Parlamento Europeu
2019-2024

Comissão do Mercado Interno e da Proteção dos Consumidores

2020/0359(COD)

14.7.2021

PARECER

da Comissão do Mercado Interno e da Proteção dos Consumidores

dirigido à Comissão da Indústria, da Investigação e da Energia

sobre a proposta de diretiva do Parlamento Europeu e do Conselho relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União e que revoga a Diretiva (UE) 2016/1148
(COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

Relator de parecer: Morten Løkkegaard

PA_Legam

JUSTIFICAÇÃO SUCINTA

De um modo geral, o relator congratula-se com a proposta legislativa de diretiva relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União (SRI 2). Em sua opinião, num mundo cada vez mais digitalizado, a segurança em linha é fundamental para garantir um ambiente digital seguro, assim como o funcionamento do mercado único, onde os consumidores e os operadores económicos podem agir livremente.

A proposta SRI 2 constitui uma melhoria significativa em relação à Diretiva (UE) 2016/1148 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União (SRI 1). Enumera as principais deficiências da SRI 1, como o baixo nível de ciber-resiliência das empresas e dos setores, bem como as diferenças em termos de resiliência e os baixos níveis de conhecimento situacional comum e de resposta conjunta a situações de crise nos e entre os Estados-Membros. O relator saúda a ambição de corrigir estas deficiências na Diretiva SRI 2.

Âmbito

O relator congratula-se com o âmbito alargado da Diretiva SRI 2, em particular com a inclusão de novos setores, como a administração pública. A lista precisa de setores e serviços incluídos reduzirá sem dúvida o poder discricionário dos Estados-Membros na definição das entidades concretas sujeitas à diretiva, reduzindo, consequentemente, a fragmentação no mercado único.

Nos setores e serviços abrangidos, a Comissão propôs a aplicação da regra da limitação com base na dimensão como critério uniforme para determinar as entidades que se enquadram no âmbito de aplicação da diretiva. Este critério apresenta incontestavelmente a vantagem de garantir a segurança jurídica, reduzindo ao mesmo tempo as divergências entre os Estados-Membros.

No entanto, embora saúde o alargamento do âmbito de aplicação setorial, o relator é de opinião que este critério geral deve ser conjugado com uma avaliação da criticidade das entidades dentro de cada setor. Esta articulação permitiria deixar de fora do âmbito da diretiva as entidades de média e grande dimensão que, após uma avaliação dos riscos, sejam consideradas de baixo nível de criticidade e dependência de outras entidades de outro modo críticas.

O relator salienta que tal não deve ser considerado uma porta aberta a uma interpretação discrepante entre os Estados-Membros. Para garantir que isto não contribui para uma aplicação fragmentada entre os Estados-Membros, a Comissão é incentivada a emitir orientações claras a este respeito.

Por último, embora acolha com agrado a exclusão das micro e pequenas empresas do âmbito de aplicação, o relator é de opinião que é necessário incentivar a sua inclusão voluntária, uma vez que as micro e pequenas entidades também estão sujeitas aos ciberataques e são afetadas por estes.

Quadros regulamentares coordenados em matéria de cibersegurança

O relator congratula-se com o capítulo que define os diferentes elementos das estratégias nacionais de cibersegurança e as respetivas ferramentas de gestão de crises. No quadro da sua

estratégia nacional de cibersegurança, propõe-se que os Estados-Membros adotem uma política que promova a utilização da criptografia e da cifragem, nomeadamente pelas PME.

O relator saúda a criação de um registo europeu de vulnerabilidade pela ENISA, mas considera importante que o registo respeite o sigilo comercial e os segredos comerciais e não imponha encargos desnecessários às entidades.

Cooperação entre os Estados-Membros

Acolhe-se com especial agrado a cooperação mais estruturada entre os Estados-Membros no âmbito do grupo de cooperação, a rede de CSIRT e o recém-criado grupo para incidentes em grande escala na proposta SRI 2. No entanto, é necessário garantir um maior nível de confiança e vontade de trocar informações entre os Estados-Membros, uma vez que a eficácia desta cooperação desempenha um papel fundamental para garantir um elevado nível de cibersegurança na UE.

À luz desta posição, foram elaboradas várias alterações destinadas a reforçar o papel das redes. O relator considera, nomeadamente, que a análise pelos pares é uma forma eficaz de aumentar a confiança mútua dos Estados-Membros, defendendo que estes devem desempenhar um papel crucial na avaliação da eficácia das políticas de cibersegurança de cada Estado-Membro.

Gestão dos riscos de cibersegurança

O alargamento da avaliação dos riscos a toda a cadeia de fornecimento (artigos 18.º e 19.º) é de louvar, mas o relator salienta que este ponto deve ser clarificado a fim de fornecer orientações claras às entidades sujeitas a este requisito e aos Estados-Membros quando procedem a uma avaliação coordenada dos riscos de segurança de setores ou cadeias de fornecimento especialmente críticos.

Obrigações de notificação

O relator considera que deve existir maior clareza sobre pontos específicos da diretiva revista, principalmente no que respeita a algumas das obrigações impostas às empresas no âmbito da proposta SRI 2. O relator procurou reduzir a burocracia e facilitar o cumprimento das novas regras pelas empresas, tendo em mente o objetivo final de uma aplicação eficaz da diretiva.

A proposta do relator é que o prazo sugerido de 24 horas nas obrigações de notificação para as primeiras notificações seja alargado para 72 horas, a fim de que as empresas possam fazer face eficazmente ao ataque à cibersegurança em curso antes da notificação. Além disso, propõe-se que seja suprimida qualquer referência à notificação obrigatória dos denominados «incidentes potenciais».

ALTERAÇÕES

A Comissão do Mercado Interno e da Proteção dos Consumidores insta a Comissão da Indústria, da Investigação e da Energia, competente quanto à matéria de fundo, a ter em conta

as seguintes alterações:

Alteração 1
Proposta de diretiva
Considerando 5

Texto da Comissão	*Alteração*
(5) Todas essas divergências implicam uma fragmentação do mercado interno e são suscetíveis de prejudicar o seu funcionamento, afetando, em especial, a prestação transfronteiriça de serviços e o nível de resiliência em matéria de cibersegurança devido à aplicação de normas diferentes. A presente diretiva visa eliminar essas divergências tão profundas entre os Estados-Membros, em especial estabelecendo regras mínimas relativas ao funcionamento de um quadro regulamentar coordenado, criando mecanismos para uma cooperação eficaz entre as autoridades responsáveis em cada Estado-Membro, atualizando a lista de setores e atividades sujeitas a obrigações em matéria de cibersegurança e prevendo vias de recurso e sanções eficazes que contribuam para a execução efetiva dessas obrigações. Por conseguinte, a Diretiva (UE) 2016/1148 deve ser revogada e substituída pela presente diretiva.	(5) Todas essas divergências implicam uma fragmentação do mercado interno e são suscetíveis de prejudicar o seu funcionamento, afetando, em especial, a prestação transfronteiriça de serviços e o nível de resiliência em matéria de cibersegurança devido à aplicação de normas diferentes. A presente diretiva visa eliminar essas divergências tão profundas entre os Estados-Membros ***e reforçar o mercado interno***, em especial estabelecendo regras mínimas relativas ao funcionamento de um quadro regulamentar coordenado, criando mecanismos para uma cooperação eficaz entre as autoridades responsáveis em cada Estado-Membro, atualizando a lista de setores e atividades sujeitas a obrigações em matéria de cibersegurança e prevendo vias de recurso e sanções eficazes que contribuam para a execução efetiva dessas obrigações. Por conseguinte, a Diretiva (UE) 2016/1148 deve ser revogada e substituída pela presente diretiva.

Alteração 2
Proposta de diretiva
Considerando 6-A (novo)

Texto da Comissão	*Alteração*
	(6-A) A diretiva aplica-se sem prejuízo das regras estabelecidas pela legislação da União aplicável à proteção dos dados pessoais.

Alteração 3
Proposta de diretiva
Considerando 9

Texto da Comissão	*Alteração*
(9) No entanto, as micro ou pequenas entidades que preencham certos critérios que indiciem o desempenho de um papel fundamental para as economias ou sociedades dos Estados-Membros ou para setores ou tipos de serviços específicos devem também estar abrangidas pela presente diretiva. Os Estados-Membros devem ser incumbidos de elaborar uma lista de tais entidades e apresentá-la à Comissão.	(9) No entanto, as micro ou pequenas entidades que preencham certos critérios que indiciem o desempenho de um papel fundamental para as economias ou sociedades dos Estados-Membros ou para setores ou tipos de serviços específicos devem também estar abrangidas pela presente diretiva. Os Estados-Membros devem ser incumbidos de elaborar uma lista de tais entidades e apresentá-la à Comissão. ***A Comissão fornece orientações claras sobre os critérios utilizados para determinar as micro ou pequenas entidades consideradas essenciais ou importantes, sobretudo nos casos em que essas entidades prestem serviços em vários Estados-Membros.***

Alteração 4
Proposta de diretiva
Considerando 10

Texto da Comissão	*Alteração*
(10) Em cooperação com o grupo de cooperação, a Comissão ***pode*** emitir orientações sobre a aplicação dos critérios relativos às micro e pequenas empresas.	(10) Em cooperação com o grupo de cooperação, a Comissão ***deve*** emitir orientações sobre a aplicação dos critérios relativos às micro e pequenas empresas.

Alteração 5
Proposta de diretiva
Considerando 12-A (novo)

Texto da Comissão	*Alteração*
	(12-A) O alargamento do âmbito de aplicação da presente diretiva implica a inclusão de entidades sujeitas a regulamentação setorial. A fim de evitar qualquer duplicação ou encargos

regulamentares, a Comissão deve assegurar a coerência com a presente diretiva dos atos setoriais que exigem que as entidades essenciais ou importantes adotem medidas de gestão dos riscos de cibersegurança ou comuniquem a ocorrência de incidentes ou de ciberameaças significativas.

Alteração 6
Proposta de diretiva
Considerando 12-B (novo)

Texto da Comissão	*Alteração*
	(12-B) A Comissão publica orientações claras que acompanhem a presente diretiva a fim de garantir a harmonização da aplicação em todos os Estados-Membros e evitar a fragmentação.

Alteração 7
Proposta de diretiva
Considerando 12-C (novo)

Texto da Comissão	*Alteração*
	(12-C) A Comissão emite também orientações para apoiar os Estados-Membros na correta aplicação das disposições relativas ao âmbito de aplicação, e para avaliar a proporcionalidade das obrigações estabelecidas na presente diretiva tendo em conta a importância das entidades abrangidas pelo âmbito de aplicação, especialmente quando este se aplica a entidades com modelos de negócio ou ambientes operacionais complexos, em que uma entidade pode simultaneamente preencher os critérios atribuídos a entidades essenciais e a entidades importantes ou pode simultaneamente desenvolver atividades das quais algumas são abrangidas pelo âmbito de aplicação da presente diretiva e outras não. Nos

casos em que a atividade principal de uma entidade não seja abrangida pelo âmbito de aplicação da presente diretiva, mas qualquer outra atividade secundária o seja, as disposições devem aplicar-se apenas à função ou unidade dessa entidade que é abrangida pelo âmbito de aplicação da presente diretiva.

Alteração 8
Proposta de diretiva
Considerando 14

Texto da Comissão	*Alteração*
(14) Tendo em conta as interligações entre a cibersegurança e a segurança física das entidades, importa assegurar uma abordagem coerente entre a Diretiva (UE) XXX/XXX do Parlamento Europeu e do Conselho[17] e a presente diretiva. Para tal, os Estados-Membros devem assegurar que as entidades críticas e as entidades equivalentes nos termos da Diretiva (UE) XXX/XXX sejam consideradas entidades essenciais no âmbito da presente diretiva. Os Estados-Membros devem ainda garantir que as suas estratégias de cibersegurança prevejam um quadro político para o reforço da cooperação entre a autoridade competente ao abrigo da presente diretiva e a autoridade competente ao abrigo da Diretiva (UE) XXX/XXX no contexto da partilha de informações sobre incidentes e ciberameaças e do exercício de funções de supervisão. As autoridades referidas nas duas diretivas devem cooperar e trocar informações, especialmente no que respeita à identificação de entidades críticas, ciberameaças, riscos de cibersegurança e incidentes que afetem entidades críticas, bem como sobre as medidas de cibersegurança adotadas por entidades críticas. A pedido das autoridades competentes ao abrigo da Diretiva (UE) XXX/XXX, as autoridades competentes ao abrigo da presente diretiva	(14) Tendo em conta as interligações entre a cibersegurança e a segurança física das entidades, importa assegurar uma abordagem coerente entre a Diretiva (UE) XXX/XXX do Parlamento Europeu e do Conselho[17] e a presente diretiva. Para tal, os Estados-Membros devem assegurar que as entidades críticas e as entidades equivalentes nos termos da Diretiva (UE) XXX/XXX sejam consideradas entidades essenciais no âmbito da presente diretiva. Os Estados-Membros devem ainda garantir que as suas estratégias ***nacionais*** de cibersegurança prevejam um quadro político para o reforço da cooperação entre a autoridade competente ao abrigo da presente diretiva e a autoridade competente ao abrigo da Diretiva (UE) XXX/XXX no contexto da ***notificação de incidentes, da*** partilha de informações sobre incidentes***, quase incidentes*** e ciberameaças e do exercício de funções de supervisão. As autoridades referidas nas duas diretivas devem cooperar e trocar informações, especialmente no que respeita à identificação de entidades críticas, ciberameaças, riscos de cibersegurança e incidentes que afetem entidades críticas, bem como sobre as medidas de cibersegurança adotadas por entidades críticas. A pedido das autoridades competentes ao abrigo da

devem poder exercer as suas competências de supervisão e execução coerciva em relação a uma entidade essencial identificada como crítica. Ambas as autoridades devem cooperar e trocar informações para este fim.	Diretiva (UE) XXX/XXX, as autoridades competentes ao abrigo da presente diretiva devem poder exercer as suas competências de supervisão e execução coerciva em relação a uma entidade essencial identificada como crítica. Ambas as autoridades devem cooperar e trocar informações para este fim.
[17] [Serviço das Publicações: inserir o título completo e a referência de publicação no JO quando forem conhecidos].	[17] [Serviço das Publicações: inserir o título completo e a referência de publicação no JO quando forem conhecidos].

Alteração 9
Proposta de diretiva
Considerando 15

Texto da Comissão	*Alteração*
(15) A proteção e conservação de um sistema de nomes de domínio (DNS) fiável, resiliente e seguro é um fator crucial para manter a integridade da Internet, sendo igualmente essencial para a continuidade e a estabilidade do seu funcionamento, das quais a sociedade e a economia digital dependem. Consequentemente, a presente diretiva deve ser aplicável a todos os prestadores de serviços de DNS ao longo da cadeia de resolução do DNS, incluindo operadores de servidores de nomes da zona raiz, servidores de nomes de domínio de topo, servidores de nomes com autoridade para nomes de domínio e servidores recursivos.	(15) A proteção e conservação de um sistema de nomes de domínio (DNS) fiável, resiliente e seguro é um fator crucial para manter a integridade da Internet, sendo igualmente essencial para a continuidade e a estabilidade do seu funcionamento, das quais a sociedade***, o mercado interno*** e a economia digital dependem. Consequentemente, a presente diretiva deve ser aplicável a todos os prestadores de serviços de DNS ao longo da cadeia de resolução do DNS, incluindo operadores de servidores de nomes da zona raiz, servidores de nomes de domínio de topo, servidores de nomes com autoridade para nomes de domínio e servidores recursivos***, bem como aos prestadores de serviços de proteção da privacidade ou de registo de servidores intermediários, corretores ou revendedores de domínios e quaisquer outros serviços relacionados com o registo de nomes de domínio***.

Alteração 10
Proposta de diretiva
Considerando 20

Texto da Comissão	*Alteração*
(20) Estas crescentes interdependências resultam de uma rede de prestação de serviços com um caráter cada vez mais transfronteiriço e interdependente, que utiliza infraestruturas essenciais em toda a União nos setores da energia, dos transportes, das infraestruturas digitais, da água potável e das águas residuais, da saúde, de certos aspetos da administração pública, bem como no setor do espaço no que se refere à prestação de certos serviços que dependem de infraestruturas terrestres detidas, geridas e operadas por Estados-Membros ou por entidades privadas, não abrangendo, portanto, as infraestruturas detidas, geridas ou operadas pela União ou em seu nome no âmbito dos seus programas espaciais. Em virtude dessas interdependências, qualquer perturbação, mesmo que inicialmente confinada a uma entidade ou a um setor, pode ter repercussões mais vastas e causar impactos negativos generalizados e duradouros na prestação de serviços em todo o mercado interno. A pandemia de COVID-19 revelou a vulnerabilidade das nossas sociedades, cada vez mais interdependentes, perante riscos com baixa probabilidade de ocorrência.	(20) Estas crescentes interdependências resultam de uma rede de prestação de serviços com um caráter cada vez mais transfronteiriço e interdependente, que utiliza infraestruturas essenciais em toda a União nos setores da energia, dos transportes, das infraestruturas digitais, da água potável e das águas residuais, da saúde, de certos aspetos da administração pública, bem como no setor do espaço no que se refere à prestação de certos serviços que dependem de infraestruturas terrestres detidas, geridas e operadas por Estados-Membros ou por entidades privadas, não abrangendo, portanto, as infraestruturas detidas, geridas ou operadas pela União ou em seu nome no âmbito dos seus programas espaciais. Em virtude dessas interdependências, qualquer perturbação, mesmo que inicialmente confinada a uma entidade ou a um setor, pode ter repercussões mais vastas e causar impactos negativos generalizados e duradouros na prestação de serviços em todo o mercado interno. A pandemia de COVID-19 revelou a vulnerabilidade das nossas sociedades, cada vez mais interdependentes, perante riscos com baixa probabilidade de ocorrência***, bem como a necessidade de proteger o mercado interno por meio de estratégias e ações conjuntas a nível da União***.

Alteração 11
Proposta de diretiva
Considerando 23

Texto da Comissão	*Alteração*
(23) As autoridades competentes ou as CSIRT devem receber as notificações de incidentes efetuadas pelas entidades de forma eficaz e eficiente. Os pontos de contacto únicos devem ser incumbidos do reencaminhamento das notificações de	(23) As autoridades competentes ou as CSIRT devem receber as notificações de incidentes efetuadas pelas entidades de forma ***normalizada,*** eficaz e eficiente. Os pontos de contacto únicos devem ser incumbidos do reencaminhamento das

incidentes para os pontos de contacto únicos de outros Estados-Membros afetados. A fim de garantir a existência de um ponto de entrada único ***ao nível das autoridades de*** cada Estado-Membro, os pontos de contacto únicos devem ser também os destinatários de informações sobre incidentes respeitantes a entidades do setor financeiro fornecidas pelas autoridades competentes ao abrigo do Regulamento XXXX/XXXX, informações essas que deverão poder transmitir, conforme adequado, às autoridades nacionais competentes nesse domínio ou às CSIRT ao abrigo da presente diretiva.	notificações de incidentes para os pontos de contacto únicos de outros Estados-Membros afetados. A fim de garantir a existência de um ponto de entrada único ***em*** cada Estado-Membro, os pontos de contacto únicos devem ser também os destinatários de informações sobre incidentes respeitantes a entidades do setor financeiro fornecidas pelas autoridades competentes ao abrigo do Regulamento XXXX/XXXX, informações essas que deverão poder transmitir, conforme adequado, às autoridades nacionais competentes nesse domínio ou às CSIRT ao abrigo da presente diretiva.

Alteração 12
Proposta de diretiva
Considerando 25

Texto da Comissão	*Alteração*
(25) No que respeita a dados pessoais, as CSIRT devem poder facultar, em conformidade com o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho[19], em nome ou a pedido de uma entidade ao abrigo da presente diretiva, uma análise ***proativa*** da rede e dos sistemas de segurança utilizados para prestarem os seus serviços. Os Estados-Membros devem procurar garantir que todas as CSIRT setoriais possuam o mesmo nível de capacidades técnicas. Os Estados-Membros poderão solicitar a assistência da Agência da União Europeia para a Cibersegurança (ENISA) no desenvolvimento de CSIRT nacionais.	(25) ***Para detetar, mitigar e prevenir ameaças específicas*** no que respeita a dados pessoais, as CSIRT devem poder facultar, em conformidade com o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho[19], em nome ou a pedido de uma entidade ao abrigo da presente diretiva, uma análise da rede e dos sistemas de segurança utilizados para prestarem os seus serviços. Os Estados-Membros devem procurar garantir que todas as CSIRT setoriais possuam o mesmo nível de capacidades técnicas. Os Estados-Membros poderão solicitar a assistência da Agência da União Europeia para a Cibersegurança (ENISA) no desenvolvimento de CSIRT nacionais.
[19] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral	[19] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral

sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1).

sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1).

Alteração 13
Proposta de diretiva
Considerando 26-A (novo)

Texto da Comissão

Alteração

(26-A) No âmbito das suas estratégias nacionais de cibersegurança, os Estados-Membros devem adotar políticas de promoção e integração de sistemas inteligentes na prevenção e deteção de incidentes e ameaças de cibersegurança. Os Estados-Membros devem, em conformidade com as suas estratégias nacionais de cibersegurança, aplicar políticas orientadas para a sensibilização para a cibersegurança e a ciberliteracia, com vista a proteger os consumidores. Ao adotarem estratégias nacionais de cibersegurança, os Estados-Membros devem prever quadros políticos para abordar a questão do acesso lícito à informação.

Alteração 14
Proposta de diretiva
Considerando 27

Texto da Comissão

Alteração

(27) Nos termos do anexo da Recomendação (UE) 2017/1548 da Comissão, sobre a resposta coordenada a incidentes e crises de cibersegurança em grande escala («plano de ação»)[20], entende-se por incidente em larga escala um incidente com um impacto significativo em, pelo menos, dois Estados-Membros ou que cause perturbações tão extensas que ultrapassem a capacidade de resposta de um Estado-Membro. Consoante a sua causa e o seu impacto, os incidentes em grande escala poderão agravar-se e

(27) Nos termos do anexo da Recomendação (UE) 2017/1548 da Comissão, sobre a resposta coordenada a incidentes e crises de cibersegurança em grande escala («plano de ação»)[20], entende-se por incidente em larga escala um incidente com um impacto significativo em, pelo menos, dois Estados-Membros ou que cause perturbações tão extensas que ultrapassem a capacidade de resposta de um Estado-Membro***, pondo assim em risco o mercado interno***. Consoante a sua causa e o seu impacto, os incidentes em grande

transformar-se em verdadeiras crises que impeçam o correto funcionamento do mercado interno. Tendo em conta o vasto alcance e, em muitos casos, o caráter transfronteiriço de tais incidentes, é importante que os Estados-Membros e as instituições, organismos e agências competentes da União cooperem a nível técnico, operacional e político para coordenarem eficazmente a resposta em toda a União.

[20] Recomendação (UE) 2017/1584 da Comissão, de 13 de setembro de 2017, sobre a resposta coordenada a incidentes e crises de cibersegurança em grande escala (JO L 239 de 19.9.2017, p. 36).

escala poderão agravar-se e transformar-se em verdadeiras crises que impeçam o correto funcionamento do mercado interno. Tendo em conta o vasto alcance e, em muitos casos, o caráter transfronteiriço de tais incidentes, é importante que os Estados-Membros e as instituições, organismos e agências competentes da União cooperem a nível técnico, operacional e político para coordenarem eficazmente a resposta em toda a União.

[20] Recomendação (UE) 2017/1584 da Comissão, de 13 de setembro de 2017, sobre a resposta coordenada a incidentes e crises de cibersegurança em grande escala (JO L 239 de 19.9.2017, p. 36).

Alteração 15
Proposta de diretiva
Considerando 28

Texto da Comissão	*Alteração*
(28) Uma vez que a exploração das vulnerabilidades das redes e dos sistemas de informação pode causar perturbações e danos consideráveis, a celeridade na identificação e correção de tais vulnerabilidades é um fator importante na redução dos riscos de cibersegurança. As entidades que desenvolvem esses sistemas devem, por conseguinte, estabelecer procedimentos adequados para fazer face a vulnerabilidades quando estas sejam detetadas. Uma vez que as vulnerabilidades são frequentemente detetadas e notificadas (divulgadas) por terceiros (entidades notificadoras), o fabricante ou fornecedor de produtos ou prestador de serviços de TIC deve adotar igualmente os procedimentos necessários para receber informações sobre vulnerabilidades fornecidas por terceiros. Nesta matéria, as normas internacionais ISO/IEC 30111 e ISO/IEC 29417 fornecem orientações sobre o tratamento de vulnerabilidades e a	(28) Uma vez que a exploração das vulnerabilidades das redes e dos sistemas de informação pode causar perturbações e danos consideráveis ***a empresas e consumidores***, a celeridade na identificação e correção de tais vulnerabilidades é um fator importante na redução dos riscos de cibersegurança. As entidades que desenvolvem esses sistemas devem, por conseguinte, estabelecer procedimentos adequados para fazer face a vulnerabilidades quando estas sejam detetadas. Uma vez que as vulnerabilidades são frequentemente detetadas e notificadas (divulgadas) por terceiros (entidades notificadoras), o fabricante ou fornecedor de produtos ou prestador de serviços de TIC deve adotar igualmente os procedimentos necessários para receber informações sobre vulnerabilidades fornecidas por terceiros. Nesta matéria, as normas internacionais ISO/IEC 30111 e ISO/IEC 29417 fornecem orientações

divulgação de vulnerabilidades, respetivamente. No que respeita à divulgação de vulnerabilidades, a coordenação entre as entidades notificadoras e os fabricantes ou fornecedores de produtos ou prestadores de serviços de TIC assume especial importância. A divulgação coordenada de vulnerabilidades especifica um processo estruturado mediante o qual as vulnerabilidades são notificadas às organizações de uma forma que lhes permite diagnosticar e corrigir as ***vulnerabilidade*** antes de serem divulgadas informações pormenorizadas sobre as mesmas a terceiros ou ao público. A divulgação coordenada de vulnerabilidades deve abranger também a coordenação entre a entidade notificadora e a organização no que respeita ao momento da correção e da publicação das vulnerabilidades.	sobre o tratamento de vulnerabilidades e a divulgação de vulnerabilidades, respetivamente. No que respeita à divulgação de vulnerabilidades, a coordenação entre as entidades notificadoras e os fabricantes ou fornecedores de produtos ou prestadores de serviços de TIC assume especial importância. A divulgação coordenada de vulnerabilidades especifica um processo estruturado mediante o qual as vulnerabilidades são notificadas às organizações de uma forma que lhes permite diagnosticar e corrigir as ***vulnerabilidades*** antes de serem divulgadas informações pormenorizadas sobre as mesmas a terceiros ou ao público. A divulgação coordenada de vulnerabilidades deve abranger também a coordenação entre a entidade notificadora e a organização no que respeita ao momento da correção e da publicação das vulnerabilidades.

Alteração 16
Proposta de diretiva
Considerando 28-A (novo)

Texto da Comissão	*Alteração*
	(28-A) A Comissão, a ENISA e os Estados-Membros devem continuar a promover o alinhamento internacional com as normas e boas práticas do setor existentes no âmbito da gestão de riscos, por exemplo, nos domínios das avaliações de segurança da cadeia de fornecimento, da partilha de informações e da divulgação de vulnerabilidades.

Alteração 17
Proposta de diretiva
Considerando 30

Texto da Comissão	*Alteração*
(30) O acesso em tempo útil a informações fidedignas sobre vulnerabilidades que afetem produtos e serviços de TIC contribui para melhorar a gestão dos riscos de cibersegurança. Nesse contexto, as fontes de informações públicas sobre vulnerabilidades constituem um instrumento importante não só para as entidades e os seus utilizadores, mas também para as autoridades nacionais competentes e as CSIRT. Por este motivo, a ENISA deve criar ***um registo*** de vulnerabilidades ***no*** qual as entidades essenciais e importantes e os respetivos fornecedores, bem como as entidades não abrangidas pelo âmbito da presente diretiva, possam, a título voluntário, divulgar vulnerabilidades e fornecer ***as*** informações conexas que permitam aos utilizadores tomarem medidas de atenuação adequadas.	(30) O acesso em tempo útil a informações fidedignas sobre vulnerabilidades que afetem produtos e serviços de TIC contribui para melhorar a gestão dos riscos de cibersegurança. Nesse contexto, as fontes de informações públicas sobre vulnerabilidades constituem um instrumento importante não só para as entidades e os seus utilizadores, mas também para as autoridades nacionais competentes e as CSIRT. Por este motivo, a ENISA deve criar ***uma base de dados*** de vulnerabilidades ***na*** qual as entidades essenciais e importantes e os respetivos fornecedores, bem como as entidades não abrangidas pelo âmbito da presente diretiva, possam, a título voluntário, divulgar vulnerabilidades e fornecer informações conexas que permitam aos utilizadores tomarem medidas de atenuação adequadas.

Alteração 18
Proposta de diretiva
Considerando 31

Texto da Comissão	*Alteração*
(31) Embora já existam bases de dados ou registos de vulnerabilidades semelhantes, as entidades responsáveis pelo seu alojamento e manutenção não estão estabelecidas na União. ***Um registo europeu*** de vulnerabilidades ***mantido*** pela ENISA melhoraria a transparência do processo de publicação antes de a vulnerabilidade ser oficialmente divulgada, bem como a resiliência em casos de perturbação ou interrupção da prestação de serviços semelhantes. A fim de evitar a duplicação de esforços e de assegurar, tanto quanto possível, a complementaridade, é importante que a ENISA explore a possibilidade de celebrar acordos de cooperação estruturados com	(31) Embora já existam bases de dados ou registos de vulnerabilidades semelhantes, as entidades responsáveis pelo seu alojamento e manutenção não estão estabelecidas na União. ***Uma base de dados europeia*** de vulnerabilidades ***mantida*** pela ENISA melhoraria a transparência do processo de publicação antes de a vulnerabilidade ser oficialmente divulgada, bem como a resiliência em casos de perturbação ou interrupção da prestação de serviços semelhantes. A fim de evitar a duplicação de esforços e de assegurar, tanto quanto possível, a complementaridade, é importante que a ENISA explore a possibilidade de celebrar acordos de cooperação estruturados com

registos ***semelhantes*** em jurisdições de países terceiros.	***bases de dados ou*** registos ***de vulnerabilidades*** em jurisdições de países terceiros ***e de transmitir relatórios aos registos adequados, desde que tais medidas não comprometam a proteção da confidencialidade e dos segredos comerciais***.

Alteração 19
Proposta de diretiva
Considerando 32

Texto da Comissão	*Alteração*
(32) O grupo de cooperação deve elaborar, de dois em dois anos, um programa de trabalho que defina as ações a empreender pelo grupo no sentido de cumprir os seus objetivos e as suas funções. O calendário do primeiro programa adotado ao abrigo da presente diretiva deve estar alinhado com o calendário do último programa adotado ao abrigo da Diretiva (UE) 2016/1148, a fim de evitar potenciais perturbações das atividades do grupo.	(32) O grupo de cooperação deve ***debater as prioridades políticas e os principais desafios em matéria de cibersegurança e*** elaborar, de dois em dois anos, um programa de trabalho que defina as ações a empreender pelo grupo no sentido de cumprir os seus objetivos e as suas funções. O calendário do primeiro programa adotado ao abrigo da presente diretiva deve estar alinhado com o calendário do último programa adotado ao abrigo da Diretiva (UE) 2016/1148, a fim de evitar potenciais perturbações das atividades do grupo.

Alteração 20
Proposta de diretiva
Considerando 32-A (novo)

Texto da Comissão	*Alteração*
	(32-A) O grupo de cooperação deve ser composto por representantes dos Estados-Membros, da Comissão e da ENISA.

Alteração 21
Proposta de diretiva
Considerando 34

Texto da Comissão	*Alteração*
(34) O grupo de cooperação deve continuar a ser um fórum flexível e estar apto a reagir a alterações das prioridades e desafios políticos ou a novas prioridades e desafios políticos, tendo simultaneamente em conta a disponibilidade de recursos. Deve organizar regularmente reuniões conjuntas com partes interessadas privadas de toda a União para discutir as atividades desenvolvidas pelo grupo e partilhar pontos de vista sobre novos desafios políticos. A fim de reforçar a cooperação a nível da União, o grupo deve equacionar a possibilidade de convidar organismos e agências da União envolvidas na política de cibersegurança, como o Centro Europeu da Cibercriminalidade (EC3), a Agência da União Europeia para a Segurança da Aviação (EASA) e a Agência da União Europeia para o Programa Espacial (EUSPA), a participarem nos seus trabalhos.	(34) O grupo de cooperação deve continuar a ser um fórum flexível e estar apto a reagir a alterações das prioridades e desafios políticos ou a novas prioridades e desafios políticos, tendo simultaneamente em conta a disponibilidade de recursos. Deve organizar regularmente reuniões conjuntas com partes interessadas privadas de toda a União para discutir as atividades desenvolvidas pelo grupo e partilhar pontos de vista sobre novos desafios políticos. A fim de reforçar a cooperação a nível da União, o grupo deve equacionar a possibilidade de convidar organismos e agências da União envolvidas na política de cibersegurança, como o Centro Europeu da Cibercriminalidade (EC3), a Agência da União Europeia para a Segurança da Aviação (EASA) e a Agência da União Europeia para o Programa Espacial (EUSPA), ***bem como outros organismos e agências competentes da União,*** a participarem nos seus trabalhos.

Alteração 22
Proposta de diretiva
Considerando 35

Texto da Comissão	*Alteração*
(35) As autoridades competentes e as CSIRT devem estar habilitadas a participar em programas de intercâmbio de funcionários com outros Estados-Membros, no intuito de ***reforçar*** a cooperação. As autoridades competentes devem tomar as medidas necessárias para permitir que os funcionários de outros Estados-Membros participem ativamente nas atividades da autoridade competente de acolhimento.	(35) As autoridades competentes e as CSIRT devem estar habilitadas a participar em programas de intercâmbio ***e programas de formação conjunta*** de funcionários com outros Estados-Membros, no intuito de ***melhorar*** a cooperação ***e reforçar a confiança entre Estados-Membros***. As autoridades competentes devem tomar as medidas necessárias para permitir que os funcionários de outros Estados-Membros participem ativamente nas atividades da autoridade competente de acolhimento ***ou CSIRT***.

Alteração 23
Proposta de diretiva
Considerando 39

Texto da Comissão	*Alteração*
(39) Para efeitos da presente diretiva, entende-se por «quase incidente» um evento que poderia ter causado danos, mas que foi impedido de se materializar plenamente.	***Suprimido***

Alteração 24
Proposta de diretiva
Considerando 45-A (novo)

Texto da Comissão	*Alteração*
	(45-A) Além disso, as entidades devem também assegurar a educação e formação adequadas em cibersegurança do seu pessoal a todos os níveis da organização.

Alteração 25
Proposta de diretiva
Considerando 46

Texto da Comissão	*Alteração*
(46) A fim de melhorar a gestão dos principais riscos da cadeia de fornecimento e de ajudar as entidades que atuam em setores abrangidos pela presente diretiva a gerirem adequadamente riscos de cibersegurança relacionados com a cadeia de fornecimento e os fornecedores, o grupo de cooperação, com a participação das autoridades nacionais competentes e em cooperação com a Comissão e a ENISA, deve realizar avaliações setoriais coordenadas dos riscos associados às cadeias de fornecimento, tal como foi já feito para as redes 5G na sequência da Recomendação (UE) 2019/534 sobre a cibersegurança das redes 5G[21], com o objetivo de identificar, em cada setor, os	*(Não se aplica à versão portuguesa.)*

produtos, sistemas ou serviços de TIC críticos, bem como as vulnerabilidades e ameaças importantes.

[21] Recomendação (UE) 2019/534 da Comissão, de 26 de março de 2019, Cibersegurança das redes 5G (JO L 88 de 29.3.2019, p. 42).

[21] Recomendação (UE) 2019/534 da Comissão, de 26 de março de 2019, Cibersegurança das redes 5G (JO L 88 de 29.3.2019, p. 42).

Alteração 26
Proposta de diretiva
Considerando 47

Texto da Comissão	*Alteração*
(47) Dadas as características do setor em causa, as avaliações dos riscos associados às cadeias de fornecimento devem ter em conta tanto fatores técnicos como, quando pertinente, fatores não técnicos, incluindo os definidos na Recomendação (UE) 2019/534, na avaliação coordenada dos riscos de segurança das redes 5G a nível da UE, e no conjunto de instrumentos da UE em matéria de cibersegurança das redes 5G acordado pelo grupo de cooperação. Na identificação das cadeias de fornecimento que devem estar sujeitas a uma avaliação coordenada dos riscos, importa ter em conta os seguintes critérios: i) em que medida as entidades essenciais e importantes utilizam e dependem de produtos, sistemas ou serviços de TIC críticos específicos; ii) a importância de produtos, sistemas ou serviços de TIC críticos específicos para o desempenho de funções críticas ou sensíveis, incluindo o tratamento de dados pessoais; iii) a disponibilidade de produtos, sistemas ou serviços de TIC alternativos; iv) a resiliência da cadeia global de fornecimento de produtos, sistemas ou serviços de TIC face a perturbações; no que respeita a produtos, sistemas ou serviços de TIC emergentes, a sua potencial importância futura para as	(47) Dadas as características do setor em causa ***e a sua importância***, as avaliações dos riscos associados às cadeias de fornecimento devem ter em conta tanto fatores técnicos como, quando pertinente, fatores não técnicos, incluindo os definidos na Recomendação (UE) 2019/534, na avaliação coordenada dos riscos de segurança das redes 5G a nível da UE, e no conjunto de instrumentos da UE em matéria de cibersegurança das redes 5G acordado pelo grupo de cooperação. Na identificação das cadeias de fornecimento que devem estar sujeitas a uma avaliação coordenada dos riscos, importa ter em conta os seguintes critérios: i) em que medida as entidades essenciais e importantes utilizam e dependem de produtos, sistemas ou serviços de TIC críticos específicos; ii) a importância de produtos, sistemas ou serviços de TIC críticos específicos para o desempenho de funções críticas ou sensíveis, incluindo o tratamento de dados pessoais; iii) a disponibilidade de produtos, sistemas ou serviços de TIC alternativos; iv) a resiliência da cadeia global de fornecimento de produtos, sistemas ou serviços de TIC face a perturbações; no que respeita a produtos, sistemas ou serviços de TIC emergentes, a sua potencial importância futura para as

atividades das entidades.

atividades das entidades.

Alteração 27
Proposta de diretiva
Considerando 51

Texto da Comissão	*Alteração*
(51) O mercado interno depende, mais do que nunca, do funcionamento da Internet. Os serviços de praticamente todas as entidades essenciais e importantes estão dependentes de serviços prestados através da Internet. Para evitar problemas na prestação dos serviços assegurados por entidades essenciais e importantes, é necessário que as redes públicas de comunicações eletrónicas, por exemplo as estruturas de base da Internet ou os cabos submarinos de comunicações, adotem medidas de cibersegurança adequadas e notifiquem incidentes relacionados com as mesmas.	(51) O mercado interno depende, mais do que nunca, do funcionamento da Internet. Os serviços de praticamente todas as entidades essenciais e importantes estão dependentes de serviços prestados através da Internet***, e os consumidores dependem dos mesmos para partes essenciais da sua vida quotidiana***. Para evitar problemas na prestação dos serviços assegurados por entidades essenciais e importantes, é necessário que as redes públicas de comunicações eletrónicas, por exemplo as estruturas de base da Internet ou os cabos submarinos de comunicações, adotem medidas de cibersegurança adequadas e notifiquem incidentes relacionados com as mesmas.

Alteração 28
Proposta de diretiva
Considerando 52

Texto da Comissão	*Alteração*
(52) ***Quando adequado,*** as entidades devem informar os destinatários dos seus serviços sobre ameaças específicas e graves e sobre as medidas que podem tomar para minimizar o risco delas resultantes a que estão expostos***. A exigência de informar os referidos destinatários de tais ameaças*** não deve isentar as entidades da obrigação de, a expensas suas, adotarem medidas adequadas e imediatas para prevenir ou remediar quaisquer ciberameaças e restabelecer o nível normal de segurança do serviço. A prestação dessas informações	(52) As entidades devem ***ter como objetivo*** informar os destinatários dos seus serviços sobre ameaças específicas e graves e sobre as medidas que podem tomar para minimizar o risco delas resultantes a que estão expostos***, especialmente quando estas medidas possam contribuir para aumentar a proteção dos consumidores. Tal*** não deve isentar as entidades da obrigação de, a expensas suas, adotarem medidas adequadas e imediatas para prevenir ou remediar quaisquer ciberameaças e restabelecer o nível normal de segurança

aos destinatários sobre ameaças à segurança deve ser gratuita.

do serviço. A prestação dessas informações aos destinatários sobre ameaças à segurança deve ser gratuita ***e feita numa linguagem fácil de compreender***.

Alteração 29
Proposta de diretiva
Considerando 53

Texto da Comissão	*Alteração*
(53) Em especial, os fornecedores de redes públicas de comunicações eletrónicas ou prestadores de serviços de comunicações eletrónicas acessíveis ao público devem informar os destinatários dos serviços sobre ameaças específicas e graves em matéria de cibersegurança e sobre as medidas que podem tomar para proteger a segurança ***das suas*** comunicações, por exemplo, recorrendo a tipos específicos de software ou tecnologias de cifragem.	(53) Em especial, os fornecedores de redes públicas de comunicações eletrónicas ou prestadores de serviços de comunicações eletrónicas acessíveis ao público devem informar os destinatários dos serviços sobre ameaças específicas e graves em matéria de cibersegurança e sobre as medidas ***adicionais*** que podem tomar para proteger a segurança ***dos seus dispositivos e*** comunicações, por exemplo, recorrendo a tipos específicos de software ou tecnologias de cifragem.

Alteração 30
Proposta de diretiva
Considerando 54

Texto da Comissão	*Alteração*
(54) Para salvaguardar a segurança das redes e serviços de comunicações eletrónicas, a utilização de cifragem, especialmente da cifragem de ponta a ponta, deve ser promovida e, se necessário, deve ser obrigatória para os fornecedores das referidas redes e serviços, em conformidade com os princípios da segurança e da privacidade por defeito e desde a conceção para efeitos ***do artigo 18.º***. A utilização da cifragem de ponta a ponta ***deve ser conciliada com*** os poderes ***que os*** Estados-Membros ***detêm*** para assegurar a proteção dos seus interesses essenciais de segurança e da segurança pública e para permitir a investigação, a	(54) Para salvaguardar a segurança das redes e serviços de comunicações eletrónicas, a utilização de cifragem, especialmente da cifragem de ponta a ponta, deve ser promovida e, se necessário, deve ser obrigatória para os fornecedores das referidas redes e serviços, em conformidade com os princípios da segurança e da privacidade por defeito e desde a conceção para efeitos ***das medidas de gestão dos riscos de cibersegurança***. A utilização da cifragem de ponta a ponta ***não prejudica*** os poderes***, as políticas e os procedimentos dos*** Estados-Membros para assegurar a proteção dos seus interesses essenciais de segurança e da segurança

deteção e a repressão de infrações penais em conformidade com o direito da União. As soluções de acesso lícito a informações em comunicações cifradas de ponta a ponta devem manter a eficácia da cifragem em termos de proteção da privacidade e da segurança das comunicações, proporcionando simultaneamente uma resposta eficaz à criminalidade.

pública e para permitir a investigação, a deteção e a repressão de infrações penais em conformidade com o direito da União. As soluções de acesso lícito a informações em comunicações cifradas de ponta a ponta devem manter a eficácia da cifragem em termos de proteção da privacidade e da segurança das comunicações, proporcionando simultaneamente uma resposta eficaz à criminalidade. ***Todas e quaisquer medidas tomadas devem respeitar estritamente os princípios da proporcionalidade e da subsidiariedade.***

Alteração 31
Proposta de diretiva
Considerando 55

Texto da Comissão	*Alteração*
(55) A presente diretiva define uma abordagem ***em duas etapas*** à notificação de incidentes, a fim de estabelecer o equilíbrio adequado entre, por um lado, uma notificação célere que ajude a minimizar a potencial propagação de incidentes e permita às entidades procurar apoio e, por outro lado, uma notificação exaustiva que retire ensinamentos valiosos de incidentes individuais e melhore gradualmente a resiliência de empresas individuais e setores inteiros face às ciberameaças. Quando tenham tido conhecimento de um incidente, as entidades devem ser obrigadas a efetuar uma notificação inicial no prazo de ***24*** horas, seguida pela apresentação de um relatório final, o mais tardar, um mês depois. A notificação inicial deve conter apenas as informações estritamente necessárias para dar conhecimento do incidente às autoridades competentes e para permitir que a entidade procure assistência, caso tal seja necessário. Se for o caso, a referida notificação deve indicar se o incidente foi presumivelmente causado por um ato ilícito ou malicioso. Os Estados-Membros devem garantir que a	(55) A presente diretiva define uma abordagem ***consecutiva*** à notificação de incidentes, a fim de estabelecer o equilíbrio adequado entre, por um lado, uma notificação célere que ajude a minimizar a potencial propagação de incidentes e permita às entidades procurar apoio e, por outro lado, uma notificação exaustiva que retire ensinamentos valiosos de incidentes individuais e melhore gradualmente a resiliência de empresas individuais e setores inteiros face às ciberameaças. Quando tenham tido conhecimento de um incidente ***ou quase incidente***, as entidades devem ser obrigadas a efetuar uma notificação inicial no prazo de ***72*** horas, seguida pela apresentação de um relatório ***exaustivo, o mais tardar, três meses após efetuada a notificação inicial e de um relatório*** final, o mais tardar, um mês depois ***de o incidente ter sido mitigado***. A notificação inicial deve conter apenas as informações estritamente necessárias para dar conhecimento do incidente às autoridades competentes e para permitir que a entidade procure assistência, caso tal seja necessário. Se for o caso, a referida notificação deve indicar se o incidente foi

obrigação de apresentar esta notificação inicial não desvia os recursos da entidade notificadora afetos a atividades relacionadas com o tratamento de incidentes, às quais deve ser atribuída prioridade. Para evitar que as obrigações de notificação de incidentes desviem recursos afetos à resposta a incidentes ou possam prejudicar, de qualquer outra forma, os esforços desenvolvidos pelas entidades nessa matéria, os Estados-Membros devem igualmente estabelecer que, em casos devidamente justificados e com a concordância das autoridades competentes ou da CSIRT, a entidade em causa poderá não cumprir o prazo ***de 24 horas para a notificação inicial ou o prazo de um mês para o relatório final***.

presumivelmente causado por um ato ilícito ou malicioso. Os Estados-Membros devem garantir que a obrigação de apresentar esta notificação inicial não desvia os recursos da entidade notificadora afetos a atividades relacionadas com o tratamento de incidentes, às quais deve ser atribuída prioridade. ***A notificação inicial deve ser precedida de um alerta precoce nas primeiras 24 horas, sem obrigação de divulgar informações adicionais. Este alerta precoce deve ser enviado com a maior celeridade, de modo a permitir que as entidades obtenham rapidamente o apoio das autoridades competentes ou das CSIRT e que as autoridades competentes ou as CSIRT mitiguem a potencial propagação do incidente notificado, além de servir de ferramenta de conhecimento situacional para as CSIRT.*** Para evitar que as obrigações de notificação de incidentes desviem recursos afetos à resposta a incidentes ou possam prejudicar, de qualquer outra forma, os esforços desenvolvidos pelas entidades nessa matéria, os Estados-Membros devem igualmente estabelecer que, em casos devidamente justificados e com a concordância das autoridades competentes ou da CSIRT, a entidade em causa poderá não cumprir o prazo ***previsto***.

Alteração 32
Proposta de diretiva
Considerando 56

Texto da Comissão	*Alteração*
(56) As entidades essenciais e importantes encontram-se frequentemente numa situação em que um determinado incidente, por força das suas características, tem de ser comunicado a várias autoridades em cumprimento de obrigações de notificação estabelecidas em diferentes instrumentos jurídicos. Essas situações criam encargos adicionais, podendo igualmente gerar dúvidas quanto	(56) As entidades essenciais e importantes encontram-se frequentemente numa situação em que um determinado incidente, por força das suas características, tem de ser comunicado a várias autoridades em cumprimento de obrigações de notificação estabelecidas em diferentes instrumentos jurídicos. Essas situações criam encargos adicionais, podendo igualmente gerar dúvidas quanto

ao formato e aos procedimentos aplicáveis a tais notificações. Por este motivo, e com o objetivo de simplificar a notificação de incidentes de segurança, os Estados-Membros devem estabelecer um ponto de entrada único para todas as notificações exigidas pela presente diretiva e também por outros instrumentos jurídicos da União, como o Regulamento (UE) 2016/679 e a Diretiva 2002/58/CE. A ENISA, em cooperação com o grupo de cooperação, deve criar modelos comuns de notificação por intermédio de orientações destinadas a simplificar e racionalizar a comunicação de informações exigidas pelo direito da União e a reduzir os encargos para as empresas.	ao formato e aos procedimentos aplicáveis a tais notificações. Por este motivo, e com o objetivo de simplificar a notificação de incidentes de segurança ***e de respeitar o princípio da declaração única***, os Estados-Membros devem estabelecer um ponto de entrada único para todas as notificações exigidas pela presente diretiva e também por outros instrumentos jurídicos da União, como o Regulamento (UE) 2016/679 e a Diretiva 2002/58/CE. A ENISA, em cooperação com o grupo de cooperação, deve criar modelos comuns de notificação por intermédio de orientações destinadas a simplificar e racionalizar a comunicação de informações exigidas pelo direito da União e a reduzir os encargos para as empresas.

Alteração 33
Proposta de diretiva
Considerando 59

Texto da Comissão	*Alteração*
(59) A manutenção de bases de dados fidedignas e completas dos nomes de domínio e dados de registo (os chamados «dados WHOIS») e a concessão de acesso lícito a tais dados é essencial para garantir a segurança, estabilidade e resiliência do DNS, o que, por sua vez, contribui para um elevado nível comum de cibersegurança na União. Quando as operações de tratamento abrangerem dados pessoais, esse tratamento deve cumprir a legislação da União em matéria de proteção de dados.	(59) A manutenção de bases de dados fidedignas***, verificadas*** e completas dos nomes de domínio e dados de registo (os chamados «dados WHOIS») e a concessão de acesso lícito a tais dados é essencial para garantir a segurança, estabilidade e resiliência do DNS, o que, por sua vez, contribui para um elevado nível comum de cibersegurança na União. Quando as operações de tratamento abrangerem dados pessoais, esse tratamento deve cumprir a legislação da União em matéria de proteção de dados.

Alteração 34
Proposta de diretiva
Considerando 61

Texto da Comissão	*Alteração*
(61) A fim de assegurar a disponibilidade de dados exatos e	(61) A fim de assegurar a disponibilidade de dados exatos e

completos relativos ao registo de nomes de domínio, os registos de domínios de topo e as entidades que prestam serviços de registo de nomes de domínio ***a esses*** registos ***(os chamados*** agentes de registo) devem recolher dados relativos ao registo de nomes de domínio e garantir a integridade e disponibilidade desses dados. Em especial, os registos de domínios de topo e as entidades que prestam serviços de registo de nomes de domínio a esses registos devem estabelecer políticas e procedimentos para recolher e manter dados de registo exatos e completos, bem como para evitar e corrigir dados de registo incorretos, em conformidade com as regras da União em matéria de proteção de dados.

completos relativos ao registo de nomes de domínio, os registos de domínios de topo e as entidades que prestam serviços de registo de nomes de domínio ***(incluindo os serviços prestados pelos*** registos ***de domínios de topo e pelos*** agentes de registo***, os prestadores de serviços de proteção da privacidade ou de registo de servidores intermediários, os corretores ou revendedores de domínios e quaisquer outros serviços relacionados com o registo de nomes de domínio***) devem recolher dados relativos ao registo de nomes de domínio e garantir a integridade e disponibilidade desses dados. Em especial, os registos de domínios de topo e as entidades que prestam serviços de registo de nomes de domínio a esses registos devem estabelecer políticas e procedimentos para recolher e manter dados de registo exatos e completos, bem como para evitar e corrigir dados de registo incorretos, em conformidade com as regras da União em matéria de proteção de dados.

Alteração 35
Proposta de diretiva
Considerando 68

Texto da Comissão	*Alteração*
(68) Importa incentivar as entidades a tirarem partido, coletivamente, dos seus conhecimentos e experiências práticas individuais a nível estratégico, tático e operacional, com vista a reforçarem as suas capacidades para avaliarem, monitorizarem, se defenderem e darem resposta, de forma adequada, às ciberameaças. Consequentemente, é necessário viabilizar a criação, a nível da União, de mecanismos de partilha de informações a título voluntário. Para tal, os Estados-Membros devem apoiar ativamente e incentivar também entidades pertinentes não abrangidas pelo âmbito da presente diretiva a participarem em tais mecanismos de partilha de informações.	(68) Importa incentivar as entidades***, com o apoio dos Estados-Membros,*** a tirarem partido, coletivamente, dos seus conhecimentos e experiências práticas individuais a nível estratégico, tático e operacional, com vista a reforçarem as suas capacidades para avaliarem, monitorizarem, se defenderem e darem resposta, de forma adequada, às ciberameaças. Consequentemente, é necessário viabilizar a criação, a nível da União, de mecanismos de partilha de informações a título voluntário. Para tal, os Estados-Membros devem apoiar ativamente e incentivar também entidades pertinentes não abrangidas pelo âmbito da presente diretiva a participarem em tais

Esses mecanismos devem respeitar plenamente as regras da União em matéria de concorrência e de proteção de dados.	mecanismos de partilha de informações. Esses mecanismos devem respeitar plenamente as regras da União em matéria de concorrência e de proteção de dados.

Alteração 36
Proposta de diretiva
Considerando 69

Texto da Comissão	*Alteração*
(69) O tratamento de dados pessoais, ***na*** medida estritamente necessária e proporcionada para assegurar a segurança da rede e das informações, por entidades, autoridades públicas, CERT, CSIRT e fornecedores de tecnologias e serviços de segurança deve ser considerado um interesse legítimo do responsável pelo tratamento de dados em causa, tal como referido no Regulamento (UE) 2016/679. Tal deve incluir medidas relacionadas com a prevenção, deteção, análise e resposta a incidentes, medidas de sensibilização relativas a ciberameaças específicas, intercâmbio de informações no contexto da correção e da divulgação coordenada de vulnerabilidades, bem como o intercâmbio voluntário de informações sobre esses incidentes, ciberameaças e vulnerabilidades, indicadores de exposição a riscos, táticas, técnicas e procedimentos, alertas de cibersegurança e ferramentas de configuração. As referidas medidas poderão implicar o tratamento dos seguintes tipos de dados pessoais: endereços IP, localizadores uniformes de recursos (URL), nomes de domínio e endereços de correio eletrónico.	(69) O tratamento de dados pessoais, ***que não deve ir além da*** medida estritamente necessária e proporcionada para assegurar a segurança da rede e das informações***, bem como a proteção dos consumidores***, por entidades, autoridades públicas, CERT, CSIRT e fornecedores de tecnologias e serviços de segurança deve ser considerado um interesse legítimo do responsável pelo tratamento de dados em causa, tal como referido no Regulamento (UE) 2016/679. Tal deve incluir medidas relacionadas com a prevenção, deteção, análise e resposta a incidentes, medidas de sensibilização relativas a ciberameaças específicas, intercâmbio de informações no contexto da correção e da divulgação coordenada de vulnerabilidades, bem como o intercâmbio voluntário de informações sobre esses incidentes, ciberameaças e vulnerabilidades, indicadores de exposição a riscos, táticas, técnicas e procedimentos, alertas de cibersegurança e ferramentas de configuração. As referidas medidas poderão implicar o tratamento dos seguintes tipos de dados pessoais: endereços IP, localizadores uniformes de recursos (URL), nomes de domínio e endereços de correio eletrónico.

Alteração 37
Proposta de diretiva
Considerando 70

Texto da Comissão	*Alteração*
(70) A fim de reforçar as ações e os poderes de supervisão que ajudam a assegurar um cumprimento efetivo, a presente diretiva deve estabelecer uma lista mínima de meios e ações de supervisão por meio dos quais as autoridades competentes poderão supervisionar entidades essenciais e importantes. Adicionalmente, a presente diretiva deve distinguir entre o regime de supervisão aplicável a entidades essenciais e a entidades importantes, com vista a garantir um equilíbrio justo das obrigações tanto para as entidades como para as autoridades competentes. Assim, as entidades essenciais devem ficar sujeitas a um regime de supervisão completo (ex ante e ex post), ao passo que as entidades importantes devem ficar sujeitas a um regime de supervisão simplificado, aplicável apenas ex post. Tal significa que as entidades importantes não são obrigadas a documentar sistematicamente o cumprimento dos requisitos em matéria de gestão dos riscos de cibersegurança e que as autoridades competentes devem adotar uma abordagem ex post reativa à supervisão, pelo que não estão sujeitas a uma obrigação geral de supervisionar essas entidades.	(70) A fim de reforçar as ações e os poderes de supervisão que ajudam a assegurar um cumprimento efetivo ***e a atingir um elevado nível comum de segurança em todo o setor digital, nomeadamente através da prevenção de riscos para os utilizadores ou para outras redes, sistemas de informação e serviços***, a presente diretiva deve estabelecer uma lista mínima de meios e ações de supervisão por meio dos quais as autoridades competentes poderão supervisionar entidades essenciais e importantes. Adicionalmente, a presente diretiva deve distinguir entre o regime de supervisão aplicável a entidades essenciais e a entidades importantes, com vista a garantir um equilíbrio justo das obrigações tanto para as entidades como para as autoridades competentes. Assim, as entidades essenciais devem ficar sujeitas a um regime de supervisão completo (ex ante e ex post), ao passo que as entidades importantes devem ficar sujeitas a um regime de supervisão simplificado, aplicável apenas ex post***, que tenha em conta uma abordagem baseada no risco***. Tal significa que as entidades importantes não são obrigadas a documentar sistematicamente o cumprimento dos requisitos em matéria de gestão dos riscos de cibersegurança e que as autoridades competentes devem adotar uma abordagem ex post reativa à supervisão, pelo que não estão sujeitas a uma obrigação geral de supervisionar essas entidades***, salvo em caso de violação comprovada das obrigações***.

Alteração 38
Proposta de diretiva
Considerando 76

Texto da Comissão	*Alteração*
(76) Com vista a reforçar a eficácia e o caráter dissuasivo das sanções aplicáveis por incumprimento das obrigações estabelecidas nos termos da presente diretiva, as autoridades competentes devem estar habilitadas a aplicar sanções que consistam na suspensão de uma certificação ou autorização ***para a totalidade ou parte dos serviços*** prestados por uma entidade essencial ***e na interdição temporária do exercício de funções de administração por uma pessoa singular***. Dada a sua severidade e o seu impacto nas atividades das entidades e, em última análise, nos seus clientes, as referidas sanções devem ser proporcionadas à gravidade da infração e ter em conta as circunstâncias concretas de cada caso, incluindo o caráter doloso ou negligente da infração e as medidas tomadas para prevenir ou atenuar os danos e/ou perdas sofridas. Essas sanções só devem ser aplicadas em último recurso, ou seja, apenas depois de esgotadas todas as outras medidas coercivas pertinentes previstas na presente diretiva, e apenas até que as entidades a elas sujeitas tenham tomado as medidas necessárias para corrigir as deficiências ou satisfazer os requisitos da autoridade competente que estiveram na origem da aplicação das sanções. A imposição de tais sanções deve estar sujeita a garantias processuais adequadas em conformidade com os princípios gerais do direito da União e da Carta dos Direitos Fundamentais da União Europeia, incluindo a tutela jurisdicional efetiva, o processo equitativo, a presunção de inocência e o direito de defesa.	(76) Com vista a reforçar a eficácia e o caráter dissuasivo das sanções aplicáveis por incumprimento das obrigações estabelecidas nos termos da presente diretiva, as autoridades competentes devem estar habilitadas a aplicar sanções que consistam na suspensão de uma certificação ou autorização ***relativa aos serviços pertinentes*** prestados por uma entidade essencial. Dada a sua severidade e o seu impacto nas atividades das entidades e, em última análise, nos seus clientes, as referidas sanções devem ser proporcionadas à gravidade da infração e ter em conta as circunstâncias concretas de cada caso, incluindo o caráter doloso ou negligente da infração e as medidas tomadas para prevenir ou atenuar os danos e/ou perdas sofridas. Essas sanções só devem ser aplicadas em último recurso, ou seja, apenas depois de esgotadas todas as outras medidas coercivas pertinentes previstas na presente diretiva, e apenas até que as entidades a elas sujeitas tenham tomado as medidas necessárias para corrigir as deficiências ou satisfazer os requisitos da autoridade competente que estiveram na origem da aplicação das sanções. A imposição de tais sanções deve estar sujeita a garantias processuais adequadas em conformidade com os princípios gerais do direito da União e da Carta dos Direitos Fundamentais da União Europeia, incluindo a tutela jurisdicional efetiva, o processo equitativo, a presunção de inocência e o direito de defesa.

Alteração 39
Proposta de diretiva
Considerando 79

Texto da Comissão	*Alteração*
(79) É necessário instituir um mecanismo de análise pelos pares, no âmbito do qual peritos designados pelos Estados-Membros possam avaliar a execução das políticas de cibersegurança, bem como o nível das capacidades e de recursos disponíveis dos Estados-Membros.	(79) É necessário instituir um mecanismo de análise pelos pares, no âmbito do qual peritos designados pelos Estados-Membros ***e peritos da ENISA*** possam avaliar a execução das políticas de cibersegurança, bem como o nível das capacidades e de recursos disponíveis dos Estados-Membros***, e o intercâmbio de boas práticas***.

Alteração 40
Proposta de diretiva
Considerando 80

Texto da Comissão	*Alteração*
(80) A fim de ter em conta novas ciberameaças, avanços tecnológicos ou especificidades setoriais, o poder de adotar atos nos termos do artigo 290.º do TFUE deve ser delegado na Comissão no que diz respeito aos elementos relativos às medidas de gestão dos riscos exigidas pela presente diretiva. A Comissão deve ficar igualmente habilitada a adotar atos delegados que especifiquem ***as categorias*** de entidades essenciais ***obrigadas a obter um certificado e os sistemas europeus de certificação da cibersegurança a que devem recorrer para o efeito***. É particularmente importante que a Comissão proceda às consultas adequadas durante os trabalhos preparatórios, inclusive ao nível de peritos, e que essas consultas sejam conduzidas de acordo com os princípios estabelecidos no Acordo Interinstitucional, de 13 de abril de 2016, sobre legislar melhor[26]. Em particular, a fim de assegurar a igualdade de participação na preparação dos atos delegados, o Parlamento Europeu e o Conselho recebem todos os documentos ao mesmo tempo que os peritos dos Estados-Membros, e os respetivos peritos têm sistematicamente acesso às reuniões dos grupos de peritos da	(80) A fim de ter em conta novas ciberameaças, avanços tecnológicos ou especificidades setoriais, o poder de adotar atos nos termos do artigo 290.º do TFUE deve ser delegado na Comissão no que diz respeito aos elementos relativos às medidas de gestão dos riscos exigidas pela presente diretiva. A Comissão deve ficar ***habilitada a adotar atos delegados que definam os elementos técnicos relacionados com as medidas de gestão de riscos. A Comissão deve ficar*** igualmente habilitada a adotar atos delegados que especifiquem ***o tipo*** de ***informação que as*** entidades essenciais ***e importantes devem apresentar sobre qualquer incidente que tenha um impacto significativo na prestação dos seus serviços ou sobre qualquer quase incidente, e que especifiquem os casos em que um incidente deve ser considerado significativo***. É particularmente importante que a Comissão proceda às consultas adequadas durante os trabalhos preparatórios, inclusive ao nível de peritos, e que essas consultas sejam conduzidas de acordo com os princípios estabelecidos no Acordo Interinstitucional, de 13 de abril de 2016, sobre legislar melhor[26]. Em particular, a fim de assegurar a igualdade

Comissão que tratem da preparação dos atos delegados.

de participação na preparação dos atos delegados, o Parlamento Europeu e o Conselho recebem todos os documentos ao mesmo tempo que os peritos dos Estados-Membros, e os respetivos peritos têm sistematicamente acesso às reuniões dos grupos de peritos da Comissão que tratem da preparação dos atos delegados.

[26] JO L 123 de 12.5.2016, p. 1.

[26] JO L 123 de 12.5.2016, p. 1.

Alteração 41
Proposta de diretiva
Considerando 81

Texto da Comissão

(81) A fim de garantir condições uniformes para a aplicação das disposições pertinentes da presente diretiva relativas às disposições processuais necessárias ao funcionamento do grupo de cooperação, ***aos elementos técnicos relacionados com as medidas de gestão dos riscos ou ao tipo de informação,*** ao formato e ao procedimento de notificação de incidentes, é necessário atribuir competências de execução à Comissão. Essas competências devem ser exercidas nos termos do Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho[27].

Alteração

(81) A fim de garantir condições uniformes para a aplicação das disposições pertinentes da presente diretiva relativas às disposições processuais necessárias ao funcionamento do grupo de cooperação, ao formato e ao procedimento de notificação de incidentes, é necessário atribuir competências de execução à Comissão. Essas competências devem ser exercidas nos termos do Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho[27].

[27] 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 (JO L 55 de 28.2.2011, p. 13).

[27] 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 (JO L 55 de 28.2.2011, p. 13).

Alteração 42
Proposta de diretiva
Artigo 1 – n.º 1

Texto da Comissão	*Alteração*
1. A presente diretiva estabelece medidas destinadas a assegurar um elevado nível comum de cibersegurança na União.	1. A presente diretiva estabelece medidas destinadas a assegurar um elevado nível comum de cibersegurança na União***, a fim de criar um ambiente digital de confiança para os consumidores e os operadores económicos e de melhorar o funcionamento do mercado interno e eliminar os obstáculos que o entravam***.

Alteração 43
Proposta de diretiva
Artigo 2 – n.º 2 – parágrafo 1 – parte introdutória

Texto da Comissão	*Alteração*
2. No entanto, a presente diretiva também se aplica às entidades ***referidas*** nos anexos I e II, independentemente da sua dimensão, nos casos em que:	2. No entanto, a presente diretiva também se aplica às entidades ***de um tipo referido*** nos anexos I e II, independentemente da sua dimensão, nos casos em que:

Alteração 44
Proposta de diretiva
Artigo 2 – n.º 2 – parágrafo 2-A (novo)

Texto da Comissão	*Alteração*
	A Comissão emite orientações para apoiar os Estados-Membros na correta aplicação das disposições relativas ao âmbito de aplicação, bem como para conceder a entidades importantes específicas eventuais derrogações ao âmbito de aplicação da diretiva ou a algumas das suas disposições, tendo em conta o seu baixo grau de importância no seu setor específico e/ou o seu baixo nível de dependência de outros setores ou tipos de serviços. Os Estados-Membros, tendo plenamente em contas as orientações da Comissão, notificam a Comissão das suas decisões fundamentadas a este respeito.

Alteração 45
Proposta de diretiva
Artigo 4 – parágrafo 1 – ponto 4

Texto da Comissão	*Alteração*
(4) «Estratégia nacional de cibersegurança»: um quadro coerente mediante o qual um Estado-Membro define prioridades e objetivos estratégicos em matéria de segurança das redes e dos sistemas de informação a nível nacional;	(4) «Estratégia nacional de cibersegurança»: um quadro coerente mediante o qual um Estado-Membro define prioridades e objetivos estratégicos em matéria de segurança das redes e dos sistemas de informação a nível nacional***, bem como as políticas necessárias para os concretizar***;

Alteração 46
Proposta de diretiva
Artigo 4 – parágrafo 1 – ponto 5-A (novo)

Texto da Comissão	*Alteração*
	(5-A) «Incidente transfronteiriço»: qualquer incidente que afete os operadores sob a supervisão das autoridades nacionais competentes de, pelo menos, dois Estados-Membros distintos;

Alteração 47
Proposta de diretiva
Artigo 4 – parágrafo 1 – ponto 6-A (novo)

Texto da Comissão	*Alteração*
	(6-A) «Quase incidente»: qualquer acontecimento que poderia potencialmente ter causado danos, mas que foi impedido de se materializar plenamente;

Alteração 48
Proposta de diretiva
Artigo 4 – parágrafo 1 – ponto 15-A (novo)

Texto da Comissão	*Alteração*
	(15-A) «Serviços de registo de nomes de domínio»: serviços prestados por registos e agentes de registo de nomes de domínio, prestadores de serviços de proteção da privacidade ou de registo de servidores intermediários, corretores ou revendedores de domínios e quaisquer outros serviços relacionados com o registo de nomes de domínio;

Alteração 49
Proposta de diretiva
Artigo 5 – n.º 1 – parte introdutória

Texto da Comissão	*Alteração*
1. Os Estados-Membros devem adotar uma estratégia nacional de cibersegurança que defina objetivos estratégicos e medidas políticas e regulamentares adequadas, com vista a alcançar e a manter um elevado nível de cibersegurança. A estratégia nacional de cibersegurança deve incluir, em especial, o seguinte:	1. Os Estados-Membros devem adotar uma estratégia nacional de cibersegurança que defina objetivos estratégicos e medidas políticas e regulamentares adequadas, ***incluindo recursos humanos e financeiros adequados,*** com vista a alcançar e a manter um elevado nível de cibersegurança. A estratégia nacional de cibersegurança deve incluir, em especial, o seguinte:

Alteração 50
Proposta de diretiva
Artigo 5 – n.º 1 – alínea b)

Texto da Comissão	*Alteração*
b) Um quadro de governação para cumprir esses objetivos e prioridades, incluindo as políticas referidas no n.º 2 e as funções e responsabilidades das entidades e organismos públicos, bem como de outros intervenientes pertinentes;	b) Um quadro de governação para cumprir esses objetivos e prioridades, incluindo as políticas referidas no n.º 2 e as funções e responsabilidades das entidades e organismos públicos, bem como de outros intervenientes pertinentes***, em particular os responsáveis pela ciberinformação e a ciberdefesa***;

Alteração 51
Proposta de diretiva
Artigo 5 – n.º 1 – alínea c)

Texto da Comissão	*Alteração*
c) Uma avaliação para identificar ativos importantes e riscos de cibersegurança nesse Estado-Membro;	c) Uma avaliação para identificar ativos importantes e riscos de cibersegurança nesse Estado-Membro***,*** ***incluindo uma potencial escassez suscetível de ter um impacto negativo no mercado único***;

Alteração 52
Proposta de diretiva
Artigo 5 – n.º 1 – alínea e)

Texto da Comissão	*Alteração*
e) Uma lista das diversas autoridades e intervenientes envolvidos na execução da estratégia nacional de cibersegurança;	e) Uma lista das diversas autoridades e intervenientes envolvidos na execução da estratégia nacional de cibersegurança***,*** ***incluindo um balcão único para as PME***;

Alteração 53
Proposta de diretiva
Artigo 5 – n.º 2 – alínea b)

Texto da Comissão	*Alteração*
b) Orientação relativas à inclusão e à especificação de requisitos em matéria de cibersegurança aplicáveis a produtos e serviços de TIC nos procedimentos de contratação pública;	b) Orientação relativas à inclusão e à especificação de requisitos em matéria de cibersegurança aplicáveis a produtos e serviços de TIC nos procedimentos de contratação pública***, incluindo a utilização de produtos de cibersegurança de código-fonte aberto***;

Alteração 54
Proposta de diretiva
Artigo 5 – n.º 2 – alínea c)

Texto da Comissão	*Alteração*
c) Uma política destinada a promover	c) Uma política destinada a promover

e facilitar a divulgação coordenada de vulnerabilidades na aceção do artigo 6.º;	e facilitar a divulgação coordenada de vulnerabilidades na aceção do artigo 6.º***, inclusive mediante a definição de orientações e boas práticas assentes em normas internacionalmente reconhecidas já estabelecidas sobre a gestão e a divulgação de vulnerabilidades***;

Alteração 55
Proposta de diretiva
Artigo 5 – n.º 2 – alínea e)

Texto da Comissão	*Alteração*
e) Uma política de promoção ***e desenvolvimento de*** competências no domínio da cibersegurança***, de sensibilização e*** de iniciativas de investigação e desenvolvimento;	e) Uma política de promoção ***da cibersegurança para os consumidores, que os sensibilize para as ciberameaças e que aumente a ciberliteracia, reforce a confiança dos utilizadores, as*** competências ***e a educação*** no domínio da cibersegurança ***neutra do ponto de vista tecnológico, bem como de promoção*** de iniciativas de investigação e desenvolvimento ***e da cibersegurança dos produtos conectados***;

Alteração 56
Proposta de diretiva
Artigo 5 – n.º 2 – alínea e-A) (nova)

Texto da Comissão	*Alteração*
	e-A) Uma política de promoção da utilização da criptografia e da cifragem, em particular pelas PME;

Alteração 57
Proposta de diretiva
Artigo 5 – n.º 2 – alínea h)

Texto da Comissão	*Alteração*
h) Uma política ***para responder*** às necessidades específicas das PME, ***especialmente*** das que estão excluídas do	h) Uma política ***que promova a cibersegurança e responda*** às necessidades específicas das PME ***para***

âmbito da presente diretiva, no que respeita a orientações e apoio para melhorarem a sua resiliência a ciberameaças.	***cumprir as obrigações estabelecidas pela presente diretiva***, ***assim como as necessidades específicas*** das que estão excluídas do âmbito da presente diretiva, no que respeita a orientações e apoio para melhorarem a sua resiliência a ciberameaças***, incluindo, por exemplo, o financiamento e a educação para apoiar a adoção de medidas de cibersegurança***.

Alteração 58
Proposta de diretiva
Artigo 5 – n.º 2 – alínea h-A) (nova)

Texto da Comissão	*Alteração*
	h-A) Esta política deve incluir a criação de um ponto de contacto único a nível nacional para as PME e de um quadro para a utilização mais eficiente dos polos de inovação digital e dos fundos disponíveis na consecução dos objetivos da política;

Alteração 59
Proposta de diretiva
Artigo 5 – n.º 2 – alínea h-B) (nova)

Texto da Comissão	*Alteração*
	h-B) Uma política que promova a utilização coerente e sinérgica dos fundos disponíveis;

Alteração 60
Proposta de diretiva
Artigo 5 – n.º 4

Texto da Comissão	*Alteração*
4. Os Estados-Membros devem avaliar as suas estratégias nacionais de cibersegurança pelo menos de quatro em quatro anos com base em indicadores-chave de desempenho e, quando	4. Os Estados-Membros devem avaliar as suas estratégias nacionais de cibersegurança pelo menos de quatro em quatro anos com base em indicadores-chave de desempenho e, quando

necessário, devem alterá-las. A pedido dos Estados-Membros, a Agência da União Europeia para a Cibersegurança (ENISA) deve ajudá-los a formular uma estratégia nacional e indicadores-chave de desempenho para a avaliação dessa estratégia.

necessário, devem alterá-las. A pedido dos Estados-Membros, a Agência da União Europeia para a Cibersegurança (ENISA) deve ajudá-los a formular uma estratégia nacional e indicadores-chave de desempenho para a avaliação dessa estratégia. ***A ENISA deve também apresentar recomendações aos Estados-Membros sobre o desenvolvimento de indicadores-chave de desempenho, comparáveis a nível da União, para a avaliação da estratégia nacional.***

Alteração 61
Proposta de diretiva
Artigo 6 – Título

Texto da Comissão	*Alteração*
Divulgação coordenada de vulnerabilidades e ***registo europeu*** de vulnerabilidades	Divulgação coordenada de vulnerabilidades e ***base de dados europeia*** de vulnerabilidades

Alteração 62
Proposta de diretiva
Artigo 6 – n.º 2

Texto da Comissão	*Alteração*
2. A ENISA deve criar e manter ***um registo europeu*** de vulnerabilidades. Para tal, deve estabelecer e manter sistemas de informação, políticas e procedimentos adequados, tendo em vista, em especial, permitir que entidades importantes e essenciais e os respetivos fornecedores de redes e sistemas de informação divulguem e registem vulnerabilidades presentes nos produtos de TIC ou serviços de TIC, bem como proporcionar acesso às informações sobre vulnerabilidades constantes do registo a todas as partes interessadas. ***O registo*** deve incluir, em especial, informações que descrevam a vulnerabilidade, o produto de TIC ou os serviços de TIC afetados e a gravidade da	2. A ENISA deve criar e manter ***uma base de dados europeia*** de vulnerabilidades. Para tal, deve estabelecer e manter sistemas de informação, políticas e procedimentos adequados, ***bem como políticas de divulgação adequadas,*** tendo em vista, em especial, permitir que entidades importantes e essenciais e os respetivos fornecedores de redes e sistemas de informação divulguem e registem ***facilmente*** vulnerabilidades presentes nos produtos de TIC ou serviços de TIC, bem como proporcionar acesso às informações ***pertinentes*** sobre vulnerabilidades constantes do registo a todas as partes interessadas***, desde que essas ações não comprometam a proteção da***

vulnerabilidade em termos das circunstâncias em que pode ser explorada, a disponibilidade de correções e, na falta de correções, orientações destinadas aos utilizadores de produtos e serviços vulneráveis sobre formas de minimizar os riscos resultantes das vulnerabilidades divulgadas.

confidencialidade e dos segredos comerciais. ***A base de dados europeia de vulnerabilidades*** deve incluir, em especial, informações que descrevam a vulnerabilidade, o produto de TIC ou os serviços de TIC afetados e a gravidade da vulnerabilidade em termos das circunstâncias em que pode ser explorada, a disponibilidade de correções e, na falta de correções, orientações destinadas aos utilizadores de produtos e serviços vulneráveis sobre formas de minimizar os riscos resultantes das vulnerabilidades divulgadas. ***A fim de evitar a duplicação de esforços, a ENISA deve celebrar um acordo relativo à partilha de informações e um acordo de cooperação estruturada com o registo de Vulnerabilidades e Exposições Comuns (CVE) e, se for caso disso, com outras bases de dados desenvolvidas e mantidas a nível mundial por parceiros de confiança.***

Alteração 63
Proposta de diretiva
Artigo 7 – n.º 1-A (novo)

Texto da Comissão	*Alteração*
	1-A. Caso um Estado-Membro designe mais de uma autoridade competente referida no n.º 1, deve indicar claramente qual das autoridades competentes será o ponto de contacto principal durante um incidente ou crise em grande escala.

Alteração 64
Proposta de diretiva
Artigo 7 – n.º 3 – alínea f)

Texto da Comissão	*Alteração*
f) Procedimentos nacionais e ***acordos*** entre as autoridades e os organismos nacionais competentes para assegurar o apoio do Estado-Membro e a sua	f) Procedimentos nacionais e ***coordenação*** entre as autoridades e os organismos nacionais competentes***, incluindo os responsáveis pela***

participação efetiva na gestão coordenada de crises e incidentes de cibersegurança em grande escala a nível da União.	***ciberinformação e pela ciberdefesa,*** para assegurar o apoio do Estado-Membro e a sua participação efetiva na gestão coordenada de crises e incidentes de cibersegurança em grande escala a nível da União.

Alteração 65
Proposta de diretiva
Artigo 10 – n.º 2 – alínea d)

Texto da Comissão	*Alteração*
d) Proceder à análise dinâmica dos riscos e dos incidentes e desenvolver o conhecimento situacional em matéria de cibersegurança;	d) Proceder à análise dinâmica dos riscos e dos incidentes e desenvolver o conhecimento situacional em matéria de cibersegurança***, nomeadamente através da análise dos alertas precoces e das notificações, como referido no artigo 20.º***;

Alteração 66
Proposta de diretiva
Artigo 10 – n.º 2 – alínea e)

Texto da Comissão	*Alteração*
e) A pedido de uma entidade, realizar uma análise ***proativa*** da rede e dos sistemas de informação utilizados para a prestação dos seus serviços;	e) A pedido de uma entidade, realizar uma análise da rede e dos sistemas de informação utilizados para a prestação dos seus serviços***, a fim de detetar, mitigar ou prevenir ameaças específicas***;

Alteração 67
Proposta de diretiva
Artigo 10 – n.º 2 – alínea f)

Texto da Comissão	*Alteração*
f) Participar na rede de CSIRT e prestar assistência mútua a outros membros da rede, a pedido destes***.***	f) Participar ***ativamente*** na rede de CSIRT e prestar assistência mútua a outros membros da rede, a pedido destes***;***

Alteração 68
Proposta de diretiva
Artigo 10 – n.º 2 – alínea f-A) (nova)

Texto da Comissão	*Alteração*
	f-A) Prestar assistência operacional e orientação às entidades referidas nos anexos I e II, em especial às PME;

Alteração 69
Proposta de diretiva
Artigo 10 – n.º 2 – alínea f-B) (nova)

Texto da Comissão	*Alteração*
	f-B) Participar em exercícios de cibersegurança conjuntos a nível da União.

Alteração 70
Proposta de diretiva
Artigo 11 – n.º 2

Texto da Comissão	*Alteração*
2. Os Estados-Membros devem assegurar que as respetivas autoridades competentes ou as respetivas CSIRT recebem as notificações de incidentes, ciberameaças significativas e quase incidentes efetuadas nos termos da presente diretiva. Caso um Estado-Membro decida que as suas CSIRT não receberão as referidas notificações, estas devem ter acesso, na medida necessária ao desempenho das suas funções, aos dados sobre os incidentes notificados pelas entidades essenciais e importantes, nos termos do artigo 20.º.	2. Os Estados-Membros devem assegurar que as respetivas autoridades competentes ou as respetivas CSIRT recebem as notificações de incidentes, ciberameaças significativas e quase incidentes efetuadas nos termos da presente diretiva. Caso um Estado-Membro decida que as suas CSIRT não receberão as referidas notificações, estas devem ter ***um*** acesso ***adequado***, na medida necessária ao desempenho ***eficaz*** das suas funções, aos dados sobre os incidentes notificados pelas entidades essenciais e importantes, nos termos do artigo 20.º.

Alteração 71
Proposta de diretiva
Artigo 11 – n.º 4

Texto da Comissão	*Alteração*
4. Na medida necessária ao desempenho das funções e ao cumprimento das obrigações estabelecidas na presente diretiva de forma eficaz, os Estados-Membros devem assegurar uma cooperação adequada entre as autoridades competentes e os pontos de contacto únicos e as autoridades policiais, as autoridades de proteção de dados, as autoridades responsáveis por infraestruturas críticas nos termos da Diretiva (UE) XXXX/XXXX [Diretiva Resiliência das Entidades Críticas] e as autoridades financeiras designadas em conformidade com o Regulamento (UE) XXXX/XXXX do Parlamento Europeu e do Conselho[39] [Regulamento DORA] de cada Estado-Membro.	4. Na medida necessária ao desempenho das funções e ao cumprimento das obrigações estabelecidas na presente diretiva de forma eficaz, os Estados-Membros devem assegurar uma cooperação adequada entre as autoridades competentes e os pontos de contacto únicos e as autoridades policiais, as autoridades de proteção de dados, as autoridades responsáveis por infraestruturas críticas nos termos da Diretiva (UE) XXXX/XXXX [Diretiva Resiliência das Entidades Críticas] e as autoridades financeiras designadas em conformidade com o Regulamento (UE) XXXX/XXXX do Parlamento Europeu e do Conselho[39] [Regulamento DORA] de cada Estado-Membro***, assim como com as autoridades de ciberdefesa e ciberinformação.***.
[39] [Serviço das Publicações: inserir o título completo e a referência de publicação no JO quando forem conhecidos].	[39] [Serviço das Publicações: inserir o título completo e a referência de publicação no JO quando forem conhecidos].

Alteração 72
Proposta de diretiva
Artigo 12 – n.º 2

Texto da Comissão	*Alteração*
2. O grupo de cooperação desempenha as suas funções com base nos programas de trabalho bienais a que se refere o n.º 6.	2. O grupo de cooperação ***reúne-se regularmente e*** desempenha as suas funções com base nos programas de trabalho bienais a que se refere o n.º 6.

Alteração 73
Proposta de diretiva
Artigo 12 – n.º 3 – parágrafo 2

Texto da Comissão	*Alteração*
Se for caso disso, o grupo de cooperação pode convidar representantes ***de partes***	Se for caso disso, o grupo de cooperação pode convidar representantes ***dos***

interessadas relevantes para participar nos seus trabalhos.	***organismos e agências da União*** relevantes***, bem como as partes interessadas,*** para participar nos seus trabalhos.

Alteração 74
Proposta de diretiva
Artigo 12 – n.º 4 – alínea a)

Texto da Comissão	*Alteração*
a) Fornecer orientações às autoridades competentes sobre a transposição e aplicação da presente diretiva;	a) Fornecer orientações às autoridades competentes sobre a transposição e aplicação da presente diretiva ***e promover a sua aplicação uniforme nos Estados-Membros***;

Alteração 75
Proposta de diretiva
Artigo 12 – n.º 4 – alínea a-A) (nova)

Texto da Comissão	*Alteração*
	a-A) Proceder ao intercâmbio de informações sobre as prioridades políticas e os principais desafios em matéria de cibersegurança e definir os principais objetivos da cibersegurança;

Alteração 76
Proposta de diretiva
Artigo 12 – n.º 4 – alínea a-B) (nova)

Texto da Comissão	*Alteração*
	a-B) Discutir as estratégias nacionais dos Estados-Membros e o seu grau de preparação;

Alteração 77
Proposta de diretiva
Artigo 12 – n.º 4 – alínea c)

Texto da Comissão	*Alteração*
c) Trocar pareceres e cooperar com a Comissão em novas iniciativas políticas no domínio da cibersegurança;	c) Trocar pareceres e cooperar com a Comissão em novas iniciativas políticas no domínio da cibersegurança***, e com o Serviço Europeu para a Ação Externa no que respeita aos aspetos geopolíticos da cibersegurança na União***;

Alteração 78
Proposta de diretiva
Artigo 12 – n.º 4 – alínea f)

Texto da Comissão	*Alteração*
f) Discutir os relatórios das análises pelos pares a que se refere o artigo 16.º, n.º 7;	f) Discutir os relatórios das análises pelos pares a que se refere o artigo 16.º, n.º 7***, avaliar o seu funcionamento e formular conclusões e recomendações***;

Alteração 79
Proposta de diretiva
Artigo 12 – n.º 4 – alínea k-A) (nova)

Texto da Comissão	*Alteração*
	k-A) Apoiar a ENISA na organização de formação conjunta das autoridades nacionais competentes a nível da União.

Alteração 80
Proposta de diretiva
Artigo 12 – n.º 6

Texto da Comissão	*Alteração*
6. Até … [***24*** meses após a data de entrada em vigor da presente diretiva] e, daí em diante, de dois em dois anos, o grupo de cooperação deve elaborar um programa de trabalho relativo às ações a desenvolver para alcançar os seus objetivos e executar as suas funções. O calendário do primeiro programa adotado ao abrigo da	6. Até … [***12*** meses após a data de entrada em vigor da presente diretiva] e, daí em diante, de dois em dois anos, o grupo de cooperação deve elaborar um programa de trabalho relativo às ações a desenvolver para alcançar os seus objetivos e executar as suas funções. O calendário do primeiro programa adotado ao abrigo da

presente diretiva deve estar alinhado com o calendário do último programa adotado ao abrigo da Diretiva (UE) 2016/1148.	presente diretiva deve estar alinhado com o calendário do último programa adotado ao abrigo da Diretiva (UE) 2016/1148.

Alteração 81
Proposta de diretiva
Artigo 12 – n.º 8-A (novo)

Texto da Comissão	*Alteração*
	8-A. O grupo de cooperação deve publicar regularmente um relatório de síntese das suas atividades, sem prejuízo da confidencialidade das informações partilhadas durante as suas reuniões.

Alteração 82
Proposta de diretiva
Artigo 13 – n.º 3 – alínea a)

Texto da Comissão	*Alteração*
a) Proceder ao intercâmbio de informações sobre as capacidades das CSIRT;	a) Proceder ao intercâmbio de informações sobre as capacidades ***e o grau de preparação*** das CSIRT;

Alteração 83
Proposta de diretiva
Artigo 13 – n.º 3 – alínea b)

Texto da Comissão	*Alteração*
b) Proceder ao intercâmbio de informações importantes sobre incidentes, quase incidentes, ciberameaças, riscos e vulnerabilidades;	b) Proceder ao intercâmbio de informações importantes sobre incidentes, quase incidentes, ciberameaças, riscos e vulnerabilidades ***e apoiar as capacidades operacionais dos Estados-Membros***;

Alteração 84
Proposta de diretiva
Artigo 13 – n.º 3 – alínea d-A) (nova)

Texto da Comissão	*Alteração*
	d-A) Proceder ao intercâmbio e discussão de informações relativas a incidentes transfronteiriços;

Alteração 85
Proposta de diretiva
Artigo 13 – n.º 3 – alínea g) – subalínea i-A (nova)

Texto da Comissão	*Alteração*
	i-A) Partilha de informações;

Alteração 86
Proposta de diretiva
Artigo 13 – n.º 3 – alínea j)

Texto da Comissão	*Alteração*
j) ***A pedido de determinada CSIRT,*** discutir as ***suas*** capacidades e o ***seu*** grau de preparação;	j) Discutir as capacidades e o grau de preparação ***das CSIRT***;

Alteração 87
Proposta de diretiva
Artigo 13 – n.º 4

Texto da Comissão	*Alteração*
4. Para efeitos da avaliação a que se refere o artigo 35.º e até [24 meses após a data de entrada em vigor da presente diretiva] e, daí em diante, ***de dois em dois*** anos, a rede de CSIRT deve avaliar os progressos alcançados no domínio da cooperação operacional e apresentar um relatório. Em especial, o relatório deve expor conclusões sobre os resultados das análises pelos pares realizadas nos termos do artigo 16.º em relação às CSIRT nacionais, incluindo conclusões e recomendações nos termos do referido artigo. Esse relatório deve ser apresentado	4. Para efeitos da avaliação a que se refere o artigo 35.º e até [24 meses após a data de entrada em vigor da presente diretiva] e, daí em diante, ***todos os*** anos, a rede de CSIRT deve avaliar os progressos alcançados no domínio da cooperação operacional e apresentar um relatório. Em especial, o relatório deve expor conclusões sobre os resultados das análises pelos pares realizadas nos termos do artigo 16.º em relação às CSIRT nacionais, incluindo conclusões e recomendações nos termos do referido artigo. Esse relatório deve ser apresentado também ao grupo de

também ao grupo de cooperação.	cooperação.

Alteração 88
Proposta de diretiva
Artigo 14 – n.º 3 – alínea a)

Texto da Comissão	*Alteração*
a) Aumentar o nível de preparação para a gestão de incidentes e crises em grande escala;	a) Aumentar o nível de preparação para a gestão de incidentes e crises em grande escala***, incluindo ciberameaças transfronteiriças***;

Alteração 89
Proposta de diretiva
Artigo 14 – n.º 5

Texto da Comissão	*Alteração*
5. A UE-CyCLONe presta regularmente informações ao grupo de cooperação sobre ciberameaças, incidentes e tendências, dedicando especial atenção ao seu impacto em entidades essenciais e importantes.	5. A UE-CyCLONe presta regularmente informações ao grupo de cooperação sobre ciberameaças, incidentes e tendências, dedicando especial atenção ao seu impacto em entidades essenciais e importantes ***e à sua resiliência***.

Alteração 90
Proposta de diretiva
Artigo 14 – n.º 6

Texto da Comissão	*Alteração*
6. A UE-CyCLONe coopera com a rede de CSIRT com base em disposições processuais acordadas.	6. A UE-CyCLONe coopera ***estreitamente*** com a rede de CSIRT com base em disposições processuais acordadas.

Alteração 91
Proposta de diretiva
Artigo 15 – n.º 1 – parte introdutória

Texto da Comissão	*Alteração*
1. A ENISA deve elaborar, em cooperação com a Comissão, um relatório	1. A ENISA deve elaborar, em cooperação com a Comissão, um relatório

bienal sobre o estado da cibersegurança na União. Este relatório deve, nomeadamente, incluir uma análise dos seguintes aspetos:	bienal sobre o estado da cibersegurança na União ***e apresentá-lo ao Parlamento Europeu***. Este relatório deve, nomeadamente, incluir uma análise dos seguintes aspetos:

Alteração 92
Proposta de diretiva
Artigo 15 – n.º 1 – alínea a)

Texto da Comissão	*Alteração*
a) O desenvolvimento das capacidades de cibersegurança em toda a União;	a) O desenvolvimento das capacidades de cibersegurança em toda a União***, incluindo o nível geral de capacidades e competências em matéria de cibersegurança, o grau geral de resiliência do mercado interno às ciberameaças e o nível de aplicação da diretiva em todos os Estados-Membros***;

Alteração 93
Proposta de diretiva
Artigo 15 – n.º 1 – alínea c)

Texto da Comissão	*Alteração*
c) Um índice de cibersegurança que contemple uma avaliação agregada do nível de maturidade das capacidades de cibersegurança***.***	c) Um índice de cibersegurança que contemple uma avaliação agregada do nível de maturidade das capacidades de cibersegurança***, incluindo uma avaliação global da cibersegurança para os consumidores;***

Alteração 94
Proposta de diretiva
Artigo 15 – n.º 1 – alínea c-A) (nova)

Texto da Comissão	*Alteração*
	c-A) Os aspetos geopolíticos que têm um impacto direto ou indireto no estado da cibersegurança na União.

Alteração 95
Proposta de diretiva
Artigo 16 – n.º 1 – parte introdutória

Texto da Comissão	*Alteração*
1. Após consulta do grupo de cooperação e da ENISA e, o mais tardar, ***18*** meses após a entrada em vigor da presente diretiva, a Comissão estabelece a metodologia e o conteúdo de um sistema de análises pelos pares destinado a avaliar a eficácia das políticas de cibersegurança dos Estados-Membros. As análises devem ser realizadas por peritos técnicos em cibersegurança provenientes de Estados-Membros diferentes do Estado-Membro avaliado e devem incidir, no mínimo, nos seguintes aspetos:	1. Após consulta do grupo de cooperação e da ENISA e, o mais tardar, ***12*** meses após a entrada em vigor da presente diretiva, a Comissão estabelece a metodologia e o conteúdo de um sistema de análises pelos pares destinado a avaliar a eficácia das políticas de cibersegurança dos Estados-Membros. As análises devem ser realizadas por peritos técnicos em cibersegurança provenientes de***, pelo menos, dois*** Estados-Membros diferentes do Estado-Membro avaliado***, bem como por peritos da ENISA,*** e devem incidir, no mínimo, nos seguintes aspetos:

Alteração 96
Proposta de diretiva
Artigo 16 – n.º 2

Texto da Comissão	*Alteração*
2. A metodologia deve incluir critérios objetivos, não discriminatórios, equitativos e transparentes com base nos quais os Estados-Membros designarão os peritos elegíveis para realizarem as análises pelos pares. A ENISA e a Comissão designam peritos para participarem nas análises pelos pares na qualidade de observadores. Com o apoio da ENISA, a Comissão estabelece, no âmbito da metodologia a que se refere o n.º 1, um sistema objetivo, não discriminatório, equitativo e transparente para a seleção e distribuição aleatória de peritos para cada análise pelos pares.	2. A metodologia deve incluir critérios objetivos, não discriminatórios, ***neutros do ponto de vista tecnológico,*** equitativos e transparentes com base nos quais os Estados-Membros designarão os peritos elegíveis para realizarem as análises pelos pares. A ENISA e a Comissão designam peritos para participarem nas análises pelos pares na qualidade de observadores. Com o apoio da ENISA, a Comissão estabelece, no âmbito da metodologia a que se refere o n.º 1, um sistema objetivo, não discriminatório, equitativo e transparente para a seleção e distribuição aleatória de peritos para cada análise pelos pares.

Alteração 97
Proposta de diretiva
Artigo 18 – n.º 1

Texto da Comissão	*Alteração*
1. Os Estados-Membros devem assegurar que as entidades essenciais e importantes tomam medidas técnicas e organizativas ***adequadas e proporcionadas*** para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam na prestação dos seus serviços. Essas medidas devem garantir um nível de segurança das redes e dos sistemas de informação adequado ao risco em causa, tendo em conta os progressos técnicos mais recentes.	1. Os Estados-Membros devem assegurar que as entidades essenciais e importantes tomam medidas técnicas e organizativas para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam na prestação dos seus serviços. ***Essas medidas devem ser adequadas e proporcionais ao grau de importância do setor ou do tipo de serviço, bem como ao nível de dependência da entidade relativamente a outros setores ou tipos de serviços, e ser adotadas após uma avaliação baseada no risco.*** Essas medidas devem garantir um nível de segurança das redes e dos sistemas de informação adequado ao risco em causa, tendo em conta os progressos técnicos mais recentes. ***Devem, nomeadamente, ser tomadas medidas para prevenir e minimizar o impacto dos incidentes de segurança para os destinatários dos seus serviços.***

Alteração 98
Proposta de diretiva
Artigo 18 – n.º 2 – alínea d)

Texto da Comissão	*Alteração*
d) Segurança da cadeia de fornecimento, ***incluindo*** aspetos de segurança respeitantes às relações entre cada entidade e os respetivos fornecedores ou prestadores de serviços, tais como os prestadores de serviços de armazenamento e tratamento de dados ou serviços de segurança geridos;	d) ***Medidas para a avaliação de riscos de*** segurança da cadeia de fornecimento, ***inclusive sobre*** aspetos de segurança respeitantes às relações entre cada entidade e os respetivos fornecedores ou prestadores de serviços, tais como os prestadores de serviços de armazenamento e tratamento de dados ou serviços de segurança geridos;

Alteração 99
Proposta de diretiva
Artigo 18 – n.º 2 – alínea f)

Texto da Comissão	*Alteração*
f) Políticas e procedimentos (testes e auditoria) para avaliar a eficácia das medidas de gestão dos riscos de cibersegurança;	f) Políticas e procedimentos (testes e auditoria) ***e exercícios de cibersegurança regulares*** para avaliar a eficácia das medidas de gestão dos riscos de cibersegurança;

Alteração 100
Proposta de diretiva
Artigo 18 – n.º 2 – alínea g)

Texto da Comissão	*Alteração*
g) A utilização de criptografia e cifragem**.**	g) A utilização de criptografia e cifragem ***e, em particular, cifragem de ponta a ponta;***

Alteração 101
Proposta de diretiva
Artigo 18 – n.º 2 – alínea g-A) (nova)

Texto da Comissão	*Alteração*
	g-A) Políticas para garantir uma formação e sensibilização adequadas em matéria de cibersegurança.

Alteração 102
Proposta de diretiva
Artigo 18 – n.º 3

Texto da Comissão	*Alteração*
3. Os Estados-Membros devem garantir que, ao ponderarem as medidas adequadas a que se refere o n.º 2, alínea d), as entidades têm em conta as vulnerabilidades específicas de cada fornecedor e cada prestador de serviços, bem como a qualidade global dos produtos	3. Os Estados-Membros devem garantir que, ao ponderarem as medidas adequadas a que se refere o n.º 2, alínea d), as entidades têm em conta***, sempre que tenham acesso às informações pertinentes,*** as vulnerabilidades específicas de cada fornecedor e cada prestador de

e as práticas de cibersegurança dos seus fornecedores e prestadores de serviços, incluindo os respetivos procedimentos de desenvolvimento seguro.	serviços, bem como a qualidade global dos produtos e as práticas de cibersegurança dos seus fornecedores e prestadores de serviços, incluindo os respetivos procedimentos de desenvolvimento seguro.

Alteração 103
Proposta de diretiva
Artigo 18 – n.º 5

Texto da Comissão	*Alteração*
5. A Comissão ***pode*** adotar atos ***de execução*** para definir as especificações técnicas e metodológicas dos elementos a que se refere o n.º 2***. Na preparação desses atos, a Comissão segue o procedimento de exame a que se refere o artigo 37.º, n.º 2,*** e cumpre, tanto quanto possível, normas internacionais e europeias, bem como as especificações técnicas aplicáveis.	5. A Comissão ***fica habilitada a*** adotar atos ***delegados*** para definir as especificações técnicas e metodológicas dos elementos a que se refere o n.º 2 e cumpre, tanto quanto possível, normas internacionais e europeias, bem como as especificações técnicas aplicáveis. ***Ao elaborar atos delegados, a Comissão consulta também todas as partes interessadas pertinentes.***

Alteração 104
Proposta de diretiva
Artigo 18 – n.º 6

Texto da Comissão	*Alteração*
6. A Comissão ***fica habilitada a adotar atos delegados nos termos do artigo 36.º para completar os elementos*** estabelecidos no n.º 2, ***a fim de ter em conta novas ciberameaças, avanços tecnológicos ou especificidades setoriais***.	6. A Comissão***, em colaboração com o grupo de cooperação e a ENISA, fornece orientações e documentos de boas práticas sobre o cumprimento pelas entidades, de forma proporcional aos requisitos*** estabelecidos no n.º 2 ***e***, ***em particular, ao requisito enunciado na alínea d) do mesmo número***.

Alteração 105
Proposta de diretiva
Artigo 19 – n.º 1

Texto da Comissão	*Alteração*
1. Em cooperação com a Comissão e a	1. ***A fim de aumentar o nível geral de***

ENISA, o grupo de cooperação pode realizar avaliações coordenadas dos riscos de segurança de cadeias de fornecimento de produtos, sistemas ou serviços de TIC críticos, tendo em conta fatores de risco de natureza técnica e, quando pertinente, de natureza não técnica.	***cibersegurança e*** em cooperação com a Comissão e a ENISA, o grupo de cooperação pode realizar avaliações coordenadas dos riscos de segurança de cadeias de fornecimento de produtos, sistemas ou serviços de TIC críticos, tendo em conta fatores de risco de natureza técnica e, quando pertinente, de natureza não técnica***, como os riscos geopolíticos***.

Alteração 106
Proposta de diretiva
Artigo 20 – n.º 1

Texto da Comissão	*Alteração*
1. Os Estados-Membros devem assegurar que as entidades essenciais e importantes notificam as autoridades competentes ou a CSIRT, sem demora injustificada e nos termos dos n.os 3 e 4, de qualquer incidente que tenha um impacto significativo na prestação dos seus serviços. Quando pertinente, essas entidades devem notificar os destinatários dos seus serviços, sem demora injustificada, de incidentes suscetíveis de afetar negativamente a prestação desse serviço. Compete aos Estados-Membros garantir que as referidas entidades comunicam, entre outras, quaisquer informações que permitam às autoridades competentes ou à CSIRT determinar o eventual impacto transfronteiriço do incidente.	1. Os Estados-Membros devem assegurar que as entidades essenciais e importantes notificam as autoridades competentes ou a CSIRT, sem demora injustificada e nos termos dos n.os 3 e 4, de qualquer incidente que tenha um impacto significativo na prestação dos seus serviços ***ou de qualquer quase incidente***. Quando pertinente, essas entidades devem notificar os destinatários dos seus serviços, sem demora injustificada, de incidentes suscetíveis de afetar negativamente a prestação desse serviço. Compete aos Estados-Membros garantir que as referidas entidades comunicam, entre outras, quaisquer informações que permitam às autoridades competentes ou à CSIRT determinar o eventual impacto transfronteiriço do ***incidente ou quase*** incidente.

Alteração 107
Proposta de diretiva
Artigo 20 – n.º 1-A (novo)

Texto da Comissão	*Alteração*
	1-A. Com o objetivo de simplificar as obrigações de notificação, os Estados-Membros devem estabelecer um ponto de

	entrada único para todas as notificações exigidas pela presente diretiva e também por outros instrumentos jurídicos da União, como o Regulamento (UE) 2016/679 e a Diretiva 2002/58/CE.

Alteração 108
Proposta de diretiva
Artigo 20 – n.º 1-B) (novo)

Texto da Comissão	*Alteração*
	1-B. A ENISA, em colaboração com o grupo de cooperação, deve criar modelos comuns de notificação por intermédio de orientações destinadas a simplificar e racionalizar a comunicação de informações exigidas pelo direito da União e a reduzir os encargos para as empresas.

Alteração 109
Proposta de diretiva
Artigo 20 – n.º 2 – parágrafo 1

Texto da Comissão	*Alteração*
2. ***Os Estados-Membros devem assegurar que as entidades essenciais e importantes notificam as autoridades competentes ou a CSIRT, sem demora injustificada, de qualquer ciberameaça significativa identificada por essas entidades que pudesse ter dado origem a um incidente significativo.***	***Suprimido***

Alteração 110
Proposta de diretiva
Artigo 20 – n.º 2 – parágrafo 2

Texto da Comissão	*Alteração*
Quando for o caso, as referidas entidades devem notificar, sem demora	***Suprimido***

injustificada, os destinatários dos seus serviços potencialmente afetados por uma ciberameaça significativa das medidas proativas ou corretivas que estes podem tomar para responder a essa ameaça. Quando pertinente, as entidades devem igualmente notificar os referidos destinatários da própria ameaça. A notificação não acarreta responsabilidades acrescidas para a entidade notificadora.

Alteração 111
Proposta de diretiva
Artigo 20 – n.º 3 – alínea a)

Texto da Comissão	*Alteração*
a) Tiver causado ***ou for suscetível de causar*** perturbações operacionais ou perdas financeiras substanciais à entidade em causa;	a) Tiver causado perturbações operacionais ou perdas financeiras substanciais à entidade em causa;

Alteração 112
Proposta de diretiva
Artigo 20 – n.º 3 – alínea b)

Texto da Comissão	*Alteração*
b) Tiver afetado ***ou for suscetível de afetar*** outras pessoas singulares ou coletivas, causando perdas materiais ou não materiais consideráveis.	b) Tiver afetado outras pessoas singulares ou coletivas, causando perdas materiais ou não materiais consideráveis.

Alteração 113
Proposta de diretiva
Artigo 20 – n.º 3-A (novo)

Texto da Comissão	*Alteração*
	3-A. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 36.º para complementar a presente diretiva especificando o tipo de informações apresentadas nos termos do

	n.º 1 do presente artigo e os casos em que um incidente deve ser considerado significativo, na aceção do n.º 3 do presente artigo.

Alteração 114
Proposta de diretiva
Artigo 20 – n.º 4 – alínea -a) (nova)

Texto da Comissão	*Alteração*
	-a) Um alerta precoce no prazo de 24 horas após o conhecimento do incidente, sem obrigação por parte da entidade envolvida de divulgar informações adicionais sobre o incidente;

Alteração 115
Proposta de diretiva
Artigo 20 – n.º 4 – alínea a)

Texto da Comissão	*Alteração*
a) Sem demora injustificada e, em qualquer caso, no prazo de ***24*** horas depois de terem tomado conhecimento do incidente, uma notificação inicial que, se for o caso, deve indicar se o incidente foi presumivelmente causado por um ato ilícito ou malicioso;	a) Sem demora injustificada e, em qualquer caso, no prazo de ***72*** horas depois de terem tomado conhecimento do incidente, uma notificação inicial que, se for o caso, deve indicar se o incidente foi presumivelmente causado por um ato ilícito ou malicioso;

Alteração 116
Proposta de diretiva
Artigo 20 – n.º 4 – alínea c) – parte introdutória

Texto da Comissão	*Alteração*
c) O mais tardar ***um mês*** após a notificação mencionada na alínea a), um relatório ***final*** que contenha, no mínimo, os seguintes elementos:	c) O mais tardar ***três meses*** após a notificação mencionada na alínea a), um relatório ***exaustivo*** que contenha, no mínimo, os seguintes elementos:

Alteração 117
Proposta de diretiva
Artigo 20 – n.º 4 – alínea c) – subalínea i)

Texto da Comissão	*Alteração*
i) uma descrição pormenorizada do incidente, da sua gravidade e do seu impacto,	i) uma descrição ***mais*** pormenorizada do incidente, da sua gravidade e do seu impacto,

Alteração 118
Proposta de diretiva
Artigo 20 – n.º 4 – alínea c-A) (nova)

Texto da Comissão	*Alteração*
	c-A) Caso o incidente ainda esteja em curso no momento da apresentação do relatório exaustivo nos termos da alínea c), deve ser apresentado um relatório final um mês após o incidente ter sido mitigado;

Alteração 119
Proposta de diretiva
Artigo 20 – n.º 7

Texto da Comissão	*Alteração*
7. Nos casos em que seja necessário sensibilizar o público para evitar um incidente ou para responder a um incidente em curso, ou em que a divulgação do incidente seja de interesse público, a autoridade competente ou a CSIRT e, se for o caso, as autoridades ou as CSIRT dos outros Estados-Membros afetados ***podem***, após consulta da entidade em causa, informar o público do incidente ou exigir que a entidade o faça.	7. Nos casos em que seja necessário sensibilizar o público para evitar um incidente ou para responder a um incidente em curso, ou em que a divulgação do incidente seja de interesse público, a autoridade competente ou a CSIRT e, se for o caso, as autoridades ou as CSIRT dos outros Estados-Membros afetados ***devem***, após consulta da entidade em causa, informar o público do incidente ou exigir que a entidade o faça.

Alteração 120
Proposta de diretiva
Artigo 20 – n.º 8

Texto da Comissão	*Alteração*
8. A pedido da autoridade competente ou da CSIRT, o ponto de contacto único deve transmitir as notificações recebidas nos termos ***dos n.os*** 1 ***e 2*** aos pontos de contacto únicos dos outros Estados-Membros afetados.	8. A pedido da autoridade competente ou da CSIRT, o ponto de contacto único deve transmitir as notificações recebidas nos termos ***do n.º*** 1 aos pontos de contacto únicos dos outros Estados-Membros afetados.

Alteração 121
Proposta de diretiva
Artigo 20 – n.º 9

Texto da Comissão	*Alteração*
9. O ponto de contacto único deve apresentar mensalmente à ENISA um relatório de síntese que inclua dados anonimizados e agregados sobre os incidentes, as ciberameaças significativas e os quase incidentes notificados nos termos ***dos n.os*** 1 ***e 2*** e do artigo 27.º A fim de contribuir para a comparabilidade das informações apresentadas, a ENISA pode emitir orientações técnicas sobre os parâmetros das informações a incluir no relatório de síntese.	9. O ponto de contacto único deve apresentar mensalmente à ENISA um relatório de síntese que inclua dados anonimizados e agregados sobre os incidentes, as ciberameaças significativas e os quase incidentes notificados nos termos ***do n.º*** 1 e do artigo 27.º A fim de contribuir para a comparabilidade das informações apresentadas, a ENISA pode emitir orientações técnicas sobre os parâmetros das informações a incluir no relatório de síntese.

Alteração 122
Proposta de diretiva
Artigo 20 – n.º 10

Texto da Comissão	*Alteração*
10. As autoridades competentes devem fornecer às autoridades competentes designadas nos termos da Diretiva (UE) XXXX/XXXX [Diretiva Resiliência das Entidades Críticas] informações sobre os incidentes e as ciberameaças notificadas nos termos ***dos n.os*** 1 ***e 2*** por entidades essenciais identificadas como entidades críticas, ou por entidades equivalentes a entidades críticas, nos termos da diretiva	10. As autoridades competentes devem fornecer às autoridades competentes designadas nos termos da Diretiva (UE) XXXX/XXXX [Diretiva Resiliência das Entidades Críticas] informações sobre os incidentes e as ciberameaças notificadas nos termos ***do n.º*** 1 por entidades essenciais identificadas como entidades críticas, ou por entidades equivalentes a entidades críticas, nos termos da diretiva supramencionada.

supramencionada.

Alteração 123
Proposta de diretiva
Artigo 20 – n.º 11

Texto da Comissão	*Alteração*
11. A Comissão pode adotar atos de execução que especifiquem o tipo de informações, o formato e o procedimento das notificações apresentadas nos termos ***dos n.os*** 1 ***e 2***. A Comissão pode ainda adotar atos de execução que especifiquem os casos em que um incidente deve ser considerado significativo, conforme referido no n.º 3. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 37.º, n.º 2.	11. A Comissão pode adotar atos de execução que especifiquem o tipo de informações, o formato e o procedimento das notificações apresentadas nos termos ***do n.º*** 1. A Comissão pode ainda adotar atos de execução que especifiquem os casos em que um incidente deve ser considerado significativo, conforme referido no n.º 3. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 37.º, n.º 2.

Alteração 124
Proposta de diretiva
Artigo 21 – n.º 1

Texto da Comissão	*Alteração*
1. A fim de demonstrar o cumprimento de certos requisitos estabelecidos no artigo 18.º, os Estados-Membros ***podem exigir que*** as entidades essenciais e importantes ***certifiquem*** determinados produtos de TIC, serviços de TIC e processos de TIC no âmbito de sistemas europeus de ***certificação da*** cibersegurança ***específicos*** adotados nos termos do artigo 49.º do Regulamento (UE) 2019/881***. Os produtos, serviços e processos sujeitos a*** certificação ***podem ser desenvolvidos por uma entidade essencial ou importante ou ser adquiridos a terceiros.***	1. A fim de demonstrar o cumprimento de certos requisitos estabelecidos no artigo 18.º ***e de aumentar o nível de cibersegurança***, os Estados-Membros***, após consulta do grupo de cooperação e da ENISA, devem incentivar*** as entidades essenciais e importantes ***a certificar*** determinados produtos de TIC, serviços de TIC e processos de TIC***, quer sejam desenvolvidos pela entidade essencial ou importante, quer sejam fornecidos por terceiros,*** no âmbito de sistemas europeus de cibersegurança adotados nos termos do artigo 49.º do Regulamento (UE) 2019/881 ***ou no âmbito de sistemas semelhantes de*** certificação ***internacionalmente reconhecidos. Sempre que possível, os Estados-Membros incentivam a utilização harmonizada dos sistemas de certificação adotados.***

Alteração 125
Proposta de diretiva
Artigo 21 – n.º 2

Texto da Comissão	*Alteração*
2. A Comissão ***fica habilitada a adotar atos delegados que especifiquem*** as categorias de entidades essenciais ***obrigadas*** a obter um certificado e os sistemas europeus de certificação da cibersegurança a que devem recorrer para o efeito nos termos do n.º 1. ***Os atos delegados são adotados em conformidade com o artigo 36.º.***	2. A Comissão ***avalia regularmente a eficiência e a utilização dos sistemas europeus de certificação da cibersegurança adotados nos termos do artigo 49.º do Regulamento (UE) 2019/881 e identifica*** as categorias de entidades essenciais ***que serão incentivadas*** a obter um certificado e os sistemas europeus de certificação da cibersegurança a que devem recorrer para o efeito nos termos do n.º 1.

Alteração 126
Proposta de diretiva
Artigo 22 – n.º -1 (novo)

Texto da Comissão	*Alteração*
	-1. A Comissão, em colaboração com a ENISA, apoia e promove o desenvolvimento e a aplicação das normas estabelecidas pelos organismos de normalização pertinentes, internacionais e da União, tendo em vista a aplicação convergente do artigo 18.º, n.os 1 e 2. A Comissão apoia a atualização das normas à luz da evolução tecnológica.

Alteração 127
Proposta de diretiva
Artigo 22 – n.º 1

Texto da Comissão	*Alteração*
1. A fim de promover a aplicação convergente do artigo 18.º, n.os 1 e 2, os Estados-Membros devem incentivar, sem imporem ou discriminarem em favor da utilização de um determinado tipo de	1. A fim de promover a aplicação convergente do artigo 18.º, n.os 1 e 2, os Estados-Membros devem incentivar, sem imporem ou discriminarem em favor da utilização de um determinado tipo de

tecnologia, a utilização de normas e especificações europeias ou internacionalmente aceites aplicáveis à segurança das redes e dos sistemas de informação.	tecnologia, ***e de acordo com as orientações da ENISA e do grupo de cooperação,*** a utilização de normas e especificações europeias ou internacionalmente aceites aplicáveis à segurança das redes e dos sistemas de informação.

Alteração 128
Proposta de diretiva
Artigo 23 – Título

Texto da Comissão	*Alteração*
Bases de dados dos nomes de domínio e dos dados de registo	***Infraestruturas de*** bases de dados dos nomes de domínio e dos dados de registo

Alteração 129
Proposta de diretiva
Artigo 23 – n.º 1

Texto da Comissão	*Alteração*
1. Com vista a contribuir para a segurança, a estabilidade e a resiliência do DNS, os Estados-Membros devem garantir que os registos de domínios de topo e as entidades que prestam serviços de registo de nomes de domínio a esses registos recolhem e mantêm dados exatos e completos relativos ao registo de nomes de domínio numa base de dados específica, com a devida diligência, em conformidade com a legislação da União em matéria de proteção de dados no que respeita aos dados pessoais.	1. Com vista a contribuir para a segurança, a estabilidade e a resiliência do DNS, os Estados-Membros devem garantir que os registos de domínios de topo e as entidades que prestam serviços de registo de nomes de domínio a esses registos recolhem***, verificam*** e mantêm dados exatos e completos relativos ao registo de nomes de domínio ***necessários à prestação dos seus serviços*** numa base de dados específica, com a devida diligência, em conformidade com a legislação da União em matéria de proteção de dados no que respeita aos dados pessoais.

Alteração 130
Proposta de diretiva
Artigo 23 – n.º 2

Texto da Comissão	*Alteração*
2. Os Estados-Membros devem assegurar que as bases de dados relativos	2. Os Estados-Membros devem assegurar que as ***infraestruturas de*** bases

ao registo de nomes de domínio a que se refere o n.º 1 contêm as informações necessárias para identificar e contactar os titulares dos nomes de domínio e os pontos de contacto que administram os nomes de domínio sob o domínio de topo.	de dados relativos ao registo de nomes de domínio a que se refere o n.º 1 contêm as informações ***pertinentes, que devem incluir, pelo menos, o nome, o endereço físico, o endereço de correio eletrónico e o número de telefone dos requerentes do registo,*** necessárias para identificar e contactar os titulares dos nomes de domínio e os pontos de contacto que administram os nomes de domínio sob o domínio de topo***, incluindo, pelo menos, o nome, o endereço físico, o endereço de correio eletrónico e o número de telefone dos requerentes do registo***.

Alteração 131
Proposta de diretiva
Artigo 23 – n.º 3

Texto da Comissão	*Alteração*
3. Os Estados-Membros devem ainda garantir que os registos de domínios de topo e as entidades que prestam serviços de registo de nomes de domínio a esses registos dispõem de políticas e procedimentos para assegurar que as bases de dados contêm informações exatas e completas. Os Estados-Membros devem certificar-se de que essas políticas e procedimentos são tornados públicos.	3. Os Estados-Membros devem ainda garantir que os registos de domínios de topo e as entidades que prestam serviços de registo de nomes de domínio a esses registos dispõem de políticas e procedimentos para assegurar que as ***infraestruturas de*** bases de dados contêm informações exatas***, verificadas*** e completas***, e que dados incorretos ou incompletos são corrigidos ou eliminados pelo requerente do registo sem demora***. Os Estados-Membros devem certificar-se de que essas políticas e procedimentos são tornados públicos.

Alteração 132
Proposta de diretiva
Artigo 23 – n.º 4

Texto da Comissão	*Alteração*
4. Os Estados-Membros devem garantir que os registos de domínios de topo e as entidades que prestam serviços de registo de nomes de domínio ***a esses***	4. Os Estados-Membros devem garantir que os registos de domínios de topo e as entidades que prestam serviços de registo de nomes de domínio

registos publicam, sem demora injustificada após o registo de um nome de domínio, os dados relativos ao registo do domínio ***que não sejam dados pessoais***.

disponibilizam publicamente, sem demora injustificada ***e, em qualquer caso, no prazo de 24 horas*** após o registo de um nome de domínio, ***todos*** os dados relativos ao registo do domínio ***de pessoas coletivas enquanto requerentes de registo***.

Alteração 133
Proposta de diretiva
Artigo 23 – n.º 5

Texto da Comissão	*Alteração*
5. Os Estados-Membros devem assegurar que os registos de domínios de topo e as entidades que prestam serviços de registo de nomes de domínio ***a esses registos concedem*** acesso a dados específicos relativos ao registo de nomes de domínio aos requerentes legítimos de acesso que apresentem um pedido ***lícito e*** devidamente justificado, em conformidade com a legislação da União em matéria de proteção de dados. Os Estados-Membros devem assegurar que ***os*** registos de domínios de topo e ***as*** entidades que ***prestam*** serviços de registo de nomes de domínio ***a esses registos*** respondem a todos os pedidos de acesso sem demora injustificada. Compete aos Estados-Membros garantir que as políticas e procedimentos de divulgação dos referidos dados são tornados públicos.	5. Os Estados-Membros devem assegurar que os registos de domínios de topo e as entidades que prestam serviços de registo de nomes de domínio ***são obrigados a conceder*** acesso a dados específicos relativos ao registo de nomes de domínio aos requerentes legítimos de acesso que apresentem um pedido devidamente justificado, em conformidade com a legislação da União em matéria de proteção de dados. Os Estados-Membros devem assegurar que registos de domínios de topo e entidades que ***prestem*** serviços de registo de nomes de domínio respondem a todos os pedidos de acesso ***lícitos e devidamente justificados*** sem demora injustificada ***e, em qualquer caso, no prazo de 72 horas***. Compete aos Estados-Membros garantir que as políticas e procedimentos de divulgação dos referidos dados são tornados públicos.

Alteração 134
Proposta de diretiva
Artigo 24 – n.º 2

Texto da Comissão	*Alteração*
2. Para efeitos da presente diretiva, considera-se que as entidades referidas no n.º 1 têm o seu estabelecimento principal na União no Estado-Membro em que são tomadas as decisões relacionadas com as	2. Para efeitos da presente diretiva, considera-se que as entidades referidas no n.º 1 têm o seu estabelecimento principal na União no Estado-Membro em que são tomadas as decisões relacionadas com as

medidas de gestão dos riscos de cibersegurança. Se tais decisões não forem tomadas num estabelecimento situado na União, considera-se que o estabelecimento principal se situa no Estado-Membro em que as entidades têm o estabelecimento com o maior número de trabalhadores na União.	medidas de gestão dos riscos de cibersegurança. Se tais decisões não forem tomadas num estabelecimento situado na União, considera-se que o estabelecimento principal se situa no Estado-Membro em que as entidades têm o estabelecimento com o maior número de trabalhadores na União. ***Tal deve ser feito de forma a assegurar que as entidades reguladoras nacionais não têm de suportar encargos desproporcionados.***

Alteração 135
Proposta de diretiva
Artigo 25 – n.º 1 – parte introdutória

Texto da Comissão	*Alteração*
1. A ENISA deve criar e manter um registo das entidades essenciais e importantes referidas no artigo 24.º, n.º 1. As entidades devem fornecer as seguintes informações à ENISA até [o mais tardar 12 meses após a entrada em vigor da diretiva]:	1. A ENISA deve criar e manter um registo das entidades essenciais e importantes referidas no artigo 24.º, n.º 1. ***Para o efeito,*** as entidades devem fornecer as seguintes informações à ENISA até [o mais tardar 12 meses após a entrada em vigor da diretiva]:

Alteração 136
Proposta de diretiva
Artigo 26 – n.º 1 – alínea b)

Texto da Comissão	*Alteração*
b) Reforce o nível de cibersegurança, em especial ao sensibilizar para as ciberameaças, limitar ou impedir a sua capacidade de disseminação e apoiar um leque de capacidades defensivas, a correção e divulgação de vulnerabilidades, as técnicas de deteção de ameaças, as estratégias de atenuação ou as fases de resposta e recuperação.	b) Reforce o nível de cibersegurança, em especial ao sensibilizar para as ciberameaças, limitar ou impedir a sua capacidade de disseminação e apoiar um leque de capacidades defensivas, a correção e divulgação de vulnerabilidades, as técnicas de deteção ***e prevenção*** de ameaças, as estratégias de atenuação ou as fases de resposta e recuperação.

Alteração 137
Proposta de diretiva
Artigo 26 – n.º 3

Texto da Comissão	*Alteração*
3. Os Estados-Membros devem definir ***regras*** que especifiquem o procedimento, os elementos operacionais (incluindo a utilização de plataformas TIC dedicadas), o teor e as condições dos acordos de partilha de informações a que se refere o n.º 2. Tais ***regras*** devem também ***definir*** os pormenores do envolvimento das autoridades públicas nesses acordos, bem como os elementos operacionais, incluindo a utilização de plataformas TIC dedicadas. Os Estados-Membros devem oferecer apoio à aplicação de tais acordos, em conformidade com as suas políticas a que se refere o artigo 5.º, n.º 2, alínea g).	3. Os Estados-Membros devem definir ***orientações*** que especifiquem o procedimento, os elementos operacionais (incluindo a utilização de plataformas TIC dedicadas), o teor e as condições dos acordos de partilha de informações a que se refere o n.º 2. Tais ***orientações*** devem também ***incluir*** os pormenores do envolvimento***, se for o caso,*** das autoridades públicas ***e dos peritos independentes*** nesses acordos, bem como os elementos operacionais, incluindo a utilização de plataformas TIC dedicadas. Os Estados-Membros devem oferecer apoio à aplicação de tais acordos, em conformidade com as suas políticas a que se refere o artigo 5.º, n.º 2, alínea g).

Alteração 138
Proposta de diretiva
Artigo 26 – n.º 5

Texto da Comissão	*Alteração*
5. Em conformidade com a legislação da União, a ENISA deve apoiar a celebração dos acordos de partilha de informações sobre cibersegurança referidos no n.º 2, fornecendo documentos de boas práticas e orientações.	5. Em conformidade com a legislação da União, a ENISA deve apoiar a celebração dos acordos de partilha de informações sobre cibersegurança referidos no n.º 2, fornecendo documentos de boas práticas e orientações ***e facilitando a partilha de informações à escala da União, sem descurar a salvaguarda de informações comerciais sensíveis***. ***A pedido das entidades essenciais e importantes, o grupo de cooperação deve ser convidado a fornecer documentos de boas práticas e orientações.***

Alteração 139
Proposta de diretiva
Artigo 27 – n.º -1 (novo)

Texto da Comissão	*Alteração*
	-1. Os Estados-Membros devem assegurar que as entidades essenciais e importantes podem apresentar, a título voluntário, notificações de ciberameaças detetadas por essas entidades que pudessem ter dado origem a um incidente significativo. Os Estados-Membros devem assegurar que, para efeitos destas notificações, as entidades aplicam o procedimento previsto no artigo 20.º. As notificações voluntárias não podem dar origem à imposição de quaisquer obrigações adicionais à entidade notificadora.

Alteração 140
Proposta de diretiva
Artigo 27 – n.º 1

Texto da Comissão	*Alteração*
Sem prejuízo do disposto no artigo 3.º, os Estados-Membros devem assegurar que as entidades não abrangidas pelo âmbito da presente diretiva podem apresentar notificações, a título voluntário, de incidentes significativos, ciberameaças ou quase incidentes. No tratamento das notificações, os Estados-Membros devem aplicar o procedimento previsto no artigo 20.º. Os Estados-Membros ***podem*** dar prioridade ao tratamento das notificações obrigatórias em relação às notificações voluntárias. A notificação voluntária não pode dar origem à imposição de quaisquer obrigações adicionais à entidade notificadora, às quais não estaria sujeita se não tivesse apresentado a notificação.	***1.*** Sem prejuízo do disposto no artigo 3.º, os Estados-Membros devem assegurar que as entidades não abrangidas pelo âmbito da presente diretiva podem apresentar notificações, a título voluntário, de incidentes significativos, ciberameaças ou quase incidentes. No tratamento das notificações, os Estados-Membros devem aplicar o procedimento previsto no artigo 20.º. Os Estados-Membros ***devem*** dar prioridade ao tratamento das notificações obrigatórias em relação às notificações voluntárias. A notificação voluntária não pode dar origem à imposição de quaisquer obrigações adicionais à entidade notificadora, às quais não estaria sujeita se não tivesse apresentado a notificação***, mas o Estado-Membro pode conceder-lhe ajuda através das CSIRT***.

Alteração 141
Proposta de diretiva
Artigo 28 – n.º 1

Texto da Comissão	*Alteração*
1. Os Estados-Membros devem assegurar que as autoridades competentes controlam eficazmente o cumprimento da presente diretiva e tomam as medidas necessárias para garantir esse cumprimento, em especial das obrigações previstas nos artigos 18.º e 20.º.	1. Os Estados-Membros devem assegurar que as autoridades competentes controlam eficazmente o cumprimento da presente diretiva e tomam as medidas necessárias para garantir esse cumprimento, em especial das obrigações previstas nos artigos 18.º e 20.º***, e que dispõem dos meios adequados para desempenhar o seu papel***.

Alteração 142
Proposta de diretiva
Artigo 28 – n.º 2

Texto da Comissão	*Alteração*
2. Quando tratarem de incidentes que tenham originado violações de dados pessoais, as autoridades competentes devem trabalhar em estreita colaboração com as autoridades encarregadas da proteção de dados.	2. Quando tratarem de incidentes que tenham originado violações de dados pessoais, as autoridades competentes devem trabalhar em estreita colaboração com as autoridades encarregadas da proteção de dados***, incluindo as autoridades encarregadas da proteção de dados de outros Estados-Membros, quando pertinente***.

Alteração 143
Proposta de diretiva
Artigo 29 – n.º 2 – alínea c)

Texto da Comissão	*Alteração*
c) Auditorias de segurança específicas com base em avaliações de riscos ou informações disponíveis relacionadas com os riscos;	c) Auditorias de segurança específicas com base em avaliações de riscos ou informações disponíveis relacionadas com os riscos***, realizadas por uma entidade independente qualificada ou por uma autoridade competente***;

Alteração 144
Proposta de diretiva
Artigo 29 – n.º 2 – alínea f)

Texto da Comissão	*Alteração*
f) Pedidos de acesso a dados, documentos ou ***quaisquer*** informações necessárias para o desempenho das suas funções de supervisão;	f) Pedidos de acesso a dados, documentos ou informações ***pertinentes*** necessárias para o desempenho das suas funções de supervisão;

Alteração 145
Proposta de diretiva
Artigo 29 – n.º 3

Texto da Comissão	*Alteração*
3. Ao exercerem os poderes previstos no n.º 2, alíneas e) a g), as autoridades competentes devem indicar a finalidade do pedido ***e*** especificar as informações solicitadas.	3. Ao exercerem os poderes previstos no n.º 2, alíneas e) a g), as autoridades competentes devem indicar a finalidade do pedido***,*** especificar as informações solicitadas ***e limitar os seus pedidos ao âmbito do incidente ou motivo de preocupação***.

Alteração 146
Proposta de diretiva
Artigo 29 – n.º 5 – parágrafo 1 – alínea a)

Texto da Comissão	*Alteração*
a) Suspender ou solicitar a um organismo de certificação ou autorização a suspensão de uma certificação ou autorização relativa a ***uma parte ou à totalidade dos*** serviços ou atividades prestadas por uma entidade essencial;	a) Suspender ou solicitar a um organismo de certificação ou autorização a suspensão de uma certificação ou autorização relativa a serviços ou atividades ***pertinentes*** prestadas por uma entidade essencial;

Alteração 147
Proposta de diretiva
Artigo 29 – n.º 5 – parágrafo 1 – alínea b)

Texto da Comissão	*Alteração*
b) Impor ou solicitar a imposição,	***Suprimido***

por parte dos organismos ou tribunais competentes, de acordo com a legislação nacional, de uma proibição temporária de exercer funções de gestão nessa entidade essencial contra qualquer pessoa com responsabilidades de gestão a nível de diretor executivo ou representante legal e qualquer outra pessoa singular considerada responsável pela violação.

Alteração 148
Proposta de diretiva
Artigo 30 – n.º 1

Texto da Comissão	*Alteração*
1. Sempre que lhes sejam apresentadas provas ou indícios de que uma entidade importante não está a cumprir as obrigações previstas na presente diretiva, em especial nos artigos 18.º e 20.º, os Estados-Membros devem assegurar que as autoridades competentes atuam em conformidade, se necessário, tomando medidas de supervisão ex post.	1. Sempre que lhes sejam apresentadas provas ou indícios de que uma entidade importante não está a cumprir as obrigações previstas na presente diretiva, em especial nos artigos 18.º e 20.º, os Estados-Membros devem assegurar que as autoridades competentes atuam em conformidade, se necessário ***e tendo em conta uma abordagem baseada no risco***, tomando medidas de supervisão ex post.

Alteração 149
Proposta de diretiva
Artigo 30 – n.º 2 – alínea b)

Texto da Comissão	*Alteração*
b) Auditorias de segurança específicas com base em avaliações de riscos ou informações disponíveis relacionadas com os riscos;	b) Auditorias de segurança específicas com base em avaliações de riscos ou informações disponíveis relacionadas com os riscos***, realizadas por uma entidade independente qualificada ou por uma autoridade competente***;

Alteração 150
Proposta de diretiva
Artigo 30 – n.º 3

Texto da Comissão	*Alteração*
3. Ao exercerem os poderes previstos no n.º 2, alíneas d) ou e), as autoridades competentes devem indicar a finalidade do pedido ***e*** especificar as informações solicitadas.	3. Ao exercerem os poderes previstos no n.º 2, alíneas d) ou e), as autoridades competentes devem indicar a finalidade do pedido***,*** especificar as informações solicitadas ***e limitar os seus pedidos ao âmbito do incidente ou motivo de preocupação***.

Alteração 151
Proposta de diretiva
Artigo 31 – n.º 4

Texto da Comissão	*Alteração*
4. Os Estados-Membros devem assegurar que as violações das obrigações previstas nos artigos 18.º ou 20.º são sujeitas, nos termos dos n.os 2 e 3 do presente artigo, a coimas num montante máximo ***não inferior a*** 10 000 000 EUR ou 2 % do volume de negócios anual a nível mundial, correspondente ao exercício financeiro anterior, da empresa a que a entidade essencial ou importante pertence, consoante o montante que for mais elevado.	4. Os Estados-Membros devem assegurar que as violações das obrigações previstas nos artigos 18.º ou 20.º são sujeitas, nos termos dos n.os 2 e 3 do presente artigo, a coimas num montante máximo ***de*** 10 000 000 EUR ou 2 % do volume de negócios anual a nível mundial, correspondente ao exercício financeiro anterior, da empresa a que a entidade essencial ou importante pertence, consoante o montante que for mais elevado.

Alteração 152
Proposta de diretiva
Artigo 32 – n.º 1

Texto da Comissão	*Alteração*
1. Se as autoridades competentes tiverem indícios de que a infração das obrigações estabelecidas nos artigos 18.º e 20.º por parte de uma entidade essencial ou importante implica uma violação de dados pessoais, na aceção do artigo 4.º, ponto 12, do Regulamento (UE) 2016/679, a qual deve ser notificada nos termos do artigo 33.º do referido regulamento, devem informar as autoridades de controlo	1. Se as autoridades competentes tiverem indícios de que a infração das obrigações estabelecidas nos artigos 18.º e 20.º por parte de uma entidade essencial ou importante implica uma violação de dados pessoais, na aceção do artigo 4.º, ponto 12, do Regulamento (UE) 2016/679, a qual deve ser notificada nos termos do artigo 33.º do referido regulamento, devem informar as autoridades de controlo

competentes nos termos dos artigos 55.º e 56.º do referido regulamento ***num*** prazo ***razoável***.	competentes nos termos dos artigos 55.º e 56.º do referido regulamento ***sem demora injustificada e, em qualquer caso, no*** prazo ***de 72 horas***.

Alteração 153
Proposta de diretiva
Artigo 32 – n.º 3

Texto da Comissão	*Alteração*
3. Se a autoridade de controlo competente nos termos do Regulamento (UE) 2016/679 estiver estabelecida num Estado-Membro diferente do da autoridade competente, esta última ***pode*** informar a autoridade de controlo estabelecida no seu Estado-Membro.	3. Se a autoridade de controlo competente nos termos do Regulamento (UE) 2016/679 estiver estabelecida num Estado-Membro diferente do da autoridade competente, esta última ***deve também*** informar a autoridade de controlo estabelecida no seu Estado-Membro.

Alteração 154
Proposta de diretiva
Artigo 36 – n.º 2

Texto da Comissão	*Alteração*
2. O poder de adotar atos delegados referido no artigo 18.º, n.º ***6***, e no artigo ***21***.º, n.º ***2***, é conferido à Comissão por um prazo de cinco anos a contar de […].	2. O poder de adotar atos delegados referido no artigo 18.º, n.º ***5***, e no artigo ***20***.º, n.º ***3***, é conferido à Comissão por um prazo de cinco anos a contar de […].

Alteração 155
Proposta de diretiva
Artigo 36 – n.º 3

Texto da Comissão	*Alteração*
3. ***A delegação de poderes referida no*** artigo 18.º, n.º ***6***, e ***no*** artigo ***21***.º, n.º ***2***, ***pode ser revogada em qualquer momento*** pelo Parlamento Europeu ou pelo Conselho. ***A decisão de revogação põe termo à delegação dos poderes nela especificados. Produz efeitos a partir do dia seguinte ao da sua publicação no***	3. ***Os atos delegados adotados nos termos do*** artigo 18.º, n.º ***5***, e ***do*** artigo ***20***.º, n.º ***3***, ***só entram em vigor se não tiverem sido formuladas objeções*** pelo Parlamento Europeu ou pelo Conselho ***no prazo de três meses a contar da notificação do ato a estas duas instituições ou se, antes do termo desse***

Jornal Oficial da União Europeia ou de uma data posterior nela especificada. A decisão de revogação não afeta os atos delegados já em vigor.	***prazo, o Parlamento Europeu e o Conselho informarem a Comissão de que não formularão objeções. O referido prazo é prorrogável por três meses por iniciativa do Parlamento Europeu ou do Conselho.***

Alteração 156
Proposta de diretiva
Artigo 36 – n.º 6

Texto da Comissão	*Alteração*
6. Os atos delegados adotados nos termos do artigo 18.º, n.º ***6***, e do artigo ***21***.º, n.º ***2***, 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 do ato ao Parlamento Europeu e ao Conselho, ou se, antes do termo desse prazo, o Parlamento Europeu e o Conselho tiverem informado a Comissão de que não têm objeções a formular. O referido prazo é prorrogável por dois meses por iniciativa do Parlamento Europeu ou do Conselho.	6. Os atos delegados adotados nos termos do artigo 18.º, n.º ***5***, e do artigo ***20***.º, n.º ***3***, 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 do ato ao Parlamento Europeu e ao Conselho, ou se, antes do termo desse prazo, o Parlamento Europeu e o Conselho tiverem informado a Comissão de que não têm objeções a formular. O referido prazo é prorrogável por dois meses por iniciativa do Parlamento Europeu ou do Conselho.

ANEXO: LISTA DE ENTIDADES OU PESSOAS SINGULARES DE QUEM O RELATOR RECEBEU CONTRIBUTOS

A seguinte lista é elaborada a título meramente facultativo, sob a responsabilidade exclusiva do relator. O relator recebeu contributos das seguintes entidades ou pessoas singulares aquando da preparação do presente parecer, até à sua aprovação em comissão:

Pessoa singular	Entidade
	BSA (The Software Alliance)
	BusinessEurope
	Confederação da indústria dinamarquesa
	Representação Permanente da Dinamarca
	Deutsche Telekom
	Europa Digital
	DOT Europe
	ETNO (Associação dos Operadores Europeus de Redes de Telecomunicações)
	Representação Permanente da França
	Representação Permanente da Alemanha
	HUAWEI
	FIIF
	INTEL
	ITI (The Information Technology Industry Council)
	Kaspersky
	MÆRSK
	Microsoft
	ICANN
	MOTION PICTURE ASSOCIATION
	Orgalim
	Palo Alto Networks

	Rettighedsalliancen

PROCESSO DA COMISSÃO ENCARREGADA DE EMITIR PARECER

Título	Medidas destinadas a garantir um elevado nível comum de cibersegurança na União e revogação da Diretiva (UE) 2016/1148
Referências	COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)
Comissão competente quanto ao fundo Data de comunicação em sessão	ITRE 21.1.2021
Parecer emitido por Data de comunicação em sessão	IMCO 21.1.2021
Relator(a) de parecer Data de designação	Morten Løkkegaard 9.2.2021
Exame em comissão	26.5.2021 21.6.2021
Data de aprovação	12.7.2021
Resultado da votação final	+: 42 –: 1 0: 2
Deputados presentes no momento da votação final	Alex Agius Saliba, Andrus Ansip, Pablo Arias Echeverría, Alessandra Basso, Brando Benifei, Adam Bielan, Hynek Blaško, Biljana Borzan, Vlad-Marius Botoş, Markus Buchheit, Andrea Caroppo, Anna Cavazzini, Dita Charanzová, Deirdre Clune, David Cormand, Carlo Fidanza, Evelyne Gebhardt, Alexandra Geese, Sandro Gozi, Maria Grapini, Svenja Hahn, Virginie Joron, Eugen Jurzyca, Marcel Kolaja, Kateřina Konečná, Andrey Kovatchev, Jean-Lin Lacapelle, Maria-Manuel Leitão-Marques, Morten Løkkegaard, Antonius Manders, Leszek Miller, Anne-Sophie Pelletier, Miroslav Radačovský, Christel Schaldemose, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Róża Thun und Hohenstein, Marco Zullo
Suplentes presentes no momento da votação final	Clara Aguilera, Maria da Graça Carvalho, Christian Doleschal, Claude Gruffat, Jiří Pospíšil, Kosma Złotowski

VOTAÇÃO NOMINAL FINAL
NA COMISSÃO ENCARREGADA DE EMITIR PARECER

42	+
ECR	Adam Bielan, Carlo Fidanza, Kosma Złotowski
ID	Alessandra Basso, Hynek Blaško, Markus Buchheit, Virginie Joron, Jean-Lin Lacapelle
PPE	Pablo Arias Echeverría, Andrea Caroppo, Maria da Graça Carvalho, Deirdre Clune, Christian Doleschal, Andrey Kovatchev, Antonius Manders, Jiří Pospíšil, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Róża Thun und Hohenstein
Renew	Andrus Ansip, Vlad-Marius Botoş, Dita Charanzová, Sandro Gozi, Morten Løkkegaard, Marco Zullo
S&D	Alex Agius Saliba, Clara Aguilera, Brando Benifei, Biljana Borzan, Evelyne Gebhardt, Maria Grapini, Maria-Manuel Leitão-Marques, Leszek Miller, Christel Schaldemose
The Left	Kateřina Konečná, Anne-Sophie Pelletier
Verts/ALE	Anna Cavazzini, David Cormand, Alexandra Geese, Claude Gruffat, Marcel Kolaja

1	-
NI	Miroslav Radačovský

2	0
ECR	Eugen Jurzyca
Renew	Svenja Hahn

Legenda dos símbolos utilizados:
+ : votos a favor
- : votos contra
0 : abstenções