

**Bruxelas, 6 de dezembro de 2024
(OR. en)**

16527/24

**CYBER 360
TELECOM 369
COSI 231
COPEN 535
CSDP/PSDC 854
DATAPROTECT 347
RECH 534
HYBRID 146
IPCR 72
JAI 1814
RELEX 1549
POLMIL 420**

RESULTADOS DOS TRABALHOS

de:	Secretariado-Geral do Conselho
para:	Delegações
Assunto:	Conclusões do Conselho sobre a ENISA

Junto se enviam, à atenção das delegações, as Conclusões do Conselho sobre a ENISA, aprovadas pelo Conselho na sua reunião realizada a 6 de dezembro de 2024.

Conclusões do Conselho sobre a ENISA

O CONSELHO DA UNIÃO EUROPEIA,

1. SALIENTA que os desafios decorrentes do ciberespaço mundial nunca foram tão complexos, diversificados e graves como nos dias de hoje, devido à sofisticação das ciberameaças emergentes, ao ambiente de segurança em constante mudança e às atuais tensões geopolíticas. Por conseguinte, a UE e os seus Estados-Membros deverão prosseguir os seus esforços para se tornarem mais resilientes, com vista a identificar e enfrentar eficazmente as ameaças e os desafios atuais e emergentes. SUBLINHA que o trabalho para aumentar o nível de ciber-resiliência deverá ser continuado, seguindo uma abordagem que englobe toda a sociedade. REALÇA que, nos próximos anos, a UE e os seus Estados-Membros deverão concentrar-se na implementação eficaz das iniciativas legislativas e não legislativas que sustentam e contribuem para todas as ações que foram empreendidas até agora neste sentido.

2. LEMBRANDO que a segurança nacional continua a ser da exclusiva responsabilidade de cada Estado-Membro, REGISTA que a UE e os seus Estados-Membros trabalharam intensamente, em conjunto, nos últimos anos para estabelecer a estrutura institucional e as formas de colaboração necessárias, tanto a nível nacional como da UE, no domínio do ciberespaço. SAÚDA as várias iniciativas legislativas e não legislativas que forneceram à UE e aos seus Estados-Membros um quadro forte e robusto neste domínio, aumentando a ciber-resiliência global da União. Este quadro tem vindo a evoluir para abranger vários aspetos do domínio do ciberespaço: segurança, diplomacia, aplicação da lei e defesa. OBSERVA que um grande número de intervenientes, incluindo as autoridades de cibersegurança dos Estados-Membros, o grupo de cooperação SRI, a rede de equipas de resposta a incidentes de segurança informática (rede de CSIRT), a Rede Europeia de Organizações de Coordenação de Cibercrises (UE-CyCLONe), a Rede de Centros Nacionais de Coordenação, o Grupo Europeu para a Certificação da Cibersegurança (GECC), a Comissão, o Serviço Europeu para a Ação Externa (SEAE), a Agência da União Europeia para a Cibersegurança (ENISA), o Centro Europeu de Competências em Cibersegurança, o Serviço de Cibersegurança para as Instituições, Órgãos e Organismos da União (CERT-UE), a Agência Europeia de Defesa (AED) e o Centro Europeu da Cibercriminalidade da Europol (EC3), fazem parte do ecossistema de cibersegurança da UE, desempenhando cada um deles a sua parte na aplicação do quadro de cibersegurança à escala da UE.
3. RECONHECE que, ao longo das últimas duas décadas, a ENISA demonstrou ser uma entidade inestimável no ecossistema europeu de cibersegurança, desempenhando um papel crucial ao ajudar ativamente os Estados-Membros e as instituições, órgãos e organismos da UE a implementarem e desenvolverem políticas de cibersegurança, a reforçarem as suas capacidades e o seu grau de preparação, a cooperarem e a promoverem a sensibilização e a certificação em matéria de cibersegurança.

RECOMENDAÇÕES GERAIS DE ATUAÇÃO

4. CONVIDA a Comissão a utilizar **a avaliação do Regulamento Cibersegurança** como uma oportunidade para analisar a forma como este pode contribuir para a simplificação do complexo ecossistema de cibersegurança, reforçando assim a eficácia e a utilização eficiente dos recursos. Por conseguinte, APELA à Comissão para que assegure que o mandato da ENISA – apoiar os Estados-Membros e as instituições, órgãos e organismos da UE – seja preciso e claramente definido, com objetivos estratégicos concretos e atribuições hierarquizadas por ordem de prioridade, para além de estabelecer uma repartição mais precisa das atribuições e competências em relação a outros intervenientes. A este respeito, CONVIDA a Comissão a analisar e a reforçar ainda mais o papel da ENISA no apoio à cooperação operacional a nível da UE e entre os Estados-Membros no sentido de melhorar a ciber-resiliência, tendo em conta as competências dos Estados-Membros neste domínio. Além disso, APELA à Comissão para que reforce o papel consultivo da ENISA no que toca a fornecer orientações e recomendações especializadas e baseadas em dados concretos no que diz respeito à implementação das atuais e futuras iniciativas legislativas e não legislativas da UE, assegurando simultaneamente um quadro coerente da UE em matéria de cibersegurança.

5. No mesmo espírito, INCENTIVA a Comissão a ponderar a possibilidade de simplificar o papel da ENISA no que diz respeito às atribuições que não estão no cerne da sua missão. SUBLINHA que **as responsabilidades da ENISA foram significativamente alargadas** por iniciativas legislativas recentes, incluindo a Diretiva SRI 2, o Regulamento de Ciber-Resiliência e o Regulamento de Cibersolidariedade, entre outras. Embora REGISTE que a ENISA recebeu recursos adicionais em resultado de algumas destas iniciativas, SALIENTA que o alargamento das responsabilidades da ENISA e a crescente complexidade das ciberameaças e dos desafios do ciberespaço conduziram a um aumento considerável das suas atribuições, o que se deverá refletir em **recursos adequados** – humanos, financeiros e técnicos – a fim de permitir à Agência executar plenamente todas as atribuições da sua competência, sem prejuízo da negociação do quadro financeiro plurianual. Para o efeito, APELA à Comissão para que hierarquize as ações e dê prioridade às atribuições relacionadas com o apoio aos Estados-Membros no reforço da sua ciber-resiliência e da sua cooperação operacional e no desenvolvimento e aplicação do direito da União aquando da elaboração do projeto de orçamento geral da União.

APOIO DA ENISA À ELABORAÇÃO E À EXECUÇÃO DAS POLÍTICAS

6. RECORDA que, ao abrigo do atual quadro jurídico em matéria de cibersegurança, a ENISA tem várias responsabilidades essenciais de apoio e aconselhamento em toda a UE. CONGRATULA-SE com o papel da ENISA a este respeito, no que toca a prestar **assistência aos Estados-Membros** na aplicação efetiva de iniciativas legislativas e não legislativas. EXORTA a ENISA, em estreita cooperação com o grupo de cooperação SRI e com a Comissão, a continuar a fornecer informações e análises gerais sobre o atual quadro jurídico em matéria de cibersegurança. INCENTIVA a ENISA a partilhar e a promover ativamente orientações técnicas e boas práticas de forma regular e estruturada, ajudando os Estados-Membros a aplicar as políticas e a legislação em matéria de cibersegurança.

7. RECONHECE o papel vital da ENISA no desenvolvimento dos **sistemas europeus de certificação da cibersegurança**, que reforçam a confiança nos produtos, serviços e processos de TIC e, também, nos serviços de segurança geridos, à luz da próxima alteração específica do Regulamento Cibersegurança. SALIENTA que os Estados-Membros e a indústria estão preocupados com o longo processo de seleção, elaboração e adoção dos sistemas de certificação da cibersegurança; por conseguinte, INSTA a Comissão a aproveitar a oportunidade da avaliação do Regulamento Cibersegurança para encontrar formas de adotar uma abordagem mais simples, baseada no risco, mais transparente e mais rápida para o desenvolvimento dos sistemas de certificação da cibersegurança da UE, SUBLINHANDO simultaneamente o importante papel dos Estados-Membros neste processo. SALIENTA ainda a importância de atribuir explicitamente a responsabilidade pela manutenção de cada sistema de certificação. Além disso, RECORDA que a ENISA deverá consultar atempadamente todas as partes interessadas pertinentes através de um processo formal, aberto, transparente e inclusivo aquando da elaboração dos projetos de sistemas, e que a Comissão deverá proceder a uma consulta aberta, transparente e inclusiva ao avaliar a eficácia e a utilização dos sistemas adotados. INCENTIVA a ENISA a continuar a reforçar a colaboração com a comunidade de proteção de dados, em particular o Comité Europeu para a Proteção de Dados, se for caso disso, e as autoridades nacionais competentes, prestando uma atenção especial à promoção de sinergias no contexto do desenvolvimento de futuros sistemas europeus de certificação da cibersegurança.

8. A fim de evitar os encargos administrativos desnecessários que poderiam resultar de um quadro complexo de comunicação de informações, APELA à ENISA, em cooperação com a Comissão, para que continue a trocar pontos de vista com os Estados-Membros sobre os aspetos práticos, a simplificação e a racionalização do procedimento de comunicação de informações. Além disso, RECORDA o seu convite à Comissão para que prepare, com o apoio da ENISA e de outras entidades pertinentes da UE, um levantamento das obrigações de comunicação pertinentes estabelecidas nos diversos atos legislativos da UE em matéria de ciberespaço e questões digitais. RECORDA que o intercâmbio de informações entre a ENISA e os Estados-Membros se baseia numa relação de confiança, em que a segurança e a confidencialidade são garantidas em conformidade com o Regulamento Cibersegurança e as regras e protocolos relevantes, e deve limitar-se ao que é pertinente e proporcionado face ao objetivo do intercâmbio. SALIENTA a necessidade de os dados e informações serem tratados com o devido cuidado.
9. SALIENTA que a ENISA é responsável pela criação e manutenção **da plataforma única de comunicação de informações ao abrigo do Regulamento de Ciber-Resiliência**, a qual terá um valor acrescentado operacional concreto, especialmente no que diz respeito às vulnerabilidades ativamente exploradas e aos incidentes graves que afetam a segurança dos produtos com elementos digitais. Tendo em conta o vasto âmbito de aplicação desta legislação horizontal, a plataforma única de comunicação de informações deverá ser um instrumento eficaz e seguro para facilitar a partilha de informações entre as CSIRT nacionais e a ENISA. Por conseguinte, INSTA a ENISA a, para além de afetar recursos humanos suficientes, acelerar a criação da plataforma como prioridade fundamental, a fim de assegurar que esteja pronta dentro do prazo estabelecido no Regulamento de Ciber-Resiliência.

10. RECONHECE o papel da ENISA na criação de uma **base de dados europeia de vulnerabilidades** destinada a melhorar a transparência no que diz respeito à divulgação de vulnerabilidades, assegurando simultaneamente o tratamento adequado dos dados sensíveis. Tendo em conta o termo do período de transposição da Diretiva SRI 2, INSTA a ENISA a acelerar todos os trabalhos necessários para assegurar o bom funcionamento desta base de dados. Em paralelo, CONVIDA o grupo de cooperação SRI, com a assistência da ENISA, a continuar a divulgar orientações, políticas e procedimentos em matéria de divulgação de vulnerabilidades.
11. RECONHECE os benefícios da **ação de apoio à cibersegurança** levada a cabo pela ENISA, que funciona como um conjunto de serviços de cibersegurança à disposição dos Estados-Membros para complementar os esforços por eles enviados, bem como a experiência adquirida pela ENISA com a execução dessa ação. A este respeito, SALIENTA que a ENISA deverá desempenhar um papel central na administração e no funcionamento da Reserva de Cibersegurança da UE. CONVIDA a ENISA a iniciar o levantamento dos serviços necessários e da sua disponibilidade assim que entrar em vigor o Regulamento de Cibersolidariedade, a fim de tornar a Reserva de Cibersegurança da UE tão útil e adaptada às necessidades dos utilizadores quanto possível em todos os Estados-Membros. CONVIDA a ENISA, uma vez incumbida da sua missão, a envolver os Estados-Membros, nomeadamente recolhendo contributos sobre os critérios exigidos e prestando informações sobre futuros concursos, numa fase precoce do processo de criação da Reserva de Cibersegurança da UE. CONVIDA a ENISA, uma vez incumbida da sua missão, a assegurar que o processo de seleção de prestadores de serviços de segurança geridos de confiança seja transparente, aberto e equitativo e permita a participação de prestadores de todos os Estados-Membros, independentemente da sua dimensão. Além disso, RECORDA que a ENISA é obrigada a emitir, sem demora injustificada, orientações em matéria de interoperabilidade para as plataformas de cibersegurança transfronteiriças.

12. SUBLINHA que o **acompanhamento das tendências relativas às tecnologias emergentes** num domínio em rápida evolução, como o ciberespaço, é fundamental para manter e reforçar ainda mais a nossa postura de cibersegurança. RECONHECE o trabalho realizado pela ENISA para chamar a atenção do público para os riscos e as possibilidades de tecnologias como a inteligência artificial e a computação quântica, facilitando assim uma melhor compreensão dos desafios atuais. INCENTIVA a ENISA a contribuir mais para estas tarefas, a defender ativamente a aplicação das suas recomendações e a aconselhar e colaborar, se for caso disso, com o Centro Europeu de Competências em Cibersegurança.

APOIO DA ENISA AOS ESTADOS-MEMBROS PARA REFORÇAR A CIBER-RESILIÊNCIA E A COOPERAÇÃO OPERACIONAL

13. SALIENTA que a ENISA desempenha um papel importante **enquanto secretariado das duas redes de cibercooperação a nível da UE impulsionadas pelos Estados-Membros, a rede de CSIRT e a UE-CyCLONE**. REALÇA a valiosa participação da ENISA no grupo de cooperação SRI, nomeadamente através da sua participação ativa e dos seus contributos técnicos nas várias vertentes de trabalho. INCENTIVA a ENISA a continuar a apoiar o funcionamento e a cooperação destas redes no futuro, uma vez que proporcionam canais fundamentais para os Estados-Membros colaborarem a diferentes níveis.
14. REITERA a necessidade de reforçar o **conhecimento situacional comum** a nível da UE, que contribui para a postura de cibersegurança da UE, no que diz respeito à deteção, prevenção e resposta a incidentes de cibersegurança. A este respeito, SALIENTA a importância das atividades prospetivas, dos relatórios periódicos e das avaliações de ameaças realizados pela ENISA, todos eles elementos que contribuem para melhorar o conhecimento situacional. INCENTIVA a ENISA a trabalhar em estreita cooperação com os Estados-Membros a fim de contribuir para o desenvolvimento do conhecimento situacional a nível da UE. Neste contexto, RECONHECE o papel importante da ENISA, juntamente com a CERT-UE e a Europol, no apoio ao Conselho com sessões de informação situacionais, no âmbito do conjunto de instrumentos de ciberdiplomacia, que complementam o conhecimento situacional proporcionado pela Capacidade Única de Análise de Informações (SIAC), e SALIENTA a necessidade de estabelecer uma panorâmica completa das ameaças a partir de várias fontes, incluindo o setor privado. INCENTIVA, neste contexto, a prossecução do desenvolvimento da cooperação da ENISA com o SEAE e, em particular, com o INTCEN, na plena observância dos respetivos mandatos.

15. SALIENTA que o centro de situação e de análise cibernética da Comissão desempenha uma função interna dentro da Comissão e é apoiado pela sua colaboração com a ENISA e a CERT-UE. A fim de criar o máximo potencial de sinergias e reduzir a complexidade no ecossistema de cibersegurança da UE, CONVIDA a Comissão a ter em conta os resultados da avaliação do Regulamento Cibersegurança, bem como os debates sobre a avaliação do Plano de Ação para a Cibersegurança, a fim de racionalizar as atribuições do centro de situação e análise cibernética da Comissão e as atribuições conexas da ENISA. INCENTIVA a Comissão a evitar a duplicação desnecessária de tarefas, salvaguardando simultaneamente o papel central da ENISA no que toca a contribuir para o desenvolvimento de um conhecimento situacional comum a nível da União para apoiar os Estados-Membros, no devido respeito pelas suas competências nacionais.
16. SALIENTA que o desenvolvimento de um conhecimento situacional comum é uma condição prévia para uma gestão atempada e eficaz das crises da União no seu conjunto. SUBLINHA que, a nível da UE, estão envolvidos vários intervenientes fundamentais **na resposta a incidentes de cibersegurança em grande escala** e que, na eventualidade de tais incidentes, a cooperação eficaz entre os Estados-Membros assenta principalmente na rede de CSIRT e na UE-CyCLONe. A ENISA desempenha um papel importante na gestão de cibercrises enquanto secretariado da rede de CSIRT e da UE-CyCLONe. EXORTA a Comissão a utilizar a avaliação do Plano de Ação para a Cibersegurança para refletir adequadamente as atribuições e responsabilidades adicionais que contribuam para o desenvolvimento de uma resposta cooperativa a incidentes ou crises de cibersegurança transfronteiriça em grande escala, bem como o papel atribuído à ENISA enquanto secretariado da rede de CSIRT e da UE-CyCLONe, e pela legislação recente em matéria de cibersegurança.

17. SUBLINHA a importância de organizar **exercícios regulares de cibersegurança** que aumentem consideravelmente a preparação da UE para responder a incidentes e crises. ESTÁ CIENTE de que a ENISA adquiriu uma valiosa e vasta experiência neste domínio, apoiando os Estados-Membros. RECONHECE o papel importante da ENISA nas fases de planeamento, preparação, execução e avaliação dos exercícios de cibersegurança, e SALIENTA que esta agência deverá continuar a ser um dos intervenientes centrais a nível da UE, tendo em conta que esses exercícios devem ser realizados com base em quadros estruturados e terminologias comuns. CONVIDA a ENISA, a rede de CSIRT e a UE-CyCLONe a utilizarem da forma mais eficiente os exercícios regulares existentes para testar e melhorar o quadro de resposta da UE a situações de crise, e a tirarem o máximo partido dos ensinamentos colhidos.

COOPERAÇÃO DA ENISA COM OUTROS INTERVENIENTES NO ECOSISTEMA DE CIBERSEGURANÇA

18. REITERA que, devido à natureza horizontal da cibersegurança, **a colaboração entre todos os intervenientes a nível dos Estados-Membros e da União** é vital, e, por conseguinte, SUBLINHA que o aumento da ciber-resiliência global a nível europeu também exige um trabalho conjunto entre a ENISA e outras entidades pertinentes no domínio do ciberespaço.
19. SUBLINHA que a capacidade das instituições, órgãos e organismos da UE para manter a cibersegurança é importante para a ciber-resiliência global a nível da UE, em que o papel da CERT-UE é inestimável. A este respeito, CONGRATULA-SE com a cooperação estruturada estabelecida entre a CERT-UE e a ENISA e INCENTIVA-as a prosseguir a sua estreita cooperação no futuro.

20. Com a autonomia financeira alcançada, o Centro Europeu de Competências em Cibersegurança contribuirá significativamente para o desenvolvimento de um ecossistema europeu sólido nos setores da investigação, da indústria e da tecnologia em matéria de ciberespaço, que reúna competências para o desenvolvimento da mão de obra, em conformidade com o seu mandato. INCENTIVA a ENISA e o Centro Europeu de Competências em Cibersegurança a prosseguirem a sua estreita cooperação, especialmente no que diz respeito às necessidades e prioridades em matéria de investigação e inovação, bem como às cibercompetências, a fim de aumentar a competitividade da indústria de cibersegurança da União. CONVIDA a Comissão a analisar a forma como as sinergias no funcionamento da ENISA e do Centro Europeu de Competências em Cibersegurança podem ser ainda mais otimizadas e a melhor forma de racionalizar as atividades de acordo com os respetivos mandatos.
21. SUBLINHA que o fornecimento de atualizações regulares sobre o cenário de ameaças contribui para identificar melhor as medidas e os instrumentos necessários para combater eficazmente a cibercriminalidade. DESTACA o valor acrescentado dos relatórios de avaliação conjunta da UE no domínio do ciberespaço (J-CAR), que são o resultado da colaboração entre a ENISA, o EC3 da Europol e a CERT-UE, e que já deram um contributo valioso para enfrentar os diferentes desafios que se colocam, incluindo a luta contra a cibercriminalidade. CONVIDA a ENISA e a Europol a continuarem a colaborar de forma estruturada no futuro.
22. SALIENTA que a ciberdefesa constitui uma parte importante e em constante evolução da luta contra as ameaças decorrentes do ciberespaço. SUBLINHA a necessidade de a ENISA colaborar com o SEAE e a Comissão, nos casos em que a ENISA tem um papel a desempenhar no apoio à execução da política de ciberdefesa da UE, em estreita cooperação com a AED, o Centro Europeu de Competências em Cibersegurança e a comunidade de ciberdefesa. SALIENTA o papel da ENISA enquanto agência civil. REALÇA a importância de aprofundar e racionalizar a cooperação civil-militar no domínio do ciberespaço na UE, inclusive através de uma divisão clara de funções e responsabilidades entre as duas comunidades e entre a UE e a OTAN, no pleno respeito dos princípios da inclusividade, da reciprocidade, da abertura mútua e da transparência, bem como da autonomia de decisão das duas organizações. INCENTIVA a ENISA a prosseguir os acordos de trabalho com a Agência de Comunicação e Informação da OTAN.

23. INCENTIVA a UE a continuar a promover os nossos valores comuns e os nossos esforços conjuntos no âmbito dos fóruns mundiais, a fim de salvaguardar um ciberespaço livre, mundial, aberto e seguro. SALIENTA que a natureza transfronteiriça das ameaças e incidentes no ciberespaço exige uma colaboração forte e eficaz, não só a nível da UE, mas também **com organizações e parceiros internacionais**. OBSERVA que a atuação da ENISA a nível internacional deverá centrar-se nos parceiros estratégicos e nos países candidatos à adesão à UE, em consonância com a política externa e de segurança comum da UE. SALIENTA que, na sua atuação internacional, a ENISA deverá agir em conformidade com o seu mandato e as disposições correspondentes do Regulamento Cibersegurança. RECONHECE a necessidade de clarificar, em conformidade com os procedimentos pertinentes, a atuação internacional da ENISA, assegurando, em particular, que o seu Conselho de Administração seja devida e atempadamente informado das atividades conexas. INCENTIVA a participação da ENISA nos quadros de cooperação internacional pertinentes em matéria de cibersegurança, incluindo organizações como a NATO e a OSCE.
24. REITERA que a UE e os seus Estados-Membros salientaram frequentemente lacunas em matéria de **competências no domínio da cibersegurança**. RECORDA que a Comissão e a ENISA introduziram um quadro amplo e abrangente para fornecer orientações a todas as partes interessadas, que inclui, nomeadamente, o Quadro Europeu de Competências em Cibersegurança, a Comunicação sobre a Academia de Competências de Cibersegurança e a Conferência Europeia sobre Cibercompetências, organizada anualmente, e INCENTIVA a Comissão e a ENISA a tirarem partido destas iniciativas, com especial destaque para o debate em curso sobre o consórcio para uma infraestrutura digital europeia (EDIC). Para o efeito, CONVIDA a Comissão a articular-se com os Estados-Membros interessados na criação de um EDIC. REGISTA que tanto a ENISA como o Centro Europeu de Competências em Cibersegurança estão mandatados para promover as competências em toda a União. CONVIDA a ENISA a dar prioridade ao apoio aos esforços dos Estados-Membros em matéria de competências e de educação e ao reforço da sensibilização do público em geral, bem como a colaborar com o Centro Europeu de Competências em Cibersegurança, se for caso disso.

25. RECONHECE que a ENISA desenvolveu a **cooperação com o setor privado** nos últimos anos. RECORDA que, uma vez que o setor privado vigia continuamente o cenário de ciberameaças, as informações recolhidas pela indústria poderão ajudar a melhorar o conhecimento situacional comum. Por conseguinte, INCENTIVA a ENISA, em estreita cooperação com os Estados-Membros e todas as entidades da UE, a reforçar a cooperação com o setor privado.
26. EXORTA a Comissão e a ENISA a estudarem formas de reforçar a colaboração entre a ENISA e os organismos europeus de **normalização**. SALIENTA a necessidade de a ENISA aumentar os seus conhecimentos especializados em matéria de normalização europeia da cibersegurança, nomeadamente dando seguimento e participando nas atividades de normalização.
27. INSTA a Comissão e a ENISA a analisarem a forma de otimizar ainda mais o funcionamento do quadro da UE em matéria de cibersegurança, tendo em conta as recomendações e propostas apresentadas nas presentes conclusões. A cooperação contínua, a priorização das atribuições e dos recursos, bem como a simplificação do panorama complexo da cibersegurança, serão elementos fundamentais para fazer face aos desafios atuais e futuros.
-