Conselho da
União Europeia

Bruxelas, 17 de outubro de 2022
(OR. en)

13664/22

CYBER 327
TELECOM 410
COSI 247
COPEN 354
DATAPROTECT 280
IND 413
RECH 547
HYBRID 99
JAI 1326
POLMIL 225
RELEX 1357

RESULTADOS DOS TRABALHOS

de:	Secretariado-Geral do Conselho
data:	17 de outubro de 2022
para:	Delegações
n.º doc. ant.:	12930/22
Assunto:	Conclusões do Conselho sobre a segurança da cadeia de abastecimento das TIC – Conclusões do Conselho aprovadas pelo Conselho na sua reunião de 17 de outubro de 2022

Junto se enviam, à atenção das delegações, as Conclusões do Conselho sobre a segurança da cadeia de abastecimento das TIC, aprovadas pelo Conselho na sua reunião realizada a 17 de outubro de 2022.

ANEXO

Conclusões do Conselho sobre a segurança da cadeia de abastecimento das TIC

O CONSELHO DA UNIÃO EUROPEIA,

RECORDANDO as suas conclusões sobre

– a Comunicação Conjunta ao Parlamento Europeu e ao Conselho intitulada: "Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE", de 20 de novembro de 2017,

– o desenvolvimento de capacidades e competências em matéria de cibersegurança na UE,

– a importância da tecnologia 5G para a economia europeia e a necessidade de atenuar os riscos de segurança a ela associados,

– construir o futuro digital da Europa,

– "Uma recuperação que promova a transição para uma indústria europeia mais dinâmica, resiliente e competitiva",

– a cibersegurança dos dispositivos conectados,

– a Estratégia de Cibersegurança da UE para a década digital,

– o desenvolvimento da postura da União Europeia no ciberespaço,

– o Relatório Especial n.º 3/2022 do Tribunal de Contas Europeu, intitulado "Lançamento da tecnologia 5G na UE: atrasos na implantação das redes e questões de segurança ainda por resolver",

RECORDANDO as conclusões do Conselho Europeu sobre

– a COVID-19, o mercado único, a política industrial, a digitalização e as relações externas, de 1 e 2 de outubro de 2020,

– a agressão militar da Rússia contra a Ucrânia, a segurança e defesa, a energia, questões económicas, a COVID-19 e as relações externas, de 24 e 25 de março de 2022,

– a Ucrânia, a segurança alimentar, a segurança e defesa, e a energia, de 30 e 31 de maio de 2022,

1. Dada a crescente importância da geopolítica para a cibersegurança, SUBLINHA que a União Europeia e os seus Estados-Membros têm de abordar a cibersegurança de forma abrangente e estratégica. A agressão militar da Rússia contra a Ucrânia provocou uma mudança de fundo no ambiente estratégico e de segurança da União Europeia e veio demonstrar a necessidade de uma União Europeia mais forte e mais capaz no domínio da segurança e defesa. Salientou que é da maior importância ter devidamente em conta o contexto geopolítico, não só na resposta a ciberatividades mal-intencionadas, mas também no desenvolvimento e na manutenção da resiliência das tecnologias da informação e comunicação (TIC). Isto é especialmente importante para as cadeias de abastecimento de produtos e serviços de TIC (cadeias de abastecimento das TIC), que podem ser comprometidas quer por rivalidade geopolítica, como foi o caso do ataque *SolarWinds*, quer afetadas por tensões e instabilidade geopolíticas, como o demonstrou a ameaça relacionada com a dependência de fornecedores de TIC russos aquando da agressão militar da Rússia contra a Ucrânia.

2. OBSERVA que a natureza dos riscos associados à cadeia de abastecimento das TIC, que é composta por um conjunto de recursos e processos interligados entre operadores económicos (na aceção do Regulamento (UE) 2019/1020) e que começa com o abastecimento de matérias-primas e passa pelo fabrico, o processamento, o manuseamento e a entrega de produtos e serviços de TIC, incluindo a prestação de apoio durante o ciclo de vida desses produtos e serviços, acarreta desafios únicos e consequências potencialmente de grande alcance. Para além dos riscos relacionados com a indisponibilidade de produtos de TIC devido a, por exemplo, escassez de matérias-primas críticas e semicondutores necessários para a sua produção, as cadeias de abastecimento de produtos e serviços de TIC estão expostas a outras ameaças. Nomeadamente, podem ser visadas ou utilizadas indevidamente por intervenientes mal-intencionados, de formas sofisticadas, e muitas vezes dissimuladas, que têm impacto na confidencialidade, na integridade e na disponibilidade de dados sensíveis transmitidos e armazenados.

3. Admitindo que é necessária uma abordagem que abrange todos os perigos para a segurança dos ativos de TIC, RECONHECE a importância da proposta de Diretiva Resiliência das Entidades Críticas para melhorar a segurança física de entidades críticas, e SUBLINHA que, para além de reforçar a resiliência contra ataques às cadeias de abastecimento perpetrados através de meios cibernéticos, é igualmente importante reforçar a resiliência e a segurança globais das cadeias de abastecimento das TIC para fazer face a toda a variedade de fatores de ameaça, como fenómenos naturais, falhas dos sistemas, ameaças internas ou erros humanos. Neste sentido, RECONHECE que a segurança da cadeia de abastecimento das TIC inclui que se garanta a proteção dos produtos e serviços de TIC produzidos, entregues, adquiridos e utilizados nas cadeias de abastecimento das TIC, inclusive através da proteção dos componentes individuais e dos dados transmitidos.

4. Com base nos ensinamentos retirados das consequências das dependências estratégicas da União Europeia em relação aos combustíveis fósseis russos, bem como dos impactos das perturbações nas cadeias de abastecimento durante a pandemia de COVID-19, nomeadamente no que diz respeito aos produtos farmacêuticos e aos semicondutores, em que ficaram expostas as dependências estratégicas da UE, INCENTIVA os Estados-Membros a trabalhar no sentido de evitar situações similares de dependências externas estratégicas indesejáveis em relação aos produtos e serviços de TIC. Devido à crescente digitalização da sociedade e à utilização cada vez maior das TIC em infraestruturas críticas, as dependências externas estratégicas relacionadas com os produtos e serviços de TIC e as respetivas cadeias de abastecimento deverão ser constantemente avaliadas e, se for caso disso, abordadas.

5. RECORDA que um dos objetivos fundamentais da União é alcançar a autonomia estratégica, preservando ao mesmo tempo uma economia aberta, o que implica identificar e reduzir as dependências estratégicas e aumentar a resiliência nos ecossistemas industriais e domínios específicos mais sensíveis, inclusive no domínio digital. Tal inclui desenvolver e implantar capacidades e infraestruturas digitais estratégicas, bem como reforçar a capacidade de fazer escolhas tecnológicas autónomas e, enquanto um dos principais pilares, garantir infraestruturas, produtos e serviços resilientes e seguros para aumentar a confiança no mercado único digital e a nível da sociedade europeia, mantendo em simultâneo a abertura, a cooperação mundial com parceiros que partilham as mesmas ideias e a competitividade, bem como tirar partido das potenciais vantagens que daí resultem. Os valores fundamentais da União Europeia preservam, em particular, a privacidade, a segurança, a igualdade, a dignidade humana, o Estado de direito e a Internet aberta como condições prévias para alcançar uma sociedade, uma economia e uma indústria impulsionadas pela digitalização e centradas no ser humano.

6. OBSERVA que, tendo em conta a evolução do panorama das ciberameaças, demonstrada pela tendência de ataques de grande impacto e sofisticados perpetrados contra a cadeia de abastecimento nos últimos anos, como o *SolarWinds*, o *Mimecast* ou o *Kaseya*, que surgiram paralelamente à externalização de serviços essenciais de TIC e se intensificaram pela dependência global em relação aos produtos e serviços de TIC fabricados, fornecidos ou mantidos por terceiros, é muito provável que ocorram no futuro mais ataques contra a cadeia de abastecimento com prejuízos substanciais para a economia e a sociedade. Tendo isto em conta, SUBLINHA a importância de reforçar a segurança e a resiliência das cadeias de abastecimento das TIC para o funcionamento do mercado único, juntamente com a necessidade de assegurar a disponibilidade, a segurança e a diversidade dos produtos e serviços de TIC no mercado único. Por conseguinte, RECONHECE a necessidade de maximizar e otimizar a utilização dos instrumentos e abordagens existentes da UE para alcançar esses objetivos, bem como a necessidade de contínua adaptação à evolução do panorama das ciberameaças, introduzindo medidas e mecanismos adicionais adequados, inclusive no que diz respeito a possíveis riscos para a segurança resultantes de tecnologias emergentes e disruptivas. A este respeito, INCENTIVA os Estados-Membros a seguirem uma abordagem baseada no risco para fazer face aos novos avanços tecnológicos.

7. RECONHECE que compreender o panorama em constante evolução das ciberameaças, bem como a complexidade dos ataques à cadeia de abastecimento, é fundamental para atenuar eficazmente os riscos associados às cadeias de abastecimento das TIC. A este respeito, SALIENTA a necessidade de haver uma adaptação a novas ameaças, acompanhando, analisando e avaliando de forma ativa e contínua o panorama das ameaças à cadeia de abastecimento, de sensibilizar e de desenvolver conhecimentos sobre ameaças e vulnerabilidades e de alertar proativamente as entidades pertinentes de uma forma adaptada. CONGRATULA-SE com o trabalho da Agência da União Europeia para a Cibersegurança (ENISA) no domínio da segurança da cadeia de abastecimento das TIC, em especial com o seu relatório intitulado "*Threat Landscape for Supply Chain Attacks*" (Panorama das ameaças de ataques à cadeia de abastecimento).

INSTRUMENTOS E ABORDAGENS TRANSETORIAIS

8. REAFIRMA a importância de os Estados-Membros ponderarem a necessidade de diversificar os fornecedores de TIC críticas, a fim de evitar ou limitar a criação de uma grande dependência de um único fornecedor, especialmente fornecedores de alto risco, uma vez que isso aumenta a exposição às consequências de potenciais perturbações. RECONHECE que o facto de evitar a vinculação a um fornecedor e diversificar os fornecedores de TIC constitui uma das componentes importantes para garantir a estabilidade e a segurança do mercado interno. DESTACA a necessidade de promover e aplicar estratégias adequadas que facilitem a diversificação e a competitividade dos fornecedores de forma tecnologicamente neutra. Além disso, INCENTIVA à integração dos aspetos relacionados com a prevenção da vinculação a um fornecedor na legislação da UE. A este respeito, TOMA NOTA da proposta de regulamento relativo a regras harmonizadas sobre o acesso equitativo aos dados e a sua utilização (Regulamento Dados), que visa aumentar a interoperabilidade dos serviços de tratamento de dados e eliminar os obstáculos à mudança entre prestadores de serviços de tratamento de dados.

9. RECONHECE a relação entre a segurança da cadeia de abastecimento das TIC e a contratação pública. SUBLINHA a necessidade de os procedimentos de contratação pública terem devidamente em conta a importância da segurança da cadeia de abastecimento das TIC, impondo, se for caso disso, critérios de seleção objetivos e baseados no risco relacionados com a capacidade de os proponentes assegurarem um elevado nível de segurança dos serviços prestados. APELA a que se procure o equilíbrio certo entre o interesse público na utilização mais eficiente e justa possível dos fundos públicos, por um lado, e o interesse público na proteção dos sistemas de informação e na garantia do bom funcionamento do mercado único, por outro. Para facilitar a aplicação de regras pertinentes de contratação pública à luz do reforço da cibersegurança, CONVIDA a Comissão a desenvolver orientações metodológicas até ao terceiro trimestre de 2023, a fim de incentivar as autoridades adjudicantes a darem uma ênfase adequada às práticas dos proponentes e respetivos subcontratantes no domínio da cibersegurança, e de avaliar e, se necessário, apresentar propostas destinadas a rever ou complementar a legislação pertinente em matéria de contratação pública.

10. RECONHECE que, apesar de os investimentos diretos estrangeiros relacionados com os produtos e serviços de TIC proporcionarem benefícios económicos e sociais aos Estados--Membros, às empresas e aos cidadãos, poderão incluir riscos para a segurança e a ordem pública, e REGISTA que o regime de análise dos investimento diretos estrangeiros da UE, juntamente com os respetivos sistemas de análise nacionais, que fornecem os meios para fazer face a esses riscos, poderão também ser aplicados como instrumentos úteis para salvaguardar a segurança e a resiliência da cadeia de abastecimento das TIC, contribuindo para a eliminação dos investimentos de alto risco que possam afetar essa segurança e resiliência. RECONHECE que as informações intercambiadas e partilhadas por meio desse regime poderão ajudar os Estados-Membros a avaliar melhor as possíveis ameaças à segurança das cadeias de abastecimento das TIC e a tomar as medidas necessárias em conformidade. APELA aos intervenientes nacionais pertinentes para que também tenham essa dimensão do regime de análise em conta, quando adequado.

11. No que diz respeito à defesa, REITERA o seu convite à Comissão para que avalie em 2023, em cooperação com os Estados-Membros, os riscos para as cadeias de abastecimento de infraestruturas críticas em vários domínios, nomeadamente o domínio digital, relacionados com os interesses da UE em matéria de segurança e defesa, bem como para que estude alternativas de reforço da cibersegurança em toda a cadeia de abastecimento da base tecnológica e industrial de defesa da UE. Além disso, CONVIDA os Estados-Membros e a Comissão a refletir sobre a segurança da cadeia de abastecimento das TIC no quadro da aplicação dos compromissos e das ações da Bússola Estratégica.

12. Reconhecendo a importância das matérias-primas críticas, bem como todos os tipos de semicondutores, como módulos básicos para a criação de produtos de TIC, INCENTIVA à realização de negociações construtivas no que diz respeito à proposta de regulamento que estabelece um quadro de medidas para reforçar o ecossistema europeu dos semicondutores (Regulamento Circuitos Integrados) e à proposta de regulamento do Conselho que altera o Regulamento (UE) 2021/2085, que cria as empresas comuns ao abrigo do Horizonte Europa, no respeitante à Empresa Comum dos Circuitos Integrados.

INSTRUMENTOS ESPECÍFICOS DO CIBERESPAÇO

13. Especificamente no que respeita à infraestrutura de telecomunicações, RECONHECE os resultados alcançados ao nível da União para melhorar a segurança da cadeia de abastecimento das redes 5G, nomeadamente através do instrumentário da UE para a segurança das redes 5G. EXORTA os Estados-Membros a continuarem a trocar informações sobre as boas práticas e metodologias relativamente à aplicação das medidas recomendadas no instrumentário da UE para a segurança das redes 5G e, em especial, a aplicarem as restrições pertinentes aos fornecedores de alto risco no que respeita a ativos essenciais definidos como críticos e sensíveis na avaliação coordenada dos riscos ao nível da UE. DESTACA que o instrumentário da UE para a segurança das redes 5G representa um instrumento flexível baseado no risco, destinado a dar resposta aos desafios de segurança identificados, que permite tratar os aspetos de cibersegurança das redes 5G de forma atempada e eficiente, respeitando simultaneamente as competências dos Estados-Membros, e RECONHECE que este é um instrumento valioso para continuar a reforçar, em total transparência, a segurança da cadeia de abastecimento das redes de telecomunicações de um modo coordenado que possa servir de inspiração para instrumentos de avaliação e atenuação dos riscos relacionados com outros setores vitais. RECORDA o convite às autoridades competentes para formularem, com base nas avaliações dos riscos, recomendações destinadas aos Estados-Membros e à Comissão, a fim de reforçar a resiliência das redes e das infraestruturas de comunicações na União Europeia, incluindo a continuação da aplicação do instrumentário da UE para a segurança das redes 5G.

14. REGISTA a importância de abordagens interoperáveis que possam abordar a vinculação a um fornecedor e diluir o risco de concentração, melhorando ao mesmo tempo a segurança da cadeia de abastecimento em toda a gama de infraestruturas e serviços de TIC. Em especial no que diz respeito às redes 5G, RECONHECE as potenciais vantagens do conceito de *Open RAN* (RAN aberta) e, ao mesmo tempo, RECORDA o relatório sobre a cibersegurança da *Open RAN*, publicado pelo grupo de cooperação SRI, que assinala que este conceito ainda se encontra em desenvolvimento e que a sua segurança, transparência e normalização ainda estão numa fase muito inicial, e SUBLINHA a importância de avaliar os riscos antes de qualquer transição para novas normas ou arquiteturas.

15. DESTACA a importância dos instrumentos legislativos horizontais em matéria de cibersegurança existentes e futuros, nomeadamente o Regulamento relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação (Regulamento Cibersegurança), a futura diretiva relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União (SRI 2), a proposta de regulamento que estabelece medidas destinadas a garantir um elevado nível comum de cibersegurança nas instituições, órgãos e organismos da União, bem como a proposta de regulamento relativo aos requisitos horizontais de cibersegurança dos produtos que integram elementos digitais (ato legislativo sobre a ciber-resiliência europeia), para reforçar a segurança da cadeia de abastecimento das TIC. Além disso, REGISTA a importante evolução da regulamentação em matéria de cibersegurança específica para cada setor, em especial o futuro regulamento relativo à resiliência operacional digital do setor financeiro (DORA), que inclui um quadro de fiscalização dos prestadores terceiros de serviços de TIC críticos para as entidades financeiras. Esta regulamentação prevê obrigações gerais relacionadas com a segurança da cadeia de abastecimento, bem como requisitos pormenorizados e específicos pertinentes para o setor em causa. Em simultâneo, SALIENTA que os fornecedores distribuem frequentemente os seus produtos e serviços em diferentes setores, não se limitando a uma única indústria. Por conseguinte, é extremamente importante assegurar que os requisitos em matéria de segurança da cadeia de abastecimento estejam, na medida do possível, alinhados em todos os setores pertinentes, em especial os setores abrangidos pela futura diretiva SRI 2, para evitar discrepâncias entre as obrigações impostas aos fornecedores, bem como para aliviar a pressão sobre os operadores de setores críticos no que respeita à avaliação do cumprimento dessas obrigações por parte dos fornecedores, tendo simultaneamente em conta as especificidades do setor.

16. CONGRATULA-SE com a proposta de ato legislativo sobre a ciber-resiliência enquanto instrumento legislativo importante para promover o desenvolvimento seguro de produtos que integram elementos digitais e para garantir que a cibersegurança é tida em conta ao longo de todo o ciclo de vida desses produtos. REGISTA que a proposta de ato legislativo sobre a ciber-resiliência tem potencial para contribuir significativamente para o reforço da segurança da cadeia de abastecimento das TIC. INCENTIVA à realização de negociações construtivas sobre o ato e à sua adoção em tempo útil.

17. A este respeito, RECONHECE os trabalhos que estão a ser conduzidos pela ENISA, juntamente com os Estados-Membros e outras partes interessadas, para fornecer à UE sistemas de certificação de produtos, serviços e processos de TIC em conformidade com o Regulamento Cibersegurança que contribuam para elevar o nível global de cibersegurança no mercado único digital. INCENTIVA todas as partes interessadas a participar nos trabalhos preparatórios no âmbito dos sistemas europeus de certificação individual, a fim de promover a confiança em produtos, processos e serviços de TIC seguros e reforçar a sua resiliências, e APELA à Comissão para que elabore rapidamente atos de execução sobre os sistemas europeus de certificação, após a conclusão dos trabalhos preparatórios, nomeadamente o sistema europeu de certificação da cibersegurança (EUCC) baseado em critérios comuns. REGISTA que os sistemas europeus de certificação deverão incluir, quando necessário, requisitos em matéria de segurança da cadeia de abastecimento, nomeadamente no que diz respeito às relações com os fornecedores.

18. DESTACA a necessidade de uma aplicação rigorosa de todas as futuras disposições da SRI 2 relacionadas com a segurança da cadeia de abastecimento das TIC. A este respeito, SUBLINHA a importância das avaliações coordenadas, ao nível da UE, dos riscos associados às cadeias de abastecimento críticas (avaliações coordenadas dos riscos associados à cadeia de abastecimento), das políticas nacionais em matéria de segurança da cadeia de abastecimento e das medidas de segurança relacionadas com a cadeia de abastecimento. OBSERVA que deverá prestar-se atenção não só aos fornecedores principais, mas também aos subcontratantes pertinentes no que se refere aos riscos para a segurança do fornecedor principal ou do cliente final. A fim de facilitar a aplicação de medidas de gestão dos riscos da cadeia de abastecimento, INCENTIVA a ENISA a efetuar, com a ajuda do grupo de cooperação SRI, um balanço das boas práticas disponíveis para a gestão dos riscos da cadeia de abastecimento e a compilar essas boas práticas em orientações metodológicas. Além disso, INCENTIVA a ENISA a acompanhar os investimentos na segurança da cadeia de abastecimento das TIC das entidades reguladas ao abrigo da futura diretiva SIR 2.

19. DESTACA igualmente os benefícios e os riscos associados à utilização de prestadores de serviços geridos (MSP) e de prestadores de serviços de segurança geridos (MSSP) no contexto da segurança da cadeia de abastecimento. Embora a utilização desses prestadores possa melhorar significativamente a segurança nas organizações e conduzir a níveis mais elevados de cibersegurança, a gestão remota de sistemas e serviços de TIC, combinada com um acesso privilegiado ao ambiente de TIC dos clientes, do qual os MSP e os MSSP poderão precisar, pode, no caso de MSP ou MSSP comprometidos, provocar importantes efeitos em cascata para um grande número de clientes. Por conseguinte, é extremamente importante que os MSP e os MSSP mantenham um elevado nível de segurança interna e a segurança dos serviços que fornecem, e que adotem uma abordagem transparente em relação aos seus clientes quanto à segurança dos serviços que prestam. A este respeito, CONGRATULA-SE com a sua inclusão no âmbito da futura diretiva SRI 2.

20. No que diz respeito à execução do mecanismo de avaliações coordenadas dos riscos associados à cadeia de abastecimento de acordo com a futura diretiva SRI 2, REGISTA a importância dos fatores de risco não técnicos neste contexto, como a influência indevida de um Estado terceiro sobre os fornecedores e os prestadores de serviços e, neste âmbito, RECONHECE os fatores que podem ser utilizados para avaliar o perfil de risco como mencionados na avaliação coordenada dos riscos a nível da UE no que respeita à cibersegurança das redes 5G. CONVIDA a Comissão a identificar até ao segundo trimestre de 2023, após consulta do grupo de cooperação SRI e da ENISA, os serviços, sistemas ou produtos de TIC específicos que poderão ser submetidos, com caráter prioritário, às avaliações coordenadas dos riscos associados à cadeia de abastecimento.

21. REGISTA que as dependências em relação a fornecedores de alto risco de produtos e serviços de TIC utilizados para o funcionamento de redes e sistemas críticos constituem uma ameaça estratégica que precisa de ser atenuada através de políticas adequadas, tanto a nível nacional como da UE, e da cooperação entre os Estados-Membros e com os parceiros internacionais que partilham as mesmas ideias. Para facilitar a atenuação desse risco estratégico e apoiar as avaliações coordenadas dos riscos associados à cadeia de abastecimento, CONVIDA o grupo de cooperação SRI a, em cooperação com a Comissão e a ENISA, desenvolver um instrumentário de medidas para reduzir os riscos associados à cadeia de abastecimento das TIC críticas (instrumentário para a cadeia de abastecimento das TIC). O instrumentário para a cadeia de abastecimento das TIC deverá basear-se nos cenários de ameaça estratégica identificados para as cadeias de abastecimento das TIC e prever medidas para reagir a esses cenários tirando proveito da experiência adquirida no âmbito do instrumentário para a segurança das redes 5G e a nível nacional. Deverá complementar, de forma transparente, as avaliações coordenadas dos riscos associados à cadeia de abastecimento de serviços, sistemas ou produtos de TIC específicos no quadro da futura diretiva SRI 2, propondo medidas genéricas para reduzir os riscos que possam ser adaptadas, de forma modulável a serviços, sistemas ou produtos de TIC específicos, com base nos riscos identificados nas avaliações coordenadas individuais dos riscos associados à cadeia de abastecimento.

22. SALIENTA o importante papel das atividades de investigação, inovação, investimento e empreendedorismo no domínio digital e da cibersegurança, bem como do financiamento dessas atividades para evitar possíveis dependências estratégicas indesejáveis no futuro e reforçar a resiliência global das cadeias de abastecimento das TIC. Neste contexto, SUBLINHA o papel e a importância das atribuições estratégicas e de execução do Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança (ECCC) e da Rede de Centros Nacionais de Coordenação por contribuírem para tirar o máximo partido dos efeitos dos investimentos destinados a reforçar a liderança e a autonomia estratégica aberta da União no domínio da cibersegurança, apoiar as capacidades e competências tecnológicas da União e aumentar a competitividade da União a nível mundial. Neste contexto, SOLICITA a rápida operacionalização do ECCC. CONVIDA o ECCC a ter em conta os aspetos relacionados com a segurança da cadeia de abastecimento das TIC, nomeadamente o desenvolvimento de software seguro, na sua agenda estratégica, garantindo ao mesmo tempo a coerência e a complementaridade e evitando a duplicação de esforços. APOIA o reforço da competitividade europeia no domínio da cibersegurança através de programas de financiamento, como o programa de investigação e inovação Horizonte Europa e o Programa Europa Digital para reforçar, desenvolver e adquirir capacidades essenciais para a economia digital, a sociedade e a democracia da UE.

MECANISMOS DE APOIO

23. INCITA ao reforço dos incentivos de apoio financeiro relacionados com as medidas que visam o fortalecimento da segurança da cadeia de abastecimento das TIC. APELA, com caráter prioritário, e também tendo em vista a futura aplicação da diretiva SRI 2, ao ECCC, à Comissão e às partes interessadas pertinentes para que analisem as possibilidades de incluir os aspetos relacionados com a segurança da cadeia de abastecimento das TIC nos próximos convites à apresentação de propostas no âmbito dos programas de trabalho em matéria de cibersegurança no quadro dos programas Europa Digital e Horizonte Europa, ou de quaisquer outras oportunidades de financiamento pertinentes. Essas oportunidades de financiamento deverão, entre outras coisas, ter por objetivo permitir que as organizações apoiem a manutenção de um elevado nível de cibersegurança no que diz respeito à aquisição de produtos e serviços de TIC em toda a cadeia de abastecimento, em especial no que se refere à substituição de serviços, sistemas ou produtos de TIC críticos específicos reconhecidos como sendo de alto risco em conformidade com as futuras avaliações coordenadas dos riscos associados à cadeia de abastecimento.

24. RECONHECE que a globalização, a especialização dos serviços de TIC e o aumento da dependência de produtos e serviços de terceiros tornam necessária uma estreita cooperação na UE e a nível internacional no que diz respeito à partilha de conhecimentos gerais e especializados entre as partes interessadas e INCENTIVA estas a chegarem a uma posição forte e coordenada que garanta a segurança da cadeia de abastecimento das TIC de forma global. RECONHECE igualmente a necessidade de continuar a estudar abordagens e técnicas de ponta pertinentes, tanto no que diz respeito a uma ciber-higiene básica adequada como a soluções a longo prazo para assegurar cadeias de abastecimento das TIC seguras e resilientes, bem como as formas mais adequadas de as promover e eventualmente incorporar nas políticas ou outras iniciativas. RECONHECE, a este respeito, que deve ser dada especial atenção ao estudo das vantagens e desvantagens das soluções sistemáticas, como os princípios de confiança zero, as listas de materiais que integram o software e soluções a longo prazo similares. RECOMENDA que, para esse efeito, se utilize o grupo de cooperação SRI.

25. REGISTA as vantagens do acompanhamento e da partilha eficaz de informações sobre ciberincidentes e ciberameaças para a prevenção, deteção e atenuação dos efeitos dos ataques à cadeia de abastecimento. SUBLINHA a necessidade de continuar a reforçar a confiança entre os Estados-Membros para assegurar a partilha eficaz dessas informações. RECORDA, a este respeito, a proposta apresentada pela Comissão no sentido de apoiar os Estados-Membros na criação e no reforço de centros de operações de segurança, a fim de implantar em toda a UE uma rede de centros destinada a continuar a acompanhar e a antecipar os sinais de ataques às redes. RECORDA a necessidade de complementaridade e coordenação nas redes e mecanismos existentes e, a este respeito, DESTACA sobretudo o papel da rede de equipas de resposta a incidentes de segurança informática e a necessidade de continuar a explorar o potencial dessas redes para promover uma cultura de partilha de informações eficiente, segura e fiável. RECORDA os esforços envidados pelos Estados-Membros, com o apoio da UE, para criar equipas de resposta a incidentes de segurança informática setoriais, nacionais e regionais, e centros de partilha e análise de informações a nível nacional ou europeu, no âmbito de uma rede eficaz de parcerias em matéria de cibersegurança na União.

26. Devido ao caráter interligado e mundial das ameaças à cadeia de abastecimento das TIC, DESTACA a importância de abordar e reforçar a segurança da cadeia de abastecimento das TIC a nível mundial. Tendo em conta o que precede, RECOMENDA que se recorra a parcerias digitais, ciberdiálogos e outras iniciativas pertinentes a nível da UE, inclusive, se for caso disso, acordos de comércio livre, para promover avaliações baseadas no risco dos fornecedores de produtos e dos prestadores de serviços de TIC, a utilização de fornecedores fiáveis, e para aplicar um ecossistema digital seguro e inovador baseado em normas abertas, interoperáveis e transparentes. Além disso, REITERA a visão das parcerias no âmbito da estratégia *Global Gateway*, bem como do Conselho de Comércio e Tecnologia UE-EUA, e as atividades levadas a cabo nos seus grupos de trabalho, para promover a utilização de fornecedores fiáveis/que não sejam de alto risco e desenvolver um mecanismo de financiamento facilitador de projetos que tornem as infraestruturas e os serviços de TIC de Estados terceiros mais seguros, resilientes e de confiança, inclusive abstendo-se de financiar aquisições de fornecedores que não sejam de confiança/sejam de alto risco, de forma tecnologicamente neutra.

27. REAFIRMA o seu compromisso de contribuir para um ciberespaço aberto, livre, mundial, estável e seguro e promovê-lo, e de aderir às normas, às regras e aos princípios do comportamento responsável dos Estados no ciberespaço estabelecidos no quadro das Nações Unidas. No que diz respeito, em especial, à segurança da cadeia de abastecimento das TIC, RECORDA a norma aprovada pelo Grupo de Peritos Governamentais e pelo grupo de trabalho aberto das Nações Unidas, que incentiva os Estados a tomarem medidas razoáveis para assegurar a integridade da cadeia de abastecimento, inclusive através do desenvolvimento de medidas de cooperação objetivas, para que os utilizadores finais possam ter confiança na segurança dos produtos de TIC, e a procurarem evitar a proliferação de instrumentos e técnicas de TIC maliciosos e a utilização de funções ocultas perigosas, e DEFENDE a sua ampla aplicação.