidade no regulamento para permitir à ENISA adaptar-se aos desafios; a importância de garantir uma interacção eficaz com os intervenientes; e a possibilidade de um aumento, ainda que limitado, dos seus recursos.

A segunda consulta pública, que decorreu de 7 de Novembro de 2008 a 9 de Janeiro de 2009, pretendeu identificar os objectivos prioritários de uma política de segurança das redes e da informação reforçada a nível europeu e os meios para conseguir realizar esses objectivos. A Comissão recebeu cerca de 600 contribuições de autoridades, instituições académicas / de investigação, associações industriais, empresas privadas e outras partes interessadas, tais como organizações de protecção de dados e empresas de consultoria, dos Estados-Membros e ainda de simples cidadãos.

A grande maioria dos respondentes<sup>9</sup> mostrou-se favorável ao prolongamento do mandato da Agência e defendeu o reforço do seu papel na coordenação das actividades no domínio da segurança das redes e da informação a nível europeu e um aumento dos seus recursos. As principais prioridades mencionadas foram a necessidade de uma abordagem mais coordenada no respeitante às ameaças aos sistemas informáticos em toda a Europa, a cooperação

---

<sup>9</sup> Ver anexo XI da Avaliação de Impacto.

transnacional para responder aos ataques informáticos de grande escala, a criação de confiança e a melhoria do processo de intercâmbio de informações entre as partes interessadas.

Em Setembro de 2009, teve início uma avaliação do impacto da proposta, baseada num estudo preparatório efectuado por uma empresa externa. Nela participou um amplo leque de partes interessadas e peritos. Entre os participantes incluíram-se: entidades dos Estados-Membros ligadas à segurança das redes e da informação, autoridades reguladoras nacionais, operadores de telecomunicações e prestadores de serviços Internet e associações do sector, associações de defesa do consumidor, fabricantes de TIC, equipas de resposta a emergências informáticas (CERT), universitários e utilizadores empresariais. Foi criado um grupo director interserviços, composto pelas Direcções-Gerais pertinentes da Comissão, para apoiar a realização da avaliação de impacto.

## **2.2. Avaliação de Impacto**

A manutenção de uma agência foi considerada uma solução adequada para atingir os objectivos da política europeia<sup>10</sup>. Após um processo de pré-selecção, foram escolhidas para análise mais aprofundada cinco opções políticas:

- Opção 1 — Nenhuma política;
- Opção 2 — Continuar como dantes, ou seja, com um mandato semelhante e o mesmo nível de recursos;
- Opção 3 — Alargar as funções da ENISA, tornando as autoridades policiais/judiciais e de protecção da privacidade partes interessadas de pleno direito;
- Opção 4 — Acrescentar às suas tarefas o combate aos ciberataques e a resposta a ciberincidentes;
- Opção 5 — Acrescentar às suas funções o apoio às autoridades policiais e judiciais na luta contra a cibercriminalidade.

Após uma análise comparativa dos custos e benefícios, concluiu-se que a opção 3 era a mais satisfatória do ponto de vista dos custos e da eficácia para atingir os objectivos estratégicos.

A opção 3 prevê uma ampliação das funções da ENISA, que passarão a incluir:

- A construção e manutenção de uma rede de contacto entre as partes interessadas e de uma rede de conhecimento que forneça à Agência uma perspectiva geral da segurança das redes e da informação na Europa;
- O apoio, enquanto centro de apoio em matéria de segurança das redes e da informação, à concepção e à aplicação de políticas (em particular no domínio da privacidade electrónica, das assinaturas electrónicas, da identidade electrónica e das normas de contratos públicos para segurança das redes e da informação);

---

<sup>10</sup> Ver anexo IV da Avaliação de Impacto.

- Apoio à política da União em matéria de protecção das infra-estruturas críticas da informação e de resiliência (exercícios, EP3R, sistema europeu de partilha de informações e de alerta, etc.);
- Criação de um quadro a nível da União para a recolha de dados sobre SRI, que preveja também métodos e práticas para a sua comunicação e partilha legais;
- Estudo da economia da SRI;
- Estímulo à cooperação com países terceiros e organizações internacionais, tendo em vista promover uma abordagem global comum da SRI e potenciar o impacto das iniciativas internacionais de alto nível na Europa;
- Execução de tarefas não operacionais relacionadas com a vertente SRI da repressão e da cooperação judicial em matéria de cibercriminalidade.

### 3. ELEMENTOS JURÍDICOS DA PROPOSTA

#### 3.1. Síntese da acção proposta

O regulamento proposto visa reforçar e modernizar a Agência Europeia para a Segurança das Redes e da Informação (ENISA) e estabelecer um novo mandato com a duração de cinco anos.

A proposta inclui algumas alterações importantes em relação ao regulamento inicial:

- (1) **Maior flexibilidade, adaptabilidade e capacidade de focalização.** As tarefas são actualizadas e reformuladas nas suas grandes linhas de modo a alargar o âmbito das actividades da Agência; são suficientemente precisas para descrever os meios através dos quais os objectivos devem ser atingidos. Deste modo, a missão da Agência é mais bem focalizada, a sua capacidade para atingir os objectivos é melhorada e as suas tarefas de apoio à implementação da política da União são reforçadas.
- (2) **Melhor alinhamento da Agência com o processo político e regulamentar da União.** As instituições e organismos europeus podem dirigir-se à Agência para obterem assistência e aconselhamento. Esta possibilidade é conforme com a evolução política e regulamentar: o Conselho começou a dirigir-se directamente à Agência em Resoluções e, no quadro regulamentar das comunicações electrónicas, o PE e o Conselho confiaram-lhe tarefas relacionadas com a segurança das redes e da informação.
- (3) **Interface com o combate à cibercriminalidade.** Na consecução dos seus objectivos, a Agência tem em conta o combate à cibercriminalidade. As autoridades policiais / judiciais e as responsáveis pela protecção da privacidade tornam-se partes interessadas de pleno direito da Agência, nomeadamente em sede do grupo permanente de partes interessadas.
- (4) **Estrutura de governação reforçada.** A proposta reforça o papel de supervisão do conselho de administração da Agência, no qual estão representados os Estados-Membros e a Comissão. Por exemplo, o conselho de administração pode emitir directrizes gerais sobre assuntos relativos ao pessoal, matéria que dantes competia

exclusivamente ao director executivo. Pode igualmente criar órgãos de trabalho para a assistir na execução das suas tarefas, inclusivamente na monitorização da aplicação das suas decisões.

- (5) **Simplificação dos procedimentos.** Os procedimentos que se revelaram inutilmente pesados são simplificados. Exemplos: a) procedimento simplificado para o regulamento interno do conselho de administração, b) o parecer sobre o programa de trabalho da ENISA é formulado pelos serviços da Comissão e não através de uma decisão desta. São também dados ao conselho de administração os recursos adequados caso necessite de tomar decisões executivas e de as implementar (por exemplo, no caso de um membro do pessoal apresentar queixa contra o director executivo ou contra o próprio conselho de administração).
- (6) **Aumento gradual dos recursos.** Para satisfazer as prioridades europeias reforçadas e responder aos desafios crescentes, sem prejuízo da proposta da Comissão para o próximo quadro financeiro plurianual, está previsto o aumento gradual dos recursos financeiros e humanos da Agência entre 2012 e 2016. Com base na proposta da Comissão relativa ao regulamento que estabelece o quadro financeiro plurianual pós-2013 e tendo em conta as conclusões da avaliação de impacto, a Comissão apresentará uma Ficha Financeira Legislativa alterada.
- (7) **Possibilidade de prolongar o mandato do director executivo.** O conselho de administração pode prolongar o mandato do director executivo por três anos.

### 3.2. Base legal

A base legal da proposta é o artigo 114.º do Tratado sobre o Funcionamento da União Europeia<sup>11</sup> (TFUE).

De acordo com o Tribunal de Justiça da União Europeia<sup>12</sup>, antes da entrada em vigor do Tratado de Lisboa, o **artigo 95.º do Tratado CE** devia ser considerado a base legal apropriada para a criação de um organismo capaz de garantir um nível elevado e eficaz de SRI na União. Ao utilizarem, no artigo 95.º, a expressão «medidas relativas à aproximação», os autores do Tratado pretenderam conferir ao legislador da União uma margem de discricionariedade quanto à escolha das medidas adequadas para atingir o resultado desejado. A melhoria da segurança e da resiliência das infra-estruturas TIC é, pois, um elemento importante que contribui para o bom funcionamento do mercado interno.

Por força do Tratado de Lisboa, o **artigo 114.º do TFUE**<sup>13</sup> descreve — quase nos mesmos termos — a responsabilidade em matéria de mercado interno. Pelas razões acima expostas, continuará a ser a base legal aplicável para a adopção de medidas que melhorem a SRI. A responsabilidade em matéria de mercado interno é agora uma competência partilhada entre a União e os Estados-Membros (artigo 4.º, n.º 2, alínea a), do TFUE). Significa isto que a União e os Estados-Membros podem adoptar medidas (vinculativas) e que o Estados-Membros agirão na medida em que a União não tenha exercido a sua competência ou tenha decidido deixar de a exercer (artigo 2.º, n.º 2, do TFUE).

---

<sup>11</sup> JO C 115 de 9.5.2008, p. 94.

<sup>12</sup> TJUE, 2.5.2006, C-217/04, Reino Unido da Grã-Bretanha e da Irlanda do Norte contra Parlamento Europeu e Conselho da União Europeia.

<sup>13</sup> Cf. supra.

As medidas enquadradas na responsabilidade em matéria de mercado interno exigirão um procedimento legislativo ordinário (artigos 289.º e 294.º do TFUE), semelhante<sup>14</sup> ao antigo procedimento de co-decisão (artigo 251.º do Tratado CE).

Com o Tratado de Lisboa, desapareceu a antiga distinção entre os pilares. A prevenção e o combate ao crime passou a ser uma competência partilhada da União. Abriu-se assim a possibilidade de a ENISA funcionar como plataforma para os aspectos SRI do combate à cibercriminalidade e de trocar pontos de vista e as melhores práticas com as autoridades responsáveis pela ciberdefesa, pela repressão do crime e pela protecção da privacidade.

### **3.3. Princípio da subsidiariedade**

A proposta é conforme com o princípio da subsidiariedade: a política de SRI exige uma abordagem colaborativa e os objectivos da proposta não podem ser atingidos pelos Estados-Membros individualmente.

Uma estratégia de total não intervenção da União nas políticas nacionais de SRI deixaria essa tarefa para os Estados-Membros, ignorando a clara interdependência entre os sistemas informáticos existentes. Uma medida que garante um grau apropriado de coordenação entre os Estados-Membros de forma a garantir que os riscos da SRI possam ser bem geridos no contexto transfronteiras em que surgem respeita, por conseguinte, o princípio da subsidiariedade. Além disso, a acção europeia melhorará a eficácia das políticas nacionais existentes, conferindo, por conseguinte, valor acrescentado.

Acresce ainda que a aplicação de uma política concertada e colaborativa em matéria de SRI terá um impacto positivo na protecção dos direitos fundamentais e especificamente do direito de protecção dos dados pessoais e da privacidade. A necessidade de proteger os dados é actualmente crucial, dado o facto de os cidadãos europeus confiarem cada vez mais os seus dados a sistemas informáticos complexos, por escolha ou por necessidade, sem necessariamente poderem avaliar correctamente os riscos daí decorrentes. Em caso de incidente, não é, pois, garantido que possam tomar as medidas adequadas nem é certo que os Estados-Membros possam resolver eficazmente eventuais incidentes internacionais na ausência de uma coordenação europeia em matéria de SRI.

### **3.4. Princípio da proporcionalidade**

A presente proposta cumpre o princípio da proporcionalidade, uma vez que não vai além do que é necessário para atingir o seu objectivo.

### **3.5. Escolha dos instrumentos**

Instrumento proposto: um regulamento, que é directamente aplicável em todos os Estados-Membros.

## **4. IMPLICAÇÕES ORÇAMENTAIS**

A proposta não terá implicações no orçamento da União.

---

<sup>14</sup> O procedimento legislativo ordinário difere, nomeadamente, em termos de maioria requerida no Conselho e no PE.

Dado o facto de as tarefas a incluir no novo mandato da ENISA serem definidas, prevê-se que sejam dados à Agência os recursos necessários para exercer as suas actividades de maneira satisfatória. A avaliação da Agência, o processo aprofundado de consulta às partes interessadas a todos níveis e a avaliação de impacto mostram que existe um consenso generalizado quanto à dimensão da Agência, considerada inferior à massa crítica, e quanto à necessidade de aumentar os seus recursos. As consequências e os efeitos do aumento do pessoal e do orçamento da Agência são analisados na avaliação de impacto que acompanha a proposta.

O financiamento por parte da UE após 2013 será examinado no contexto de um debate alargado a toda a Comissão sobre todas as propostas para o período após 2013.

## **5. OBSERVAÇÕES COMPLEMENTARES**

### **5.1. Período de vigência**

O regulamento vigorará durante cinco anos.

### **5.2. Cláusula de revisão**

O regulamento prevê uma avaliação da Agência, que abrangerá o período desde a avaliação anterior, em 2007. Será avaliada a eficácia da Agência na consecução dos seus objectivos, tal como descritos no regulamento, a continuação da sua eficácia enquanto instrumento e a conveniência ou não em prolongar novamente o seu mandato. Com base nas conclusões, o conselho de administração formulará recomendações dirigidas à Comissão relativamente a alterações ao presente regulamento, à Agência e aos seus métodos de trabalho. Para permitir à Comissão preparar em tempo útil uma eventual proposta de prolongamento do mandato, a avaliação deverá ter lugar no final do segundo ano do mandato previsto pelo regulamento.

### **5.3. Medidas provisórias**

A Comissão tem consciência de que o processo legislativo no Parlamento Europeu e no Conselho pode exigir um certo tempo para debate da proposta, correndo-se o risco de se criar um vazio legal se o novo mandato da Agência não for adoptado em tempo útil antes do termo do actual mandato. A Comissão propõe, por conseguinte, juntamente com a presente proposta, um regulamento que prolonga o actual mandato da Agência por 18 meses para dar tempo ao debate e ao devido desenrolar dos procedimentos.

**Proposta de**

**REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO**

**relativo à Agência Europeia para a Segurança das Redes e da Informação (ENISA)**

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia e, nomeadamente, o seu artigo 114.º,

Tendo em conta a proposta da Comissão Europeia,

Tendo em conta o parecer do Comité Económico e Social Europeu<sup>15</sup>,

Tendo em conta o parecer do Comité das Regiões<sup>16</sup>,

Após transmissão da proposta aos parlamentos nacionais,

Deliberando nos termos do processo legislativo ordinário,

Considerando o seguinte:

- (1) As comunicações, as infra-estruturas e os serviços electrónicos são um factor essencial do desenvolvimento económico e social. São fundamentais para a sociedade e tornaram-se tão indispensáveis como o abastecimento de electricidade ou de água. A sua perturbação pode originar prejuízos económicos consideráveis, o que acentua a importância de medidas que visem aumentar a protecção e a resiliência para garantir a continuidade de serviços críticos. A protecção das comunicações, das infra-estruturas e dos serviços electrónicos, em particular a sua integridade e disponibilidade, enfrenta desafios crescentes. É uma questão cada vez mais preocupante para a sociedade, nomeadamente devido à eventualidade de surgirem problemas decorrentes da complexidade dos sistemas, acidentes, erros e ataques, que podem ter consequências na infra-estrutura física que permite a entrega de serviços críticos para o bem-estar dos cidadãos europeus.
- (2) A natureza das ameaças muda constantemente e os incidentes de segurança podem abalar a confiança dos utilizadores. Embora as perturbações graves das comunicações, infra-estruturas e serviços electrónicos possam ter importantes repercussões económicas e sociais, as violações da segurança, os problemas e os transtornos no dia-a-dia também podem abalar a confiança do público na tecnologia, nas redes e nos serviços.

---

<sup>15</sup> JO C [...] de [...], p. [...].

<sup>16</sup> JO C [...] de [...], p. [...].

- (3) É, por conseguinte, importante para os decisores políticos, as empresas e os utilizadores que se proceda a uma avaliação regular da situação das redes e da informação em termos de segurança na Europa, com base em dados europeus fiáveis.
- (4) Os representantes dos Estados-Membros, reunidos no Conselho Europeu de 13 de Dezembro de 2003, decidiram que a Agência Europeia para a Segurança das Redes e da Informação (ENISA), que iria ser criada com base na proposta apresentada pela Comissão, teria sede numa cidade da Grécia, a determinar pelo Governo grego.
- (5) Em 2004, o Parlamento Europeu e o Conselho adoptaram o Regulamento (CE) n.º 460/2004<sup>17</sup>, que cria a Agência Europeia para a Segurança das Redes e da Informação, no intuito de contribuir para a realização do objectivo de garantir um elevado nível de segurança das redes e da informação na União e desenvolver uma cultura de segurança das redes e da informação em benefício dos cidadãos, dos consumidores, das empresas e das administrações públicas. Em 2008, o Parlamento Europeu e o Conselho adoptaram o Regulamento (CE) n.º 1007/2008<sup>18</sup> que prolonga o mandato da Agência até Março de 2012.
- (6) Desde que a Agência foi criada, a segurança das redes e da informação tem-se visto confrontada com desafios que vão mudando em função da evolução tecnológica, socioeconómica e dos mercados e que têm sido objecto de reflexões e debates aprofundados. Em resposta à evolução dos desafios, a União actualizou as suas prioridades no que toca à política de segurança das redes e da informação numa série de documentos, entre os quais a Comunicação da Comissão de 2006 intitulada *Estratégia para uma sociedade da informação segura – Diálogo, parcerias e maior poder de intervenção*<sup>19</sup>, a Resolução do Conselho de 2007 relativa a uma Estratégia para uma Sociedade da Informação Segura na Europa<sup>20</sup>, a Comunicação de 2009 intitulada *Protecção de infra-estruturas críticas da informação - «Proteger a Europa contra os ciberataques e as perturbações em grande escala: melhorar a preparação, a segurança e a resiliência»*<sup>21</sup>, as Conclusões da Presidência da Conferência Ministerial sobre Protecção de Infra-Estruturas Críticas da Informação (CIIP), a Resolução do Conselho de 2009 sobre uma abordagem de cooperação europeia no domínio da segurança das redes e da informação<sup>22</sup>. Foi reconhecida a necessidade de modernizar e reforçar a Agência para que esta contribua positivamente para os esforços das instituições europeias e dos Estados-Membros no sentido de desenvolverem na Europa uma capacidade de resposta aos desafios da segurança das redes e da informação. Mais recentemente, a Comissão adoptou a Agenda Digital para a Europa<sup>23</sup>, uma iniciativa emblemática enquadrada na estratégia «Europa 2020». Esta agenda geral visa explorar e desenvolver o potencial das TIC e transformá-lo em crescimento sustentável e inovação. Um dos seus principais objectivos é promover a confiança na sociedade da informação, para o que anunciou uma série de acções a levar a cabo pela Comissão nesse domínio, entre as quais se inclui a presente proposta.

---

<sup>17</sup> JO L 77 de 13.3.2004, p. 1.

<sup>18</sup> JO L 293 de 31.10.2008, p. 1.

<sup>19</sup> COM(2006) 251 de 31.5.2006.

<sup>20</sup> Resolução do Conselho de 22 de Março de 2007 sobre a estratégia para uma sociedade da informação segura na Europa (JO C 68 de 24.3.2007, p. 1).

<sup>21</sup> COM(2009) 149 de 30.3.2009.

<sup>22</sup> Resolução do Conselho de 18 de Dezembro de 2009 sobre uma abordagem de colaboração europeia no domínio da segurança das redes e da informação (JO C 321 de 29.12.2009, p. 1).

<sup>23</sup> COM(2010) 245 de 19.5.2010.

- (7) As medidas em prol do mercado interno respeitantes à segurança das comunicações electrónicas e, de um modo mais geral, à segurança das redes e da informação exigem diferentes formas de aplicações técnicas e organizacionais por parte dos Estados-Membros e da Comissão. A aplicação heterogénea dessas exigências pode conduzir a soluções ineficazes e criar obstáculos ao mercado interno. É, pois, necessário criar a nível europeu um centro especializado que forneça orientações, conselhos e, quando solicitado, assistência em questões relacionadas com a segurança das redes e da informação, e com o qual os Estados-Membros e as instituições europeias possam contar. A Agência pode responder a essas necessidades desenvolvendo e mantendo um alto nível de especialização e prestando assistência aos Estados-Membros, à Comissão e, por consequência, à comunidade empresarial por forma a ajudá-los a cumprir os requisitos legais e regulamentares da segurança das redes e da informação, contribuindo assim para o bom funcionamento do mercado interno.
- (8) A Agência deve desempenhar as tarefas que lhe são confiadas pela actual legislação da União no domínio das comunicações electrónicas e, de um modo geral, contribuir para aumentar o nível de segurança das comunicações electrónicas, nomeadamente oferecendo competências especializadas e conselhos e promovendo o intercâmbio de boas práticas.
- (9) A Directiva 2002/21/CE do Parlamento Europeu e do Conselho, de 7 de Março de 2002, relativa a um quadro regulamentar comum para as redes e serviços de comunicações electrónicas (Directiva-Quadro)<sup>24</sup>, exige, além disso, que os fornecedores de redes de comunicações electrónicas públicas ou de serviços de comunicações electrónicas publicamente disponíveis tomem as medidas adequadas para proteger a sua integridade e segurança e torna obrigatória a notificação das violações de segurança e das perdas de integridade. Se for caso disso, a Agência deve igualmente ser notificada pelas autoridades reguladoras nacionais, que devem também apresentar à Comissão e à Agência um relatório anual sucinto sobre as notificações recebidas e as medidas tomadas. A Directiva 2002/21/CE insta igualmente a Agência a contribuir para a harmonização de medidas técnicas e organizacionais adequadas através da formulação de pareceres.
- (10) A Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva Privacidade e Comunicações Electrónicas)<sup>25</sup> exige que os prestadores de serviços de comunicações electrónicas publicamente disponíveis tomem as medidas técnicas e organizativas adequadas para garantirem a segurança dos seus serviços e exige também a confidencialidade das comunicações e dos correspondentes dados de tráfego. A Directiva 2002/58/CE impõe aos prestadores de serviços de comunicações electrónicas a obrigação de informação e de notificação das violações de dados pessoais. Além disso, exige que a Comissão consulte a Agência sobre todas as medidas técnicas de execução a adoptar relativas às circunstâncias, ao formato e aos procedimentos aplicáveis às exigências em matéria de informação e de notificação. A Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados<sup>26</sup>,

---

<sup>24</sup> JO L 108 de 24.4.2002, p. 33.

<sup>25</sup> JO L 201 de 31.7.2002, p. 37.

<sup>26</sup> JO L 281 de 23.11.1995, p. 31.

exige que os Estados-Membros estabeleçam que o responsável pelo tratamento deve pôr em prática medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição accidental ou ilícita, a perda accidental, a alteração, a difusão ou o acesso não autorizados, nomeadamente quando o tratamento dos dados implicar a sua transmissão por rede, e contra qualquer outra forma de tratamento ilícito.

- (11) A Agência deverá contribuir para um elevado nível de segurança das redes e da informação dentro da União e para o desenvolvimento de uma cultura de segurança das redes e da informação em benefício dos cidadãos, dos consumidores, das empresas e das organizações do sector público na União Europeia, contribuindo assim para o normal funcionamento do mercado interno.
- (12) Um conjunto de tarefas deverá indicar o modo como a Agência deve atingir os seus objectivos, permitindo-lhe ao mesmo tempo uma certa flexibilidade nas suas operações. Entre as tarefas da Agência deverão constar a recolha das informações e dos dados necessários para efectuar análises dos riscos para a segurança e a resiliência das comunicações, das infra-estruturas e dos serviços electrónicos e para avaliar, em cooperação com os Estados-Membros, a situação em matéria de segurança das redes e da informação na Europa. A Agência deverá garantir a coordenação com os Estados-Membros e reforçar a cooperação entre as partes interessadas na Europa, nomeadamente envolvendo nas suas actividades os organismos nacionais competentes e peritos do sector privado no domínio da segurança das redes e da informação. A Agência deverá prestar assistência à Comissão e aos Estados-Membros no seu diálogo com as empresas sobre os problemas de segurança associados ao hardware e ao software, contribuindo assim para uma abordagem concertada da segurança das redes e da informação.
- (13) A Agência deverá funcionar como ponto de referência e instaurar a confiança em virtude da sua independência, da qualidade dos conselhos dados e das informações que divulga, da transparência dos seus procedimentos e métodos de operação e da sua diligência no exercício das funções que lhe estão atribuídas. A Agência deverá tirar partido dos esforços nacionais e da União e, por conseguinte, desempenhar as suas tarefas em plena cooperação com os Estados-Membros e estar aberta a contactos com as empresas do sector e outras partes interessadas pertinentes. Além disso, a Agência deverá tirar partido dos contributos do sector privado e da cooperação com este sector, que desempenha um papel importante na securização das comunicações, das infra-estruturas e dos serviços electrónicos.
- (14) A Comissão lançou uma parceria europeia público-privada para a resiliência, que constitui um quadro europeu flexível de gestão da resiliência das infra-estruturas TIC, na qual a Agência deverá desempenhar um papel de facilitador, reunindo os interessados do sector público e do sector privado para discutirem as prioridades de política pública, as dimensões económica e comercial dos desafios e as medidas em prol da resiliência das infra-estruturas, e para definirem as suas responsabilidades.
- (15) A Agência deverá aconselhar a Comissão através da formulação de pareceres e da realização de análises técnicas e socioeconómicas, a pedido da Comissão ou por sua própria iniciativa, apoiando-a na elaboração de políticas no domínio da segurança das redes e da informação. A Agência deverá também prestar assistência aos Estados-Membros e às instituições e organismos europeus, se para isso a solicitarem, nos seus

esforços para desenvolverem políticas e capacidades no domínio da segurança das redes e da informação.

- (16) A Agência deverá prestar assistência aos Estados-Membros e às instituições europeias nos seus esforços para construir e melhorarem as suas capacidades e o seu nível de preparação transfronteiras para prevenir, detectar, mitigar e responderem a problemas e incidentes no domínio da segurança das redes e da informação; nesta matéria, a Agência deverá facilitar a cooperação entre os Estados-Membros e entre estes e a Comissão. Para isso, a Agência deverá desempenhar um papel activo de apoio aos Estados-Membros nos seus esforços constantes para melhorarem a sua capacidade de resposta e organizarem e realizarem exercícios nacionais e europeus sobre incidentes de segurança.
- (17) A Directiva 95/46/CE rege o tratamento dos dados pessoais efectuado em aplicação do presente regulamento.
- (18) Para compreender melhor os desafios no domínio da segurança das redes e da informação, a Agência deve analisar os riscos actuais e emergentes. Para isso, a Agência deverá, em cooperação com os Estados-Membros e, se necessário, com os institutos de estatísticas, recolher informações relevantes. Além disso, a Agência deverá assistir os Estados-Membros e as instituições e organismos europeus nos seus esforços para recolherem, analisarem e divulgarem dados sobre a segurança das redes e da informação.
- (19) No exercício das suas actividades de monitorização na União, a Agência deverá facilitar a cooperação entre a União e os Estados-Membros para fins de avaliação da situação em matéria de segurança das redes e da informação na Europa e contribuir para as actividades de avaliação em cooperação com os Estados-Membros.
- (20) A Agência deverá facilitar a cooperação entre os organismos públicos competentes dos Estados-Membros, nomeadamente apoiando o desenvolvimento e o intercâmbio de boas práticas e de normas para programas educativos e de sensibilização. Uma maior troca de informações entre os Estados-Membros facilitará esta acção. A Agência deverá igualmente favorecer a cooperação entre as partes interessadas públicas e privadas ao nível da União, em parte através da promoção da partilha de informações, de campanhas de sensibilização e de programas educativos e de formação.
- (21) Políticas de segurança eficazes deverão basear-se em métodos bem desenvolvidos de avaliação dos riscos, tanto no sector público como no sector privado. Utilizam-se a diferentes níveis métodos e procedimentos para a avaliação dos riscos, sem que exista uma prática comum de aplicação eficaz. A promoção e o desenvolvimento das melhores práticas em matéria de avaliação dos riscos e de soluções interoperáveis de gestão de riscos nas organizações dos sectores público e privado aumentarão o nível de segurança das redes e dos sistemas informáticos na Europa. Para isso, a Agência deverá apoiar a cooperação entre as partes interessadas públicas e privadas ao nível da União, facilitando os seus esforços no que respeita ao desenvolvimento e à implementação de normas para a gestão dos riscos e para tornar mensurável a segurança dos produtos, sistemas, redes e serviços electrónicos.

- (22) O trabalho da Agência deverá aproveitar as actividades de investigação, desenvolvimento e avaliação tecnológica em curso, nomeadamente as realizadas no âmbito das várias iniciativas da União Europeia no domínio da investigação.
- (23) Sempre que tal se revele conveniente e útil para a sua esfera de acção, os seus objectivos e as suas atribuições, a Agência deverá partilhar experiências e informação geral com as agências e os organismos criados ao abrigo da legislação da União Europeia que lidem com a segurança das redes e da informação.
- (24) Nas suas relações com os organismos policiais/judiciais no que respeita aos aspectos de segurança da cibercriminalidade, a Agência deverá utilizar os canais de informação existentes e as redes estabelecidas, tais como os pontos de contacto mencionados na proposta de Directiva do Parlamento Europeu e do Conselho relativa aos ataques contra os sistemas de informação, que revoga a Decisão-quadro 2005/222/JAI, ou a equipa da Europol composta pelos chefes das unidades que se ocupam da criminalidade de alta tecnologia.
- (25) Para garantir a plena consecução dos seus objectivos, a Agência deve estar em contacto com os organismos policiais/judiciais e as autoridades responsáveis pela protecção da privacidade para analisarem e encontrarem a devida resposta para os aspectos do combate à cibercriminalidade que se prendem com a segurança das redes e da informação. Os representantes dessas autoridades deverão tornar-se partes interessadas de pleno direito da Agência e estar representados no seu grupo permanente de partes interessadas.
- (26) Os problemas de segurança das redes e da informação têm uma dimensão mundial. Impõe-se reforçar a cooperação internacional a fim de melhorar as normas de segurança e o intercâmbio de informações e promover uma abordagem global comum dos problemas de segurança das redes e da informação. Para esse efeito, a Agência deverá apoiar a cooperação com os países terceiros e as organizações internacionais, em concertação, se for caso disso, com o Serviço Europeu para a Acção Externa (SEAE).
- (27) No exercício das suas funções, a Agência não deverá interferir com as competências, nem deverá obstar, impedir ou sobrepor-se aos poderes e às funções das autoridades reguladoras nacionais, definidas nas directivas relativas às redes e serviços de comunicações electrónicas, assim como do Organismo dos Reguladores Europeus das Comunicações Electrónicas (ORECE), instituído pelo Regulamento (CE) n.º 1211/2009<sup>27</sup> do Parlamento Europeu e do Conselho, do Comité das Comunicações referido na Directiva 2002/21/CE, dos organismos de normalização europeus, dos organismos de normalização nacionais e do Comité Permanente previsto na Directiva 98/34/CE do Parlamento Europeu e do Conselho, de 22 de Junho de 1998, relativa a um procedimento de informação no domínio das normas e regulamentações técnicas e das regras relativas aos serviços da sociedade da informação<sup>28</sup>, e das autoridades de supervisão dos Estados-Membros responsáveis pela protecção das pessoas singulares no que respeita ao tratamento dos dados pessoais e à livre circulação desses dados.

---

<sup>27</sup> JO L 337 de 18.12.2009, p. 1.

<sup>28</sup> JO L 204 de 21.7.1998, p. 37.

- (28) Para assegurar a eficácia da Agência, os Estados-Membros e a Comissão deverão estar representados no conselho de administração, o qual deverá definir a orientação geral das operações da Agência e garantir que esta executa as suas tarefas de acordo com o presente regulamento. O conselho de administração deverá ser dotado dos necessários poderes para estabelecer o orçamento, verificar a sua execução, aprovar as regras financeiras adequadas, definir procedimentos de trabalho transparentes no tocante à tomada de decisões pela Agência, aprovar o programa de trabalho da Agência, aprovar o seu próprio regulamento interno e o regulamento interno da Agência, nomear o director executivo e decidir do prolongamento ou do termo do mandato deste último. O conselho de administração deverá poder criar grupos de trabalho para o assistirem nas suas tarefas; esses órgãos poderão, por exemplo, elaborar as suas decisões ou monitorizar a aplicação das mesmas.
- (29) O normal funcionamento da Agência exige que o seu director executivo seja nomeado com base no mérito e em capacidades de gestão e administrativas documentadas, bem como na competência e na experiência pertinentes para a segurança das redes e da informação, e que desempenhe as suas funções com total independência no que respeita à organização do funcionamento interno da Agência. Para isso, o director executivo deverá preparar uma proposta de programa de trabalho para a Agência, após consulta dos serviços da Comissão, e tomar todas as medidas necessárias para garantir a boa execução desse programa de trabalho. Deverá preparar todos os anos um projecto de relatório geral a apresentar ao conselho de administração, elaborar um projecto de mapa previsional das receitas e despesas da Agência e executar o orçamento.
- (30) O director executivo deverá ter a possibilidade de criar grupos de trabalho *ad hoc* para questões específicas, designadamente de natureza científica ou técnica, legal ou socioeconómica. Para a criação dos grupos de trabalho *ad hoc*, o director executivo deverá procurar obter e ter em conta os necessários pareceres de peritos externos, para que a Agência possa ter acesso às mais recentes informações disponíveis sobre os desafios, em matéria de segurança, que o desenvolvimento da sociedade da informação levanta. A Agência deverá garantir que os membros dos grupos de trabalho *ad hoc* sejam seleccionados de acordo com os mais elevados padrões de especialização, tendo na devida conta a necessidade de garantir uma representação equilibrada, se for caso disso em função das questões específicas, entre administrações públicas dos Estados-Membros, sector privado, incluindo empresas, utilizadores e académicos especialistas em segurança das redes e da informação. A Agência pode, se necessário, convidar, a título individual, peritos reconhecidos como competentes no domínio em causa a participarem nas actividades dos grupos de trabalho, caso a caso. As suas despesas deverão ser custeadas pela Agência de acordo com as suas próprias regras internas e em conformidade com os regulamentos financeiros existentes.
- (31) A Agência deverá compreender um grupo permanente de partes interessadas enquanto órgão consultivo, para garantir o diálogo regular com o sector privado, as organizações de consumidores e outras partes interessadas pertinentes. Esse grupo permanente - criado pelo conselho de administração por proposta do director executivo - deverá centrar-se em questões pertinentes para todas as partes interessadas e apresentá-las à Agência. Se necessário, e de acordo com a ordem de trabalhos das reuniões, o director executivo poderá convidar representantes do Parlamento Europeu e de outros organismos competentes a participarem nas reuniões do grupo.

- (32) A Agência deverá funcionar no respeito, respectivamente, (i) do princípio da subsidiariedade, garantindo um grau adequado de coordenação entre os Estados-Membros sobre as questões de segurança das redes e da informação e melhorando a eficácia das políticas nacionais, conferindo-lhes, pois, valor acrescentado, e (ii) do princípio da proporcionalidade, não indo além do necessário para atingir os objectivos definidos pelo presente regulamento.
- (33) A Agência deverá aplicar a legislação pertinente da União respeitante ao acesso do público a documentos, consubstanciada do Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho<sup>29</sup>, e à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais, consubstanciada no Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de Dezembro de 2000, relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados<sup>30</sup>.
- (34) Dentro da sua esfera de acção, dos seus objectivos e da execução das suas atribuições, a Agência deverá cumprir, designadamente, as disposições aplicáveis às instituições europeias, bem como a legislação nacional relativa ao tratamento de documentos sensíveis. O conselho de administração deverá ter o poder de tomar uma decisão que permita à Agência tratar informações classificadas.
- (35) A fim de assegurar a plena autonomia e independência da Agência, considera-se necessário dotá-la de um orçamento próprio, cujas receitas sejam essencialmente constituídas por uma contribuição da União e por contribuições dos países terceiros que participam nos trabalhos da Agência. O Estado-Membro anfitrião, ou qualquer outro Estado-Membro, deve poder fazer contribuições voluntárias para as receitas da Agência. O procedimento orçamental da União permanece aplicável no que diz respeito a todas as subvenções imputadas ao orçamento geral da União Europeia. Além disso, o Tribunal de Contas deverá proceder à auditoria das contas.
- (36) A Agência deverá suceder à ENISA, criada pelo Regulamento (CE) n.º 460/2004. No quadro da decisão dos representantes dos Estados-Membros, reunidos no Conselho Europeu de 13 de Dezembro de 2003, o Estado-Membro de acolhimento deverá manter e desenvolver as actuais disposições práticas para garantir o funcionamento normal e eficiente da Agência, no que respeita, designadamente, à cooperação e prestação de assistência à Comissão, aos Estados-Membros e seus organismos competentes, às outras instituições e organismos europeus e às partes interessadas, públicas e privadas, de toda a Europa.
- (37) A Agência deverá ser instituída por um período de tempo limitado. As suas actividades deverão ser avaliadas no que respeita à eficácia na consecução dos objectivos e das suas práticas de trabalho, para determinar se os seus objectivos

---

<sup>29</sup> Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho, de 30 de Maio de 2001, relativo ao acesso do público aos documentos do Parlamento Europeu, do Conselho e da Comissão (JO L 145 de 31.5.2001, p. 43).

<sup>30</sup> Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de Dezembro de 2000, relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados (JO L 8 de 12.1.2001, p. 1).

continuam ou não válidos e, em função disso, se a duração das suas actividades deve ser prolongada,

ADOPTARAM O PRESENTE REGULAMENTO:

## **CAPÍTULO 1 ÂMBITO DE APLICAÇÃO, OBJECTIVOS E FUNÇÕES**

### *Artigo 1.º*

#### **Objecto e âmbito de aplicação**

1. O presente regulamento institui uma agência europeia para a segurança das redes e da informação (a seguir denominada «a Agência») com o propósito de contribuir para um nível elevado de segurança das redes e da informação na União e de sensibilizar e desenvolver uma cultura de segurança das redes e da informação na sociedade, em benefício dos cidadãos, dos consumidores, das empresas e das organizações do sector público da União, contribuindo assim para o normal funcionamento do mercado interno.
2. Os objectivos e as funções da Agência em nada afectam as competências dos Estados-Membros em matéria de segurança das redes e da informação nem, em caso algum, as actividades em matéria de segurança pública, defesa, segurança do Estado (incluindo o bem-estar económico do Estado quando as questões se relacionem com a segurança do Estado), nem as actividades do Estado em domínios do direito penal.
3. Para efeitos do presente regulamento, entende-se por «*segurança das redes e da informação*» a capacidade das redes ou sistemas informáticos para resistirem, com um dado nível de confiança, a eventos acidentais ou acções ilícitas ou maliciosas que comprometam a disponibilidade, autenticidade, integridade e confidencialidade dos dados armazenados ou transmitidos e dos serviços conexos oferecidos ou acessíveis através dessas redes ou sistemas.

### *Artigo 2.º*

#### **Objectivos**

1. A Agência presta assistência à Comissão e aos Estados-Membros para que cumpram as exigências legais e regulamentares da legislação actual e futura da União em matéria de segurança das redes e da informação, contribuindo desse modo para o normal funcionamento do mercado interno.
2. A Agência reforça a capacidade e o grau de preparação da União e dos Estados-Membros para prevenirem, detectarem e responderem a problemas e incidentes no domínio da segurança das redes e da informação.
3. A Agência desenvolve e mantém um elevado nível de competências especializadas e utiliza-as para estimular uma ampla cooperação entre os actores dos sectores público e privado.

### *Artigo 3.º*

#### **Funções**

1. Com o propósito exposto no artigo 1.º, a Agência exerce as seguintes funções:

- a) Assiste a Comissão, a pedido desta ou por sua própria iniciativa, na elaboração da sua política em matéria de segurança das redes e da informação, fornecendo-lhe conselhos e pareceres, análises técnicas e socioeconómicas e trabalhos preparatórios para a elaboração e a actualização da legislação da União no domínio da segurança das redes e da informação;
- b) Facilita a cooperação entre os Estados-Membros e entre estes e a Comissão nos seus esforços de dimensão transfronteiras para prevenirem, detectarem e responderem a incidentes de segurança das redes e da informação;
- c) Assiste os Estados-Membros e as instituições e organismos europeus nos seus esforços para recolherem, analisarem e divulgarem dados sobre a segurança das redes e da informação;
- d) Avalia regularmente, em cooperação com os Estados-Membros e as instituições europeias, a situação da segurança das redes e da informação na Europa;
- e) Apoia a cooperação entre os organismos públicos competentes da Europa, nomeadamente apoiando os seus esforços para desenvolverem e trocarem boas práticas e normas;
- f) Assiste a União e os Estados-Membros na promoção da utilização de boas práticas e de normas em matéria de gestão de riscos e de segurança para os produtos, sistemas e serviços electrónicos;
- g) Apoia a cooperação entre as partes interessadas públicas e privadas a nível da União, através, nomeadamente, da promoção da partilha de informações e da sensibilização, assim como da facilitação dos seus esforços para desenvolverem e adoptarem normas para a gestão dos riscos e para a segurança dos produtos, das redes e dos serviços electrónicos;
- h) Facilita o diálogo e o intercâmbio de boas práticas entre as partes interessadas públicas e privadas sobre a segurança das redes e da informação, incluindo aspectos do combate à cibercriminalidade; assiste a Comissão na elaboração de políticas que tenham em conta a vertente «segurança das redes e da informação» do combate à cibercriminalidade;
- i) Assiste os Estados-Membros e as instituições e organismos europeus, a pedido, nos seus esforços para desenvolverem capacidades de detecção, análise e resposta em matéria de segurança das redes e da informação;
- j) Apoia o diálogo e a cooperação entre a União e os países terceiros e organizações internacionais, em concertação, se for caso disso, com o SEAE, para promover a cooperação internacional e uma abordagem global comum dos problemas de segurança das redes e da informação;
- k) Executa as tarefas que lhe são confiadas por actos legislativos da União.

## **CAPÍTULO 2 ORGANIZAÇÃO**

### *Artigo 4.º* **Órgãos da Agência**

A Agência é composta por:

- a) um conselho de administração;
- b) um director executivo e o pessoal; e
- c) um grupo permanente de partes interessadas.

*Artigo 5.º*

**Conselho de administração**

1. O conselho de administração define a orientação geral das actividades da Agência e assegura que esta trabalhe de acordo com as regras e princípios estabelecidos no presente regulamento. Assegura também a coerência do trabalho da Agência com as actividades conduzidas pelos Estados-Membros, assim como a nível da União.
2. O conselho de administração adopta o seu regulamento interno de comum acordo com os serviços da Comissão pertinentes.
3. O conselho de administração adopta o regulamento interno da Agência de comum acordo com os serviços da Comissão pertinentes. Essas regras são tornadas públicas.
4. O conselho de administração nomeia o director executivo em conformidade com o artigo 10.º, n.º 2, e pode demiti-lo. O conselho de administração exerce autoridade disciplinar sobre o director executivo.
5. O conselho de administração adopta o programa de trabalho da Agência, em conformidade com o artigo 13.º, n.º 3, e o relatório geral de actividades da Agência relativo ao ano anterior, em conformidade com o artigo 14.º, n.º 2.
6. O conselho de administração adopta as regras financeiras aplicáveis à Agência. Essas regras não podem divergir do disposto no Regulamento (CE, Euratom) n.º 2343/2002 da Comissão, de 19 de Novembro de 2002, que institui o Regulamento Financeiro Quadro dos organismos referidos no artigo 185.º do Regulamento (CE, Euratom) n.º 1605/2002 do Conselho, que institui o Regulamento Financeiro aplicável ao orçamento geral das Comunidades Europeias<sup>31</sup>, a menos que as exigências específicas do funcionamento da Agência o imponham e com o consentimento prévio da Comissão.
7. O conselho de administração adopta, com o acordo da Comissão, normas de execução apropriadas, em conformidade com o disposto no artigo 110.º do Estatuto dos Funcionários das Comunidades Europeias.
8. O conselho de administração pode criar grupos de trabalho, constituídos por membros do próprio conselho, para lhe prestarem assistência na execução das suas funções, incluindo a elaboração das suas decisões e o acompanhamento da aplicação das mesmas.
9. O conselho de administração pode adoptar o plano plurianual em matéria de política de pessoal, depois de consultar os serviços da Comissão e de informar devidamente a autoridade orçamental.

---

<sup>31</sup> JO L 357 de 31.12.2002, p. 72.

#### *Artigo 6.º*

### **Composição do conselho de administração**

1. O conselho de administração é composto por um representante de cada Estado-Membro, três representantes da Comissão por ela designados e ainda três representantes sem direito a voto designados pela Comissão, cada um dos quais representando um dos seguintes grupos:

- a) as empresas do sector das tecnologias da informação e das comunicações;
- b) os consumidores;
- c) os especialistas do mundo académico no domínio da segurança das redes e da informação.

2. Os membros do conselho de administração são designados com base no seu grau de experiência e de conhecimentos especializados no domínio da segurança das redes e da informação.

3. O mandato dos representantes dos grupos referidos no n.º 1, alíneas a), b) e c) é de quatro anos. O mandato é renovável uma vez. Se um representante deixar de pertencer ao respectivo grupo de interesse, a Comissão nomeia um substituto.

#### *Artigo 7.º*

### **Presidente do conselho de administração**

O conselho de administração elege de entre os seus membros um presidente e um vice-presidente, por um período de três anos, renovável. O vice-presidente substitui automaticamente o presidente na eventualidade de este não poder cumprir as suas funções.

#### *Artigo 8.º*

### **Reuniões**

1. O conselho de administração reúne-se por convocação do seu presidente.

2. O conselho de administração realiza uma reunião ordinária duas vezes por ano. Além disso, reúne-se a título extraordinário por iniciativa do presidente ou a pedido de, pelo menos, um terço dos seus membros com direito a voto.

3. O director executivo participa nas reuniões do conselho de administração, sem direito a voto.

#### *Artigo 9.º*

### **Votação**

1. O conselho de administração toma as suas decisões por maioria dos seus membros com direito a voto.

2. É necessária uma maioria de dois terços de todos os membros do conselho de administração com direito a voto para a aprovação do seu regulamento interno, do regulamento interno da Agência, do orçamento, do programa de trabalho anual, bem como para a nomeação, prolongamento do mandato e exoneração do director executivo.

*Artigo 10.º*  
**Director executivo**

1. A Agência é gerida pelo seu director executivo, que deve desempenhar as suas funções com independência.

2. O director executivo é nomeado e exonerado pelo conselho de administração. A nomeação é feita a partir de uma lista de candidatos propostos pela Comissão para um período de cinco anos, com base no mérito e nas capacidades comprovadas no domínio da administração e da gestão, assim como na competência e na experiência específicas. Antes de ser nomeado, o candidato seleccionado pelo conselho de administração pode ser convidado a proferir uma declaração perante a comissão competente do Parlamento Europeu e a responder às perguntas formuladas pelos seus membros.

3. No decurso dos nove meses que antecedem o termo desse período, a Comissão procede a uma avaliação, no âmbito da qual examina, designadamente:

- o desempenho do Director Executivo;
- as incumbências e necessidades da Agência nos próximos anos.

4. O conselho de administração, agindo por proposta da Comissão, tendo em conta o relatório de avaliação, e apenas nos casos em que as funções e as necessidades da Agência o justifiquem, pode prolongar o mandato do director executivo por um período máximo de três anos.

5. O conselho de administração informa o Parlamento Europeu da sua intenção de prolongar o mandato do director executivo. No mês anterior à extensão do seu mandato, o director executivo pode ser convidado a proferir uma declaração perante a comissão competente do Parlamento e responder a perguntas dos respectivos membros.

6. Se o mandato não for prolongado, o director permanece em funções até à nomeação do seu sucessor.

7. O director executivo é responsável por:

- a) assegurar a gestão corrente da Agência;
- b) executar o programa de trabalho e as decisões adoptadas pelo conselho de administração;
- c) assegurar que a Agência execute as suas tarefas em conformidade com as exigências dos utilizadores dos seus serviços, designadamente em termos de adequação dos serviços prestados;
- d) todos os assuntos que digam respeito especificamente ao pessoal, garantindo o cumprimento das orientações gerais do conselho de administração e das suas decisões de carácter geral;
- e) desenvolver e manter o contacto com as instituições e organismos europeus;

- f) desenvolver e manter o contacto com a comunidade empresarial e com as organizações de consumidores, para assegurar o diálogo regular com as partes interessadas pertinentes;
- g) outras tarefas que lhe sejam atribuídas pelo presente regulamento.

8. Se necessário e no quadro dos objectivos e tarefas da Agência, o director executivo pode criar grupos de trabalho *ad hoc* constituídos por peritos. O conselho de administração deve ser antecipadamente informado do facto. Os procedimentos relativos nomeadamente à composição, à nomeação dos peritos pelo director executivo e ao funcionamento dos grupos de trabalho *ad hoc* são especificados no regulamento interno da Agência.

9. O director executivo coloca o pessoal de apoio administrativo e outros recursos à disposição do conselho de administração, sempre que necessário.

#### *Artigo 11.º*

### **Grupo permanente de partes interessadas**

1. Por proposta do director executivo, o conselho de administração cria um grupo permanente de partes interessadas composto por peritos representantes das partes interessadas, como as empresas de tecnologias da informação e das comunicações, grupos de consumidores, peritos do meio académico no domínio da segurança das redes e da informação, autoridades policiais/judiciais e autoridades responsáveis pela protecção da privacidade.

2. Os procedimentos relativos, nomeadamente, ao número, composição e nomeação dos membros pelo conselho de administração, à proposta do director executivo e ao funcionamento do grupo são especificados no regulamento interno da Agência e tornados públicos.

3. O grupo é presidido pelo director executivo.

4. Os seus membros têm um mandato de dois anos e meio. Os membros do conselho de administração não podem ser membros do grupo. O pessoal da Comissão pode estar presente nas reuniões e participar nos trabalhos do grupo.

5. O grupo aconselha a Agência no exercício das suas actividades. O grupo aconselha, em particular, o director executivo na elaboração da proposta de programa de trabalho da Agência, assim como no que respeita à comunicação com as partes interessadas pertinentes sobre todas as questões ligadas ao programa de trabalho.

## **CAPÍTULO 3 FUNCIONAMENTO**

#### *Artigo 12.º*

### **Programa de trabalho**

1. A Agência executa as suas tarefas de acordo com o seu programa de trabalho, do qual devem constar todas as suas actividades planeadas. O programa de trabalho não deve obstar a que a Agência assuma actividades imprevistas que se insiram nos seus objectivos e funções,

nos limites do orçamento que lhe está atribuído. O director executivo informa o conselho de administração das actividades da Agência que não estejam previstas no programa de trabalho.

2. O director executivo é o responsável pela elaboração do projecto de programa de trabalho da Agência após consulta dos serviços da Comissão. Antes de 15 de Março de cada ano, o director executivo apresenta ao conselho de administração o projecto de programa de trabalho para o ano seguinte.

3. Antes de 30 de Novembro de cada ano, o conselho de administração adopta o programa de trabalho da Agência para o ano seguinte, em concertação com os serviços da Comissão. O programa de trabalho deve incluir uma perspectiva plurianual. O conselho de administração garante que o programa de trabalho seja coerente com os objectivos da Agência e com as prioridades legislativas e políticas da União no domínio da segurança das redes e da informação.

4. O programa de trabalho é organizado de acordo com o princípio da gestão por actividades (GPA). O programa de trabalho deve ser conforme com o mapa previsionial das receitas e despesas da Agência e com o orçamento da Agência para o mesmo exercício financeiro.

5. Uma vez aprovado pelo conselho de administração, o director executivo transmite o programa de trabalho ao Parlamento Europeu, ao Conselho, à Comissão e aos Estados-Membros e assegura a sua publicação.

#### *Artigo 13.º*

#### **Relatório geral**

1. Todos os anos, o director executivo apresenta ao conselho de administração um projecto de relatório geral abrangendo todas as actividades da Agência no ano anterior.

2. Antes de 31 de Março de cada ano, o conselho de administração aprova o relatório geral das actividades da Agência relativo ao ano anterior.

3. Uma vez aprovado pelo conselho de administração, o director executivo transmite o relatório geral da Agência ao Parlamento Europeu, ao Conselho, à Comissão, ao Tribunal de Contas, ao Comité Económico e Social Europeu e ao Comité das Regiões e assegura a sua publicação.

#### *Artigo 14.º*

#### **Pedidos dirigidos à Agência**

1. Os pedidos de aconselhamento e de assistência que se enquadrem nos objectivos e nas funções da Agência devem ser endereçados ao director executivo e acompanhados de informações que contextualizem e expliquem a questão a tratar. O director executivo informa o conselho de administração dos pedidos recebidos e, no momento oportuno, do seguimento que lhes foi dado. A Agência deve justificar a eventual recusa de um pedido.

2. Os pedidos mencionados no n.º 1 podem ser apresentados:

a) pelo Parlamento Europeu;

b) pelo Conselho;

c) pela Comissão;

d) por qualquer organismo competente designado por um Estado-Membro, nomeadamente uma autoridade reguladora nacional, conforme definida no artigo 2.º da Directiva 2002/21/CE.

3. As regras de execução dos n.ºs 1 e 2, designadamente no que respeita à apresentação, à definição de prioridades, ao seguimento e à informação do conselho de administração relativamente aos pedidos feitos à Agência, são estabelecidas pelo próprio conselho de administração no regulamento interno da Agência.

#### *Artigo 15.º*

#### **Declaração de interesses**

1. O director executivo, bem como os agentes destacados pelos Estados-Membros a título temporário, devem fazer, por escrito, uma declaração de compromisso e uma declaração que indique a ausência de quaisquer interesses directos ou indirectos que possam ser considerados prejudiciais para a sua independência.

2. Os peritos externos que participem em grupos de trabalho *ad hoc* devem declarar, em cada reunião, os eventuais interesses que possam ser considerados prejudiciais para a sua independência em relação aos pontos da ordem de trabalhos e abster-se de participar na discussão desses pontos.

#### *Artigo 16.º*

#### **Transparência**

1. A Agência garante que as suas actividades sejam executadas com um elevado nível de transparência e em conformidade com o disposto nos artigos 13.º e 14.º.

2. A Agência assegura que o público e qualquer parte interessada receba, sempre que adequado, informações objectivas, fiáveis e facilmente acessíveis, nomeadamente no que respeita aos resultados do seu trabalho. A Agência também torna públicas as declarações de interesses feitas pelo director executivo e pelos agentes destacados pelos Estados-Membros a título temporário, bem como as declarações de interesses feitas pelos peritos relativamente aos pontos da ordem de trabalhos das reuniões dos grupos de trabalho *ad hoc*.

3. O conselho de administração pode, por proposta do director executivo, autorizar partes interessadas a observarem o desenrolar de algumas das actividades da Agência.

4. A Agência estabelece, no seu regulamento interno, as disposições práticas para a aplicação das regras de transparência previstas nos n.ºs 1 e 2.

#### *Artigo 17.º*

#### **Confidencialidade**

1. Sem prejuízo do disposto no artigo 14.º, a Agência não divulga a terceiros informações por si processadas ou recebidas para as quais tenha sido pedido um tratamento confidencial.

2. Os membros do conselho de administração, o director executivo, os membros do grupo permanente de partes interessadas, os peritos externos que participam nos seus grupos de trabalho *ad hoc* e os funcionários da Agência, incluindo os agentes destacados pelos Estados-Membros a título temporário, estão sujeitos à obrigação de confidencialidade prevista no artigo 339.º do Tratado, mesmo após a cessação das suas funções.

3. A Agência estabelece no seu regulamento interno as regras de execução das normas de confidencialidade previstas nos n.ºs 1 e 2.

4. O conselho de administração pode decidir autorizar a Agência a tratar informações classificadas. Nesse caso, o conselho de administração adopta, de comum acordo com os serviços da Comissão pertinentes, regras internas de funcionamento que respeitem os princípios de segurança contidos na Decisão 2001/844/CE, CECA, Euratom da Comissão, de 29 Novembro de 2001, que altera o seu Regulamento Interno<sup>32</sup>. São abrangidas, nomeadamente, as disposições relativas ao intercâmbio, tratamento e armazenamento de informações classificadas.

#### *Artigo 18.º*

#### **Acesso aos documentos**

1. O Regulamento (CE) n.º 1049/2001 é aplicável aos documentos na posse da Agência.
2. O conselho de administração aprova as disposições de execução do Regulamento (CE) n.º 1049/2001 no prazo de seis meses a contar da data de criação da Agência.
3. As decisões tomadas pela Agência ao abrigo do artigo 8.º do Regulamento (CE) n.º 1049/2001 podem ser objecto de queixa junto do Provedor de Justiça Europeu ou ser impugnadas junto do Tribunal de Justiça da União Europeia, em conformidade, respectivamente, com os artigos 228.º e 263.º do Tratado.

### **CAPÍTULO 4 DISPOSIÇÕES FINANCEIRAS**

#### *Artigo 19.º*

#### **Adopção do orçamento**

1. As receitas da Agência provêm de uma contribuição do orçamento da União Europeia, de contribuições dos países terceiros que participam no trabalho da Agência, tal como previsto no artigo 29.º, e de contribuições dos Estados-Membros.
2. As despesas da Agência incluem a remuneração do pessoal, a assistência administrativa e técnica, as despesas de infra-estrutura e de funcionamento e as despesas decorrentes de contratos celebrados com terceiros.
3. Até 1 de Março de cada ano, o director executivo elabora um projecto de mapa previsional das receitas e despesas da Agência para o exercício orçamental seguinte e transmite-o ao conselho de administração, acompanhado de um projecto do quadro de pessoal.

---

<sup>32</sup> JO L 317 de 3.12.2001, p. 1.

4. As receitas e as despesas devem ser equilibradas.
5. O conselho de administração elabora anualmente, com base num projecto de mapa previsional das receitas e despesas elaborado pelo director executivo, o mapa previsional das receitas e despesas da Agência para o exercício orçamental seguinte.
6. Este mapa previsional, que deve incluir um projecto de quadro de pessoal e ser acompanhado do projecto de programa de trabalho, é transmitido pelo conselho de administração, até 31 de Março, à Comissão, bem como aos Estados com os quais a União Europeia tenha concluído acordos nos termos do disposto no artigo 24.º.
7. A Comissão transmite esse mapa previsional ao Parlamento Europeu e ao Conselho (a seguir designados “autoridade orçamental”) juntamente com o projecto de orçamento geral da União Europeia.
8. Com base nesse mapa previsional, a Comissão inscreve no projecto de orçamento geral da União Europeia as previsões que considere necessárias no que respeita ao quadro de pessoal e o montante da subvenção a cargo do orçamento geral e submete-o à apreciação da autoridade orçamental nos termos do disposto no artigo 314.º do Tratado.
9. A autoridade orçamental autoriza as dotações a título da subvenção destinada à Agência.
10. A autoridade orçamental adopta o quadro de pessoal da Agência.
11. O conselho de administração adopta o orçamento da Agência ao mesmo tempo que o programa de trabalho. O orçamento torna-se definitivo após a aprovação do orçamento geral da União Europeia. Se necessário, o conselho de administração ajusta o orçamento e o programa de trabalho da Agência em função do orçamento geral da União Europeia. O conselho de administração transmite-o sem demora à Comissão e à autoridade orçamental.

#### *Artigo 20.º*

#### **Luta contra a fraude**

1. Para combater a fraude, a corrupção e outras acções ilegais, as disposições do Regulamento (CE) n.º 1073/1999 do Parlamento Europeu e do Conselho, de 25 de Maio de 1999, relativo aos inquéritos efectuados pelo Organismo Europeu de Luta Antifraude (OLAF)<sup>33</sup>, são aplicáveis sem quaisquer restrições.
2. A Agência adere ao Acordo Interinstitucional de 25 de Maio de 1999 entre o Parlamento Europeu, o Conselho da União Europeia e a Comissão das Comunidades Europeias em matéria de inquéritos internos do Organismo Europeu de Luta Antifraude (OLAF)<sup>34</sup>, e publica, sem demora, as disposições adequadas aplicáveis a todo o seu pessoal.

#### *Artigo 21.º*

#### **Execução do orçamento**

1. O director executivo executa o orçamento da Agência.

---

<sup>33</sup> JO L 136 de 31.5.1999, p. 1.

<sup>34</sup> JO L 136 de 31.5.1999, p. 15.

2. O auditor interno da Comissão exerce, em relação à Agência, as mesmas competências que as exercidas em relação aos serviços da Comissão.
3. Até ao dia 1 de Março seguinte ao exercício encerrado, o contabilista da Agência envia ao contabilista da Comissão as contas provisórias acompanhadas do relatório sobre a gestão orçamental e financeira do exercício. O contabilista da Comissão consolida as contas provisórias das instituições e dos organismos descentralizados nos termos do artigo 128.º do Regulamento (CE, Euratom) n.º 1605/2002 do Conselho, de 25 de Junho de 2002, que institui o Regulamento Financeiro aplicável ao orçamento geral das Comunidades Europeias<sup>35</sup> (a seguir designado por «Regulamento Financeiro geral»).
4. O mais tardar até ao dia 31 de Março seguinte a cada exercício encerrado, o contabilista da Comissão envia ao Tribunal de Contas as contas provisórias da Agência, acompanhadas do relatório sobre a gestão orçamental e financeira do exercício. O relatório sobre a gestão orçamental e financeira do exercício é igualmente enviado à autoridade orçamental.
5. Após recepção das observações formuladas pelo Tribunal de Contas relativamente às contas provisórias da Agência, nos termos do disposto no artigo 129.º do Regulamento Financeiro geral, o director executivo elabora as contas definitivas da Agência, sob sua própria responsabilidade, e transmite-as, para parecer, ao conselho de administração.
6. O conselho de administração emite parecer sobre as contas definitivas da Agência.
7. O mais tardar até 1 de Julho seguinte a cada exercício encerrado, o director executivo transmite as contas definitivas ao Parlamento Europeu, ao Conselho, à Comissão e ao Tribunal de Contas, acompanhadas do parecer do conselho de administração.
8. O director executivo publica as contas finais.
9. O director executivo envia ao Tribunal de Contas uma resposta às observações deste último, o mais tardar até 30 de Setembro. O director executivo transmite essa resposta igualmente ao conselho de administração.
10. O director executivo submete à apreciação do Parlamento Europeu, a pedido deste último, tal como previsto no artigo 146.º, n.º 3, do Regulamento Financeiro geral, todas as informações necessárias ao bom desenrolar do processo de quitação relativamente ao exercício em causa.
11. Antes de 30 de Abril do exercício anual N+2, o Parlamento Europeu, deliberando sobre recomendação do Conselho, dá quitação ao director executivo quanto à execução do orçamento para o exercício N.

---

<sup>35</sup> JO L 248 de 16.9.2002, p. 1.

## CAPÍTULO 5 DISPOSIÇÕES GERAIS

### *Artigo 22.º* **Estatuto jurídico**

1. A Agência é um organismo da União. A Agência tem personalidade jurídica.
2. Em cada um dos Estados-Membros, a Agência goza da mais ampla capacidade jurídica reconhecida às pessoas colectivas pelas legislações nacionais. Pode, designadamente, adquirir ou alienar bens móveis e imóveis e ser parte em processos judiciais.
3. A Agência é representada pelo seu director executivo.

### *Artigo 23.º* **Pessoal**

1. As regras e regulamentos aplicáveis aos funcionários e outros agentes da União Europeia aplicam-se ao pessoal da Agência, incluindo ao seu director executivo.
2. Em relação ao director executivo, o conselho de administração exerce os poderes conferidos à autoridade investida de poder de nomeação pelo Estatuto dos Funcionários e à entidade habilitada a celebrar contratos pelo Regime Aplicável aos Outros Agentes das Comunidades Europeias.
3. Em relação ao pessoal da Agência, o director executivo exerce os poderes conferidos à autoridade investida de poder de nomeação pelo Estatuto dos Funcionários e à entidade habilitada a celebrar contratos pelo Regime Aplicável aos Outros Agentes das Comunidades Europeias.
4. A Agência pode empregar peritos nacionais destacados pelos Estados-Membros. A Agência fixa, nas suas regras internas de funcionamento, as modalidades práticas de aplicação desta disposição.

### *Artigo 24.º* **Privilégios e imunidades**

É aplicável à Agência e ao seu pessoal o Protocolo relativo aos privilégios e imunidades das Comunidades Europeias.

### *Artigo 25.º* **Responsabilidade**

1. A responsabilidade contratual da Agência é regulada pelo direito aplicável ao contrato em causa.

O Tribunal de Justiça da União Europeia é competente para se pronunciar por força de cláusula de arbitragem constante dos contratos celebrados pela Agência.

2. Em matéria de responsabilidade extracontratual, a Agência indemniza, de acordo com os princípios gerais comuns às legislações dos Estados-Membros, os danos causados por si ou pelos seus agentes no exercício das suas funções.

O Tribunal de Justiça é competente em qualquer litígio relativo à reparação desses danos.

3. A responsabilidade pessoal dos agentes perante a Agência é regulada pelas disposições pertinentes do regime aplicável ao pessoal da Agência.

#### *Artigo 26.º*

##### **Línguas**

1. São aplicáveis à Agência as disposições do Regulamento n.º 1, de 15 de Abril de 1958, que estabelece o regime linguístico da Comunidade Económica Europeia<sup>36</sup>. Os Estados-Membros e os outros organismos por eles designados podem dirigir-se à Agência e receber resposta na língua da União Europeia da sua escolha.

2. Os serviços de tradução necessários ao funcionamento da Agência são assegurados pelo Centro de Tradução dos Organismos da União Europeia.

#### *Artigo 27.º*

##### **Protecção de dados pessoais**

No processamento de dados pessoais, a Agência está sujeita às disposições do Regulamento (CE) n.º 45/2001.

#### *Artigo 28.º*

##### **Participação de países terceiros**

1. A Agência está aberta à participação de países terceiros que tenham concluído acordos com a União Europeia por força dos quais tenham adoptado e apliquem a legislação da União no domínio abrangido pelo presente regulamento.

2. No âmbito das disposições pertinentes dos referidos acordos, devem ser adoptadas cláusulas que especifiquem, designadamente, a natureza, a medida e as modalidades da participação desses países nos trabalhos da Agência, incluindo disposições relativas à participação nas iniciativas desenvolvidas pela Agência, às contribuições financeiras e ao pessoal.

---

<sup>36</sup> JO 17 de 6.10.1958, p. 385/58. Regulamento com a última redacção que lhe foi dada pelo Acto de Adesão de 1994.

## CAPÍTULO 6 DISPOSIÇÕES FINAIS

### *Artigo 29.º*

#### **Cláusula de revisão**

1. No prazo de três anos após a data de instituição referida no artigo 34.º, a Comissão, tendo em conta os pareceres de todas as partes interessadas relevantes, procede a uma avaliação com base no caderno de encargos acordado com o conselho de administração. Essa avaliação incide no impacto e na eficácia da Agência na consecução dos objectivos definidos no artigo 2.º e na eficácia das suas práticas de trabalho. A Comissão efectua esta avaliação nomeadamente para determinar se uma agência continua a ser um instrumento eficaz e se o mandato da Agência deve ser prolongado para além do período previsto no artigo 34.º.
2. A Comissão envia os resultados da avaliação ao Parlamento Europeu e ao Conselho e torna-os públicos.
3. O conselho de administração recebe a avaliação e formula recomendações, dirigidas à Comissão, sobre alterações a introduzir no presente regulamento, na Agência e nas práticas de trabalho da mesma. O conselho de administração e o director executivo têm em consideração os resultados da avaliação no planeamento plurianual da Agência.

### *Artigo 30.º*

#### **Cooperação do Estado-Membro de acolhimento**

O Estado-Membro de acolhimento da Agência deve assegurar as melhores condições possíveis para o funcionamento normal e eficiente da mesma.

### *Artigo 31.º*

#### **Controlo administrativo**

As actividades da Agência estão sujeitas à supervisão do Provedor de Justiça Europeu, nos termos do disposto no artigo 228.º do Tratado.

### *Artigo 32.º*

#### **Revogação e sucessão**

1. O Regulamento (CE) n.º 460/2004 é revogado.

As referências ao Regulamento (CE) n.º 460/2004 e à ENISA consideram-se como referências ao presente regulamento e à Agência.

2. A Agência sucede à Agência que foi instituída pelo Regulamento (CE) n.º 460/2004 no que respeita a todos os direitos de propriedade, acordos, obrigações legais, contratos de trabalho, compromissos financeiros e responsabilidades.

*Artigo 33.º*

**Duração**

A Agência é instituída em [...] por um período de cinco anos.

*Artigo 34.º*

**Entrada em vigor**

O presente regulamento entra em vigor no dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia* e produz efeitos a partir de 14 de Março de 2012 ou, se a sua publicação for posterior a esta data, a partir do dia seguinte ao da publicação.

O presente regulamento é obrigatório em todos os seus elementos e directamente aplicável em todos os Estados-Membros.

Feito em [...],

*Pelo Parlamento Europeu*  
*O Presidente*

*Pelo Conselho*  
*O Presidente*

## FICHA FINANCEIRA LEGISLATIVA PARA PROPOSTAS

### 1. CONTEXTO DA PROPOSTA/INICIATIVA

#### 1.1. Denominação da proposta/iniciativa

Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à Agência Europeia para a Segurança das Redes e da Informação (ENISA)

#### 1.2. Domínio(s) de intervenção abrangidos(s) segundo a estrutura ABM/ABB<sup>37</sup>

Sociedade da Informação e Meios de Comunicação

Quadro regulamentar da Agenda Digital

#### 1.3. Natureza da proposta/iniciativa

A proposta/iniciativa refere-se a **uma nova acção**

A proposta/iniciativa refere-se a **uma nova acção na sequência de um projecto-piloto/acção preparatória**<sup>38</sup>

A proposta/iniciativa refere-se à **prorrogação de uma acção existente**

A proposta/iniciativa refere-se a **uma acção reorientada para uma nova acção**

#### 1.4. Objectivos

##### 1.4.1. Objectivo(s) estratégico(s) plurianual(is) da Comissão visado(s) pela proposta/iniciativa

**Coerência das abordagens regulamentares** – fornecer orientações e conselhos à Comissão e aos Estados-Membros para que actualizem e elaborem um quadro normativo global no domínio da segurança das redes e da informação (SRI).

**Prevenção, detecção e resposta** – melhorar a preparação, contribuindo para a instauração de uma capacidade europeia de alerta precoce e de resposta a incidentes, planos de emergência e exercícios pan-europeus.

**Desenvolvimento dos conhecimentos dos decisores** – prestar assistência e aconselhamento à Comissão e aos Estados-Membros para que atinjam um elevado nível de conhecimento, em toda a União, sobre as questões relacionadas com a SRI e a sua aplicação às empresas interessadas. Este objectivo inclui também a produção, a análise e a disponibilização de dados sobre a economia e o impacto das violações da SRI, de factores de incentivo para que as partes interessadas invistam em medidas de SRI, identificação dos riscos, indicadores do estado da SRI na União, etc.

<sup>37</sup> ABM: Activity Based Management (gestão por actividades) – ABB: Activity Based Budgeting (orçamentação por actividades).

<sup>38</sup> Conforme referidos no artigo 49.º, n.º 6, alíneas a) ou b), do Regulamento Financeiro.

**Responsabilização das partes interessadas** – desenvolver uma cultura de segurança e de gestão dos riscos, através do estímulo à partilha de informações e à ampla cooperação entre os actores do sector público e do privado, também em benefício directo dos cidadãos, e desenvolver uma cultura de sensibilização para a SRI.

**Protecção da Europa contra as ameaças internacionais** – elevar o nível da cooperação com os países terceiros e organizações internacionais, tendo em vista promover uma abordagem global comum da SRI e potenciar o impacto das iniciativas internacionais de alto nível na Europa.

**Para uma aplicação concertada** – facilitar a colaboração na aplicação das políticas no domínio da SRI.

**Combate à cibercriminalidade** – integrar a vertente SRI do combate à cibercriminalidade nas discussões e no intercâmbio de boas práticas entre as partes interessadas públicas e privadas, em particular através da cooperação com as autoridades dos (antigos) 2.º e 3.º pilares, como a Europol.

1.4.2. *Objectivo(s) específico(s) e actividade(s) ABM/ABB em causa*

Objectivo específico

Aumentar a segurança das redes e da informação, desenvolver uma cultura de segurança das redes e da informação no interesse dos cidadãos, dos consumidores, das empresas e das organizações do sector público e identificar os desafios políticos suscitados pelas futuras redes e pela futura Internet.

Actividade(s) ABM/ABB em causa

Política de comunicações electrónicas e segurança das redes

#### 1.4.3. Resultado(s) e impacto esperados

Prevê-se que a iniciativa produza os seguintes efeitos económicos:

- uma maior disponibilidade de informações sobre os desafios actuais e futuros e sobre os riscos para a segurança e a resiliência;
- a não duplicação de esforços de cada Estado-Membro na recolha de informações sobre os riscos, as ameaças e as vulnerabilidades;
- um maior nível de informação dos decisores políticos ao tomarem decisões;
- maior qualidade das disposições políticas em matéria de SRI nos Estados-Membros devido à difusão das melhores práticas;
- economias de escala na resposta a incidentes a nível da UE;
- mais investimentos induzidos por objectivos políticos e normas comuns para a segurança e a resiliência a nível da UE;
- riscos operacionais mais baixos para as empresas, devido ao maior nível de segurança e de resiliência;
- maior coerência das medidas de combate à cibercriminalidade.

Prevê-se que a iniciativa produza os seguintes efeitos sociais:

- uma maior confiança dos utilizadores nos serviços e sistemas da sociedade da informação;
- uma maior confiança no funcionamento do mercado interno da UE devido à obtenção de níveis de protecção mais elevados;
- um maior intercâmbio de informações e conhecimentos com países de fora da UE;
- uma melhor salvaguarda dos direitos humanos fundamentais da UE através da garantia de níveis iguais de protecção dos dados pessoais e da privacidade dos cidadãos da UE.

Os impactos previstos no ambiente são marginais:

- menores efeitos das emissões de CO<sub>2</sub>, devido, por exemplo, à diminuição do número de viagens pelo facto de existir maior confiança na utilização dos sistemas e serviços TIC, e ao menor consumo de energia decorrente das economias de escala na aplicação das obrigações de segurança.

#### 1.4.4. Indicadores de resultados e de impacto

Os indicadores de acompanhamento relativos aos diferentes objectivos são os seguintes:

##### **Coerência das abordagens regulatórias:**

- Número de Estados-Membros que seguiram as recomendações da Agência no seu processo de definição de políticas.
- Número de estudos que visam identificar as lacunas e incoerências na paisagem normativa no que respeita à SRI.
- Diminuição das divergências entre as abordagens dos Estados-Membros relativamente à SRI.

##### **Prevenção, detecção e resposta:**

- Número de formações organizadas sobre segurança das redes.

- Disponibilidade de um sistema funcional de alerta rápido para novos riscos e ataques.
- Número de exercícios SRI a nível da UE coordenados pela Agência.

**Desenvolvimento dos conhecimentos dos decisores:**

- Número de estudos destinados a reunir informações sobre os riscos actuais e previstos no domínio da SRI e sobre as tecnologias para prevenção dos mesmos.
- Número de consultas aos organismos públicos responsáveis pela SRI.
- Existência de um quadro europeu para a organização da recolha de dados sobre a SRI.

**Responsabilização das partes interessadas:**

- Número de boas práticas identificadas nas empresas.
- Nível de investimento das partes interessadas privadas em medidas de segurança.

**Protecção da Europa contra ameaças internacionais:**

- Número de conferências / reuniões entre os Estados-Membros da UE para definirem objectivos comuns para a SRI.
- Número de reuniões entre peritos europeus e internacionais em matéria de SRI.

**Para uma aplicação concertada:**

- Número de avaliações da conformidade com a regulamentação.
- Número de práticas SRI à escala da UE.

**Luta contra a cibercriminalidade:**

- Regularidade das interacções com as agências dos antigos 2.º e 3.º pilares.
- Número de casos em que se forneceram competências especializadas para investigações criminais.

**1.5. Justificação da proposta/iniciativa**

*1.5.1. Necessidade(s) a satisfazer a curto ou a longo prazo*

A ENISA foi originalmente criada em 2004 para responder às ameaças à SRI e às possíveis violações subsequentes da SRI. Desde então, os desafios relacionados com a segurança das redes e da informação têm evoluído à medida da evolução tecnológica e dos mercados e têm sido objecto de maior reflexão e debate, o que permite hoje uma actualização e uma descrição mais detalhada dos problemas concretos identificados e do modo como estes são influenciados pelas alterações na paisagem da SRI.

*1.5.2. Valor acrescentado da intervenção da UE*

Os problemas que afectam a SRI não se detêm nas fronteiras nacionais e, por conseguinte, não podem ser resolvidos eficazmente apenas a nível nacional. Ao mesmo tempo, verifica-se grande diversidade na maneira como o problema é tratado pelas autoridades públicas dos diferentes Estados-Membros. Essas diferenças podem constituir um obstáculo importante à aplicação de mecanismos adequados à escala da União para melhorar a SRI na Europa. Devido à interconexão natural das infra-estruturas TIC, a eficácia das medidas tomadas a nível nacional num dado Estado-Membro é ainda fortemente condicionada pela dimensão mais

limitada de medidas tomadas noutros Estados-Membros e pela falta de cooperação transfronteiras sistemática. A insuficiência das medidas em matéria de SRI num Estado-Membro pode originar incidentes susceptíveis de perturbar serviços de outros Estados-Membros.

Além disso, a multiplicação das exigências de segurança impõe custos às empresas que operam a nível da União Europeia e conduz à fragmentação e à falta de competitividade do mercado interno europeu.

Ao mesmo tempo que aumenta a dependência das redes e dos sistemas informáticos, a preparação para resolver incidentes parece ser insuficiente.

Os actuais sistemas nacionais de alerta precoce e de resolução de incidentes apresentam grandes defeitos. Os processos e as práticas de monitorização e comunicação de incidentes de segurança das redes variam significativamente de Estado-Membro para Estado-Membro. Nalguns países, os processos não estão formalizados, ao passo que noutros não existe uma autoridade competente para receber e tratar os relatórios de incidentes. Não existem sistemas europeus. Em resultado disso, um incidente de SRI pode perturbar completamente os sistemas que permitem responder às necessidades básicas, pelo que devem ser preparadas respostas adequadas. A Comunicação da Comissão sobre a protecção das infra-estruturas críticas da informação também sublinhou a necessidade de dotar a Europa de uma capacidade de alerta precoce e de resposta a incidentes, eventualmente alicerçada em exercícios à escala europeia.

Há uma necessidade clara de instrumentos políticos que visem identificar de forma pró-activa os riscos e as vulnerabilidades em termos de SRI, que estabeleçam mecanismos de resposta adequados (nomeadamente através da identificação e difusão de boas práticas) e que garantam que esses mecanismos de resposta sejam conhecidos e aplicados pelas partes interessadas.

### *1.5.3. Principais ensinamentos retirados de experiências análogas anteriores*

*Ver os pontos 1.5.1 e 1.5.2.*

### *1.5.4. Coerência e eventual sinergia com outros instrumentos relevantes*

Esta iniciativa é totalmente coerente com o debate geral sobre a SRI e com outras iniciativas políticas centradas no seu futuro. É uma das principais componentes da Agenda Digital para a Europa, uma iniciativa emblemática da estratégia Europa 2020.

## 1.6. Duração e impacto financeiro

Proposta/iniciativa de **duração limitada**

–  O ponto de partida do prolongamento de 5 anos será 14/3/2012 ou o dia em que o novo regulamento entrar em vigor, se esta data for posterior.

–  Impacto financeiro de 2012 a 2017

Proposta/iniciativa de **duração ilimitada**

– Aplicação com um período de arranque entre AAAA e AAAA,

– seguido de um funcionamento em pleno.

## 1.7. Modalidade(s) de gestão prevista(s)<sup>39</sup>

**Gestão centralizada directa** pela Comissão

**Gestão centralizada indirecta** por delegação de funções de execução em:

–  agências de execução

–  organismos criados pelas Comunidades<sup>40</sup>

–  organismos públicos nacionais/organismos com missão de serviço público

–  pessoas encarregadas da execução de acções específicas por força do Título V do Tratado da União Europeia, identificadas no acto de base pertinente na acepção do artigo 49.º do Regulamento Financeiro

**Gestão partilhada** com os Estados-Membros

**Gestão descentralizada** com países terceiros

**Gestão conjunta** com organizações internacionais (*a especificar*)

---

<sup>39</sup> As explicações sobre as modalidades de gestão e as referências ao Regulamento Financeiro estão disponíveis no sítio BudgWeb: [http://www.cc.cec/budg/man/budgmanag/budgmanag\\_en.html](http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html)

<sup>40</sup> Referidos no artigo 185.º do Regulamento Financeiro.

## 2. MEDIDAS DE GESTÃO

### 2.1. Disposições em matéria de acompanhamento e de prestação de informações

O director executivo é responsável pela monitorização e avaliação eficazes do desempenho da Agência face aos seus objectivos e presta contas anualmente ao conselho de administração.

O director executivo redige um relatório geral sobre todas as actividades da Agência no ano anterior, em que, nomeadamente, compara os resultados atingidos com os objectivos do programa de trabalho anual. Após a sua adopção pelo conselho de administração, este relatório é transmitido ao Parlamento Europeu, ao Conselho, à Comissão, ao Tribunal de Contas, ao Comité Económico e Social Europeu e ao Comité das Regiões e publicado.

### 2.2. Sistema de gestão e de controlo

#### 2.2.1. *Risco(s) identificado(s)*

Desde a sua criação, em 2004, a ENISA foi objecto de avaliações externas e internas.

Nos termos do artigo 25.º do Regulamento ENISA, a primeira etapa desse processo foi a avaliação independente da ENISA por um painel de peritos externos em 2006/2007. O relatório elaborado pelo painel de peritos externos<sup>41</sup> confirmou que os fundamentos políticos iniciais para a criação da ENISA e os seus objectivos iniciais continuavam válidos e, além disso, foi fundamental para o levantamento de problemas que exigem resposta.

Em Março de 2007, a Comissão fez relatório da avaliação ao conselho de administração, que formulou depois as suas próprias recomendações sobre o futuro da Agência e sobre as alterações ao Regulamento ENISA<sup>42</sup>.

Em Junho de 2007, a Comissão apresentou a sua própria apreciação dos resultados da avaliação externa e das recomendações do conselho de administração numa Comunicação ao Parlamento Europeu e ao Conselho<sup>43</sup>. A Comunicação declarava que havia que escolher entre prolongar o mandato da agência ou substituí-la por outro mecanismo, como um fórum permanente de partes interessadas ou uma rede de organizações da área da segurança. A Comunicação lançou igualmente uma consulta pública sobre a matéria, pedindo contributos às partes interessadas europeias com base numa lista de perguntas que orientariam as discussões posteriores<sup>44</sup>.

<sup>41</sup> [http://ec.europa.eu/dgs/information\\_society/evaluation/studies/index\\_en.htm](http://ec.europa.eu/dgs/information_society/evaluation/studies/index_en.htm).

<sup>42</sup> Como previsto no seu artigo 25.º. O texto integral do documento adoptado pelo conselho de administração da ENISA, que contém igualmente as suas considerações, está disponível no seguinte sítio Web: [http://enisa.europa.eu/pages/03\\_02.htm](http://enisa.europa.eu/pages/03_02.htm).

<sup>43</sup> Comunicação da Comissão ao Parlamento Europeu e ao Conselho - Avaliação da Agência Europeia para a Segurança das Redes e da Informação (ENISA), COM(2007) 285 final de 1.6.2007: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0285:EN:NOT>.

<sup>44</sup> <http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=EnisaFuture&lang=en>.

2.2.2. *Meio(s) de controlo previsto(s)*

Ver pontos 2.1 e 2.2.1 supra.

**2.3. Medidas de prevenção de fraudes e irregularidades**

O pagamento de qualquer serviço ou estudo solicitado é controlado pelo pessoal da Agência antes de ser efectuado, tendo em conta todas as obrigações contratuais, os princípios económicos e as boas práticas financeiras ou de gestão. Serão incluídas disposições antifraude (supervisão, apresentação de relatórios, etc.) em todos os acordos ou contratos celebrados entre a Agência e os beneficiários dos pagamentos.

### 3. IMPACTO FINANCEIRO ESTIMADO DA PROPOSTA/INICIATIVA\*

#### 3.1. Rubrica(s) do quadro financeiro plurianual e rubrica(s) orçamental(is) de despesas envolvidas

- Rubricas orçamentais de despesas existentes

Rubrica do quadro financeiro plurianual	Rubrica orçamental	Natureza da despesa	Participação			
	Número / Descrição	DD/DND <sup>(45)</sup>	dos países EFTA <sup>46</sup>	dos países candidatos <sup>47</sup>	de países terceiros	na acepção do artigo 18.º, n.º 1, alínea aa), do Regulamento Financeiro
1.a Competitividade para o crescimento e o emprego	09 02 03 01 Agência Europeia para a Segurança das Redes e da Informação – Subvenção no âmbito dos Títulos 1 e 2	DD	SIM	NÃO	NÃO	NÃO
	09 02 03 02 Agência Europeia para a Segurança das Redes e da Informação – Subvenção no âmbito do Título 3	DD	SIM	NÃO	NÃO	NÃO
5 Despesas administrativas	09 01 01 Despesas relativas ao pessoal no activo do domínio de intervenção "Sociedade da informação e <i>Media</i> "	DND	NÃO	NÃO	NÃO	NÃO
	09 01 02 11 Outras despesas de gestão	DND	NÃO	NÃO	NÃO	NÃO

\* O impacto financeiro estimado da proposta no período posterior ao actual período de programação financeira (2007-2013) não é coberto pela presente Ficha Financeira Legislativa. Com base na proposta da Comissão relativa ao regulamento que estabelece o quadro financeiro plurianual pós-2013 e tendo em conta as conclusões da avaliação de impacto, a Comissão apresentará uma Ficha Financeira Legislativa alterada.

<sup>45</sup> DD = dotações diferenciadas/DND = dotações não diferenciadas.

<sup>46</sup> EFTA: Associação Europeia de Comércio Livre.

<sup>47</sup> Países candidatos e, se for caso disso, países candidatos potenciais dos Balcãs Ocidentais.

### 3.2. Impacto estimado nas despesas

#### 3.2.1. Síntese do impacto estimado nas despesas

Em milhões de euros (3 casas decimais)

<b>Rubrica do quadro financeiro plurianual:</b>	1.a	Competitividade para o crescimento e o emprego
---	-----	--

ENISA			1 Jan-13 Mar 2012	14 Mar-31 Dez 2012	2013	2014	2015	2016	1 Jan-13 Mar 2017	TOTAL 14 Mar 2012 – 13 Mar 2017
Dotações operacionais										
09 02 03 02 Agência Europeia para a Segurança das Redes e da Informação – Subvenção no âmbito do Título 3	Autorizações	(1)	0,454	1,976	2,470	--	--	--	--	--
	Pagamentos	(2)	0,454	1,976	2,470	--	--	--	--	--
Dotações administrativas										
09 02 03 01 Agência Europeia para a Segurança das Redes e da Informação – Subvenção no âmbito dos Títulos 1 e 2		(3)	1,293	4,697	6,120	--	--	--	--	--
<b>TOTAL das dotações para a RUBRICA 1.a</b>	Autorizações	=1+3	1,747	6,673	8,590	--	--	--	--	--
	Pagamentos	=2+3	1,747	6,673	8,590	--	--	--	--	--

TOTAL das dotações operacionais	Autorizações	(4)	0,454	1,976	2,470	--	--	--	--	--
	Pagamentos	(5)	0,454	1,976	2,470	--	--	--	--	--
TOTAL das dotações de natureza administrativa financiadas a partir da dotação de programas específicos		(6)	1,293	4,697	6,120	--	--	--	--	--
<b>TOTAL das dotações Para a RUBRICA 1.a</b> do programa-quadro plurianual	Autorizações	=4+ 6	1,747	6,673	8,590	--	--	--	--	--
	Pagamentos	=5+ 6	1,747	6,673	8,590	--	--	--	--	--

Em milhões de euros (3 casas decimais)

<b>Rubrica do quadro financeiro plurianual:</b>	5	Despesas administrativas
---	---	--------------------------

	1 Jan-13 Mar 2012	14 Mar-31 Dez 2012	2013	2014	2015	2016	1 Jan-13 Mar 2017	Total
Recursos humanos	0,085	0,342	0,427	--	--	--	--	--
Outras despesas administrativas	0,002	0,013	0,015	--	--	--	--	--
<b>TOTAL DG INFSO</b>	<b>Dotações</b>	0,087	0,355	0,442	--	--	--	--

<b>TOTAL das dotações para a RUBRICA 5 do quadro financeiro plurianual</b>	(Total das autorizações = Total dos pagamentos)	0,087	0,355	0,442	--	--	--	--	--
--	---	-------	-------	-------	----	----	----	----	----

	1 Jan-13 Mar 2012	14 Mar-31 Dez 2012	2013	2014	2015	2016	1 Jan-13 Mar 2017	Total
<b>TOTAL das dotações para as RUBRICAS 1 a 5 do quadro financeiro plurianual</b>	Autorizações	1,834	7,028	9,032	--	--	--	--
	Pagamentos	1,834	7,028	9,032	--	--	--	--

### 3.2.2. Impacto estimado nas dotações operacionais

- A proposta/iniciativa não acarreta a utilização de dotações operacionais
- A proposta/iniciativa acarreta a utilização de dotações operacionais, tal como explicitado seguidamente:

Dotações de autorização em milhões de euros (3 casas decimais)

Indicar os objectivos e as realizações	1 Jan-13 Mar 2012	14 Mar-31 Dez 2012	2013	2014	2015	2016	1 Jan-13 Mar 2017	TOTAL 14 Mar 2012 – 13 Mar 2017
↓								
Coerência das abordagens regulamentares:	0,114	0,494	0,620	--	--	--	--	--
Prevenção, detecção e resposta:	0,114	0,494	0,620	--	--	--	--	--
Desenvolvimento dos conhecimentos dos decisores:	0,068	0,297	0,370	--	--	--	--	--
Responsabilização das partes interessadas	0,050	0,218	0,270	--	--	--	--	--
Protecção da Europa contra ameaças internacionais	0,023	0,099	0,120	--	--	--	--	--
Para uma aplicação concertada:	0,064	0,276	0,340	--	--	--	--	--
Luta contra a cibercriminalidade	0,023	0,098	0,120	--	--	--	--	--
<b>CUSTO TOTAL</b>	0,454	1,976	2,460	--	--	--	--	--

### 3.2.3. Impacto estimado nas dotações de natureza administrativa<sup>48</sup>

#### 3.2.3.1. Síntese

- A proposta/iniciativa não acarreta a utilização de dotações de natureza administrativa
- A proposta/iniciativa acarreta a utilização de dotações de natureza administrativa, tal como explicitado seguidamente:

#### a) Despesas administrativas no âmbito da Rubrica 5 do quadro financeiro plurianual

Em milhões de euros (3 casas decimais)

<b>RUBRICA 5 do quadro financeiro plurianual</b>	1 Jan-13 Mar 2012	14 Mar-31 Dez 2012	2013	2014	2015	2016	1 Jan-13 Mar 2017	<b>TOTAL 14 Mar 2012 – 13 Mar 2017</b>
--	----------------------	-----------------------	------	------	------	------	----------------------	--

Recursos humanos	0,085	0,342	0,427	--	--	--	--	--
Outras despesas administrativas	0,002	0,013	0,015	--	--	--	--	--

<b>TOTAL</b>	0,087	0,355	0,442	--	--	--	--	--
--------------	-------	-------	-------	----	----	----	----	----

#### b) Despesas administrativas relacionadas com a ENISA – no âmbito da rubrica orçamental «09.020301 Agência Europeia para a Segurança das Redes e da Informação: Título 1 – Pessoal e Título 2 – Functionamento da Agência».

Em milhões de euros (3 casas decimais)

	1 Jan-13 Mar 2012	14 Mar-31 Dez 2012	2013	2014	2015	2016	1 Jan-13 Mar 2017	<b>TOTAL 14 Mar 2012 – 13 Mar 2017</b>
--	----------------------	-----------------------	------	------	------	------	----------------------	--

Recursos humanos - Título 1 – Pessoal	1,153	4,329	5,607	--	--	--	--	--
Outras despesas de natureza administrativa – Título 2 – Functionamento da Agência	0,140	0,368	0,513	--	--	--	--	--

<b>TOTAL</b>	<b>1,293</b>	<b>4,697</b>	<b>6,120</b>	--	--	--	--	--
--------------	--------------	--------------	--------------	----	----	----	----	----

<sup>48</sup> O anexo da Ficha Financeira Legislativa não está preenchido dado que não se aplica à actual proposta.

### 3.2.3.2. Necessidades estimadas de recursos humanos

Todos os anos, o quadro de efectivos da Agência é explicado e justificado num documento designado «plano em matéria de política de pessoal», que é apresentado à autoridade orçamental.

- A proposta/iniciativa não acarreta a utilização de recursos humanos
- A proposta/iniciativa acarreta a utilização de recursos humanos, tal como explicitado seguidamente:

#### a) Recursos humanos no seio da Comissão

	1 Jan-13 Mar 2012	14 Mar-31 Dez 2012	2013	2014	2015	2016	1 Jan-13 Mar 2017
<b>Lugares do quadro do pessoal (postos de funcionários e de agentes temporários)</b>							
XX 01 01 01 (na sede e nos gabinetes de representação da Comissão)	3,5	3,5	3,5	--	--	--	--
<b>TOTAL</b>	<b>3,5</b>	<b>3,5</b>	<b>3,5</b>	--	--	--	--

#### b) Recursos humanos da ENISA

	1 Jan-13 Mar 2012	14 Mar-31 Dez 2012	2013	2014	2015	2016	1 Jan-13 Mar 2017
<b>Quadro de pessoal da ENISA (em equivalentes tempo inteiro - ETI)</b>							
Funcionários e agentes temporários	AD	29	31	31	--	--	--
	AST	15	16	16	--	--	--
TOTAL funcionários ou pessoal temporário	44	47	47	--	--	--	--
<b>Outro pessoal (em ETI)</b>							
Agentes contratuais	13	14	14	--	--	--	--
Peritos nacionais destacados (PND)	5	5	5	--	--	--	--
Total outro pessoal	18	19	19	--	--	--	--
<b>TOTAL</b>	<b>62</b>	<b>66</b>	<b>66</b>	--	--	--	--

Descrição das tarefas a executar pelo pessoal da Agência:

<p>Funcionários temporários e agentes</p>	<p>A Agência continuará a:</p> <ul style="list-style-type: none"> <li>– desempenhar funções consultivas e de coordenação, no exercício das quais <b>reúne e analisa dados</b> sobre a segurança da informação. Hoje em dia, tanto as organizações públicas como as privadas reúnem, com objectivos diferentes, dados relativos a incidentes no domínio das TI e outros dados pertinentes para a segurança da informação. Não existe, porém, uma entidade central a nível europeu, que possa, de modo sistemático, coligir e analisar dados e fornecer pareceres e aconselhamento para apoiar o trabalho político da União em matéria de segurança das redes e da informação;</li> <li>– <b>servir de centro especializado</b> a que os Estados-Membros e as instituições europeias possam recorrer para obterem <b>pareceres e aconselhamento sobre questões técnicas</b> relacionadas com a segurança;</li> <li>– contribuir para uma <b>ampla cooperação entre os diferentes intervenientes</b> no domínio da segurança da informação, nomeadamente prestar assistência nas actividades de acompanhamento com o fim de garantir a segurança dos negócios electrónicos. Essa cooperação será um pré-requisito fundamental para o funcionamento seguro das redes e dos sistemas de informação na Europa. É necessária a participação e o envolvimento de todas as partes interessadas;</li> <li>– contribuir para uma abordagem coordenada da segurança da informação fornecendo <b>apoio aos Estados-Membros</b>, designadamente na <b>promoção de acções de avaliação dos riscos</b> e de sensibilização;</li> <li>– garantir a <b>interoperabilidade das redes e dos sistemas de informação</b> quando os Estados-Membros <b>aplicarem</b> requisitos técnicos que afectem a segurança;</li> <li>– identificar as <b>necessidades de normalização nesta matéria</b>, avaliar as normas de segurança e os regimes de certificação existentes e promover a maior generalização possível da sua utilização em apoio da legislação europeia;</li> </ul> <p>– apoiar a <b>cooperação internacional</b> neste domínio, cada vez mais necessária dado o carácter mundial das questões de segurança das redes e da informação.</p>
<p>Pessoal externo</p>	<p>Ver acima</p>

### 3.2.4. *Compatibilidade com o actual quadro financeiro plurianual*

- A proposta/iniciativa é compatível com o actual quadro financeiro plurianual.
- A proposta/iniciativa requer uma reprogramação da rubrica pertinente do quadro financeiro plurianual.
- A proposta/iniciativa requer a mobilização do instrumento de flexibilidade ou a revisão do quadro financeiro plurianual<sup>49</sup>.

O financiamento pela UE após 2013 será examinado no contexto de um debate alargado a toda a Comissão sobre todas as propostas para o período após 2013. Significa isto que, uma vez apresentada a sua proposta para o próximo quadro financeiro plurianual, a Comissão apresentará uma ficha financeira legislativa alterada, tendo em conta as conclusões da avaliação de impacto.

### 3.2.5. *Participação de terceiros no financiamento*

- A proposta/iniciativa não prevê o co-financiamento por terceiros
- A proposta/iniciativa prevê o seguinte co-financiamento estimado:

Dotações indicativas em milhões de euros (3 casas decimais)

	1 Jan-13 Mar 2012	14 Mar-31 Dez 2012	2013	2014	2015	2016	1 Jan-13 Mar 2017	<b>TOTAL 14 Mar 2012 – 13 Mar 2017</b>
EFTA	0,042	0,160	0,206	--	--	--	--	--

<sup>49</sup> Ver pontos 19 e 24 do Acordo Interinstitucional.

### 3.3. Impacto estimado nas receitas

- A proposta/iniciativa não tem impacto financeiro nas receitas
- A proposta/iniciativa tem o impacto financeiro a seguir descrito:
  - nos recursos próprios
  - nas receitas diversas