Comissão da Indústria, da Investigação e da Energia

2013/0027(COD)

13.1.2014

PARECER

da Comissão da Indústria, da Investigação e da Energia

dirigido à Comissão do Mercado Interno e da Proteção dos Consumidores

sobre a proposta de Diretiva do Parlamento Europeu e do Conselho relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União
(COM(2013)0048 – C7-0035/2013 – 2013/0027(COD))

Relatora de parecer: Pilar del Castillo Vera

(*) Comissão associada – Artigo 50.º do Regimento

PA_Legam

JUSTIFICAÇÃO SUCINTA

Em fevereiro de 2013, a Comissão Europeia, tal como solicitado pelo Parlamento Europeu no seu relatório de iniciativa sobre uma Agenda Digital para a Europa, apresentou uma proposta de diretiva relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, juntamente com a primeira estratégia de cibersegurança da UE. Tendo em conta que, segundo uma análise dos dados disponíveis, os incidentes relacionados com as TIC de natureza maliciosa podem implicar custos diretos superiores a 560 milhões de euros por ano só para as PME e que todos os tipos de incidentes (incluindo problemas ambientais ou físicos a montante, tais como catástrofes naturais) podem implicar custos diretos superiores a 2,3 mil milhões, a relatora saúda vivamente a proposta.

Relativamente à sua estrutura, a relatora concorda com uma série de medidas propostas, tais como o alargamento das disposições em matéria de comunicação de incidentes de segurança, atualmente limitadas aos fornecedores de telecomunicações nos termos do artigo 13.º-A da Diretiva-Quadro de 2009, a outros setores de infraestruturas críticos. Neste sentido, propostas como exigir que todos os Estados-Membros possuam equipas de resposta a emergências informáticas a funcionar corretamente e designar uma autoridade competente para integrar uma rede pan-europeia segura de intercâmbio eletrónico de dados, a fim de permitir uma partilha e uma troca seguras de informação relacionada com a cibersegurança, são bem recebidas e têm potencial para contribuir significativamente para a consecução do objetivo da diretiva proposta, nomeadamente assegurar um elevado nível comum de segurança das redes e da informação em toda a União.

Todavia, a relatora considera que ainda é possível melhorar a proposta, aplicando o prisma de dois princípios fundamentais: eficiência e confiança.

Primeiro princípio - Eficiência

Em relação às obrigações dos Estados-Membros de designar uma autoridade competente responsável pelo acompanhamento da aplicação da diretiva a todos os setores constantes do anexo II da proposta, a relatora entende que cada Estado-Membro deve não só ter liberdade para escolher o modelo de governação de cibersegurança que considere mais adequado, como também evitar imperativamente a duplicação das estruturas institucionais que conduzirão potencialmente a conflitos em termos de competências e a perturbações nas comunicações. Nesse sentido, a relatora considera que as estruturas nacionais existentes que estão já a funcionar de forma eficaz e dão resposta às necessidades e aos requisitos constitucionais dos Estados-Membros não devem ser perturbadas. Contudo, crê que, de modo a garantir o intercâmbio de informações a nível da União, a notificação de alertas precoces de ameaças e a participação na rede de cooperação de uma forma eficaz, cada Estado-Membro tem de designar um **Balcão Único**.

No mesmo espírito de maximização da eficácia da diretiva proposta, a relatora considera que as medidas propostas relativamente à criação de uma **equipa de resposta a emergências informáticas (CERT)** nacional poderão não ser o requisito mais adequado, na medida em que estas não têm em conta as diferentes naturezas e composições das CERT existentes. Além de a maioria dos Estados-Membros não possuir mais do que uma CERT, estes também lidam

com diferentes tipos de incidentes. A quantidade e a qualidade de atividades também diferem, consoante sejam alojadas ou exploradas por instituições académicas ou de investigação, governos ou pelo setor privado. Além disso, a presente proposta perturbaria as redes de cooperação internacionais e europeias existentes, às quais as CERT atuais já pertencem e que provaram ser eficientes na coordenação de respostas internacionais e europeias a incidentes. Consequentemente, a relatora considera que, em vez de se referir a uma única CERT nacional, a diretiva deve visar todas as CERT que prestam serviços aos setores constantes do anexo II, permitindo assim que, por exemplo, uma CERT preste serviços a todos os setores do anexo II e que várias CERT prestem serviços ao mesmo setor. No entanto, a relatora defende que os Estados-Membros devem garantir que as suas CERT estão plena e permanentemente operacionais e que possuem recursos técnicos, financeiros e humanos suficientes para funcionarem adequadamente e participarem em redes de cooperação internacionais e comunitárias.

Além disso, o princípio da eficiência requer que sejam efetuadas alterações à diretiva proposta no que se refere ao **âmbito de aplicação**. Embora a relatora concorde que seja necessário um alargamento das obrigações do sistema de comunicação aos setores da energia, transportes, saúde e financeiros, a proposta de alargar as medidas obrigatórias previstas no capítulo IV a todos os operadores do mercado na «economia da Internet» é desproporcionada e impraticável. É desproporcionada porque a imposição indiscriminada de novas obrigações a uma categoria aberta e não definida, designadamente todos os «fornecedores de serviços da sociedade de informação que permitem a prestação de outros serviços da sociedade da informação» é incompreensível e não está devidamente justificada quanto a possíveis danos provocados por um incidente de segurança, bem como tem potencial para acrescentar mais burocracia ao nosso setor industrial, nomeadamente às PME. É impraticável na medida em que existem sérias dúvidas de que as autoridades competentes sejam capazes de lidar com todas as potenciais notificações de uma forma proativa que incentive um diálogo bidirecional com os operadores do mercado, a fim de resolver a ameaça à segurança.

Relativamente às **administrações públicas**, a diretiva deve equilibrar a necessidade de maior desenvolvimento de serviços da administração pública em linha com as obrigações de diligência já existentes nas administrações públicas em matéria de gestão e de proteção das suas redes e dos seus sistemas informáticos. Consequentemente, a relatora considera que, embora os requisitos de intercâmbio de informações estabelecidos no artigo 14.º devam aplicar-se plenamente às administrações públicas, estas não devem estar sujeitas às obrigações previstas no artigo 15.º.

Segundo princípio - Confiança

A relatora considera que uma grande parte do sucesso da diretiva consiste na sua capacidade para incentivar a participação dos operadores do mercado, conduzindo à criação de um ambiente de SRI fiável, no qual os que se encontram no terreno estão dispostos a participar proativamente. Se não conseguir alcançar este objetivo, falhará. A este respeito, a relatora propõe que se garanta que a participação e notificação dos operadores do mercado não sofram um impacto negativo decorrente de publicações desnecessárias de incidentes de segurança por eles notificados ou que possam ser responsabilizados por perdas de informação por parte das autoridades competentes ou de balcões únicos. Além disso, deve ser encetado um diálogo

bidirecional entre operadores e autoridades competentes, bem como incentivada a participação dos operadores do mercado em todos os fóruns, incluindo na rede de cooperação.

A relatora considera ainda que a confiança deve ser o pilar da participação das autoridades competentes e/ou dos balcões únicos, nomeadamente em relação ao intercâmbio de informações. Por forma a garantir isso mesmo, as disposições relativas aos requisitos de confidencialidade e segurança da rede devem estar refletidas na diretiva.

ALTERAÇÕES

A Comissão da Indústria, da Investigação e da Energia insta a Comissão do Mercado Interno e da Proteção dos Consumidores, competente quanto à matéria de fundo, a incorporar as seguintes alterações no seu relatório:

Alteração 1

Proposta de diretiva
Considerando 1

Texto da Comissão	*Alteração*
(1) As redes e os sistemas e serviços informáticos desempenham um papel vital na sociedade. A sua fiabilidade e segurança são essenciais para as atividades económicas e o bem-estar social e, em especial, para o funcionamento do mercado interno.	(1) As redes e os sistemas e serviços informáticos desempenham um papel vital na sociedade. A sua fiabilidade e segurança são essenciais para ***a liberdade e a segurança geral dos cidadãos da UE, bem como para*** as atividades económicas e o bem-estar social e, em especial, para o funcionamento do mercado interno.

Alteração 2

Proposta de diretiva
Considerando 2

Texto da Comissão	*Alteração*
(2) A amplitude ***e*** a frequência de incidentes de segurança ***deliberados ou acidentais*** está a aumentar e constitui uma importante ameaça para o funcionamento das redes e dos sistemas informáticos. Esses incidentes podem impedir o exercício das atividades económicas, gerar perdas financeiras importantes, minar a	(2) A amplitude***,*** a frequência ***e o impacto*** de incidentes de segurança está a aumentar e constitui uma importante ameaça para o funcionamento das redes e dos sistemas informáticos. ***Estes sistemas podem, igualmente, tornar-se um alvo fácil de ações prejudiciais deliberadas, destinadas a danificar ou a interromper a operação***

confiança dos utilizadores e causar graves prejuízos à economia da União.	***dos sistemas.*** Esses incidentes podem ***ameaçar a saúde e a segurança da população,*** impedir o exercício das atividades económicas, gerar perdas financeiras importantes, minar a confiança dos utilizadores ***e investidores*** e causar graves prejuízos à economia da União.

Justificação

Os ataques cibernéticos a empresas cotadas em bolsa são generalizados e incluem o roubo de ativos financeiros, de propriedade intelectual ou a perturbação das operações dos seus clientes ou parceiros comerciais e podem ter impacto nas relações dos acionistas, bem como nas decisões de potenciais investidores.

Alteração 3

Proposta de diretiva
Considerando 3

Texto da Comissão	*Alteração*
(3) Enquanto instrumentos de comunicação sem fronteiras, os sistemas de informação digitais, e essencialmente a Internet, desempenham um papel crucial na facilitação da circulação transfronteiras de mercadorias, serviços e pessoas. Devido a essa natureza transnacional, as perturbações significativas desses sistemas num Estado-Membro podem igualmente afetar outros Estados-Membros e a União no seu conjunto. Por consequência, a resiliência e a estabilidade das redes e dos sistemas informáticos é essencial para o bom funcionamento do mercado interno.	(3) Enquanto instrumentos de comunicação sem fronteiras ***tradicionais***, os sistemas de informação digitais, e essencialmente a Internet, desempenham um papel crucial na facilitação da circulação transfronteiras de mercadorias, serviços***, ideias*** e pessoas. Devido a essa natureza transnacional, as perturbações significativas desses sistemas num Estado-Membro podem igualmente afetar outros Estados-Membros e a União no seu conjunto. Por consequência, a resiliência e a estabilidade das redes e dos sistemas informáticos é essencial para o bom funcionamento do mercado interno ***e, além disso, também para o funcionamento dos mercados externos***.

Justificação

A resiliência e a estabilidade das redes e dos sistemas informáticos do mercado interno são também fundamentais para a interação com os mercados mundiais e regionais, tais como a América do Norte e a Ásia, entre outros.

Alteração 4

Proposta de diretiva
Considerando 4

Texto da Comissão	*Alteração*
(4) Deverá ser estabelecido um mecanismo de cooperação a nível da União, a fim de permitir o intercâmbio de informações e a deteção e resposta coordenadas a ameaças à segurança das redes e da informação («SRI»). Para que esse mecanismo seja eficaz e inclusivo, é indispensável que todos os Estados-Membros tenham um mínimo de capacidades e uma estratégia que garanta um elevado nível de SRI no seu território. Deverão também aplicar-se requisitos mínimos de segurança ***às administrações públicas e*** aos operadores das infraestruturas ***críticas*** de informação, a fim de promover uma cultura de gestão dos riscos e assegurar a comunicação dos incidentes mais graves.	(4) Deverá ser estabelecido um mecanismo de cooperação a nível da União, a fim de permitir o intercâmbio de informações e a ***prevenção,*** deteção e resposta coordenadas a ameaças à segurança das redes e da informação («SRI»). Para que esse mecanismo seja eficaz e inclusivo, é indispensável que todos os Estados-Membros tenham um mínimo de capacidades e uma estratégia que garanta um elevado nível de SRI no seu território. Deverão também aplicar-se requisitos mínimos de segurança aos operadores ***públicos e privados*** das infraestruturas de ***informação e às empresas cotadas em bolsa***, a fim de promover uma cultura de gestão dos riscos e assegurar a comunicação dos incidentes mais graves. ***O quadro jurídico deve basear-se na necessidade de salvaguardar a privacidade e a integridade dos cidadãos. A Rede de Alerta para as Infraestruturas Críticas (RAIC) deve ser alargada a estes operadores em particular.***

Justificação

As violações da segurança de empresas cotadas em bolsa podem afetar materialmente os produtos da empresa, os seus serviços, as relações com os clientes e fornecedores e as condições de concorrência em geral, tendo, portanto, um grande impacto no funcionamento do mercado interno (e externo). Por conseguinte, as empresas cotadas em bolsa devem ser também abrangidas pela presente diretiva.

Alteração 5

Proposta de diretiva
Considerando 4-A (novo)

Texto da Comissão	*Alteração*
	(4-A) A presente diretiva deve centrar-se nas infraestruturas críticas, fundamentais para a manutenção das atividades económicas e societais essenciais nos domínios da energia, dos transportes, da banca, das infraestruturas dos mercados financeiros e da saúde.

Alteração 6

Proposta de diretiva
Considerando 4-B (novo)

Texto da Comissão	*Alteração*
	(4-B) Por forma a assegurar que os governos não excedam nem abusem do seu poder, é fundamental que os sistemas de informação e segurança das autoridades públicas sejam transparentes, legítimos, bem definidos e adotados de modo transparente através de um processo democrático.

Alteração 7

Proposta de diretiva
Considerando 6

Texto da Comissão	*Alteração*
(6) As capacidades existentes não são suficientes para garantir um elevado nível de segurança das redes e da informação na União. Os Estados-Membros possuem níveis muito diversos de preparação que conduzem a abordagens fragmentadas em toda a União. Esta situação conduziria a um nível desigual de defesa dos consumidores e das empresas e compromete o nível global de SRI na	(6) As capacidades existentes não são suficientes para garantir um elevado nível de segurança das redes e da informação na União. Os Estados-Membros possuem níveis muito diversos de preparação que conduzem a abordagens fragmentadas em toda a União. Esta situação conduziria a um nível desigual de defesa dos consumidores e das empresas e compromete o nível global de SRI na

União. Por sua vez, a inexistência de requisitos mínimos comuns a respeitar ***pelas administrações públicas e*** pelos operadores do mercado torna impossível criar um mecanismo eficaz e global para a cooperação a nível da União.	União. Por sua vez, a inexistência de requisitos mínimos comuns a respeitar pelos operadores do mercado torna impossível criar um mecanismo eficaz e global para a cooperação a nível da União***, prejudicando ainda a eficácia da cooperação internacional e, consequentemente, a luta contra os desafios colocados à segurança a nível mundial, e põe em causa a posição internacional de liderança da União no domínio da garantia e promoção de uma Internet livre, eficiente e segura***.

Alteração 8

Proposta de diretiva
Considerando 7

Texto da Comissão	*Alteração*
(7) Uma resposta eficaz aos desafios que se colocam à segurança das redes e dos sistemas informáticos exige, assim, uma abordagem global a nível da União, que abranja os requisitos mínimos comuns de desenvolvimento de capacidades e de planificação, o intercâmbio de informações e a coordenação de ações, bem como requisitos mínimos comuns de segurança ***para todos os operadores do mercado em causa e as administrações públicas***.	(7) Uma resposta eficaz aos desafios que se colocam à segurança das redes e dos sistemas informáticos exige, assim, uma abordagem global a nível da União, que abranja os requisitos mínimos comuns de desenvolvimento de capacidades e de planificação, ***desenvolvimento de aptidões de cibersegurança suficientes,*** o intercâmbio de informações e a coordenação de ações, bem como requisitos mínimos comuns de segurança para todos os operadores do mercado em causa e as administrações públicas. ***As normas comuns mínimas devem ser aplicadas de acordo com as recomendações adequadas dos Grupos de Coordenação da Cibersegurança.***

Alteração 9

Proposta de diretiva
Considerando 9

Texto da Comissão	*Alteração*
(9) A fim de atingir e manter um nível elevado comum de segurança das redes e dos sistemas informáticos, cada Estado-Membro deve dispor de uma estratégia nacional de SRI que defina os objetivos estratégicos e as ações estratégicas concretas a executar. É necessário desenvolver planos de cooperação SRI a nível nacional que cumpram os requisitos essenciais, a fim de alcançar níveis de capacidade de resposta que permitam uma cooperação eficaz e eficiente a nível nacional e da União em caso de ocorrência de incidentes.	(9) A fim de atingir e manter um nível elevado comum de segurança das redes e dos sistemas informáticos, cada Estado-Membro deve dispor de uma estratégia nacional de SRI que defina os objetivos estratégicos e as ações estratégicas concretas a executar. É necessário desenvolver planos de cooperação SRI a nível nacional que cumpram os requisitos essenciais, ***com base nos requisitos mínimos definidos na presente diretiva,*** a fim de alcançar níveis de capacidade de resposta que permitam uma cooperação eficaz e eficiente a nível nacional e da União em caso de ocorrência de incidentes. ***Cada Estado-Membro deve, por conseguinte, ser obrigado a respeitar as normas comuns relativas ao formato dos dados e à intermutabilidade dos dados a partilhar e avaliar. Os Estados-Membros podem solicitar a assistência da Agência Europeia para a Segurança das Redes e da Informação («ENISA») ao elaborarem as suas estratégias nacionais em matéria de SRI, baseadas num plano mínimo comum de estratégia em matéria de SRI.***

Justificação

A ENISA já é reconhecida pelas partes interessadas relevantes como um centro de excelência altamente competente e um instrumento fiável para a promoção da cibersegurança na UE. Por conseguinte, a UE deve evitar a duplicação de esforços e estruturas, baseando-se nos conhecimentos da ENISA, e deve solicitar à ENISA que ofereça serviços de aconselhamento aos Estados-Membros com falta de instituições SRI e experiência e que solicitem este tipo de apoio.

Alteração 10

Proposta de diretiva
Considerando 10

Texto da Comissão	*Alteração*
(10) Para permitir a aplicação eficaz das disposições adotadas ao abrigo da presente diretiva, em cada Estado-Membro deverá ser criada ou designada uma entidade responsável pela coordenação das questões da SRI e que sirva de ponto focal para a cooperação transfronteiras a nível da União. Estas entidades deverão dispor de recursos técnicos, financeiros e humanos adequados para garantir a realização eficaz e eficiente das tarefas que lhes sejam atribuídas e assim alcançar os objetivos da presente diretiva.	(10) Para permitir a aplicação eficaz das disposições adotadas ao abrigo da presente diretiva, em cada Estado-Membro deverá ser criada ou designada uma entidade responsável pela coordenação das questões da SRI e que sirva de ponto focal ***único tanto para a coordenação interna como*** para a cooperação transfronteiras a nível da União. ***Estes balcões únicos nacionais devem ser designados sem prejudicar a capacidade de cada Estado-Membro de designar mais de uma autoridade nacional competente, responsável pela segurança da informação da rede, de acordo com os seus requisitos constitucionais, jurisdicionais ou administrativos, devendo, no entanto, ser-lhes atribuído um mandato de coordenação a nível nacional e da União.*** Estas entidades deverão dispor de recursos técnicos, financeiros e humanos adequados para garantir a realização ***contínua,*** eficaz e eficiente das tarefas que lhes sejam atribuídas e assim alcançar os objetivos da presente diretiva.

Alteração 11

Proposta de diretiva
Considerando 10-A (novo)

Texto da Comissão	*Alteração*
	Tendo em conta as diferenças nas estruturas de governação nacionais e a fim de salvaguardar os acordos setoriais já existentes e evitar duplicações, os Estados-Membros devem poder designar mais do que uma autoridade nacional competente, responsável pelo cumprimento das funções associadas à segurança das redes e dos sistemas informáticos dos operadores de mercado, nos termos da presente diretiva. No

entanto, para garantir a boa cooperação e a comunicação transfronteiras, é necessário que cada Estado-Membro designe apenas um balcão único, responsável pela cooperação transfronteiras a nível da União. Caso a estrutura constitucional ou outros acordos assim o exijam, um Estado-Membro deve poder designar apenas uma autoridade para desempenhar as funções da autoridade competente e do balcão único.

Alteração 12

Proposta de diretiva
Considerando 11

Texto da Comissão	*Alteração*
(11) Todos os Estados-Membros deverão estar equipados adequadamente, em termos de capacidades técnicas e organizacionais, para impedir, detetar, reagir e reduzir os incidentes e riscos ligados às redes e aos sistemas informáticos. Por conseguinte, devem ser instituídas em todos os Estados-Membros equipas de resposta a emergências informáticas que cumpram as condições essenciais para assegurar capacidades reais e compatíveis para lidar com os incidentes e riscos e garantir uma cooperação eficaz a nível da União.	(11) Todos os Estados-Membros ***e operadores do mercado*** deverão estar equipados adequadamente, em termos de capacidades técnicas e organizacionais, para impedir, detetar, reagir e reduzir***, em qualquer momento,*** os incidentes e riscos ligados às redes e aos sistemas informáticos. ***Os sistemas de segurança das administrações públicas devem ser seguros e objeto de controlo e análise democráticos. O equipamento e as capacidades habitualmente exigidos devem cumprir as normas técnicas aprovadas em comum, bem como os Procedimentos Operativos Normalizados (PON).*** Por conseguinte, devem ser instituídas em todos os Estados-Membros equipas de resposta a emergências informáticas ***(CERT)*** que cumpram as condições essenciais para assegurar capacidades reais e compatíveis para lidar com os incidentes e riscos e garantir uma cooperação eficaz a nível da União. ***Estas CERT devem poder interagir com base nas normas técnicas comuns e nos PON. Tendo em conta as diferentes***

	características das CERT existentes, que respondem a diferentes intervenientes e necessidades que esta matéria exige, os Estados-Membros devem garantir que cada um dos setores abrangidos pelo anexo II usufrui dos serviços de, pelo menos, uma CERT. Relativamente à cooperação transfronteiras das CERT, os Estados-Membros devem assegurar que estas possuem meios suficientes para participarem nas redes de cooperação internacionais e europeias existentes já em funcionamento.

Justificação

A interoperabilidade deve ser assegurada.

Alteração 13

Proposta de diretiva
Considerando 12

Texto da Comissão	*Alteração*
(12) Aproveitando os progressos significativos realizados no âmbito do Fórum Europeu dos Estados-Membros (***FEEM***) para promover debates e intercâmbios de boas práticas políticas, incluindo a definição de princípios de cooperação informática europeia em situação de crise, os Estados-Membros e a Comissão deverão formar uma rede para se manterem em comunicação permanente e apoiar a sua cooperação. Este mecanismo de cooperação seguro e eficaz deverá permitir que o intercâmbio de informações, a deteção e a resposta sejam estruturados e coordenados a nível da União.	(12) Aproveitando os progressos significativos realizados no âmbito do Fórum Europeu dos Estados-Membros ***(«FEEM»)***para promover debates e intercâmbios de boas práticas políticas, incluindo a definição de princípios de cooperação informática europeia em situação de crise, os Estados-Membros e a Comissão deverão formar uma rede para se manterem em comunicação permanente e apoiar a sua cooperação. Este mecanismo de cooperação seguro e eficaz***, no qual está assegurada a participação dos operadores do mercado,*** deverá permitir que o intercâmbio de informações, a deteção e a resposta sejam estruturados e coordenados a nível da União.

Alteração 14

Proposta de diretiva
Considerando 13

Texto da Comissão	*Alteração*
(13) A Agência Europeia para a Segurança das Redes e da Informação («ENISA») deverá assistir os Estados-Membros e a Comissão através da oferta das suas competências especializadas e aconselhamento e da facilitação do intercâmbio de boas práticas. Em particular, na aplicação da presente diretiva, a Comissão ***deverá*** consultar a ENISA. A fim de garantir a informação eficaz e atempada dos Estados-Membros e da Comissão, os alertas rápidos sobre os incidentes e riscos devem ser notificados à rede de cooperação. Para que os Estados-Membros possam adquirir conhecimentos, a rede de cooperação deverá também servir de instrumento para o intercâmbio de boas práticas, ajudando os seus membros a reforçar as suas capacidades e orientando a organização de avaliações interpares e dos exercícios de SRI.	(13) A Agência Europeia para a Segurança das Redes e da Informação («ENISA») deverá assistir os Estados-Membros e a Comissão através da oferta das suas competências especializadas e aconselhamento e da facilitação do intercâmbio de boas práticas. Em particular, na aplicação da presente diretiva, a Comissão ***e os Estados-Membros deverão*** consultar a ENISA. A fim de garantir a informação eficaz e atempada dos Estados-Membros e da Comissão, os alertas rápidos sobre os incidentes e riscos devem ser notificados à rede de cooperação. Para que os Estados-Membros possam adquirir conhecimentos, a rede de cooperação deverá também servir de instrumento para o intercâmbio de boas práticas, ajudando os seus membros a reforçar as suas capacidades e orientando a organização de avaliações interpares e dos exercícios de SRI.

Alteração 15

Proposta de diretiva
Considerando 14

Texto da Comissão	*Alteração*
(14) Dever-se-á estabelecer uma infraestrutura de partilha de informações segura que permita o intercâmbio de informações sensíveis e confidenciais no âmbito da rede de cooperação. Sem prejuízo da sua obrigação de notificar incidentes e riscos de dimensão europeia à rede de cooperação, o acesso às informações confidenciais de outros	(14) Dever-se-á estabelecer***, sob supervisão da ENISA,*** uma infraestrutura de partilha de informações segura que permita o intercâmbio de informações sensíveis e confidenciais no âmbito da rede de cooperação. Sem prejuízo da sua obrigação de notificar incidentes e riscos de dimensão europeia à rede de cooperação, o acesso às informações

Estados-Membros só deve ser concedido aos Estados-Membros que demonstrem que os seus recursos e processos técnicos, financeiros e humanos, bem como a sua infraestrutura de comunicação, asseguram uma participação na rede eficaz, eficiente e segura.	confidenciais de outros Estados-Membros só deve ser concedido aos Estados-Membros que demonstrem que os seus recursos e processos técnicos, financeiros e humanos, bem como a sua infraestrutura de comunicação, asseguram uma participação na rede eficaz, eficiente e segura. ***Para que a rede de cooperação consiga cumprir a sua missão com eficácia, a Comissão deve criar para esta uma rubrica orçamental.***

Alteração 16

Proposta de diretiva
Considerando 14-A (novo)

Texto da Comissão	*Alteração*
	(14-A) Quando adequado, os operadores do mercado podem igualmente ser convidados a participar nas atividades da rede de cooperação.

Alteração 17

Proposta de diretiva
Considerando 15

Texto da Comissão	*Alteração*
(15) Uma vez que a maioria das redes e dos sistemas informáticos é explorada pelo setor privado, a cooperação entre este setor e o setor público é essencial. Os operadores do mercado deverão ser encorajados a prosseguir os seus próprios mecanismos de cooperação informal para garantir a segurança das redes e da informação. Deverão também cooperar com o setor público e partilhar informações e boas práticas ***em*** troca de apoio operacional em caso de incidentes.	(15) Uma vez que a maioria das redes e dos sistemas informáticos é explorada pelo setor privado, a cooperação entre este setor e o setor público é essencial. Os operadores do mercado deverão ser encorajados a prosseguir os seus próprios mecanismos de cooperação informal para garantir a segurança das redes e da informação. Deverão também cooperar com o setor público e partilhar ***mutuamente*** informações e boas práticas***, incluindo a*** troca ***recíproca de informações relevantes e*** de apoio operacional em caso de incidentes. ***Por forma a incentivar de modo eficaz a partilha de informação e***

	boas práticas, é fundamental assegurar que os operadores do mercado, que participam nos referidos intercâmbios, não ficam em desvantagem devido à sua cooperação. São necessárias garantias adequadas para assegurar que tal cooperação não expõe estes operadores a um maior risco de incumprimento ou a novas responsabilidades no âmbito, inter alia, da concorrência, propriedade intelectual, proteção dos dados ou legislação em matéria de cibercriminalidade, nem os expõe a maiores riscos operacionais ou de segurança.

Alteração 18

Proposta de diretiva
Considerando 16

Texto da Comissão	*Alteração*
(16) Para garantir a transparência e informar devidamente os cidadãos e os operadores do mercado da UE, ***as autoridades competentes*** deverão criar um sítio Web comum para publicar informações não confidenciais sobre os incidentes ***e*** riscos.	(16) Para garantir a transparência e informar devidamente os cidadãos e os operadores do mercado da UE, ***os balcões únicos*** deverão criar um sítio Web comum ***à escala da União*** para publicar informações não confidenciais sobre os incidentes***,*** riscos ***e medidas para atenuar os riscos, e para eventualmente aconselhar sobre as medidas de manutenção adequadas***.

Alteração 19

Proposta de diretiva
Considerando 17

Texto da Comissão	*Alteração*
(17) Caso as informações sejam consideradas confidenciais em	(17) ***A política de classificação da informação, mencionada no considerando***

conformidade com as regras nacionais e da União em matéria de sigilo comercial, essa confidencialidade deve ser assegurada no exercício das atividades e no cumprimento dos objetivos estabelecidos pela presente diretiva.	***14, deve seguir o protocolo relativo a sinalização luminosa para a partilha de informação recomendado pela ENISA. Qualquer informação partilhada deve ser classificada e tratada de acordo com o seu nível de sensibilidade, como determinado pela fonte da informação.*** Caso as informações sejam consideradas confidenciais em conformidade com as regras nacionais e da União em matéria de sigilo comercial, essa confidencialidade deve ser assegurada no exercício das atividades e no cumprimento dos objetivos estabelecidos pela presente diretiva.

Alteração 20

Proposta de diretiva
Considerando 18

Texto da Comissão	*Alteração*
(18) Com base, nomeadamente, nas experiências nacionais de gestão de crises e em cooperação com a ENISA, a Comissão e os Estados-Membros deverão elaborar um plano de cooperação da União em matéria de SRI que defina mecanismos de cooperação para fazer face aos riscos e incidentes. Esse plano deverá ser devidamente tido em conta no desencadear de alertas rápidos no âmbito da rede de cooperação.	(18) Com base, nomeadamente, nas experiências nacionais de gestão de crises e em cooperação com a ENISA, a Comissão e os Estados-Membros deverão elaborar um plano de cooperação da União em matéria de SRI que defina mecanismos de cooperação***, boas práticas e padrões operacionais para evitar, detetar, relatar e*** fazer face aos riscos e incidentes. Esse plano deverá ser devidamente tido em conta no desencadear de alertas rápidos no âmbito da rede de cooperação.

Alteração 21

Proposta de diretiva
Considerando 19

Texto da Comissão	*Alteração*
(19) A notificação de um alerta precoce na rede deverá ser exigida apenas quando a escala e a gravidade do incidente ou do	(19) A notificação de um alerta precoce na rede deverá ser exigida apenas quando a escala e a gravidade do incidente ou do

risco em causa forem ou puderem vir a ser de tal modo significativas que sejam necessárias informações ou a coordenação da resposta a nível da União. Os alertas precoces devem, por conseguinte, limitar-se aos incidentes ou riscos ***reais ou potenciais*** que ganhem rapidamente dimensão, excedam a capacidade de resposta nacional ou afetem mais de um Estado-Membro. A fim de permitir uma avaliação adequada, todas as informações relevantes para a avaliação dos riscos ou incidentes deverão ser comunicadas à rede de cooperação.	risco em causa forem ou puderem vir a ser de tal modo significativas que sejam necessárias informações ou a coordenação da resposta a nível da União. Os alertas precoces devem, por conseguinte, limitar-se aos incidentes ou riscos que ganhem rapidamente dimensão, excedam a capacidade de resposta nacional ou afetem mais de um Estado-Membro. A fim de permitir uma avaliação adequada, todas as informações relevantes para a avaliação dos riscos ou incidentes deverão ser comunicadas à rede de cooperação.

Alteração 22

Proposta de diretiva
Considerando 20

Texto da Comissão	*Alteração*
(20) Após receção de um alerta precoce e sua avaliação, ***as autoridades competentes*** devem chegar a acordo quanto a uma resposta coordenada no âmbito do plano de cooperação da União em matéria de SRI. ***As autoridades competentes***, bem como a Comissão, deverão ser informadas das medidas adotadas a nível nacional em resultado da resposta coordenada.	(20) Após receção de um alerta precoce e sua avaliação, ***os balcões únicos*** devem chegar a acordo quanto a uma resposta coordenada no âmbito do plano de cooperação da União em matéria de SRI. ***Os balcões únicos, a ENISA,*** bem como a Comissão, deverão ser informados das medidas adotadas a nível nacional em resultado da resposta coordenada.

Alteração 23

Proposta de diretiva
Considerando 22

Texto da Comissão	*Alteração*
(22) As responsabilidades na garantia da SRI incumbem, em grande medida, às administrações públicas e aos operadores do mercado. Dever-se-á promover e	(22) As responsabilidades na garantia da SRI incumbem, em grande medida, às administrações públicas e aos operadores do mercado. Dever-se-á promover e

desenvolver uma cultura de gestão dos riscos, que abranja a avaliação dos riscos e a implementação de medidas de segurança adequadas aos riscos enfrentados através de requisitos regulamentares adequados e práticas setoriais voluntárias. Estabelecer condições de concorrência equitativas é também essencial para um funcionamento eficaz da rede de cooperação tendo em vista assegurar a eficácia da cooperação entre todos os Estados-Membros.

desenvolver uma cultura de gestão dos riscos***, cooperação estreita e confiança***, que abranja a avaliação dos riscos e a implementação de medidas de segurança adequadas aos riscos enfrentados através de requisitos regulamentares adequados e práticas setoriais voluntárias. Estabelecer condições de concorrência equitativas ***fiáveis*** é também essencial para um funcionamento eficaz da rede de cooperação tendo em vista assegurar a eficácia da cooperação entre todos os Estados-Membros.

Alteração 24

Proposta de diretiva
Considerando 24

Texto da Comissão	*Alteração*
(24) Essas obrigações não devem cingir-se ao setor das comunicações eletrónicas, mas ser extensíveis aos principais prestadores de serviços da sociedade da informação, tal como definidos na Diretiva 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[27], que estão na base dos serviços da sociedade da informação ou das atividades em linha, como as plataformas de comércio eletrónico, portais de pagamento Internet, redes sociais, motores de pesquisa, serviços de computação em nuvem, lojas de aplicações em linha***. A perturbação destes serviços da sociedade da informação horizontais impede a prestação de outros serviços deste setor que neles se baseiam. Os responsáveis pelo desenvolvimento de software e os fabricantes de hardware não são prestadores de serviços da sociedade da informação, pelo que são excluídos.***	(24) Essas obrigações não devem cingir-se ao setor das comunicações eletrónicas, mas ser extensíveis aos ***operadores das infraestruturas que dependem em larga medida das tecnologias da informação e da comunicação e são essenciais para a manutenção de funções económicas ou sociais essenciais como a eletricidade e o gás, os transportes, as instituições de crédito, as infraestruturas dos mercados financeiros e a saúde. A perturbação dessas redes e sistemas informáticos afetaria o mercado interno. Embora as obrigações previstas na presente diretiva não sejam extensíveis aos*** principais prestadores de serviços da sociedade da informação, tal como definidos na Diretiva 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[27], que estão na base dos serviços da sociedade da informação ou das atividades em linha,

Essas obrigações deverão ser também alargadas às administrações públicas e aos operadores das infraestruturas críticas que dependem em larga medida das tecnologias da informação e da comunicação e são essenciais para a manutenção de funções económicas ou sociais vitais como a eletricidade e o gás, os transportes, as instituições de crédito, a bolsa e a saúde. A perturbação dessas redes e sistemas informáticos afetaria o mercado interno.	como as plataformas de comércio eletrónico, portais de pagamento Internet, redes sociais, motores de pesquisa, serviços de computação em nuvem ***em geral ou*** lojas de aplicações em linha***, estas podem, voluntariamente, informar a autoridade competente ou o balcão único dos incidentes relacionados com a segurança da rede que considerem adequados, devendo a autoridade competente ou o balcão único, se razoavelmente possível, apresentar aos operadores do mercado que informaram acerca do incidente informações analisadas estrategicamente que ajudarão a resolver a ameaça à segurança***.
[27] JO L 204 de 21.7.1998, p. 37.	[27] JO L 204 de 21.7.1998, p. 37.

Alteração 25

Proposta de diretiva
Considerando 25

Texto da Comissão	*Alteração*
(25) As medidas técnicas e organizacionais impostas às administrações públicas e aos operadores do mercado não deverão exigir que um determinado produto das tecnologias da informação e da comunicação para fins comerciais seja concebido, desenvolvido ou fabricado de um modo específico.	(25) As medidas técnicas e organizacionais impostas aos operadores do mercado não deverão exigir que um determinado produto das tecnologias da informação e da comunicação para fins comerciais seja concebido, desenvolvido ou fabricado de um modo específico. ***Por outro lado, deve exigir-se a utilização de normas internacionais relativas à cibersegurança.***

Alteração 26

Proposta de diretiva
Considerando 28

Texto da Comissão	*Alteração*
(28) As autoridades competentes deverão esforçar-se por manter canais informais e de confiança para a partilha de informações entre os operadores do mercado e entre o setor público e o setor privado. Deverá existir um justo equilíbrio entre a publicidade dada aos incidentes comunicados às autoridades competentes e o interesse do público em ser informado acerca das ameaças que comportem eventuais danos comerciais e de reputação para ***as administrações públicas e*** os operadores do mercado que comunicam esses incidentes. No cumprimento das obrigações de notificação, as autoridades competentes deverão ter em especial atenção a necessidade de manter as informações sobre as vulnerabilidades dos produtos estritamente confidenciais antes da ***divulgação*** das medidas de segurança adequadas para as resolver.	(28) As autoridades competentes ***e os balcões únicos*** deverão esforçar-se por manter canais informais e de confiança para a partilha de informações entre os operadores do mercado e entre o setor público e o setor privado. ***As vulnerabilidades e os incidentes anteriormente desconhecidos, comunicados às autoridades competentes, devem ser notificados aos fabricantes e prestadores de serviços dos produtos e serviços de TIC afetados.*** Deverá existir um justo equilíbrio entre a publicidade dada aos incidentes comunicados às autoridades competentes ***e aos balcões únicos*** e o interesse do público em ser informado acerca das ameaças que comportem eventuais danos comerciais e de reputação para os operadores do mercado que comunicam esses incidentes. ***De modo a salvaguardar a confiança e a eficiência, os incidentes só devem ser tornados públicos após consulta àqueles que comunicaram o incidente e apenas quando estritamente necessário para atingir os objetivos da presente diretiva.*** No cumprimento das obrigações de notificação, as autoridades competentes ***e os balcões únicos*** deverão ter em especial atenção a necessidade de manter as informações sobre as vulnerabilidades dos produtos estritamente confidenciais antes da ***execução*** das medidas de segurança adequadas para as resolver***, embora não devam atrasar a notificação mais do que o exigido***. ***Por norma, os balcões únicos não devem divulgar dados pessoais de indivíduos envolvidos em incidentes. Os balcões únicos apenas devem divulgar dados pessoais caso a divulgação destes seja necessária e proporcional ao objetivo visado.***

Justificação

Caso as autoridades tenham conhecimento de vulnerabilidades de determinados produtos ou serviços de TIC, devem notificar os fabricantes e os prestadores de serviços a fim de permitir que estes adaptem os seus produtos e serviços em tempo útil.

Alteração 27

Proposta de diretiva
Considerando 29

Texto da Comissão	*Alteração*
(29) As autoridades competentes devem ser ***dotadas*** dos meios necessários para desempenharem as suas funções, incluindo o poder de obter informações suficientes dos operadores do mercado e das administrações públicas com o objetivo de avaliarem o nível de segurança das redes e dos sistemas informáticos, bem como dados completos e fiáveis sobre eventuais incidentes que tenham tido impacto no seu funcionamento.	(29) As autoridades competentes ***e os balcões únicos*** devem ser ***dotados*** dos meios necessários para desempenharem as suas funções, incluindo o poder de obter informações suficientes dos operadores do mercado com o objetivo de avaliarem o nível de segurança das redes e dos sistemas informáticos, ***medirem o número, a escala e o âmbito dos incidentes,*** bem como dados completos e fiáveis sobre eventuais incidentes que tenham tido impacto no seu funcionamento.

Alteração 28

Proposta de diretiva
Considerando 30

Texto da Comissão	*Alteração*
(30) Em muitos casos, o incidente é causado por atividades criminosas. É possível suspeitar da origem criminosa de um incidente mesmo que não existam provas suficientemente claras desde o início. Neste contexto, a cooperação adequada entre as autoridades competentes e as autoridades policiais e judiciais deverá inscrever-se numa resposta global e eficaz à ameaça de incidentes no domínio da segurança. Em especial, a promoção de um	(30) Em muitos casos, o incidente é causado por atividades criminosas ***ou de guerra cibernética***. É possível suspeitar da origem criminosa de um incidente mesmo que não existam provas suficientemente claras desde o início. Neste contexto, a cooperação adequada entre as autoridades competentes***, os balcões únicos*** e as autoridades policiais e judiciais***, bem como a cooperação com o EC3 (Centro Europeu de Cibercriminalidade na***

ambiente seguro, protegido e mais resiliente requer a notificação sistemática dos incidentes que se suspeite terem uma origem criminosa grave às autoridades responsáveis. O caráter de crime grave atribuído aos incidentes deverá ser avaliado à luz da legislação da UE sobre a cibercriminalidade.

Europol) e a ENISA, deverá inscrever-se numa resposta global e eficaz à ameaça de incidentes no domínio da segurança. Em especial, a promoção de um ambiente seguro, protegido e mais resiliente requer a notificação sistemática dos incidentes que se suspeite terem uma origem criminosa grave às autoridades responsáveis. O caráter de crime grave atribuído aos incidentes deverá ser avaliado à luz da legislação da UE sobre a cibercriminalidade.

Alteração 29

Proposta de diretiva
Considerando 31

Texto da Comissão	*Alteração*
(31) Os dados pessoais ficam em muitos casos comprometidos em consequência de incidentes. Neste contexto, as autoridades competentes e as autoridades encarregadas da proteção de dados devem cooperar e trocar informações sobre todas as questões pertinentes para combater as violações de dados pessoais resultantes de incidentes. ***Os Estados-Membros cumprirão*** a obrigação de notificar os incidentes de segurança de um modo que minimize a carga administrativa caso o incidente em causa constitua também uma violação de dados pessoais***, em conformidade com o Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados[28]. Em colaboração com as autoridades competentes e as autoridades encarregadas da proteção dos dados pessoais,*** a ENISA ***poderá*** dar a sua contribuição desenvolvendo mecanismos de intercâmbio de informações e ***modelos que evitem a necessidade de dois modelos***	(31) Os dados pessoais ficam em muitos casos comprometidos em consequência de incidentes. ***Os Estados-Membros e os operadores do mercado devem proteger os dados pessoais armazenados, tratados ou transmitidos contra a destruição acidental ou ilícita, perda ou alteração acidental e armazenamento, acesso ou divulgação não autorizada ou ilícita, difusão ou acesso; e devem assegurar a aplicação de uma política de segurança no domínio do tratamento de dados pessoais.*** Neste contexto, as autoridades competentes***, os balcões únicos*** e as autoridades encarregadas da proteção de dados devem cooperar e trocar informações sobre todas as questões pertinentes para combater as violações de dados pessoais resultantes de incidentes. A obrigação de notificar os incidentes de segurança ***deve ser concretizada*** de um modo que minimize a carga administrativa caso o incidente em causa constitua também uma violação de dados pessoais ***que tem de ser comunicada em conformidade com a legislação aplicável.*** A ENISA ***deve*** dar a sua

de notificação. Este único modelo de notificação ***facilitaria*** a comunicação de incidentes que comprometam os dados pessoais, aligeirando assim a carga administrativa que recai sobre as empresas e as administrações públicas.

contribuição desenvolvendo mecanismos de intercâmbio de informações e ***um*** único modelo de notificação ***que facilite*** a comunicação de incidentes que comprometam os dados pessoais, aligeirando assim a carga administrativa que recai sobre as empresas e as administrações públicas.

---

[28] SEC(2012) 72 final

Justificação

Em consonância com o projeto de diretiva relativa à proteção de dados.

Alteração 30

Proposta de diretiva
Considerando 32

Texto da Comissão	*Alteração*
(32) A normalização dos requisitos de segurança é um processo dirigido pelo mercado. A fim de garantir uma aplicação convergente das normas de segurança, os Estados-Membros deverão incentivar o cumprimento ou a conformidade com as normas especificadas para assegurar um elevado nível de segurança a nível da União. Para o efeito, poderá ser ***necessário elaborar*** normas harmonizadas, o que deverá ser efetuado em conformidade com o Regulamento (UE) n.° 1025/2012 do Parlamento Europeu e do Conselho, de 25 de outubro de 2012, relativo à normalização europeia, que altera as Diretivas 89/686/CEE e 93/15/CEE do Conselho e as Diretivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE do Parlamento Europeu e do Conselho e revoga a Decisão 87/95/CEE do Conselho e a Decisão n.° 1673/2006/CE do Parlamento Europeu e do Conselho[29].	(32) A normalização dos requisitos de segurança é um processo dirigido pelo mercado***, de natureza voluntária, que deve permitir que os operadores do mercado utilizem meios alternativos para atingir, pelo menos, resultados semelhantes***. A fim de garantir uma aplicação convergente das normas de segurança, os Estados-Membros deverão incentivar o cumprimento ou a conformidade com as normas ***interoperáveis*** especificadas para assegurar um elevado nível de segurança a nível da União. Para o efeito, ***deve ser considerada a aplicação de normas internacionais abertas na segurança das redes e da informação ou a criação de tais instrumentos. Outro passo em frente necessário*** poderá ser ***a elaboração de*** normas harmonizadas, o que deverá ser efetuado em conformidade com o Regulamento (UE) n.° 1025/2012 do Parlamento Europeu e do Conselho, de 25 de outubro de 2012, relativo à

	normalização europeia, que altera as Diretivas 89/686/CEE e 93/15/CEE do Conselho e as Diretivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE do Parlamento Europeu e do Conselho e revoga a Decisão 87/95/CEE do Conselho e a Decisão n.° 1673/2006/CE do Parlamento Europeu e do Conselho[29]. ***Em particular, o ETSI, o CEN e o CENELEC devem ser mandatados no sentido de sugerir normas europeias de segurança abertas, eficazes e eficientes, em que as preferências tecnológicas sejam evitadas tanto quanto possível, e que devem ser facilmente exequíveis por pequenos e médios operadores do mercado. As normas internacionais relativas à cibersegurança devem ser cuidadosamente aprovadas, a fim de assegurar que não foram comprometidas e que fornecem níveis adequados de segurança, garantindo, assim, que o cumprimento obrigatório das normas relativas à cibersegurança melhora o nível geral da cibersegurança da União e não o contrário.***
[29] JO L 316 de 14.11.2012, p. 12.	[29] JO L 316 de 14.11.2012, p. 12.

Alteração 31

Proposta de diretiva
Considerando 33

Texto da Comissão	*Alteração*
(33) A Comissão deverá rever periodicamente a presente diretiva, nomeadamente para decidir da eventual necessidade de alterações à luz da evolução tecnológica ou do mercado.	(33) A Comissão deverá rever periodicamente a presente diretiva, ***em consulta com todas as partes interessadas,*** nomeadamente para decidir da eventual necessidade de alterações à luz da evolução ***social, política,*** tecnológica ou do mercado.

Alteração 32

Proposta de diretiva
Considerando 34

Texto da Comissão	*Alteração*
(34) A fim de permitir o bom funcionamento da rede de cooperação, o poder de adotar atos em conformidade com o artigo 290.º do Tratado sobre o Funcionamento da União Europeia deve ser delegado à Comissão no que diz respeito à definição dos critérios a cumprir para que um Estado-Membro seja autorizado a participar num sistema seguro de troca de informações, a uma melhor especificação dos eventos desencadeadores de um alerta rápido e à definição das condições em que os operadores de mercado e as administrações públicas são obrigados a notificar os incidentes.	***Suprimido***

Alteração 33

Proposta de diretiva
Considerando 35

Texto da Comissão	*Alteração*
(35) É particularmente importante que a Comissão proceda a consultas adequadas durante os seus trabalhos preparatórios, incluindo a nível de peritos. A Comissão***, ao preparar e redigir atos delegados,*** deverá assegurar a transmissão simultânea, atempada e adequada dos documentos relevantes ao Parlamento Europeu e ao Conselho.	(35) É particularmente importante que a Comissão proceda a consultas adequadas durante os trabalhos preparatórios, incluindo ***todas as partes interessadas e, nomeadamente,*** a nível de peritos. A Comissão deverá assegurar a transmissão simultânea, atempada e adequada dos documentos relevantes ao Parlamento Europeu e ao Conselho.

Alteração 34

Proposta de diretiva
Considerando 36

Texto da Comissão	*Alteração*
(36) A fim de assegurar condições uniformes de aplicação da presente diretiva, devem ser conferidas competências de execução à Comissão no que diz respeito à cooperação com ***as autoridades competentes*** no âmbito da rede de cooperação, ***ao acesso às*** infraestruturas seguras de partilha de informações, ao plano de cooperação da União em matéria de SRI, aos meios e procedimentos aplicáveis à ***informação do público sobre a ocorrência*** de incidentes ***e às normas e/ou especificações técnicas pertinentes para a SRI***. Essas competências deverão ser exercidas em conformidade com o Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho, de 16 de fevereiro de 2011, que estabelece as regras e os princípios gerais relativos aos mecanismos de controlo pelos Estados-Membros do exercício das competências de execução pela Comissão[30].	(36) A fim de assegurar condições uniformes de aplicação da presente diretiva, devem ser conferidas competências de execução à Comissão no que diz respeito à cooperação com ***os balcões únicos*** no âmbito da rede de cooperação, ***sem prejuízo dos mecanismos de cooperação existentes a nível nacional, do conjunto comum de normas de interligação e de segurança para as*** infraestruturas seguras de partilha de informações, do plano de cooperação da União em matéria de SRI, ***bem como dos*** meios e procedimentos aplicáveis à ***notificação*** de incidentes ***significativos***. Essas competências deverão ser exercidas em conformidade com o Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho, de 16 de fevereiro de 2011, que estabelece as regras e os princípios gerais relativos aos mecanismos de controlo pelos Estados Membros do exercício das competências de execução pela Comissão[30].
[30] JO L 55 de 28.2.2011, p. 13.	[30] JO L 55 de 28.2.2011, p. 13.

Alteração 35

Proposta de diretiva
Considerando 37

Texto da Comissão	*Alteração*
(37) Na aplicação da presente diretiva, a Comissão deve assegurar as ligações adequadas com os comités setoriais pertinentes e os organismos competentes	(37) Na aplicação da presente diretiva, a Comissão deve assegurar as ligações adequadas com os comités setoriais pertinentes e os organismos competentes

criados a nível da UE, em especial no domínio ***da*** energia, transportes e saúde.	criados a nível da UE, em especial no domínio ***do governo eletrónico,*** energia, transportes e saúde.

Alteração 36

Proposta de diretiva
Considerando 38

Texto da Comissão	*Alteração*
(38) As informações que sejam consideradas confidenciais por uma autoridade competente, em conformidade com as regras nacionais e da União em matéria de sigilo comercial, só devem ser trocadas com a Comissão ***e*** outras autoridades competentes nos casos em que tal seja estritamente necessário para a aplicação da presente diretiva. As informações comunicadas deverão limitar-se ao que for pertinente e adequado ao objetivo dessa comunicação.	(38) As informações que sejam consideradas confidenciais por uma autoridade competente ***ou um balcão único***, em conformidade com as regras nacionais e da União em matéria de sigilo comercial, só devem ser trocadas com a Comissão***, as suas agências relevantes, os balcões únicos e/ou*** outras autoridades ***nacionais*** competentes nos casos em que tal seja estritamente necessário para a aplicação da presente diretiva. As informações comunicadas deverão limitar-se ao que for pertinente***, necessário*** e adequado ao objetivo dessa comunicação***, respeitando simultaneamente os critérios predefinidos para a confidencialidade, a segurança e os protocolos de classificação que regem os procedimentos de partilha de informações***.

Alteração 37

Proposta de diretiva
Considerando 39

Texto da Comissão	*Alteração*
(39) A partilha de informações sobre os riscos e incidentes na rede de cooperação e o cumprimento da obrigatoriedade de notificação de incidentes às autoridades nacionais competentes podem requerer o tratamento de dados pessoais. Esse tratamento é necessário para alcançar os	(39) A partilha de informações sobre os riscos e incidentes na rede de cooperação e o cumprimento da obrigatoriedade de notificação de incidentes às autoridades nacionais competentes ***ou aos balcões únicos*** podem requerer o tratamento de dados pessoais. Esse tratamento é

objetivos de interesse público prosseguidos pela presente diretiva e é, pois, legítimo, nos termos do artigo 7.° da Diretiva 95/46/CE. Não constitui, em relação a estes objetivos legítimos, uma interferência desproporcionada e intolerável que lese a própria essência do direito à proteção de dados pessoais consagrado no artigo 8.º da Carta dos Direitos Fundamentais. Na aplicação da presente diretiva, o Regulamento (CE) n.° 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[31], deve aplicar se conforme adequado. Nos casos em que os dados sejam tratados pelas instituições e órgãos da União, esse tratamento para efeitos de aplicação da presente diretiva deve ser conforme com o Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados.	necessário para alcançar os objetivos de interesse público prosseguidos pela presente diretiva e é, pois, legítimo, nos termos do artigo 7.° da Diretiva 95/46/CE. Não constitui, em relação a estes objetivos legítimos, uma interferência desproporcionada e intolerável que lese a própria essência do direito à proteção de dados pessoais consagrado no artigo 8.º da Carta dos Direitos Fundamentais. Na aplicação da presente diretiva, o Regulamento (CE) n.° 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[31], deve aplicar-se conforme adequado. Nos casos em que os dados sejam tratados pelas instituições e órgãos da União, esse tratamento para efeitos de aplicação da presente diretiva deve ser conforme com o Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados.
[31] JO L 145 de 31.05.2001, p. 43.	[31] JO L 145 de 31.05.2001, p. 43.

Alteração 38

Proposta de diretiva
Considerando 41-A (novo)

Texto da Comissão	*Alteração*
	(41-A) Nos termos da declaração política conjunta dos Estados-Membros e da Comissão sobre os documentos explicativos, de 28 de setembro de 2011, os Estados-Membros assumiram o compromisso de fazer acompanhar a notificação das suas medidas de transposição, nos casos em que tal se

	justifique, por um ou mais documentos destinados a explicar a relação entre os componentes de uma diretiva e as partes correspondentes dos instrumentos de transposição nacionais. Em relação à presente diretiva, o legislador considera que a transmissão desses documentos se justifica.

Alteração 39

Proposta de diretiva
Artigo 1 – n.º 2 – alínea b)

Texto da Comissão	*Alteração*
(b) cria um mecanismo de cooperação entre os Estados-Membros a fim de garantir uma aplicação uniforme da presente diretiva na União e, se for caso disso, um tratamento e uma resposta coordenados e eficazes aos riscos e incidentes que afetam as redes e os sistemas informáticos;	(b) cria um mecanismo de cooperação entre os Estados-Membros a fim de garantir uma aplicação uniforme da presente diretiva na União e, se for caso disso, um tratamento e uma resposta coordenados e eficazes aos riscos e incidentes que afetam as redes e os sistemas informáticos ***com a participação das partes interessadas pertinentes***;

Alteração 40

Proposta de diretiva
Artigo 1 – n.º 6

Texto da Comissão	*Alteração*
6. A partilha de informações no quadro da rede de cooperação nos termos do capítulo III e as notificações de incidentes que afetam a SRI ao abrigo do artigo 14.º podem requerer o tratamento de dados pessoais. Esse tratamento, que é necessário para alcançar os objetivos de interesse público prosseguidos pela presente diretiva, deve ser autorizado pelo Estado-Membro em conformidade com o artigo 7.° da Diretiva 95/46/CE e com a Diretiva 2002/58/CE, tal como transpostos	6. A partilha de informações no quadro da rede de cooperação nos termos do capítulo III e as notificações de incidentes que afetam a SRI ao abrigo do artigo 14.º podem requerer ***a comunicação a terceiros de confiança e*** o tratamento de dados pessoais. Esse tratamento, que é necessário para alcançar os objetivos de interesse público prosseguidos pela presente diretiva, deve ser autorizado pelo Estado-Membro em conformidade com o artigo 7.° da Diretiva 95/46/CE e com a

para o direito nacional.	Diretiva 2002/58/CE, tal como transpostos para o direito nacional. ***Os Estados-Membros adotam medidas legislativas de acordo com o artigo 13.º da Diretiva 95/46/CE, com vista a assegurar que as administrações públicas, os operadores do mercado e as autoridades competentes não são responsabilizados pelo tratamento de dados pessoais, necessários para a troca de informações no âmbito da rede de cooperação e notificação de incidentes.***

Alteração 41

Proposta de diretiva
Artigo 2 – n.º 1

Texto da Comissão	*Alteração*
Os Estados-Membros não devem ser impedidos de adotar ou manter disposições que assegurem um nível de segurança superior, desde que tal não prejudique o cumprimento das obrigações que lhes incumbem por força da legislação da União.	Os Estados-Membros não devem ser impedidos de adotar ou manter disposições que assegurem um nível de segurança superior, ***em conformidade com a Carta dos Direitos Fundamentais da UE,*** desde que tal não prejudique o cumprimento das obrigações que lhes incumbem por força da legislação da União.

Justificação

A discricionariedade conferida aos Estados-Membros em matéria de segurança deve estar sujeita ao respeito pelos direitos reconhecidos na Carta dos Direitos Fundamentais da UE, nomeadamente, e entre outros, o direito ao respeito pela vida e comunicações privadas, à proteção dos dados pessoais, à liberdade de empresa e ao recurso judicial.

Alteração 42

Proposta de diretiva
Artigo 3 – parágrafo 1 – n.º 1 – alínea b)

Texto da Comissão	*Alteração*
(b) qualquer dispositivo ou grupo de dispositivos interligados ou associados, dos	(b) qualquer dispositivo ou grupo de dispositivos interligados ou associados, dos

quais um ou mais efetuam, com base num programa, o tratamento automático dos dados ***informáticos***,	quais um ou mais efetuam, com base num programa, o tratamento automático dos dados ***digitais***,

Alteração 43

Proposta de diretiva
Artigo 3 – parágrafo 1 – n.º 1 – alínea c)

Texto da Comissão	*Alteração*
(c) os dados ***informáticos*** armazenados, tratados, obtidos ou transmitidos por elementos indicados nas alíneas a) e b) tendo em vista a sua exploração, utilização, proteção e manutenção.	(c) os dados ***digitais*** armazenados, tratados, obtidos ou transmitidos por elementos indicados nas alíneas a) e b) tendo em vista a sua exploração, utilização, proteção e manutenção.

Alteração 44

Proposta de diretiva
Artigo 3 – parágrafo 1 – n.º 2

Texto da Comissão	*Alteração*
(2) «Segurança»: a capacidade de uma rede ou sistema informático para resistir, com um dado nível de confiança, a eventos acidentais ou a ações dolosas que comprometem a disponibilidade, autenticidade, integridade e confidencialidade dos dados armazenados ou transmitidos e dos serviços conexos oferecidos ou acessíveis através dessa rede ou sistema;	(2) «Segurança»: a capacidade de uma rede ou sistema informático para resistir, com um dado nível de confiança, a eventos acidentais ou a ações dolosas que comprometem a disponibilidade, autenticidade, integridade e confidencialidade dos dados armazenados ou transmitidos e dos serviços conexos oferecidos ou acessíveis através dessa rede ou sistema; ***a «segurança», como aqui definida, inclui dispositivos técnicos, soluções e procedimentos operacionais adequados que asseguram os requisitos de segurança definidos na presente diretiva.***

Alteração 45

Proposta de diretiva
Artigo 3 – parágrafo 1 – n.º 4

Texto da Comissão	*Alteração*
(4) «Incidente»: qualquer circunstância ou evento com um efeito adverso real na segurança;	(4) «Incidente»: qualquer circunstância ou evento ***razoavelmente identificável*** com um efeito adverso real na segurança;

Justificação

A redação original é demasiado abrangente e dificultaria a aplicação da definição.

Alteração 46

Proposta de diretiva
Artigo 3 – parágrafo 1 – n.º 5

Texto da Comissão	*Alteração*
(5) «Serviço da sociedade da informação»: um serviço na aceção do artigo 1.º, n.º 2, da Diretiva 98/34/CE;	***Suprimido***

Alteração 47

Proposta de diretiva
Artigo 3 – parágrafo 1 – n.º 8 – alínea a)

Texto da Comissão	*Alteração*
(a) um fornecedor de serviços da sociedade de informação que permitem a prestação de outros serviços da sociedade da informação, cuja lista não exaustiva consta do anexo II;	***Suprimido***

Alteração 48

Proposta de diretiva

Artigo 3 – parágrafo 1 – n.º 7

Texto da Comissão	*Alteração*
(7) «Tratamento de incidentes»: todos os procedimentos de apoio à análise, contenção e resposta em caso de incidente;	(7) «Tratamento de incidentes»: todos os procedimentos de apoio à ***deteção, prevenção,*** análise, contenção e resposta em caso de incidente;

Alteração 49

Proposta de diretiva
Artigo 3 – parágrafo 1 – n.º 8

Texto da Comissão	*Alteração*
(a) um fornecedor de serviços da sociedade de informação que permitem a prestação de outros serviços da sociedade da informação, cuja lista não exaustiva consta do anexo II;	
(b) um operador de infraestruturas críticas essenciais para a manutenção de atividades económicas e sociais vitais nos domínios da energia, dos transportes, da banca, ***da bolsa*** e da saúde, cuja lista ***não exaustiva*** consta do anexo II.	(b) um operador ***público ou privado*** de infraestruturas essenciais para a manutenção de atividades económicas e sociais vitais nos domínios da energia, dos transportes, da banca, ***dos mercados financeiros*** e da saúde, cuja lista consta do anexo II***, e cuja interrupção ou destruição teria um impacto negativo significativo num Estado-Membro, em resultado da impossibilidade de continuar a assegurar essas funções***.

Alteração 50

Proposta de diretiva
Artigo 3 – parágrafo 1 – n.º 8-A) (novo)

Texto da Comissão	*Alteração*
	(8-A) «incidente com um impacto significativo»: um incidente que afeta a segurança e continuidade de uma rede ou

	sistema de informação que conduz a uma grande perturbação das funções económicas e sociais vitais;

Alteração 51

Proposta de diretiva
Artigo 3 – parágrafo 1 – n.º 8-B) (novo)

Texto da Comissão	*Alteração*
	(8-B) «serviço»: serviço prestado por um operador do mercado, excluindo quaisquer outros serviços da mesma entidade.

Alteração 52

Proposta de diretiva
Artigo 3 – parágrafo 1 – n.º 11-A (nova)

Texto da Comissão	*Alteração*
	(11-A) «mercado regulamentado»: um mercado regulamentado tal como definido no artigo 4.º, n.º 14, da Diretiva 2004/39/CE do Parlamento Europeu e do Conselho[28a];
	[28a] Diretiva 2004/39/CE do Parlamento Europeu e do Conselho, de 21 de abril de 2004, relativa aos mercados de instrumentos financeiros (JO L 45 de 16.2.2005, p. 18).

Alteração 53

Proposta de diretiva
Artigo 3 – parágrafo 1 – n.º 11-B) (novo)

Texto da Comissão	*Alteração*
	(11-B) «sistema de negociação multilateral (MTF)»: um sistema de

	negociação multilateral tal como definido no artigo 4.º, n.º 15, da Diretiva 2004/39/CE;

Alteração 54

Proposta de diretiva
Artigo 3 – parágrafo 1 – n.º 11-C) (novo)

Texto da Comissão	*Alteração*
	(11-C) «sistema de negociação organizado»: um sistema ou dispositivo multilateral que não um mercado regulamentado nem um sistema de negociação multilateral ou uma contraparte central, operado por uma empresa de investimento ou um operador do mercado, dentro do qual múltiplos interesses de compra e venda de obrigações, produtos financeiros estruturados, licenças de emissão ou derivados, manifestados por terceiros, podem interagir no sistema para que tal resulte num contrato, em conformidade com o disposto no título II da Diretiva 2004/39/CE;

Alteração 55

Proposta de diretiva
Artigo 4 – 1 – n.º 1

Texto da Comissão	*Alteração*
Os Estados-Membros devem garantir um elevado nível de segurança das redes e dos sistemas informáticos no seu território, em conformidade com a presente diretiva.	Os Estados-Membros devem garantir um nível ***elevado, sustentado e contínuo*** de segurança das redes e dos sistemas informáticos no seu território, em conformidade com ***a Carta dos Direitos Fundamentais da União Europeia e com*** a presente diretiva.

Justificação

A discricionariedade conferida aos Estados-Membros em matéria de segurança deve estar sujeita ao respeito pelos direitos reconhecidos na Carta dos Direitos Fundamentais da UE, nomeadamente, e entre outros, o direito ao respeito pela vida e comunicações privadas, à proteção dos dados pessoais, à liberdade de empresa e ao recurso judicial.

Alteração 56

Proposta de diretiva
Artigo 5 – n.º 1 – alínea e-A) (nova)

Texto da Comissão	*Alteração*
	(e-A) Os Estados-Membros podem solicitar a assistência da Agência Europeia para a Segurança das Redes e da Informação («ENISA») para a elaboração das suas estratégias nacionais e dos seus planos de cooperação nacional em matéria de SRI, baseados num plano mínimo comum de estratégia e cooperação em matéria de SRI.

Alteração 57

Proposta de diretiva
Artigo 5 – n.º 2 – alínea a)

Texto da Comissão	*Alteração*
(a) ***Um plano de avaliação*** dos riscos ***para identificar os riscos e avaliar os*** impactos de potenciais incidentes;	(a) ***Um quadro de gestão*** dos riscos ***que inclua a identificação, a definição de prioridades, a avaliação e o tratamento de riscos, a avaliação dos*** impactos de potenciais incidentes***, as opções de prevenção e de controlo e os critérios para a escolha de possíveis medidas preventivas***;

Alteração 58

Proposta de diretiva
Artigo 5 – n.º 2 – alínea b)

Texto da Comissão	*Alteração*
(b) A definição das funções e responsabilidades ***dos*** diferentes intervenientes envolvidos na execução do ***plano***;	(b) A definição das funções e responsabilidades ***das*** diferentes ***autoridades e de outros*** intervenientes envolvidos na execução do ***quadro***;

Alteração 59

Proposta de diretiva
Artigo 6 – título

Texto da Comissão	*Alteração*
Autoridade nacional competente em matéria de segurança das redes e dos sistemas informáticos	***Autoridades nacionais e balcões únicos competentes*** em matéria de segurança das redes e dos sistemas informáticos

Alteração 60

Proposta de diretiva
Artigo 6 – n.º 1

Texto da Comissão	*Alteração*
1. Cada Estado-Membro designa uma ***autoridade nacional competente*** em matéria de segurança das redes e dos sistemas informáticos («autoridade competente»).	1. Cada Estado-Membro designa uma ***ou mais autoridades nacionais competentes*** em matéria de segurança das redes e dos sistemas informáticos (***a seguir designada*** «autoridade competente»).

Alteração 61

Proposta de diretiva
Artigo 6 – n.º 2-A (novo)

Texto da Comissão	*Alteração*
	2-A. Caso um Estado-Membro designe mais de uma autoridade competente, deve designar uma autoridade nacional, por exemplo uma autoridade competente, enquanto balcão único nacional para a segurança da rede e dos sistemas

	informáticos (a seguir designado «balcão único»). Caso um Estado-Membro designe apenas uma autoridade competente, esta será também o balcão único.

Alteração 62

Proposta de diretiva
Artigo 6 – n.º 2-B (novo)

Texto da Comissão	*Alteração*
	2-B. As autoridades competentes e o balcão único do mesmo Estado-Membro cooperam estreitamente no que diz respeito às obrigações previstas na presente diretiva.

Alteração 63

Proposta de diretiva
Artigo 6 – n.º 2-C (novo)

Texto da Comissão	*Alteração*
	2-C. O balcão único assegura a cooperação transfronteiras com outros balcões únicos.

Alteração 64

Proposta de diretiva
Artigo 6 – n.º 3

Texto da Comissão	*Alteração*
3. Os Estados-Membros asseguram que as autoridades competentes disponham de recursos técnicos, financeiros e humanos adequados para realizar de modo eficaz e eficiente as tarefas que lhes sejam atribuídas e, deste modo, cumprir os objetivos da presente diretiva. Os Estados-Membros garantem a cooperação	3. Os Estados-Membros asseguram que as autoridades competentes ***e os balcões únicos*** disponham de recursos técnicos, financeiros e humanos adequados para realizar de modo eficaz e eficiente as tarefas que lhes sejam atribuídas e, deste modo, cumprir os objetivos da presente diretiva. Os Estados-Membros garantem a

eficaz, eficiente e segura ***das autoridades competentes*** através da rede referida no artigo 8.º.	cooperação eficaz, eficiente e segura ***dos balcões únicos*** através da rede referida no artigo 8.º.

Alteração 65

Proposta de diretiva
Artigo 6 – n.º 4

Texto da Comissão	*Alteração*
4. Os Estados-Membros asseguram que as autoridades competentes sejam ***notificadas*** dos incidentes ocorridos ***pelas administrações públicas e*** pelos operadores do mercado, tal como especificado no artigo 14.º, n.º 2, e lhes sejam atribuídos poderes de execução e de repressão, tal como referido no artigo 15.°.	4. Os Estados-Membros asseguram que as autoridades competentes ***e os balcões únicos*** sejam ***notificados*** dos incidentes ocorridos pelos operadores do mercado, tal como especificado no artigo 14.º, n.º 2, e lhes sejam atribuídos poderes de execução e de repressão, tal como referido no artigo 15.º.

Alteração 66

Proposta de diretiva
Artigo 6 – n.º 5

Texto da Comissão	*Alteração*
5. ***Sempre que necessário,*** as autoridades competentes consultam as autoridades policiais e judiciais nacionais ***e as autoridades encarregadas da proteção de dados, com elas cooperando***.	5. As autoridades competentes consultam ***as autoridades encarregadas da proteção de dados e, sempre que necessário, cooperam com*** as autoridades policiais e judiciais nacionais.

Justificação

O equilíbrio entre a garantia da segurança e a salvaguarda da liberdade seria perturbado se uma única autoridade competente exercesse o poder de controlo a nível nacional sem a colaboração de outro organismo de compensação.

Alteração 67

Proposta de diretiva
Artigo 6 – n.º 5

Texto da Comissão	*Alteração*
5. Sempre que necessário, as autoridades competentes consultam as autoridades policiais e judiciais nacionais e as autoridades encarregadas da proteção dos dados, com elas cooperando.	5. Sempre que necessário, as autoridades competentes ***e os balcões únicos*** consultam as autoridades policiais e judiciais nacionais e as autoridades encarregadas da proteção dos dados, com elas cooperando.

Alteração 68

Proposta de diretiva
Artigo 6 – n.º 6

Texto da Comissão	*Alteração*
6. Cada Estado-Membro notifica sem demora à Comissão a designação ***da autoridade competente***, as suas funções, bem como quaisquer posteriores alterações. Cada Estado-Membro torna pública a sua designação ***da autoridade competente***.	6. Cada Estado-Membro notifica sem demora à Comissão a designação ***das autoridades competentes e do balcão único***, as suas funções, bem como quaisquer posteriores alterações. Cada Estado-Membro torna pública a sua designação ***das autoridades competentes***.

Alteração 69

Proposta de diretiva
Artigo 7 – n.º 1

Texto da Comissão	*Alteração*
1. Cada Estado-Membro cria uma equipa de resposta a emergências informáticas (a seguir designada por «CERT»), responsável pelo tratamento de incidentes e riscos de acordo com um processo bem definido, que deve cumprir as condições estabelecidas no anexo I, ponto 1. A CERT pode ser estabelecida no âmbito da autoridade competente.	1. Cada Estado-Membro cria ***pelo menos*** uma equipa de resposta a emergências informáticas (a seguir designada por «CERT») ***para cada um dos setores definidos no anexo II***, responsável pelo tratamento de incidentes e riscos de acordo com um processo bem definido, que deve cumprir as condições estabelecidas no anexo I, ponto 1. A CERT pode ser estabelecida no âmbito da autoridade competente.

Alteração 70

Proposta de diretiva
Artigo 7 – n.º 5

Texto da Comissão	*Alteração*
5. ***A*** CERT ***funciona*** sob a supervisão da autoridade competente, que deve rever periodicamente a adequação dos seus recursos, ***o seu mandato*** e a eficácia do seu processo de tratamento de incidentes.	5. ***As*** CERT ***funcionam*** sob a supervisão da autoridade competente ***ou do balcão único***, que deve rever periodicamente a adequação dos seus recursos, ***mandatos*** e a eficácia do seu processo de tratamento de incidentes.

Alteração 71

Proposta de diretiva
Artigo 7 – n.º 5-A (novo)

Texto da Comissão	*Alteração*
	5-A. Os Estados-Membros devem assegurar que as CERT possuam recursos humanos e financeiros adequados, de modo a participarem ativamente em redes de cooperação internacionais e, nomeadamente, da União.

Alteração 72

Proposta de diretiva
Artigo 7 – n.º 5 – ponto 1 (novo)

Texto da Comissão	*Alteração*
	(1) As CERT devem poder e ser incentivadas a iniciar e participar em exercícios conjuntos com outras CERT, com todas as CERT dos Estados-Membros e com as instituições adequadas dos Estados não membros, bem como com as CERT de organismos multi-institucionais e instituições internacionais, tais como a NATO e a ONU.

Alteração 73

Proposta de diretiva
Artigo 7 – n.º 5-A (novo)

Texto da Comissão	*Alteração*
	5-A. Os Estados-Membros podem solicitar a assistência da Agência Europeia para a Segurança das Redes e da Informação («ENISA») ou de outros Estados-Membros para a criação das suas CERT nacionais.

Alteração 74

Proposta de diretiva
Artigo 8

Texto da Comissão	*Alteração*
1. ***As autoridades competentes*** e a Comissão devem constituir uma rede («rede de cooperação») para cooperarem contra os riscos e os incidentes que afetem as redes e os sistemas informáticos.	1. ***Os balcões únicos, a Agência Europeia para a Segurança das Redes e da Informação («ENISA»)*** e a Comissão devem constituir uma rede («rede de cooperação») para cooperarem contra os riscos e os incidentes que afetem as redes e os sistemas informáticos.
2. A rede de cooperação põe em comunicação permanente a Comissão e ***as autoridades competentes***. ***Quando for solicitada,*** a Agência Europeia para a Segurança das Redes e da informação («ENISA») apoiará a rede de cooperação, fornecendo conhecimentos especializados e aconselhamento.	2. A rede de cooperação põe em comunicação permanente a Comissão e ***os balcões únicos***. A Agência Europeia para a Segurança das Redes e da informação («ENISA») apoiará a rede de cooperação, fornecendo conhecimentos especializados e aconselhamento. ***Se for caso disso, a rede de cooperação cooperará com as autoridades encarregadas da proteção dos dados.***
3. No âmbito da rede de cooperação, as autoridades competentes devem:	3. No âmbito da rede de cooperação, os balcões únicos devem:
(a) Difundir alertas rápidos sobre os riscos e os incidentes, em conformidade com o	(a) Difundir alertas rápidos sobre os riscos e os incidentes, em conformidade com o

artigo 10.°;	artigo 10.°;
(b) Assegurar uma resposta coordenada em conformidade com o artigo 11.º;	(b) Assegurar uma resposta coordenada em conformidade com o artigo 11.º;
(c) Publicar periodicamente num sítio Web comum informações não confidenciais sobre alertas rápidos em curso e a resposta coordenada;	(c) Publicar periodicamente num sítio Web comum informações não confidenciais sobre alertas rápidos em curso e a resposta coordenada;
	(c-A) Conjuntamente debater, acordar sobre a interpretação comum e a aplicação coerente e coordenar as suas medidas em matéria de exigências de segurança e notificação de incidentes, referidas no artigo 14.º, e em matéria de aplicação e cumprimento, como referido no artigo 15.º;
(d) Debater e avaliar conjuntamente***, a pedido de um Estado-Membro ou da Comissão,*** uma ou mais estratégias e planos de cooperação nacionais em matéria de SRI referidos no artigo 5.°, no âmbito da presente diretiva;	(d) Debater e avaliar conjuntamente uma ou mais estratégias e planos de cooperação nacionais em matéria de SRI referidos no artigo 5.°, no âmbito da presente diretiva;
(e) Debater e avaliar conjuntamente, a pedido de um Estado-Membro ou da Comissão, a eficácia das CERT, em particular aquando da realização de exercícios de SRI a nível da União;	(e) Debater e avaliar conjuntamente, a pedido ***da ENISA,*** de um Estado-Membro ou da Comissão, a eficácia das CERT, em particular aquando da realização de exercícios de SRI a nível da União***, e aplicar medidas para resolver as deficiências identificadas sem demora***;
(f) Cooperar e trocar informações sobre todas as questões pertinentes ***com o Centro Europeu da Cibercriminalidade na Europol e*** com outros organismos europeus competentes, em especial nos domínios da ***proteção de dados,*** energia, transportes, banca, ***bolsa*** e saúde;	(f) Cooperar e trocar informações sobre todas as questões pertinentes ***sobre segurança das redes e da informação*** com outros organismos europeus competentes, em especial nos domínios da energia, transportes, banca, ***mercados financeiros*** e saúde;
	(f-A) Debater e acordar conjuntamente sobre a interpretação comum, a aplicação coerente e a execução harmoniosa na União das disposições do capítulo IV;
(g) Proceder ao intercâmbio de informações e de boas práticas entre si e com a Comissão e prestar assistência mútua tendo em vista o desenvolvimento de capacidades em matéria de SRI;	(g) Proceder ao intercâmbio de informações e de boas práticas entre si e com a Comissão e prestar assistência mútua tendo em vista o desenvolvimento de capacidades em matéria de SRI;

(h) Organizar análises regulares pelos pares das capacidades e do grau de preparação;	(h) Organizar análises regulares pelos pares das capacidades e do grau de preparação;
(i) Organizar exercícios sobre SRI a nível da União e, se tal se afigurar adequado, participar nesse tipo de exercícios a nível internacional.	(i) Organizar exercícios sobre SRI a nível da União e, se tal se afigurar adequado, participar nesse tipo de exercícios a nível internacional.
	(i-A) Promover ativamente o envolvimento, bem como a consulta e o intercâmbio de informações, com operadores do mercado.
	A Comissão deve informar, regularmente, a rede de cooperação sobre a investigação em matéria de segurança e outros programas relevantes do Horizonte 2020.
	3-A. Se for caso disso, as administrações públicas competentes e os operadores do mercado pertinentes serão convidados a participar nas atividades da rede de cooperação referidas no n.º 3, alíneas c), g), h) e i).
	3-B. Sempre que a informação, os alertas rápidos e as boas práticas provenientes de operadores do mercado ou administrações públicas forem partilhadas dentro da rede de cooperação ou divulgadas por esta, essas partilhas ou divulgações devem ser realizadas de acordo com a classificação da informação determinada pela fonte original em conformidade com o artigo 9.º, n.º 1.
	3-C. A Comissão publica anualmente um relatório, com base nas atividades da rede e no relatório resumido, referente aos 12 meses anteriores, apresentado em conformidade com o artigo 14.º, n.º 4, da presente diretiva. Deverá existir um justo equilíbrio entre a publicidade dada aos incidentes individuais comunicados às autoridades competentes e aos balcões únicos e o interesse do público em ser informado sobre as ameaças que comportem eventuais danos de reputação e comerciais para os operadores do mercado que os comunicaram, podendo essa publicidade ocorrer apenas após

	consulta prévia.
4. A Comissão deve estabelecer, por meio de atos de execução, as modalidades necessárias para facilitar a cooperação entre ***as autoridades competentes*** e a Comissão referida nos n.°s 2 e 3. Os atos de execução correspondentes devem ser adotados em conformidade com o procedimento de consulta referido no artigo 19.º, n.º 2.	4. A Comissão deve estabelecer, por meio de atos de execução, as modalidades necessárias para facilitar a cooperação entre ***os balcões únicos, a ENISA*** e a Comissão referida nos n.°s 2 e 3. Os atos de execução correspondentes devem ser adotados em conformidade com o procedimento de consulta referido no artigo 19.º, n.º 2.

Alteração 75

Proposta de diretiva
Artigo 9 – n.º 1

Texto da Comissão	*Alteração*
1. O intercâmbio de informações sensíveis e confidenciais na rede de cooperação deve ocorrer através de uma infraestrutura segura.	O intercâmbio de informações sensíveis e confidenciais na rede de cooperação deve ocorrer através de uma infraestrutura segura ***operada sob supervisão da ENISA***. ***Os Estados-Membros devem assegurar que as informações partilhadas, sensíveis ou confidenciais, de outros Estados ou da Comissão não sejam partilhadas com países terceiros ou utilizadas para fins desconhecidos, como, por exemplo, para operações secretas ou em tomadas de decisões no domínio financeiro.***

Alteração 76

Proposta de diretiva
Artigo 9 – n.º 2 – parte introdutória

Texto da Comissão	*Alteração*
2. A Comissão tem poderes para adotar atos ***delegados*** em conformidade com o artigo ***18.°*** para definir os critérios a cumprir para que um ***Estado-Membro*** seja autorizado a participar num sistema de	2. A Comissão tem poderes para adotar atos ***de execução*** em conformidade com o artigo ***19.º*** para definir os critérios a cumprir para que um ***balcão único*** seja autorizado a participar num sistema de

partilha de informações seguro, no que diz respeito:	partilha de informações seguro, no que diz respeito:
Alteração 77	
Proposta de diretiva **Artigo 9 – n.º 3**	
Texto da Comissão	*Alteração*
3. A Comissão adota, por meio de atos de execução, ***decisões sobre o acesso dos Estados-Membros a esta infraestrutura segura, de acordo com os critérios referidos nos n.°s 2 e 3***. Os referidos atos de execução são adotados em conformidade com o procedimento de exame referido no artigo 19.°, n.° 3.	3. A Comissão adota, por meio de atos de execução, ***um conjunto comum de normas de interligação e de segurança que os balcões únicos devem cumprir de modo a trocar informações***. Os referidos atos de execução são adotados em conformidade com o procedimento de exame referido no artigo 19.°, n.° 3.
Alteração 78	
Proposta de diretiva **Artigo 10**	
Texto da Comissão	*Alteração*
1. ***As autoridades competentes*** ou a Comissão devem emitir um alerta rápido na rede de cooperação sobre os riscos e incidentes que preencham, pelo menos, uma das seguintes condições:	1. ***Os balcões únicos*** ou a Comissão devem emitir um alerta rápido na rede de cooperação sobre os riscos e incidentes que preencham, pelo menos, uma das seguintes condições:
(a) Aumentem rapidamente ou possam aumentar rapidamente em escala;	
(b) ***Excedam ou possam exceder*** a capacidade nacional de resposta;	(b) ***O balcão único avalie que o risco ou incidente cresça ou possa crescer rapidamente em escala e exceda potencialmente*** a capacidade nacional de resposta;
(c) ***Afetem ou possam afetar*** mais de um Estado-Membro.	(c) ***Os balcões únicos ou a Comissão avaliem que o risco ou incidente afeta*** mais de um Estado-Membro.
2. Nos alertas rápidos, ***as autoridades competentes*** e a Comissão devem comunicar todas as informações	2. Nos alertas rápidos, ***os balcões únicos*** e a Comissão devem comunicar ***sem demora injustificada*** todas as informações

pertinentes de que dispõem e possam ser úteis para avaliar o risco ou o incidente.	pertinentes de que dispõem e possam ser úteis para avaliar o risco ou o incidente. ***As informações consideradas classificadas ou confidenciais pelo operador do mercado em causa e a identidade deste último devem ser divulgadas apenas na medida do necessário para avaliar o risco ou o incidente.***
3. A pedido de um Estado-Membro ou por sua própria iniciativa, a Comissão pode solicitar a um Estado-Membro que forneça todas as informações úteis de que dispõe sobre um determinado risco ou incidente.	3. A pedido de um Estado-Membro ou por sua própria iniciativa, a Comissão pode solicitar a um Estado-Membro que forneça todas as informações úteis ***não classificadas*** de que dispõe sobre um determinado risco ou incidente.
4. Se se suspeitar que o risco ou incidente objeto de um alerta rápido é de natureza criminosa, ***as autoridades competentes*** ou a Comissão devem ***informar*** o Centro Europeu da Cibercriminalidade na Europol.	4. Se se suspeitar que o risco ou incidente objeto de um alerta rápido é de natureza criminosa ***grave***, ***os balcões únicos*** ou a Comissão devem***, se for caso disso, colaborar com as autoridades nacionais da cibercriminalidade, permitindo-lhes cooperar e trocar informações com*** o Centro Europeu da Cibercriminalidade na Europol ***sem demora injustificada***.
	4-A. Os membros da rede de cooperação não tornam públicas quaisquer informações recebidas relativamente a riscos e incidentes nos termos do n.º 1, sem terem recebido aprovação prévia por parte do balcão único notificante.
	4-B. Se se suspeitar que o risco ou incidente objeto de um alerta rápido é de natureza técnica transfronteiras grave, os balcões únicos ou a Comissão devem informar a ENISA;
5. A Comissão tem poderes para adotar atos ***delegados*** em conformidade com o artigo ***18.º*** para especificar melhor os riscos e incidentes que desencadeiam o alerta rápido referido no n.º 1.	5. A Comissão tem poderes para adotar atos ***de execução*** em conformidade com o artigo ***19.º*** para especificar melhor os riscos e incidentes que desencadeiam o alerta rápido referido no n.º 1***, bem como os procedimentos para a partilha de informações sensíveis para os operadores do mercado***.

Alteração 79

Proposta de diretiva
Artigo 11 – n.º 1

Texto da Comissão	*Alteração*
1. Na sequência de um alerta rápido referido no artigo 10.º, ***as autoridades competentes*** devem, após a avaliação das informações pertinentes, chegar a acordo quanto a uma resposta coordenada, conforme com o plano de cooperação da União em matéria de SRI referido no artigo 12.º.	1. Na sequência de um alerta rápido referido no artigo 10.º, ***os balcões únicos*** devem, após a avaliação das informações pertinentes, chegar a acordo ***sem demora injustificada*** quanto a uma resposta coordenada, conforme com o plano de cooperação da União em matéria de SRI referido no artigo 12.º.

Alteração 80

Proposta de diretiva
Artigo 12 – n.º 2 – alínea a) – travessão 1

Texto da Comissão	*Alteração*
– uma definição do formato e dos procedimentos para a recolha e a partilha ***pelas autoridades competentes*** de informações compatíveis e comparáveis sobre os riscos e incidentes,	– uma definição do formato e dos procedimentos para a recolha e a partilha ***pelos balcões únicos*** de informações compatíveis e comparáveis sobre os riscos e incidentes,

Alteração 81

Proposta de diretiva
Artigo 12 – n.º 3

Texto da Comissão	*Alteração*
3. O plano de cooperação da União em matéria de SRI deve ser adotado o mais tardar um ano após a entrada em vigor da presente diretiva e ser revisto periodicamente.	3. O plano de cooperação da União em matéria de SRI deve ser adotado o mais tardar um ano após a entrada em vigor da presente diretiva e ser revisto periodicamente. ***Os resultados de cada revisão são comunicados ao Parlamento Europeu.***

Alteração 82

Proposta de diretiva
Artigo 12 – n.º 3-A (novo)

Texto da Comissão	*Alteração*
	3-A. A Comissão deve disponibilizar um orçamento para o desenvolvimento do plano de cooperação da União em matéria de SRI.

Alteração 83

Proposta de diretiva
Artigo 13 – parágrafo 1

Texto da Comissão	*Alteração*
Sem prejuízo da possibilidade de a rede de cooperação manter uma cooperação informal a nível internacional, a União pode concluir acordos internacionais com países terceiros ou organizações internacionais, que permitam e organizem a sua participação em algumas atividades da rede de cooperação. ***Esses acordos devem ter em conta a necessidade de assegurar uma proteção adequada*** dos dados pessoais que circulam na rede de cooperação.	Sem prejuízo da possibilidade de a rede de cooperação manter uma cooperação informal a nível internacional, a União pode concluir acordos internacionais com países terceiros ou organizações internacionais, que permitam e organizem a sua participação em algumas atividades da rede de cooperação. ***Estes acordos especificam o procedimento de controlo a seguir para assegurar a proteção*** dos dados pessoais que circulam na rede de cooperação. ***O Parlamento Europeu deve ser informado sobre a negociação dos acordos, cuja transparência deve ser garantida. Qualquer transferência de dados pessoais para destinatários em países fora da União deve ser efetuada em conformidade com os artigos 25.º e 26.º da Diretiva 95/46/CE e o artigo 9.º do Regulamento (CE) n.º 45/2001.***

Justificação

Os acordos internacionais celebrados com outros países ou agências de segurança devem abranger, obrigatoriamente, um mecanismo de controlo da observância dos direitos civis. Além disso, deve ser exercido um controlo democrático efetivo dos acordos por parte do Parlamento Europeu, que deve ser informado atempadamente sobre o conteúdo das

negociações dos acordos.

Alteração 84

Proposta de diretiva
Artigo 14

Texto da Comissão	*Alteração*
1. Os Estados-Membros devem assegurar que ***as administrações públicas e*** os operadores do mercado adotem medidas técnicas e organizacionais adequadas para gerir os riscos que se colocam à segurança das redes e dos sistemas informáticos que controlam e utilizam na sua atividade. Tendo em conta ***os progressos técnicos***, essas medidas devem garantir um nível de segurança adequado em função do risco existente. Em particular, devem ser tomadas medidas para impedir e minimizar o impacto ***dos incidentes que afetam a sua rede e sistema informático*** nos serviços essenciais oferecidos, assegurando assim a continuidade dos serviços assentes nessas redes e sistemas.	1. Os Estados-Membros devem assegurar que os operadores do mercado adotem medidas técnicas e organizacionais adequadas para ***detetar e*** gerir ***eficazmente*** os riscos que se colocam à segurança das redes e dos sistemas informáticos que controlam e utilizam na sua atividade. Tendo em conta ***o desenvolvimento tecnológico***, essas medidas ***adequadas*** devem garantir um nível de segurança adequado em função do risco existente. Em particular, devem ser tomadas medidas para impedir ***incidentes que afetem a segurança das redes e dos sistemas informáticos*** e minimizar o ***seu*** impacto nos serviços essenciais oferecidos, assegurando assim a continuidade dos serviços assentes nessas redes e sistemas.
2. Os Estados-Membros devem assegurar que ***as administrações públicas e*** os operadores do mercado notifiquem às autoridades competentes os incidentes com impacto ***significativo*** na segurança dos serviços essenciais que fornecem.	2. Os Estados-Membros devem ***criar mecanismos para*** assegurar que os operadores do mercado notifiquem ***sem demora injustificada*** às autoridades competentes ***ou aos balcões únicos*** os incidentes com impacto na segurança ***ou continuidade*** dos serviços essenciais que fornecem. ***A notificação não deve expor a parte notificante a responsabilidades acrescidas. Para determinar a importância do impacto de um incidente, devem ser tidos em conta, entre outros, os seguintes parâmetros:*** ***(a) O número de utilizadores cujo serviço essencial é afetado;*** ***(b) A duração do incidente;*** ***(c) A repartição geográfica no que se refere à área afetada pelo incidente.***

Estes critérios devem ser especificados de forma mais aprofundada, de acordo com o artigo 8.º, n.º 3, alínea c-A) (nova).

2-A. As entidades não abrangidas pelo anexo II podem notificar incidentes, como especificado no artigo 14.°, n.° 2, voluntariamente.

2-B. O recetor de uma notificação de incidente deve, logo que possível, informar a entidade que comunicou o incidente sobre as medidas, decisões ou recomendações tomadas, bem como sobre todos os terceiros informados, e os protocolos de segurança e confidencialidade que regem a partilha de informações.

3. As exigências previstas nos n.°s 1 e 2 aplicam-se a todos os operadores do mercado que fornecem serviços na União Europeia.

3. As exigências previstas nos n.°s 1 e 2 aplicam-se a todos os operadores do mercado que fornecem serviços na União Europeia. ***Os operadores do mercado que não forneçam serviços na União Europeia podem notificar incidentes voluntariamente.***

3-A. Os Estados-Membros devem assegurar que os operadores de mercado notificam os incidentes a que se referem os n.ºs 1 e 2 às autoridades competentes ou aos balcões únicos no Estado-Membro onde o serviço essencial é afetado. Quando são afetados serviços essenciais em mais de um Estado-Membro, o balcão único que recebeu a notificação alerta, com base na informação fornecida pelo operador do mercado, os outros balcões únicos em causa. O operador do mercado deve ser informado, o mais rapidamente possível, sobre os outros balcões únicos que foram informados do incidente, bem como das medidas tomadas, resultados ou qualquer informação relevante para o incidente.

4. A autoridade competente ***pode*** informar o público ***ou exigir que as administrações públicas e os operadores do mercado o façam, caso considere que a revelação do incidente é do interesse público***. ***Uma vez***

4. ***Após consultar*** a autoridade competente ***e o operador de mercado em causa, o balcão único deve*** informar o público ***sobre incidentes individuais, caso seja necessário sensibilizar o público para***

por ano, ***a autoridade competente*** apresenta à rede de cooperação um relatório resumido sobre as notificações recebidas e as medidas tomadas em conformidade com o presente número.

evitar um incidente ou lidar com um incidente em curso, para permitir ao público atenuar os riscos para ele próprio decorrente do incidente, ou caso o operador de mercado, confrontado com um incidente, tenha recusado analisar uma vulnerabilidade estrutural grave associada ao incidente, sem demora injustificada. O balcão único deve justificar adequadamente a sua decisão. A autoridade competente ou o balcão único devem, se razoavelmente possível, apresentar aos operadores do mercado que comunicaram o incidente informações analisadas estrategicamente que ajudarão a resolver a ameaça à segurança. Duas vezes por ano, ***o balcão único*** apresenta à rede de cooperação um relatório resumido sobre as notificações recebidas e as medidas tomadas em conformidade com o presente número. ***Deverá existir um justo equilíbrio entre a publicidade dada aos incidentes individuais comunicados às autoridades competentes e aos balcões únicos e o interesse do público em ser informado sobre as ameaças que comportem eventuais danos de reputação e comerciais para os operadores do mercado que os comunicaram, podendo essa publicidade ocorrer apenas após consulta prévia.***

No caso de incidentes notificados à rede de cooperação referida no artigo 8.º, outras autoridades nacionais competentes não devem tornar públicas quaisquer informações recebidas relativas a riscos e incidentes sem autorização da autoridade competente notificante.

5. A Comissão tem poderes para adotar atos delegados em conformidade com o artigo 18.º para definir as circunstâncias em que as administrações públicas e os operadores do mercado são obrigados a notificar incidentes.

6. ***Sob reserva de quaisquer atos***

6. As autoridades competentes ***ou os***

delegados adotados ao abrigo do n.º 5, as autoridades competentes ***podem adotar*** orientações ***e, se for caso disso, emitir instruções*** sobre as circunstâncias em que ***as administrações públicas e*** os operadores do mercado são obrigados a notificar incidentes.	***balcões únicos adotam*** orientações sobre as circunstâncias em que os operadores do mercado são obrigados a notificar incidentes.
7. A Comissão tem poderes para definir, por meio de atos de execução, as modalidades e procedimentos aplicáveis para efeitos do disposto no n.° 2. Os referidos atos de execução são adotados em conformidade com o procedimento de exame referido no artigo 19.°, n.° 3.	7. A Comissão tem poderes para definir, por meio de atos de execução, as modalidades e procedimentos aplicáveis para efeitos do disposto no n.° 2. Os referidos atos de execução são adotados em conformidade com o procedimento de exame referido no artigo 19.°, n.° 3.
8. Os n.°s 1 e 2 não se aplicam às microempresas na aceção da Recomendação 2003/361/CE da Comissão, de 6 de maio de 2003, relativa à definição de micro, pequenas e médias empresas[35].	8. Os n.°s 1 e 2 não se aplicam às microempresas na aceção da Recomendação 2003/361/CE da Comissão, de 6 de maio de 2003, relativa à definição de micro, pequenas e médias empresas[35].
[35] JO L 124 de 20.05.2003, p. 36.	[35] JO L 124 de 20.05.2003, p. 36.

Alteração 85

Proposta de diretiva
Artigo 14 – n.º 4 – parágrafo 1 (novo)

Texto da Comissão	*Alteração*
	Além de comunicar às autoridades competentes, os operadores do mercado devem ser incentivados a divulgar incidentes que envolvam a sua sociedade nos relatórios financeiros voluntariamente.

Justificação

Os incidentes informáticos podem implicar grandes perdas financeiras e custos substanciais. Os acionistas e investidores devem ser informados sobre as consequências destes incidentes. Ao incentivar as empresas a divulgar os seus incidentes informáticos voluntariamente, poderão estimular-se os debates transversais relativos à probabilidade de incidentes futuros, a dimensão desses riscos, bem como a adequação das medidas preventivas tomadas para reduzir as violações da cibersegurança.

Alteração 86

Proposta de diretiva
Artigo 15

Texto da Comissão	*Alteração*
1. Os Estados-Membros devem assegurar que as autoridades competentes tenham ***todos*** os poderes necessários para ***investigar os casos de incumprimento por parte das administrações públicas ou dos operadores do mercado*** das obrigações que lhes incumbem por força do artigo 14.º, bem como os efeitos desse incumprimento na segurança das redes e sistemas informáticos.	1. Os Estados-Membros devem assegurar que as autoridades competentes ***e os balcões únicos*** tenham os poderes necessários para ***assegurar o cumprimento*** das obrigações que lhes incumbem por força do artigo 14.º, bem como os efeitos desse incumprimento na segurança das redes e sistemas informáticos.
2. Os Estados-Membros devem assegurar que as autoridades competentes tenham poderes para exigir aos operadores do mercado ***e às administrações públicas***:	2. Os Estados-Membros devem assegurar que as autoridades competentes ***e os balcões únicos*** tenham poderes para exigir aos operadores do mercado:
(a) que forneçam as informações necessárias para avaliar a segurança das suas redes e sistemas informáticos, incluindo documentação sobre as políticas de segurança;	(a) que forneçam as informações necessárias para avaliar a segurança das suas redes e sistemas informáticos, incluindo documentação sobre as políticas de segurança;
(b) que ***se submetam a*** uma auditoria de segurança efetuada por um organismo qualificado independente ou autoridade nacional e coloquem ***os resultados*** à disposição da autoridade competente.	(b) que ***apresentem provas da aplicação efetiva das políticas de segurança, nomeadamente os resultados de*** uma auditoria de segurança efetuada por ***auditores internos,*** um organismo qualificado independente ou autoridade nacional***,*** e coloquem ***as provas*** à disposição da autoridade competente ***ou do balcão único. Se necessário, a autoridade competente ou o balcão único podem exigir provas adicionais ou excecionalmente, apresentando a devida justificação, levar a cabo uma auditoria suplementar.***
	Ao transmitir o pedido, as autoridades competentes e os balcões únicos declaram a finalidade do mesmo e especificam de forma satisfatória a informação exigida.

3. Os Estados-Membros devem assegurar que as autoridades competentes tenham poderes para emitir instruções vinculativas ***aos*** operadores do mercado ***e às administrações públicas***.	3. Os Estados-Membros devem assegurar que as autoridades competentes ***e os balcões únicos*** tenham poderes para emitir instruções vinculativas ***a todos os*** operadores do mercado ***referidos no anexo II***.
4. As autoridades competentes devem ***notificar os incidentes que se suspeite serem de caráter criminoso grave às*** autoridades policiais e judiciais.	4. As autoridades competentes ***e os balcões únicos*** devem ***informar os operadores do mercado em causa acerca da possibilidade de mover uma ação penal junto das*** autoridades policiais e judiciais ***em caso de incidentes que se suspeite serem de caráter criminoso grave***.
5. As autoridades competentes devem trabalhar em estreita colaboração com as autoridades responsáveis pela proteção dos dados pessoais quando tratarem de incidentes de que resultou a violação desses dados.	5. ***Sem prejuízo da legislação aplicável em matéria de proteção dos dados,*** as autoridades competentes ***e os balcões únicos*** devem trabalhar em estreita colaboração com as autoridades responsáveis pela proteção dos dados pessoais quando tratarem de incidentes de que resultou a violação desses dados. ***Os balcões únicos e as autoridades encarregadas da proteção dos dados desenvolvem, em cooperação com a ENISA, mecanismos de intercâmbio de informações e um modelo único, ambos utilizados para as notificações, nos termos do artigo 14.º, n.º 2, da presente diretiva e do Regulamento n.º 95/46 do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.*** ***A Comissão pode adotar, por meio de atos de execução e tendo em conta quaisquer mecanismos de intercâmbio de informações e modelos únicos desenvolvidos pelos balcões únicos e pelas autoridades encarregadas da proteção dos dados, em cooperação com a ENISA, procedimentos para os mecanismos de intercâmbio de informações e o formato dos modelos únicos.***
6. Os Estados-Membros devem assegurar que todas as obrigações ***impostas às administrações públicas e*** aos operadores	6. Os Estados-Membros devem assegurar que todas as obrigações impostas e aos operadores do mercado ao abrigo do

do mercado ao abrigo do presente capítulo possam ser objeto de avaliação judicial.	presente capítulo possam ser objeto de avaliação judicial.

Alteração 87

Proposta de diretiva
Artigo 16

Texto da Comissão	*Alteração*
1. Para garantir a aplicação convergente do artigo 14.º, n.º 1, os Estados-Membros devem encorajar a utilização das normas e/ou especificações pertinentes para a segurança das redes e da informação.	1. Para garantir a aplicação convergente do artigo 14.º, n.º 1, os Estados-Membros***, sem exigirem a utilização de qualquer tecnologia em particular,*** devem encorajar a utilização das normas e/ou especificações ***abertas e interoperáveis da UE e internacionais*** pertinentes para a segurança das redes e da informação***, cumprindo a legislação da UE***.
2. A Comissão ***estabelece, por meio de atos de execução,*** uma lista das normas referidas no n.º 1, que será publicada no Jornal Oficial da União Europeia.	2. A Comissão ***confere um mandato a um organismo europeu de normalização relevante para, após consulta às partes interessadas pertinentes, estabelecer*** uma lista das normas ***e/ou especificações*** referidas no n.º 1, que será publicada no Jornal Oficial da União Europeia.

Alteração 88

Proposta de diretiva
Artigo 17 – n.º 1

Texto da Comissão	*Alteração*
1. Os Estados-Membros determinam o regime de sanções aplicável às violações das disposições nacionais aprovadas em execução da presente diretiva e adotam as medidas necessárias para assegurar a aplicação dessas disposições. As sanções impostas devem ser efetivas, proporcionadas e dissuasivas. O mais tardar até à data da transposição da presente diretiva, os Estados-Membros	1. Os Estados-Membros determinam o regime de sanções aplicável às violações ***negligentes ou intencionais*** das disposições nacionais aprovadas em execução da presente diretiva e adotam as medidas necessárias para assegurar a aplicação dessas disposições. As sanções impostas devem ser efetivas, proporcionadas e dissuasivas. O mais tardar até à data da transposição da

notificam à Comissão as referidas disposições, devendo notificá-la imediatamente de qualquer alteração posterior das mesmas.	presente diretiva, os Estados-Membros notificam à Comissão as referidas disposições, devendo notificá-la imediatamente de qualquer alteração posterior das mesmas.

Justificação

Deve ficar claro que as sanções só podem ser aplicadas às violações em que os operadores do mercado não conseguiram tomar todas as medidas que se esperava, razoavelmente, que tomassem. Caso contrário, os operadores do mercado poderiam ser desencorajados a notificar os incidentes.

Alteração 89

Proposta de diretiva
Artigo 17 – n.º 1-A (novo)

Texto da Comissão	*Alteração*
	1-A. Os Estados-Membros devem assegurar que as sanções referidas no n.º 1 do presente artigo apenas se apliquem quando o operador do mercado não tiver cumprido as suas obrigações nos termos do capítulo IV, deliberadamente ou por negligência grave.

Alteração 90

Proposta de diretiva
Artigo 18

Texto da Comissão	*Alteração*
Artigo 18.º	***Suprimido***
Exercício da delegação	
1. O poder de adotar os atos delegados conferido à Comissão está sujeito às condições estabelecidas no presente artigo.	
2. É conferido à Comissão o poder de adotar os atos delegados referidos nos artigos 9.º, n.º 2, 10.º, n.º 5, e 14.º, n.º 5. A	

Comissão elabora um relatório sobre a delegação de poderes o mais tardar nove meses antes do final do período de cinco anos. A delegação de poderes é tacitamente prorrogada por períodos de igual duração, salvo se o Parlamento Europeu ou o Conselho a tal se opuserem pelo menos três meses antes do final de cada período.

3. A delegação de poderes referida nos artigos 9.º, n.º 2, 10.º, n.º 5, e 14.º, n.º 5, pode ser revogada a qualquer momento pelo Parlamento Europeu ou pelo Conselho. Uma decisão de revogação põe termo à delegação dos poderes especificados nessa decisão. A revogação produz efeitos no dia seguinte ao da sua publicação no Jornal Oficial da União Europeia ou numa data posterior nela indicada. A decisão de revogação não afeta a validade de qualquer ato delegado em vigor.

4. Assim que adotar um ato delegado, a Comissão deve notificá-lo simultaneamente ao Parlamento Europeu e ao Conselho.

5. Os atos delegados adotados nos termos do artigo 9.º, n.º 2, do artigo 10.º, n.º 5, e do artigo 14.º, n.º 5, só entram em vigor se não tiverem sido formuladas objeções pelo Parlamento Europeu ou pelo Conselho no prazo de dois meses a contar da notificação desse ato ao Parlamento Europeu e ao Conselho, ou se, antes do termo desse prazo, o Parlamento Europeu e o Conselho informarem a Comissão de que não têm objeções a formular. O referido prazo pode ser prorrogado por dois meses por iniciativa do Parlamento Europeu ou do Conselho.

Alteração 91

Proposta de diretiva
Artigo 20 – parágrafo 1

Texto da Comissão	*Alteração*
A Comissão deve avaliar ***periodicamente*** a aplicação da presente diretiva e apresentar um relatório ao Parlamento Europeu e ao Conselho. O primeiro relatório deve ser apresentado no prazo de ***três*** anos após a data de transposição referida no artigo 21.º. Para o efeito, a Comissão pode solicitar aos Estados-Membros que lhe forneçam informações sem demora injustificada.	A Comissão deve avaliar ***de três em três anos*** a aplicação da presente diretiva e apresentar um relatório ao Parlamento Europeu e ao Conselho. O primeiro relatório deve ser apresentado no prazo de ***dois*** anos após a data de transposição referida no artigo 21.º. Para o efeito, a Comissão pode solicitar aos Estados-Membros que lhe forneçam informações sem demora injustificada.

Justificação

Por forma a acompanhar a evolução das ameaças e condições no âmbito da cibersegurança, o anexo II deve ser revisto e editado regularmente.

Alteração 92

Proposta de diretiva
Anexo I – título 1

Texto da Comissão	*Alteração*
Obrigações a cumprir e tarefas ***da equipa*** de resposta a emergências informáticas (CERT)	Obrigações a cumprir e tarefas ***das equipas*** de resposta a emergências informáticas (CERT)

Alteração 93

Proposta de diretiva
Anexo I – parágrafo 1 – parte introdutória

Texto da Comissão	*Alteração*
As obrigações a cumprir e as tarefas ***da*** CERT devem ser definidas de modo claro e adequado e apoiadas por políticas e/ou regulamentação nacionais. Devem incluir os seguintes elementos:	As obrigações a cumprir e as tarefas ***das*** CERT devem ser definidas de modo claro e adequado e apoiadas por políticas e/ou regulamentação nacionais. Devem incluir os seguintes elementos:

(Esta modificação aplica-se à totalidade do texto do anexo I)

Alteração 94

Proposta de diretiva
Anexo I – parágrafo 1 – ponto 1 – alínea a)

Texto da Comissão	*Alteração*
(a) ***A*** CERT ***deve*** garantir uma elevada disponibilidade dos seus serviços de comunicações, evitando as falhas pontuais e dispondo de vários meios para contactar e ser contactada. Além disso, os canais de comunicação devem ser claramente especificados e bem conhecidos da sua base de clientes e dos parceiros de cooperação.	(a) ***As*** CERT ***devem*** garantir uma elevada disponibilidade dos seus serviços de comunicações, evitando as falhas pontuais e dispondo de vários meios para contactarem e serem ***contactadas a qualquer momento***. Além disso, os canais de comunicação devem ser claramente especificados e bem conhecidos da sua base de clientes e dos parceiros de cooperação.

Alteração 95

Proposta de diretiva
Anexo I – parágrafo 1 – ponto 1 – alínea c)

Texto da Comissão	*Alteração*
(c) Os gabinetes ***da*** CERT e os sistemas informáticos de apoio devem estar situados em locais seguros.	(c) Os gabinetes ***das*** CERT e os sistemas informáticos de apoio devem estar situados em locais seguros ***com redes e sistemas informáticos seguros***.

Alteração 96

Proposta de diretiva
Anexo I – parágrafo 1 – ponto 2 – alínea a) – travessão 1

Texto da Comissão	*Alteração*
– Monitorizar os incidentes a nível nacional;	***– Detetar e*** monitorizar os incidentes a nível nacional;

Alteração 97

Proposta de diretiva
Anexo I – parágrafo 1 – ponto 2 – alínea a) – travessão 5-A (novo)

Texto da Comissão	*Alteração*
	- Participar ativamente em redes de cooperação CERT comunitárias e internacionais;

Alteração 98

Proposta de diretiva
Anexo II

Texto da Comissão	*Alteração*
Lista de operadores do mercado	Lista de operadores do mercado
1. Energia	1. Energia
	(a) Eletricidade
	- Fornecedores
	- Operadores da rede de distribuição e retalhistas que vendem aos consumidores finais
	- Operadores da rede de transporte de eletricidade
	- Operadores do mercado da eletricidade
	(b) Petróleo
	- Oleodutos e armazenamento de petróleo
	- Operadores de instalações de produção, refinamento e tratamento, armazenamento e transporte de petróleo
	(c) Gás
	- Fornecedores
	- Operadores da rede de distribuição e retalhistas que vendem aos consumidores finais
	- Operadores da rede de transporte de gás natural, operadores de sistemas de

	armazenamento e operadores de sistemas de GNL
	- Operadores de instalações de produção, refinamento e tratamento, de instalações de armazenamento e transporte de gás natural
	- Operadores do mercado do gás
2. Transportes	2. Transportes
	(a) Transporte rodoviário
	(i) Operadores de controlo da gestão do tráfego
	(ii) Serviços logísticos auxiliares:
	- depósito e armazenagem,
	- movimentação de carga, e
	- outras atividades auxiliares de transporte
	(b) Transporte ferroviário
	(i) Transportes ferroviários (gestores de infraestruturas, empresas integradas e operadores de transportes ferroviários)
	(ii) Operadores de controlo da gestão do tráfego
	(iii) Serviços logísticos auxiliares:
	- depósito e armazenagem,
	- movimentação de carga, e
	- outras atividades auxiliares de transporte
	(c) Transportes aéreos
	(i) Transportadores aéreos (transporte aéreo de mercadorias e passageiros)
	(ii) Aeroportos
	(iii) Operadores de controlo da gestão do tráfego
	(iv) Serviços logísticos auxiliares:
	- armazenagem,
	- movimentação de carga, e
	- outras atividades auxiliares de

	transporte
	(d) Transportes marítimos
	(i) Transportadores marítimos (companhias de transporte marítimo, costeiro e em águas interiores de passageiros e companhias de transporte marítimo, costeiro e em águas interiores de mercadorias)
	(ii) Portos
	(iii) Operadores de controlo da gestão do tráfego
	(iv) Serviços logísticos auxiliares:
	- depósito e armazenagem,
	- movimentação de carga, e
	- outras atividades auxiliares de transporte
	2-A. Serviços hídricos
3. Setor bancário: instituições de crédito, em conformidade com o artigo 4.º, n.º 1, da Diretiva 2006/48/CE	3. Setor bancário: instituições de crédito, em conformidade com o artigo 4.º, n.º 1, da Diretiva 2006/48/CE
4. Infraestruturas do mercado financeiro: ***bolsas*** e contrapartes centrais	4. Infraestruturas do mercado financeiro: ***mercados regulamentados, sistemas de negociação multilateral, sistemas de negociação organizados*** e contrapartes centrais
5. Setor da saúde: instalações de prestação de cuidados de saúde (nomeadamente hospitais e clínicas privadas) e outras entidades envolvidas na prestação de cuidados de saúde	5. Setor da saúde: instalações de prestação de cuidados de saúde (nomeadamente hospitais e clínicas privadas) e outras entidades envolvidas na prestação de cuidados de saúde
	6. TIC: Serviços de computação em nuvem utilizados por um operador para fornecer qualquer dos serviços enumerados no ponto 1-5.
	Esta lista deve ser revista de dois em dois anos.

PROCESSO

Título	Elevado nível comum de segurança das redes e da informação em toda a União
Referências	COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)
Comissão competente quanto ao fundo Data de comunicação em sessão	IMCO 15.4.2013
Parecer emitido por Data de comunicação em sessão	ITRE 15.4.2013
Comissões associadas - data de comunicação em sessão	12.9.2013
Relator(a) de parecer Data de designação	Pilar del Castillo Vera 23.5.2013
Exame em comissão	14.10.2013 4.11.2013
Data de aprovação	16.12.2013
Resultado da votação final	+: 36 –: 5 0: 0
Deputados presentes no momento da votação final	Amelia Andersdotter, Josefa Andrés Barea, Bendt Bendtsen, Fabrizio Bertot, Reinhard Bütikofer, Maria Da Graça Carvalho, Giles Chichester, Pilar del Castillo Vera, Christian Ehler, Vicky Ford, Adam Gierek, Norbert Glante, Robert Goebbels, Fiona Hall, Romana Jordan, Philippe Lamberts, Marisa Matias, Judith A. Merkies, Angelika Niebler, Jaroslav Paška, Vittorio Prodi, Miloslav Ransdorf, Herbert Reul, Teresa Riera Madurell, Paul Rübig, Amalia Sartori, Salvador Sedó i Alabart, Evžen Tošenovský, Claude Turmes, Marita Ulvskog, Vladimir Urutchev
Suplente(s) presente(s) no momento da votação final	Daniel Caspary, António Fernando Correia de Campos, Françoise Grossetête, Roger Helmer, Jolanta Emilia Hibner, Seán Kelly, Eija-Riitta Korhola, Holger Krahmer, Zofija Mazej Kukovič, Silvia-Adriana Ţicău, Lambert van Nistelrooij
Suplente(s) (nº 2 do art. 187º) presente(s) no momento da votação final	María Auxiliadora Correa Zamora